Uniqueness of the Real Numbers

The objective of the axiom system for the real numbers is to characterize this system completely. In the preceding discussion we noted that the axioms allow one to derive some important and familiar properties of real numbers. However, in order to conclude that the axioms are a complete characterization of the real numbers, we need to show that all systems satisfying the axioms are "***the same for all practical purposes***." A more formal way of expressing this is to say that if we are given two systems satisfying the axioms there is a one-to-one correspondence between them that preserves all the relevant algebraic structure; such a map is called an isomorphism. More precisely, we have the following definition:

Definition. Let (X, A_X, M_X, O_X) and (Y, A_Y, M_Y, O_Y) be two systems satisfying the axioms for the real numbers, where A and M denote the respective additions and multiplications and O denotes the respective linear orderings. An ***isomorphism*** is a one-to-one correspondence $f : X \to Y$ such that for all $u, v \in X$ we have the following relations:

> **(1)** $f(A_X(u, v)) = A_Y(f(u), f(v))$. [Less formally, $f(u + v) = f(u) + f(v)$, or f is ***additive***.]
>
> **(2)** $f(M_X(u, v)) = M_Y(f(u), f(v))$. [Less formally, $f(u\,v) = f(u)\,f(v)$, or f is ***multiplicative***.]
>
> **(3)** If $(u, v) \in O_X$, then $(f(u), f(v)) \in O_Y$. [Less formally, if $u < v$, then $f(u) < f(v)$, or f is ***order preserving***.]

We say that that X is ***isomorphic*** to Y if there is an isomorphism from X to Y. It is an elementary exercise to verify that if f defines an isomorphism from X to Y, then the inverse function f^{-1} defines an isomorphism from Y to X. In particular, if X is isomorphic to Y, then Y is isomorphic to X and one can simply say that X ***and*** Y ***are isomorphic***. We can now state the main result.

Uniqueness Theorem. *If X and Y are two systems satisfying the axioms for the real numbers, then X and Y are isomorphic.*

PROOF. The construction of an isomorphism starts with its definition for natural numbers and the proceeds to its definition for the (signed) integers, the rational numbers and ultimately the real numbers.

The proof itself is relatively straightforward and elementary but somewhat tedious; however, it is absolutely necessary if we want to talk about **THE** real number system. A detailed argument is included here because most textbooks simply refer to the result or

leave it to the reader as an exercise.

First step. We have already noted that there are (unique) embeddings of the natural numbers — say e_X and e_Y — into X and Y sending the least element 0 of $\mathbf{N}$ to the zero elements 0_X and 0_Y of X and Y respectively and satisfying the basic conditions

$$e_X(\sigma(n)) = e_X(n) + 1_X, \quad e_Y(\sigma(n)) = e_Y(n) + 1_Y$$

where 1_X and 1_Y are the unit elements of X and Y respectively. For each $x \in X$ there is at most one $n \in \mathbf{N}$ such that $x = e_X(n)$, and therefore we can construct a well-defined function

$$f_1 : e_X[\mathbf{N}] \to e_Y[\mathbf{N}]$$

by setting $f_1(e_X(n)) = e_Y(n)$ for $n \in \mathbf{N}$. By construction this defines a one-to-one correspondence between $e_X[\mathbf{N}]$ and $e_Y[\mathbf{N}]$

Claim: The map f_1 satisfies the conditions

$$f_1(A_X(u, v)) = A_Y(f_1(u), f_1(v)),$$

$$f_1(M_X(u, v)) = M_Y(f_1(u), f_1(v)),$$

$$\text{if } (u, v) \in O_X, \text{ then } (f_1(u), f_1(v)) \in O_Y$$

for all $u, v \in \mathbf{N}$. Using the maps e_X and e_Y we may rewrite these conditions as

$$f_1(A_X(e_X(m), e_X(n))) = A_Y(f_1(e_X(m)), f_1(e_X(n))),$$

$$f_1(M_X(e_X(m), e_X(n))) = M_Y(f_1(e_X(m)), f_1(e_X(n))),$$

$$\text{if } (e_X(m), e_X(n)) \in O_X, \text{ then } (f_1(e_X(m)), f_1(e_X(n))) \in O_Y$$

for all $m, n \in \mathbf{N}$. We shall verify the first two of these by induction on n; in order to simplify the notation and stress the underlying ideas we shall use the standard algebraic terminology to denote the addition, multiplication and linear orderings on X and Y.

