Chapter 1

The Natural Numbers

1.1 Multiplication

Definition 1.1.1 (Multiplication of natural numbers)**.** *Let m be a natural number. To multiply zero by m, we define $0 \times m 0$. Now suppose inductively that we have defined how to multiply n by m. Then we can multiply $n{+}{+}$ by m by defining $(n{+}{+}) \times m (n \times m) + m$.*

Corollary 1.1.2. *The product of two natural numbers is a natural number.*

i:ac:2.3.1. Let n and m be two natural numbers. We induct on n. For $n = 0$, by i:2.3.1, we have $0 \times m = 0$, which is a natural number by i:2.1. So the base case holds. Suppose inductively that for some natural number n, we know that $n \times m$ is a natural number. We want to show that $(n{+}{+}) \times m$ is a natural number. By i:2.3.1, $(n{+}{+}) \times m = (n \times m) + m$. By the induction hypothesis, $n \times m$ is a natural number. By i:ac:2.2.1, $(n \times m) + m$ is a natural number. Thus, $(n{+}{+}) \times m$ is a natural number. This closes the induction. □

Corollary 1.1.3. *Let n be a natural number. Then $n \times 0 = 0$.*

i:ac:2.3.2. We induct on n. For $n = 0$, by i:2.3.1, we have $0 \times 0 = 0$. So the base case holds. Suppose inductively that for some natural number n, we have $n \times 0 = 0$. Then for $n{+}{+}$, we have

$$\begin{aligned} (n{+}{+}) \times 0 &= (n \times 0) + 0 && i : 2.3.1 \\ &= 0 + 0 \\ &= 0. && i : 2.2.1 \end{aligned}$$

This closes the induction. □

Corollary 1.1.4. *Let n and m be natural numbers. Then $n \times (m{+}{+}) = (n \times m) + n$.*

i:ac:2.3.3. We induct on n and fix m. For $n = 0$, by i:2.3.1, we have $0 \times (m{+}{+}) = 0$. So the base case holds. Suppose inductively that for some natural number n, we have

$n \times (m{+}{+}) = (n \times m) + n$. Then for $n{+}{+}$, we have

$$\begin{aligned}
(n{+}{+}) \times (m{+}{+}) &= (n \times (m{+}{+})) + (m{+}{+}) && i:2.3.1 \\
&= ((n \times m) + n) + (m{+}{+}) \\
&= (n \times m) + (n + (m{+}{+})) && i:2.2.5 \\
&= (n \times m) + ((n + m){+}{+}) && i:2.2.3 \\
&= (n \times m) + ((m + n){+}{+}) && i:2.2.4 \\
&= (n \times m) + (m + (n{+}{+})) && i:2.2.3 \\
&= ((n \times m) + m) + (n{+}{+}) && i:2.2.5 \\
&= ((n{+}{+}) \times m) + (n{+}{+}). && i:2.3.1
\end{aligned}$$

This closes the induction. □

Lemma 1.1.5 (Multiplication is commutative)**.** *Let n and m be natural numbers. Then $n \times m = m \times n$.*

i:2.3.2. We induct on n and fix m. For $n = 0$, by i:2.3.1, we have $0 \times m = 0$, and by i:ac:2.3.2, we have $m \times 0 = 0$. So the base case holds. Suppose inductively that for some natural number n, we have $n \times m = m \times n$. Then for $n{+}{+}$, we have

$$\begin{aligned}
(n{+}{+}) \times m &= (n \times m) + m && i:2.3.1 \\
&= (m \times n) + m \\
&= m \times (n{+}{+}). && i:ac:2.3.3
\end{aligned}$$

This closes the induction. □

Remark 1.1.6. *We will now abbreviate $n \times m$ as nm, and use the convention that multiplication takes precedence over addition. Thus, for instance, $ab + c$ means $(a \times b) + c$, not $a \times (b + c)$.*

Lemma 1.1.7 (Positive natural numbers have no zero divisors)**.** *Let n and m be natural numbers. Then $n \times m = 0$ iff at least one of n or m equals zero. In particular, if n and m are both positive, then nm is also positive.*

i:2.3.3. First, suppose that $n \times m = 0$. Suppose for the sake of contradiction that $n \neq 0 \neq m$. By i:2.2.7, this means n and m are positive natural numbers. Then by i:2.2.10, there exist some natural numbers a and b such that $n = a{+}{+}$ and $m = b{+}{+}$. Thus, we have

$$\begin{aligned}
n \times m &= (a{+}{+}) \times (b{+}{+}) \\
&= a \times (b{+}{+}) + (b{+}{+}). && i:2.3.1
\end{aligned}$$

By i:2.3, we know that $b{+}{+} \neq 0$. Thus, by i:2.2.8, we know that $n \times m$ is a positive natural number. But this contradicts $n \times m = 0$. Thus, we must have either $n = 0$ or $m = 0$.

