Theorem 2.3. $x + y = y + x$.

Proof: By induction on y. The result follows from Lemma 2.1 when $y = 0$. Supposing the result holds for y, we have

$$\begin{aligned} x + Sy &= S(x + y) && \text{(df +)} \\ &= S(y + x) && \text{(hyp)} \\ &= Sy + x && \text{(Lemma 2.2).} \end{aligned}$$

Theorem 2.4. $x + (y + z) = (x + y) + z$.

Proof: Use induction on z:

$$x + (y + 0) = x + y = (x + y) + 0.$$

Supposing the result holds for z, we argue thus:

$$\begin{aligned} x + (y + Sz) &= x + S(y + z) && \text{(df +)} \\ &= S(x + (y + z)) && \text{(df +)} \\ &= S((x + y) + z) && \text{(hyp)} \\ &= (x + y) + Sz && \text{(df +).} \end{aligned}$$

Theorem 2.5. $x^z y^z = (xy)^z$.

Proof: $x^0 y^0 = 1 \cdot 1 = 1 \cdot S0 = (1 \cdot 0) + 1 = 0 + 1 = 1 = (xy)^0$, so the result is true when $z = 0$. Suppose it holds for z. Then $x^{Sz} y^{Sz} = (x^z x)(y^z y)$ and $(xy)^{Sz} = (xy)^z xy = (x^z y^z)xy$ (hyp). The result now follows by mathematical induction on z — provided we can first establish the associativity and commutativity of multiplication. This we leave to the reader.

Theorem 2.6. *If* $x + y = x + z$ *then* $y = z$.

Proof: By Theorem 2.3, this is true when $x = 0$. Assume it holds for x. If $Sx + y = Sx + z$ then $S(x + y) = S(x + z)$ (Lemma 2.2) and hence, by Peano's second axiom, $x+y = x+z$. By the induction hypothesis, $y = z$.

Every natural number except 0 has a predecessor. We can define a *naive predecessor* as follows:

$$\begin{aligned} P0 &= 0, \\ PSy &= y. \end{aligned}$$

Given the naive predecessor function, it is easy to define naive subtraction. Again, we use a recursive definition:

$$\begin{aligned} x \dot{-} 0 &= x, \\ x \dot{-} Sy &= P(x \dot{-} y). \end{aligned}$$

The reason we use the sign $\dot{-}$ rather than the sign $-$ is that naive subtraction is not quite the same as ordinary subtraction. We cannot say that $1-3=-2$ since -2 is not a natural number. Instead we say that $1\dot{-}3=0$. Using the above definition, we have

$$1\dot{-}3 = 1\dot{-}S2 = P(1\dot{-}2) = P(1\dot{-}S1) = P(P(1\dot{-}1)) = P(P(1\dot{-}S0))$$

$$= P(P(P(1\dot{-}0))) = P(P(P(1))) = P(P(P(S0))) = P(P(0)) = P(0) = 0.$$

We define $\min(x,y)$ as $x\dot{-}(x\dot{-}y)$, and $\max(x,y)$ as $x+y\dot{-}\min(x,y)$.

Giuseppe Peano (1858–1932) published essentially this system in his *Arithmetices Principia* (1889), a book written in a language he invented.

Exercises

1. Prove that $0\cdot x=0$ without using the commutative law for multiplication.
2. Prove $1^x=1$.
3. Prove $x(y+z)=xy+xz$.
4. Prove $xy=yx$.
5. Prove $x\dot{-}x=0$.
6. Prove $Sx\dot{-}Sy=x\dot{-}y$.
7. Prove $\max(x,y)+\min(x,y)=x+y$.
8. In the *Arithmetices Principia*, Peano actually defines $x\dot{-}y$ as

$$x\dot{-}y = \begin{cases} z \text{ such that } y+z=x & \text{if there is such a } z \\ 0 & \text{otherwise} \end{cases}$$

   (a) Why can't there be two natural numbers z and w such that $y+z=x$ and $y+w=x$?

   (b) Show that Peano's definition of $\dot{-}$ is equivalent to the recursive definition given above.

3

The Integers

It is not difficult, though rather boring, to construct the integers from the natural numbers. Instead, we shall demonstrate in the next chapter how to construct the rationals from the integers, by essentially the same process. But first let us state the properties which make the set of integers into what is called an *integral domain.*

A *ring* $(R, 0, -, +, 1, \cdot)$ is a set R with operations 0, $-$, $+$, 1, and $\cdot$, where $+$ and $\cdot$ are *binary* operations, $-$ is a *unary* operation and 0 and 1 are *nullary* operations, that is, specified elements of R, which moreover satisfy the following axioms or identities:

1. $(x + y) + z = x + (y + z)$ (associativity),
2. $x + 0 = x$,
3. $x + (-x) = 0$,
4. $x + y = y + x$ (commutativity),
5. $x \cdot 1 = x = 1 \cdot x$,
6. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associativity),
7. $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$,
   $z \cdot (x + y) = (z \cdot x) + (z \cdot y)$ (distributivity).

We may take this opportunity to review a bit of abstract algebra. Axioms

(1) to (3) make $(R, 0, -, +)$ into a group. It is not difficult to prove that, in a group,

$$(2') \qquad 0 + x = x,$$

$$(3') \qquad -x + x = 0.$$

A group is said to be *Abelian* if it also satisfies the commutative law (4). We have stated this as an axiom, even though it is a consequence of the remaining axioms of a ring (not of a group). The operation $\cdot$ may or may not obey the commutative law for multiplication:

$$(8) \qquad x \cdot y = y \cdot x.$$

If it does, we call the ring *commutative*. For example, **Z** and **Q** are commutative rings, but the ring of 2 × 2 matrices with entries from **Z** is not commutative.

A commutative ring is called an *integral domain* if

$$(9) \qquad 0 \neq 1 \text{ and } x \cdot y = 0 \text{ implies } x = 0 \text{ or } y = 0.$$

It is called a *field* provided

(10) $0 \neq 1$ and, if $x \neq 0$, there exists an element y such that $x \cdot y = 1 = y \cdot x$.

Z is an integral domain, but not a field. On the other hand, **Q** is a field as well as an integral domain. In fact, every field is an integral domain.

Exercises

1. Prove that (2′) and (3′) must hold in a group.

2. Prove that, in a ring, $x \cdot 0 = 0 = 0 \cdot x$ and $x \cdot (-1) = -x = (-1) \cdot x$.

3. Prove that (4) follows from the other axioms of a ring.

4. Show that every field is an integral domain.

5. In a group, if $0'$ is another element such that, for all x, $x + 0' = x$, show that $0' = 0$.

6. In a group, if $\sim$ is another unary operation such that, for all x, $x + (\sim x) = 0$, show that $\sim x = -x$.

7. Prove that, in any integral domain, we have the following *cancellation law* : if $a \cdot c = b \cdot c$ and $c \neq 0$ then $a = b$.