Addition. Suppose that $n = 0$. Then

$$f_1(e_X(m) + e_X(0)) = f_1(e_X(m) + 0_X) = f_1(e_X(m)) = e_Y(m) + 0_Y = e_Y(m) + e_Y(0) = f_1(e_X(m)) + f_1(e_X(0)).$$

Thus the equation is true for $n = 0$ and all m. Suppose now that it is true for $n = k$ and all m; we need to show it is true for $n = \sigma(k)$ and all m. But

$$f_1\big(e_X(m) + e_X(\sigma(k))\big) = f_1\big(e_X(m) + e_X(k) + 1_X\big) = f_1\big(e_X(m) + e_X(k) + 1_X\big) =$$
$$f_1\big(e_X(m) + 1_X + e_X(k)\big) = f_1\big(e_X(\sigma(m)) + e_X(k)\big)$$

and by the induction hypothesis the last expression is equal to

$$f_1\big(e_X(\sigma(m))\big) + f_1(e_X(k)).$$

The latter in turn is equal to

$$e_Y(\sigma(m)) + e_Y(k) = e_Y(m) + 1_Y + e_Y(k) = e_Y(m) + e_Y(\sigma(k)) =$$
$$f_1\big(e_X(m)\big) + f_1\big(e_X(\sigma(k))\big).$$

This completes the verification of the inductive step.

Multiplication. Suppose that $n = 0$. Then

$$f_1\big(e_X(m) \cdot e_X(0)\big) = f_1\big(e_X(m) \cdot 0_X\big) = f_1(0_X) = 0_Y = e_Y(m) \cdot 0_Y = e_Y(m) \cdot e_Y(0)$$
$$= f_1\big(e_X(m)\big) \cdot f_1(e_X(0)).$$

Thus the equation is true for $n = 0$ and all m. Suppose that we know the equation is true for $n = k$ and all m; we need to show it is true for $n = \sigma(k)$ and all m. But

$$f_1\big(e_X(m) \cdot e_X(\sigma(k))\big) = f_1\big(e_X(m) \cdot e_X(k) + e_X(m)\big) =$$
$$f_1\big(e_X(m) \cdot e_X(k)\big) + f_1\big(e_X(m)\big)$$

because we have already verified that f_1 is additive, and by the induction hypothesis the last expression is equal to $f_1\big(e_X(m)\big) \cdot f_1\big(e_X(k)\big)\big) + f_1\big(e_X(m)\big)$. The latter in turn is equal to

$$e_Y(m) \cdot e_Y(k) + e_Y(m) = e_Y(m) \cdot e_Y\big(\sigma(k)\big) = f_1\big(e_X(m)\big) \cdot f_1\big(e_X(\sigma(k))\big).$$

As before, this completes the verification of the inductive step.

Ordering. If $e_X(m) < e_X(n)$ then there is a nonzero natural number $c \in \mathbf{N}$ such that $e_X(m) + e_X(c) = e_X(n)$. Since f_1 is one-to-one, it follows that $e_Y(c) = f_1(e_X(c)) \neq 0_Y$, so that $e_Y(c) > 0_Y$. By the additivity of f_1 it follows that

$$f_1\big(e_X(m)\big) = e_Y(m) = e_Y(m) + 0_Y < e_Y(m) + e_Y(c) =$$
$$f_1\big(e_X(m) + e_X(c)\big) = f_1\big(e_X(n)\big)$$

as required.

Notational conventions. Let F be a system satisfying the axioms for the real number system, and let $e_F : \mathbf{N} \to F$ be the embedding of the natural numbers that has been used extensively in the preceding step of the proof. We define the ***integers*** in F to be the set of all objects of the form $e_F(a) - e_F(b)$ for some $a, b \in \mathbf{N}$, and we shall denote this set by $\mathbf{Z}(F)$. Similarly, we define the ***rational numbers*** or ***rationals*** in F to be the set of m/n where m and n are integers in F and n is nonzero, and we shall denote this set by $\mathbf{Q}(F)$. If we are dealing with one fixed system in a given context we shall omit the "(F)" to simplify and standardize the notation.

