Integers and exponents

Definition. A set of real numbers is called an inductive set if

(a) The number 1 is in the set.

(b) For every $x$ in the set, the number $x + 1$ is in the set also.

The set $\mathbb{R}^+$ of positive real numbers is an example of an inductive set. [The number 1 is in $\mathbb{R}^+$ because $1 > 0$. And if $x$ is in $\mathbb{R}^+$ (so that $x > 0$), then $x + 1$ is in $\mathbb{R}^+$ (since $x + 1 > 1 > 0$).]

Definition. A real number that belongs to every inductive set is called a positive integer; such a number is necessarily positive because $\mathbb{R}^+$ is an inductive set.

Let $P$ denote the set of positive integers. We prove some basic properties of this set.

Theorem 1. Every element of $P$ is greater than or equal to 1.

Proof. We shall show that the set $A$ of all real numbers greater than or equal to 1 is inductive. It then follows that every positive integer belongs to this set.

The number 1 belongs to the set $A$, since $1 \geq 1$.

Suppose $x$ belongs to the set $A$. Then $x \geq 1$; it follows that $x + 1 \geq 1 + 1 > 1$, so that $x + 1$ belongs to the set $A$. Thus $A$ is inductive. $\Box$
Theorem 2. 1 is in P.

Proof. 1 belongs to every inductive set (by definition of "inductive."). Hence 1 belongs to P (by definition of P). □

Theorem 3. If x is in P, so is x + 1.

Proof. Suppose that x is a given element of P. Let I be an arbitrary inductive set. Then x is in I (by definition of P). Hence x + 1 is in I (by definition of "inductive"). Since I is arbitrary, x + 1 is in I for every inductive set I. We conclude that x + 1 is in P (by definition of P). □

Theorem 4 (Principle of induction). Let S be a set of positive integers. If 1 is in S, and if for every x in S, x + 1 is also in S, then necessarily S contains every positive integer.

Proof. S is inductive, by hypothesis. Therefore every positive integer is in S, by definition of P. □

Now we show that P is closed under addition and multiplication.

Theorem 5. If a and b are in P, so is a + b.

Proof. Let a be a fixed positive integer. Then we let S be the set of all positive integers b for which a + b is a positive integer. We shall show that S contains all
positive integers; then the theorem is proved. We use the principle of induction.

The number 1 is in S, because a + 1 is a positive integer (by Theorem 3). Given an element b in S, we show that b + 1 is in S. Now a + b is a positive integer by hypothesis; hence (a+b) + 1 is a positive integer by Theorem 3. Thus a + (b+1) is a positive integer, so b + 1 belongs to S, by definition of S. Thus S is inductive. □

Theorem 6. If a and b are in P, so is a · b.

The proof is left as an exercise.

Definition. A number x is called an integer if it is 0, or is a positive integer, or is the negative of a positive integer. It is easy to see that the negative of any integer is an integer, since \(-(-a) = a\) and \(-0 = 0\).

Let Z denote the set of integers. We now show that Z is closed under addition, multiplication, and subtraction. Closure under multiplication is easy, so we leave the proof as an exercise:

Theorem 7. If a and b are in Z, so is a · b. □

Closure under addition and subtraction are more difficult:

Theorem 8. If a and b are in Z, so are a + b and a - b.

Proof. We proceed in several steps.
Step 1. We show that the theorem is true in the case where \( a \) is a positive integer and \( b = 1 \). That is, if \( a \) is a positive integer, we show that \( a + 1 \) and \( a - 1 \) are integers. That \( a + 1 \) is an integer (in fact, a positive integer) has already been proved. We prove that \( a - 1 \) is an integer, by induction on \( a \). It is true if \( a = 1 \), since \( a - 1 = 0 \) if \( a = 1 \). Supposing it true for \( a \), we prove it true for \( a + 1 \). That is, we show \( (a+1) - 1 \) is an integer. But that is trivial, since \( (a+1) - 1 = a \), which is an integer by hypothesis (in fact, a positive integer).

Step 2. We show the theorem is true if \( a \) is any integer and \( b = 1 \).

We consider three cases. If \( a \) is a positive integer, this result follows from Step 1. If \( a = 0 \), the result is immediate, since

\[
0 + 1 = 1 \quad \text{and} \quad 0 - 1 = -1.
\]

Finally, suppose \( a = -c \), where \( c \) is a positive integer. Then

\[
a + 1 = -c + 1 = -(c-1),
\]

\[
a - 1 = -c - 1 = -(c+1).
\]
Both $c - 1$ and $c + 1$ are integers, by Step 1; then $a + 1$ and $a - 1$ are also integers.

**Step 3.** We show the theorem is true if $a$ is any integer and $b$ is a positive integer.

We proceed by induction on $b$, holding $a$ fixed. We know the theorem holds if $b = 1$, by Step 2. Supposing it holds for $b$, we show it holds for $b + 1$. That is, we show that $a + (b+1)$ and $a - (b+1)$ are integers. Now

$$a + (b+1) = (a+b) + 1,$$

$$a - (b+1) = (a-b) - 1.$$

Both $a + b$ and $a - b$ are integers, by the induction hypothesis; then Step 2 applies to show that $(a+b) + 1$ and $(a-b) - 1$ are integers.