Now suppose that $n = 0$ or $m = 0$. If $n = 0$, then we have $n \times m = 0 \times m = 0$ by i:2.3.1. If $m = 0$, then we have $n \times m = n \times 0 = 0$ by i:ac:2.3.2. In either case, we have $n \times m = 0$.

From all proofs above, we conclude that $n \times m = 0 \iff (n = 0) \vee (m = 0)$. Thus, we have $n \times m \neq 0 \iff (n \neq 0) \wedge (m \neq 0)$. By i:2.2.7, we see that n and m are positive natural numbers iff $n \times m \neq 0$. □

Corollary 1.1.8. *Let n be a natural number. Then $n1 = 1n = n$.*

i:ac:2.3.4. By i:2.3.2, we know that $n1 = 1n$. Thus, we only need to show that $n1 = n$. We induct on n. For $n = 0$, we have $0 \times 1 = 0$ by i:2.3.3. So the base case holds. Suppose inductively that $n1 = n$ is true for some natural number n. Then for $n + 1$, we have $(n+1) \times 1 = n1+1$ by i:2.3.1. By the induction hypothesis, we have $n1 = n$. Thus, we have $(n + 1) \times 1 = n + 1$, and this closes the induction. □

Proposition 1.1.9 (Distributive law)**.** *For any natural numbers a, b, c, we have $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.*

i:2.3.4. Since multiplication is commutative, we only need to show the first identity $a(b+c) = ab + ac$. We keep a and b fixed, and we induct on c. Let's prove the base case $c = 0$, i.e., $a(b+0) = ab+a0$. The left-hand side is ab, while the right-hand side is $ab+0 = ab$, so we are done with the base case. Now let us suppose inductively that $a(b + c) = ab + ac$, and let us prove that $a(b+(c{+}{+})) = ab+a(c{+}{+})$. The left-hand side is $a((b+c){+}{+}) = a(b+c)+a$ by i:ac:2.3.3, while the right-hand side is $ab+ac+a = a(b+c)+a$ by the induction hypothesis, and so we can close the induction. □

Proposition 1.1.10 (Multiplication is associative)**.** *For any natural numbers a, b, c, we have $(a \times b) \times c = a \times (b \times c)$.*

i:2.3.5. We keep a and b fixed, and we induct on c. For $c = 0$, by i:ac:2.3.2, we have $(a \times b) \times 0 = 0 = a \times 0 = a \times (b \times 0)$. So the base case holds. Suppose inductively that for some natural number c, we have $(a \times b) \times c = a \times (b \times c)$. Then for $c{+}{+}$, we have

$$\begin{aligned}
(a \times b) \times (c{+}{+}) &= (a \times b) \times c + a \times b && i : ac : 2.3.3 \\
&= a \times (b \times c) + a \times b \\
&= a \times (b \times c + b) && i : 2.3.4 \\
&= a \times (b \times (c{+}{+})). && i : ac : 2.3.3
\end{aligned}$$

This closes the induction. □

Proposition 1.1.11 (Multiplication preserves order)**.** *If a, b, c are natural numbers such that $a < b$, and c is positive, then $ac < bc$.*

i:2.3.6. Since $a < b$, we have $b = a + d$ for some positive d by i:2.2.12(f). Multiplying by c and using the distributive law (i:2.3.4), we obtain $bc = ac + dc$. Since d is positive, and c is positive, dc is positive (i:2.3.3), and hence $ac < bc$ (by i:2.2.11), as desired. □

Corollary 1.1.12 (Cancellation law)**.** *Let a, b, c be natural numbers such that $ac = bc$ and c is non-zero. Then $a = b$.*

i:2.3.7. By the trichotomy of order (i:2.2.13), we have three cases: $a < b$, $a = b$, $a > b$. Suppose first that $a < b$, then by i:2.3.6, we have $ac < bc$, a contradiction. We can obtain a similar contradiction when $a > b$. Thus, the only possibility is that $a = b$, as desired. □