Second step. We need to extend f_1 to negative integers. Clearly we want a definition sending a negative number of the form $-e_X(n) \in X$ to $-e_Y(n) = -f_1\big(e_Y(n)\big)$, but we shall take a slightly less direct approach that will be helpful in verifying the crucial properties of the extended map without a succession of case by case arguments.

By the preceding definition, every integer $n \in X$ can be represented as a difference $e_X(a) - e_X(b)$ for some $a, b \in \mathbf{N}$; this representation is not unique, but it is elementary to check that $e_X(a) - e_X(b) = e_X(c) - e_X(d)$ if and only if

$$e_X(a) + e_X(d) = e_X(b) + e_X(c).$$

We shall extend f_1 to a map f_2 on integers by setting

$$f_2\big(e_X(a) - e_X(b)\big) = e_Y(a) - e_Y(b) = f_1\big(e_X(a)\big) - f_1\big(e_X(b)\big).$$

Before proceeding any further we need to show that f_2 is well-defined; in other words, we need to verify that

$$\textit{if } e_X(a) - e_X(b) = e_X(c) - e_X(d), \textit{ then } e_Y(a) - e_Y(b) = e_Y(c) - e_Y(d).$$

Equivalently, we need to show that

$$\textit{if } e_X(a) + e_X(d) = e_X(b) + e_X(c), \textit{ then } e_Y(a) + e_Y(d) = e_Y(b) + e_Y(c).$$

To see the latter, apply f_1 to both sides of the first equation and note that the additivity of f_1 on $\mathbf{N}$ implies that

$$e_Y(a) + e_Y(d) = f_1\big(e_X(a)\big) + f_1\big(e_X(d)\big) = f_1\big(e_X(a) + e_X(d)\big) =$$
$$f_1\big(e_X(b) + e_X(c)\big) = f_1\big(e_X(b)\big) + f_1\big(e_X(c)\big) = e_Y(b) + e_Y(c)$$

so that f_2 is well-defined.

Throughout the remainder of this step in the proof we shall consider two integers in X of

the form $m = e_X(a) - e_X(b)$ and $n = e_X(c) - e_X(d)$.

We must now show that f_2 is one-to-one. To see this, suppose that $f_2(m) = f_2(n)$. By construction it follows that $e_Y(a) - e_Y(b) = e_Y(c) - e_Y(d)$ so that $e_Y(a) + e_Y(d) = e_Y(b) + e_Y(c)$. The identities of the previous paragraph now imply that

$$f_1\big(e_X(a) + e_X(d)\big) = f_1\big(e_X(b) + e_X(c)\big)$$

and since f_1 is one-to-one it follows that $e_X(a) + e_X(d) = e_X(b) + e_X(c)$. But the latter implies $e_X(a) - e_X(b) = e_X(c) - e_X(d)$ which in turn implies that $m = n$. By construction it follows that the image of f_2 is the set of all differences of elements in the image of e_Y; in other words, f_2 ***maps the integers in*** X ***onto the integers in*** Y.

We next verify that f_2 is additive:

$$\begin{gathered}
f_2(m+n) = f_2\big(e_X(a) - e_X(b) + e_X(c) - e_X(d)\big) = \\
f_2\big(e_X(a) + e_X(c) - e_X(b) - e_X(d)\big) = \\
f_2\big((e_X(a) + e_X(c)) - (e_X(b) + e_X(d))\big) = \\
f_1\big(e_X(a) + e_X(c)\big) - f_1\big(e_X(b) + e_X(d)\big) = \\
\big(e_Y(a) + e_Y(c)\big) - \big(e_Y(b) + e_Y(d)\big) = \\
e_Y(a) - e_Y(b) + e_Y(c) - e_Y(d) = \\
f_2(m) + f_2(n).
\end{gathered}$$