**Step 4.** The theorem is true in general. Let $a$ be any integer. The case where $b$ is a positive integer was treated in Step 3, and the case where $b = 0$ is trivial. Consider finally the case where $b = -d$, where $d$ is a positive integer. Then

$$a + b = a - d \quad \text{and} \quad a - b = a + d;$$
Step 3 applies to show that both $a - d$ and $a + d$ are integers. □

Now we prove the "obvious" fact that if $n$ is an integer, then $n + 1$ is the "next" integer after $n$:

**Theorem 9.** If $n$ is in $\mathbb{Z}$ and $n < a < n + 1$, then $a$ is not in $\mathbb{Z}$.

**Proof.** From the hypothesis of the theorem, it follows that

$$0 < a - n < 1.$$ 

If $a$ were in $\mathbb{Z}$, then $a - n$ would be an integer, by the preceding theorem. But 1 is the smallest positive integer, by Theorem 1. Therefore $a$ is not in $\mathbb{Z}$. □

Now we define integral exponents.

**Definition.** Let $a$ be any real number. We define $a^n$, when $n$ is a positive integer, by induction, as follows. We define

$$a^1 = a,$$

and supposing $a^n$ is defined, we define

$$a^{n+1} = a^n \cdot a.$$
Then $a^n$ is defined for every positive integer $n$. The number $n$ in this expression is called the **exponent**, and the number $a$ is called the **base**.

Exponents satisfy three basic laws, which are stated in the following three theorems. They are called the **laws of exponents**.

**Theorem 10.** $a^n \cdot a^m = a^{n+m}$.

**Proof.** Let $a$ and $n$ be fixed. We prove the theorem "by induction on $m."$ The theorem is true for $m = 1$, since $a^n \cdot a^1 = a^n \cdot a = a^{n+1}$ by definition. Suppose it is true for $m$; we show it is true for $m + 1$. It follows that it holds for all $m$. We have

$$a^n \cdot a^{m+1} = a^n \cdot (a^m \cdot a) \text{ by definition,}$$

$$= (a^n \cdot a^m) \cdot a \text{ by associativity of multiplication,}$$

$$= (a^{n+m}) \cdot a \text{ by the induction hypothesis,}$$

$$= a^{(n+m)+1} \text{ by definition,}$$

$$= a^{n+(m+1)} \text{ by associativity of addition.}$$

Thus the theorem is proved for $m + 1$, as desired. $\Box$
Similar proofs hold for the following two theorems, whose proofs are left as exercises:

Theorem 11. \((a^n)^m = a^{nm}\). □

Theorem 12. \(a^n \cdot b^n = (a \cdot b)^n\). □

Now we define negative exponents.

Definition. Let \(a\) be a real number different from zero. We define zero and negative exponents by the rules:

\[ a^0 = 1, \]

\[ a^{-n} = \frac{1}{a^n} \text{ if } n \text{ is a positive integer}. \]

Theorem 13. The "laws of exponents" hold when \(n\) and \(m\) are arbitrary integers, provided \(a\) and \(b\) are non-zero.

The proof is left as an exercise.

Later on, (in Section G) we shall extend this definition to define "rational exponents"; that is, we shall define \(a^r\) when \(a\) is positive and \(r\) is rational. Still later (in Section M), we shall extend the definition still further to define \(a^x\) when \(a\) is positive and \(x\) is an arbitrary real number. In each of these cases, the same three laws of exponents will hold.
Exercises

1. Prove Theorems 6 and 7.

2. Prove Theorems 11 and 12.

3. Show that if a set $A$ of integers is bounded above, then $A$ has a largest element. [Hint: Use the least upper bound axiom.]

4. Let $F$ be the set of all real numbers of the form $a + b\sqrt{2}$, where $a$ and $b$ are rational. Show that $F$ is closed under addition, subtraction, multiplication, and division. Conclude that $F$ is an "ordered field", that is, that $F$ satisfies Axioms 1 - 9. Show that $F$ does not contain $\sqrt{3}$.

5. Let $n$ and $m$ be positive integers; let $a$ and $b$ be non-zero real numbers. Let $p$ be any integer. Given that the laws of exponents hold for positive integral exponents, prove them for arbitrary integral exponents as follows:

(a) Show $a^n a^{-m} = a^{n-m}$ in the three cases $n - m > 0$ and $n - m = 0$ and $n - m < 0$.

(b) Show $a^{-n} a^{-m} = a^{-n-m}$; and $a^0 a^p = a^p$.

(c) Show $(a^n)^{-m} = a^{-nm} = (a^{-n})^m$.

(d) Show $(a^{-n})^m = a^{mn}$, and $(a^0)^p = (a^p)^0 = a^0$.

(e) Show $a^{-n} b^{-n} = (ab)^{-n}$, and $a^0 b^0 = (ab)^0$. 
6. Let \( a \) and \( h \) be real numbers; let \( m \) be a positive integer. Show by induction that if \( a \) and \( a + h \) are positive, then

\[(a+h)^m \geq a^m + ma^{m-1}h.\]

[Note: Be explicit about where you use the fact that \( a \) and \( a + h \) are positive. Note that \( h \) is not assumed to be positive.]

We shall use this result later on.