Remark 1.1.13. *Just as i:2.2.6 will allow for a "virtual subtraction" which will eventually let us define genuine subtraction, i:2.3.7 provides a "virtual division" which will be needed to define genuine division later on.*

Proposition 1.1.14 (Euclid's division lemma)**.** *Let n be a natural number, and let q be a positive natural number. Then there exist natural numbers m and r such that $0 \le r < q$ and $n = mq + r$.*

i:2.3.9. We induct on n and fix q. For $n = 0$, let $r = m = 0$. Then we have

$$\begin{aligned} mq + r &= 0q + 0 \\ &= 0 + 0 && i:2.3.1 \\ &= 0, && i:2.2.1 \end{aligned}$$

and

$$\begin{aligned} 0 \le 0 &= r && i:2.2.12[a] \\ &< q. && i:2.2.11 \end{aligned}$$

So the base case holds. Suppose inductively that for some natural number n, there exist some natural numbers m and r such that $n = mq + r$ and $0 \le r < q$. Then for $n{+}{+}$, we have

$$\begin{aligned} n{+}{+} &= (mq + r){+}{+} \\ &= mq + (r{+}{+}). && i:2.2.3 \end{aligned}$$

Since $r < q$, we have $r{+}{+} \le q$ by i:2.2.12(e). Now we split into two cases:

- If $r{+}{+} < q$, then we have $0 \le r < r{+}{+} < q$, and we are done in this case.
- If $r{+}{+} = q$, then by i:2.3.1, we have

  $$n{+}{+} = mq + (r{+}{+}) = mq + q = (m{+}{+}) \times q = (m{+}{+}) \times q + r',$$

  where $r' = 0$ and $0 \le r' < q$ by i:ac:2.2.4, and we are also done in this case.

From all cases above, we can find some natural numbers m and r such that $n{+}{+} = mq + r$ and $0 \le r < q$. This closes the induction. □

Remark 1.1.15. *In other words, we can divide a natural number n by a positive number q to obtain a quotient m (another natural number) and a remainder r (less than q). This algorithm marks the beginning of* number theory*, which is a beautiful and important subject that is beyond this text's scope.*

Definition 1.1.16 (Exponentiation for natural numbers)**.** *Let m be a natural number. To raise m to the power 0, we define $m^0 1$; in particular, we define $0^0 1$. Now suppose recursively that m^n has been defined for some natural number n, then we define $m^{n++} m^n \times m$.*

Corollary 1.1.17. *For any natural number n, we have $n^1 = n$.*

i:ac:2.3.5. We have

$$\begin{aligned} n^1 &= n^0 \times n = 1 \times n && i:2.3.11 \\ &= n. && i:ac:2.3.4 \end{aligned}$$

□

Exercises

2.3.1 Prove i:2.3.2.

i:ex:2.3.1. See i:2.3.2 □

2.3.2 Prove i:2.3.3

i:ex:2.3.2. See i:2.3.3 □

2.3.3 Prove i:2.3.5

i:ex:2.3.3. See i:2.3.5 □

2.3.4 Prove the identity $(a+b)^2 = a^2 + 2ab + b^2$ for all natural numbers a and b.

i:ex:2.3.4. We have

$$\begin{aligned}
(a+b)^2 &= (a+b)^1 \times (a+b) && i:2.3.11 \\
&= (a+b) \times (a+b) && i:ac:2.3.5 \\
&= a(a+b) + b(a+b) = aa + ab + ba + bb && i:2.3.4 \\
&= a^1 \times a + ab + ba + b^1 \times b && i:ac:2.3.5 \\
&= a^2 + ab + ba + b^2 && i:2.3.11 \\
&= a^2 + ab + ab + b^2 && i:2.3.2 \\
&= a^2 + 1 \times ab + 1 \times ab + b^2 && i:ac:2.3.4 \\
&= a^2 + (1+1) \times ab + b^2 = a^2 + 2ab + b^2. && i:2.3.4
\end{aligned}$$

□

2.3.5 Prove i:2.3.9

i:ex:2.3.5. See i:2.3.9 □