The verification that f_2 is multiplicative proceeds similarly:

$$\begin{gathered}
f_2(m \cdot n) = f_2\big((e_X(a) - e_X(b)) \cdot (e_X(c) - e_X(d))\big) = \\
f_2\big((e_X(a) \cdot e_X(c) + e_X(b) \cdot e_X(d)) - (e_X(a \cdot e_X(d) + e_X(b) \cdot e_X(c))\big) = \\
f_1\big(e_X(a) \cdot e_X(c) + e_X(b) \cdot e_X(d)\big) - f_1\big(e_X(a) \cdot e_X(d) + e_X(b) \cdot e_X(c)\big) = \\
\big(f_1(e_X(a)) \cdot f_1(e_X(c)) + f_1(e_X(b)) \cdot f_1(e_X(d))\big) - \\
\big(f_1(e_X(a)) \cdot f_1(e_X(d)) + f_1(e_X(b)) \cdot f_1(e_X(c))\big) = \\
\big(e_Y(a) \cdot e_Y(c) + e_Y(b) \cdot e_Y(d)\big) - \big(e_Y(a) \cdot e_Y(d) + e_Y(b) \cdot e_Y(c)\big) = \\
\big(e_Y(a) - e_Y(b)\big) \cdot \big(e_Y(c) - e_Y(d)\big) = f_2(m) \cdot f_2(n).
\end{gathered}$$

To prove that f_2 is order preserving, suppose that $m < n$, so that we have

$$e_X(a) - e_X(b) < e_X(c) - e_X(d).$$

Adding $e_X(b) - e_X(d)$ to both sides of this inequality yields

$$e_X(a) + e_X(d) < e_X(b) + e_X(c)$$

and since f_1 is order preserving the latter in turn implies

$$e_Y(a) + e_Y(d) = f_1(e_X(a)) + f_1(e_X(d)) = f_1\big(e_X(a) + e_X(d)\big) <$$
$$f_1\big(e_X(b) + e_X(c)\big) = f_1(e_X(b)) + f_1(e_X(c)) = e_Y(a) + e_Y(c).$$

If we now subtract $e_Y(b) + e_Y(d)$ from both sides of the outside inequality we obtain the desired conclusion:

$$f_2(m) = e_Y(a) - e_Y(b) < e_Y(c) - e_Y(d) = f_2(n)$$

This completes the second step of the proof.

Third step. We need to extend f_2 to rational numbers of the form a/b where a and b are integers and b is nonzero. Recall from elementary algebra that two fractions a/b and c/d (with b and d nonzero) are equal if and only if $ad = bc$.

The idea is to consider a number $q \in X$ of the form a/b, where a and b are integers in X and b is nonzero, and to define $f_3(q) = f_2(a)/f_2(b)$. In order to show that this is a valid definition we need to check two things. First of all, since f_2 is one-to-one it follows that $f_2(b)$ is nonzero if b is nonzero, so the quotient is actually defined. Second, we need to show that the value obtained by the formula is the same if we write q as a quotient of integers in two different ways. In other words, we need to show that if $a/b = c/d$ (with b and d nonzero) then we also have $f_2(a)/f_2(b) = f_2(c)/f_2(d)$. To do this, begin with the previous observation that $ad = bc$ and apply f_2 to both sides of the equation to obtain $f_2(a) \cdot f_2(d) = f_2(b) \cdot f_2(c)$. If we then divide both sides of this equation by $f_2(b) \cdot f_2(d)$ we obtain $f_2(a)/f_2(b) = f_2(c)/f_2(d)$ as required.

By construction the image of f_3 consists of all expressions of the form u/v where u and v are in the image of f_2 and v is nonzero; in other words, f_3 ***maps the rationals in*** X ***onto the rationals in*** Y. We claim that f_3 is also one-to-one.

Throughout the remainder of this step in the proof we shall consider two rational numbers in X of the form $p = a/b$ and $q = c/d$ where a, b, c, d are integers in X and b and d are nonzero.

To prove that f_3 is one-to-one suppose that $f_3(p) = f_3(q)$. By construction it follows that $f_2(a)/f_2(b) = f_2(c)/f_2(d)$, which is equivalent to $f_2(a) \cdot f_2(d) = f_2(b) \cdot f_2(c)$. Since f_2 is multiplicative we have

$$f_2(ad) = f_2(a) \cdot f_2(d) = f_2(b) \cdot f_2(c) = f_2(bc)$$

and since f_2 is one-to-one this implies $ad = bc$, which in turn implies $a/b = c/d$ and

hence that f_3 ***is one-to-one.***

The ***verification that*** f_3 ***is additive*** follows from the string of equations

$$f_3\left(\frac{a}{b}+\frac{c}{d}\right)=f_3\left(\frac{ad+bc}{bd}\right)=\frac{f_2(ad+bc)}{f_2(bd)}=\frac{f_2(a)\,f_2(d)+f_2(b)\,f_2(c)}{f_2(b)\,f_2(d)}=$$

$$\frac{f_2(a)}{f_2(b)}+\frac{f_2(c)}{f_2(d)}\quad=\quad f_3\left(\frac{a}{b}\right)+f_3\left(\frac{c}{d}\right).$$

Similarly, the ***verification that*** f_3 ***is multiplicative*** follows from the somewhat different string of equations

$$f_3\left(\frac{a}{b}\cdot\frac{c}{d}\right)=f_3\left(\frac{ac}{bd}\right)=\frac{f_2(ac)}{f_2(bd)}=\frac{f_2(a)\,f_2(c)}{f_2(b)\,f_2(d)}=$$

$$\frac{f_2(a)}{f_2(b)}\cdot\frac{f_2(c)}{f_2(d)}\quad=\quad f_3\left(\frac{a}{b}\right)+f_3\left(\frac{c}{d}\right).$$

Finally we need to ***show that*** f_3 ***is order preserving.*** We shall do this using the fact that a fraction a/b is positive if and only if the product of the number and denominator ab is positive (the second number is the product of the first with the positive number b^2). Therefore suppose that $p < q$; then $p - q$ is positive, and by the observation on the signs of fractions in the previous sentence it follows that the integer $(bc - ad)\cdot bd$ is also positive. Since f_2 is order preserving it follows that

$$f_2\left((bc-ad)\cdot bd\right)=\left(f_2(b)\cdot f_2(c)-f_2(a)\cdot f_2(d)\right)\cdot\left(f_2(b)\,f_2(d)\right)$$

is also positive. But the right hand side of this equation is equal to $f_3(q) - f_3(p)$, so the preceding observations imply that $f_3(q) > f_3(p)$ as required.

Fourth step. We need to extend f_3 to all elements of X. Given a number $r \in X$, consider the set $D(r)$ of all rational numbers $q \in X$ such that $q < r$. Let k be a positive integer that is greater than r, and consider the set $f_3(D(r)) \subset Y$. Since f_3 is order preserving it follows that $f_3(k)$ is an upper bound for $f_3(D(r))$ and therefore by completeness the set $f_3(D(r))$ has a (unique) least upper bound; we take $f(r)$ to be this least upper bound. This definition may be rewritten as follows:

$$f(r) = \text{L.U.B.}_{q<r}\ f_3(q)$$

The first order of business is to show that $f_3(r) = f(r)$ if r is rational. If r is rational

and $q \in D(r)$, then by the previous work we know that $f_3(q) < f_3(r)$, so that $f_3(r)$ is an upper bound for $f_3(D(r))$ and consequently is greater than or equal to the least upper bound, which is $f(r)$. Suppose now that $f(r) < f_3(r)$. It follows that there is a rational number $t \in X$ such that

$$f(r) < f_3(t) < f_3(r).$$

But f_3 is order preserving, and therefore the second inequality implies that $t < r$. The latter in turn implies that $t \in D(r)$ and hence that $f_3(t) \leq f(r)$, which when combined with the previously displayed inequality $f(r) < f_3(t)$ yields a contradiction. It follows that $f(r) = f_3(r)$.

To ***show that*** f ***is one-to-one***, assume that r and s are real numbers in X such that $r < s$. Choose rational numbers p and q such that $r < p < q < s$. As before, it follows that $f_3(p)$ is an upper bound for $f_3(D(r))$ and therefore $f(r) \leq f_3(p) = f(p)$. Furthermore, since $f_3 = f$ for rational numbers it follows that $f(p) < f(q)$, and since $q \in D(s)$ it follows that $f(q) = f_3(q) \leq f(s)$. If we put these inequalities together we find that $f(r) < f(s)$ and consequently that f ***is one-to-one.***

Note that ***this argument also shows that*** f ***is order preserving.***

We shall next ***verify that the function*** f ***maps*** X ***onto all of*** Y. Let $y \in Y$ be arbitrary, and let $D^*(y)$ be the set of all rational numbers $q \in Y$ such that $q < y$; by construction y is an upper bound for $D^*(y)$, and in fact y is the least upper bound of $D^*(y)$ because if $z < y$ then there is a rational number p such that $z < p < y$. As before there is a positive integer $k \in Y$ such that $y < k$, and since the function f_3 is order preserving it follows that $k_0 = f_3^{-1}(k)$ is an upper bound for the set $f_3^{-1}(D^*(y))$. Therefore the latter set has an upper bound that we shall denote by x. We claim that $f(x) = y$, and we shall do this by showing that $y \leq f(x)$ and strict inequality does not hold. To show the inequality, suppose that $q < y$, and choose a rational number $p \in Y$ such that $q < p < y$. If we write $q_0 = f_3^{-1}(q)$ and $p_0 = f_3^{-1}(p)$ then $q_0 < p_0$, and since both belong to the set $f_3^{-1}(D^*(y))$ it follows that $q_0 < p_0 < x$. Since the function f is order preserving the identities $p = f_3(p_0) = f(p_0)$ and $q = f_3(q_0) = f(q_0)$ imply that $q < p < f(x)$. Thus $f(x)$ is an upper bound for $D^*(y)$; since y is the least upper bound $D^*(y)$ we must have $y \leq f(x)$. The proof that $y = f(x)$ thus reduces to showing that $f(x)$ is not strictly greater than y.

Assume the contrary. Then there is a rational number q satisfying $y < q < f(x)$, and write $q = f_3(q_0) = f(q_0)$ as before. Since the function f is order preserving, it follows that $q_0 < x$. But the definition of x as a least upper bound implies the existence of a rational number p_0 such that $q_0 < p_0$ and $p = f_3^{-1}(p_0)$ lies in $D^*(y)$; *i.e.*, $p < y$. Once again we have

$$q = f_3(q_0) < f_3(p_0) = p$$

and if we combine this with the other inequalities we obtain the string of inequalities

$$y < q < p < y$$

which is a contradiction. This completes the proof that $y = f(x)$.

The next step is to ***show that*** f ***is additive.*** Let u and v be arbitrary real numbers in X. Consider first the special case where one of these numbers (say v) is rational. In this case the set $D(u + v)$ is the set of all numbers expressible as sums

$$f_3(q) + f_3(v) = f_3(q) + f(v)$$

where $q \in D(u)$, and therefore we have

$$f(u + v) = \text{L.U.B.}_{q < u + v}\ f_3(q) = \left(\text{L.U.B.}_{p < u}\ f_3(p)\right) + f(v) = f(u) + f(v)$$

and hence f is additive if v is rational and u is arbitrary.

We now consider the general case. If q is a rational number such that $q < v$, then

$$f(u) + f(q) = f(u + q) < f(u + v)$$

because f is order preserving and it is also additive if one of the summands is rational. Therefore $q < v$ implies that

$$f_3(q) = f(q) < f(u + v) - f(u)$$

and consequently we have

$$f(v) = \text{L.U.B.}_{q < v}\ f_3(q) \leq f(u + v) - f(u).$$

Additivity will follow if we can show that $f(v) < f(u + v) - f(u)$ is impossible, so assume that it does hold. In this case there is a rational number $r \in Y$ such that

$$f(v) < r < f(u + v) - f(u)$$

and because f is onto we may write $r = f(q)$ for some rational number $q \in X$. Since f is order preserving we know that $v < q$, and consequently the order preserving and partial additivity properties of f imply that

$$f(q) = r < f(u + v) - f(u) < f(u + q) - f(u) = f(u) + f(q) - f(u) = f(q)$$

which is a contradiction. Therefore the assumption $f(v) < f(u + v) - f(u)$ must be

incorrect, and by the preceding discussion it follows that f must be additive.

At this point, ***the only statement that remains to be established is that*** f ***is multiplicative.*** We first observe that f is multiplicative if at least one of the factors is 0 or ± 1. If one of the factors is $+1$, this is immediate because $f(1_X) = 1_Y$. If one of the factors is zero, this follows quickly because the product of anything with zero is zero and $f(0_X) = 0_Y$. If one of the factors is -1, this will follow provided we can show that $f(-a) = -f(a)$ for all $a \in X$, for then we have

$$f(-1_X) = -f(1_X) = -1_Y$$

and furthermore

$$f((-1_X)\cdot a) = f(-a) = -f(a) = (-1_Y)\cdot f(a) = f(-1_X)\cdot f(a).$$

To see that $f(-a) = -f(a)$, let $b = -a$. Since f is additive we have that

$$0_Y = f(0_X) = f(a+b) = f(a) + f(b)$$

and the latter implies that $f(b) = -f(a)$ as required. We shall need the basic identity $f(-a) = -f(a)$ in order to complete the final step in the verification that f is multiplicative.

The next step in verifying that f ***is multiplicative is to show this is true if both of the factors are positive.*** The proof of this fact is very similar to the proof of additivity (since the exponential map defines an order preserving isomorphism from the additive group of real numbers to the multiplicative group of positive real numbers, this should not be surprising). Let u and v be arbitrary ***positive*** real numbers in X. Since f is order and zero preserving it follows that both $f(u)$ and $f(v)$ are positive.

Consider first the special case where one of these numbers (say v) is rational (and positive!). In this case, the set $D(u\cdot v)$ is the set of all real numbers expressible as sums $f_3(q)\cdot f_3(v) = f_3(q)\cdot f(v)$ where $q \in D(u)$, and therefore we have

$$f(u\cdot v) = \text{L.U.B.}_{q < u\cdot v}\, f_3(q) = \left(\text{L.U.B.}_{p < u}\, f_3(p)\right)\cdot f(v) = f(u)\cdot f(v)$$

and hence f is multiplicative if v is rational and u is arbitrary.

We now consider the general case. If q is a rational number such that $q < v$, then

$$f(u)\cdot f(q) = f(u\cdot q) < f(u\cdot v)$$

because f is order preserving and it is also additive if one of the summands is rational. Therefore $q < v$ implies that

$$f_3(q) = f(q) < f(u \cdot v)/f(u)$$

and consequently we have

$$f(v) = \text{L.U.B.}_{q<v}\, f_3(q) \le f(u \cdot v)/f(u).$$

Multiplicativity will follow if we can show that $f(v) < f(u \cdot v)/f(u)$ is impossible, so assume that it does hold. In this case there is a rational number $r \in Y$ such that

$$f(v) < r < f(u \cdot v)/f(u)$$

and because f is onto we may write $r = f(q)$ for some rational number $q \in X$. Since f is order preserving we know that $v < q$, and consequently the order preserving and partial multiplicativity properties of f imply that

$$f(q) = r < f(u \cdot v)/f(u) < f(u \cdot q)/f(u) = f(u) \cdot f(q)/f(u) = f(q)$$

which is a contradiction. Therefore the assumption $f(v) < f(u \cdot v)/f(u)$ must be incorrect, and by the preceding discussion it follows that f must be multiplicative.

Finally, ***we need to verify that*** f ***is multiplicative in all cases.*** Given a nonzero real number a, set $\varepsilon(a)$ equal to $+1$ if a is positive and -1 if a is negative. Then we may express $a = \varepsilon(a) \cdot |a|$ where the absolute value $|a|$ is positive. Using the multiplicativity of f for the product $|u| \cdot |v|$ and the identity $f(\varepsilon \cdot a) = \varepsilon \cdot f(a)$ for $\varepsilon = \pm 1$ we have

$$f(u \cdot v) = f\left((\varepsilon(u) \cdot |u|) \cdot (\varepsilon(v) \cdot |v|)\right) =$$
$$f\left(\varepsilon(u) \cdot \varepsilon(v) \cdot |u| \cdot |v|\right) = \left(\varepsilon(u) \cdot \varepsilon(v)\right) \cdot f(|u| \cdot |v|) =$$
$$\left(\varepsilon(u) \cdot \varepsilon(v)\right) \cdot f(|u|) \cdot f(|v|) = \left(\varepsilon(u) \cdot f(|u|)\right) \cdot \left(\varepsilon(v) \cdot f(|v|)\right) =$$
$$\left(f(\varepsilon(u) \cdot |u|)\right) \cdot \left(f(\varepsilon(v) \cdot |v|)\right) = f(u) \cdot f(v)$$

and this completes the proof that f is multiplicative.■

Rigidity of the Real Numbers

It turns out that the isomorphism constructed above is unique. This is equivalent to saying that the only automorphism of $\mathbf{R}$ with itself that preserves addition, multiplication and ordering is the identity. In fact, it turns out that there is only one automorphism from $\mathbf{R}$ to itself that preserves addition and multiplication.

Theorem. *If* $f: \mathbf{R} \to \mathbf{R}$ *is a one-to-one correspondence that is additive and multiplicative, then f is the identity.*

PROOF. The proof begins with a couple of simple observations:

(a) *The only element* $u \in \mathbf{R}$ *such that* $xu = x$ *for all* $x \in \mathbf{R}$ *is the unit element.*

(b) *The only element* $z \in \mathbf{R}$ *such that* $x\,z = z$ *for all* $x \in \mathbf{R}$ *is the zero element.*

These follow because $u = 1 \cdot u = 1$ and $0 = 0 \cdot z = z$. Since f sends elements with properties **(a)** and **(b)** into elements with the corresponding properties, it follows that we must have $f(1) = 1$ and $f(0) = 0$.

We shall also need two other standard elementary properties of automorphisms (and isomorphisms):

(c) *For all* $x \in \mathbf{R}$ *we have* $f(-x) = -f(x)$.

(d) *For all nonzero* $x \in \mathbf{R}$ *we have* $f(x^{-1}) = f(x)^{-1}$.

The proof of **(c)** is the same argument that was used in the uniqueness proof, and the proof of **(d)** is based upon similar considerations:

$$1 = f(1) = f(x\,x^{-1}) = f(x)\,f(x^{-1}) \quad \Rightarrow \quad f(x^{-1}) = f(x)^{-1}$$

The main idea behind the proof is to show successively that f must be the identity on each of the following:

1. The natural numbers $\mathbf{N}$.
2. The integers $\mathbf{Z}$.
3. The rational numbers $\mathbf{Q}$.
4. All real numbers.

Predictably, we take these in the order listed.

The natural numbers. Let $e : \mathbf{N} \to \mathbf{R}$ be the embedding described in the section on axioms for the real numbers. We shall show that $f(e(n)) = e(n)$ by induction on n; we have already verified this if $n = 0$ or $n = 1$. Suppose that this is known for $n = k$. Then by the additivity of f and the inductive hypothesis we have

$$f\left(e(\sigma(k))\right) = f\left(e(k) + 1\right) = f\left(e(k)\right) + 1 = e(k) + 1 = e(\sigma(k)),$$

and hence f is the identity on the natural numbers (more correctly, on the image of the natural numbers in the reals).

The integers. Given an integer $n \in \mathbf{Z}$ write $n = e(a) - e(b)$ where $a, b \in \mathbf{Z}$. Then by the preceding step in the proof, additivity and property **(c)** above we have

$$f(n) = f\left(e(a) - e(b)\right) = f\left(e(a)\right) - f\left(e(b)\right) = e(a) - e(b) = n$$

as required.

The rational numbers. Given a rational number $q \in \mathbf{Q}$ express q as a quotient $a\,b^{-1}$ where $a, b \in \mathbf{Q}$ and b is nonzero. As before, by the immediately preceding step in the proof, the multiplicativity of f and property **(d)** above we have

$$f(q) = f(a\,b^{-1}) = f(a)\,f(b^{-1}) = f(a)\,f(b)^{-1} = a\,b^{-1} = q$$

as required.

The set of all real numbers. The crucial step in the proof is to ***show that*** f ***is order preserving.*** Suppose that $a, b \in \mathbf{R}$ satisfy $a > b$. If $c = a - b$ then $c > 0$ and therefore c has a unique positive square root that we shall call d. If we apply f to both sides of the equation $d^2 = a - b$ we obtain the equation

$$f(d)^2 = f(d^2) = f(a - b) = f(a) - f(b);$$

this quantity is nonzero because f is one-to-one (look at the right hand side), and it is nonnegative because it is a square (look at the left hand side). Therefore the quantity in question is positive as claimed.

To conclude the proof, let $a \in \mathbf{R}$ be arbitrary. We need to show that neither of the strict inequalities $a > f(a)$ or $a < f(a)$ can hold. The proofs in both cases are similar so we shall do them simultaneously. Suppose that $a > f(a)$ or $a < f(a)$ is true, and in the respective cases choose a rational number q such that

$$a > q > f(a) \quad \text{or} \quad a < q < f(a).$$

Since f is order preserving and is the identity on rational numbers, these inequalities respectively imply

$$f(a) > f(q) = q > f(a) \quad \text{and} \quad f(a) < f(q) = q < f(a).$$

In either case we obtain a contradiction, and therefore we must have $f(a) = a$. ■