Real numbers

Lesson 11

Binary operator

Definition

A *binary operator* on a set S is a function from $S \times S$ to S. A binary operator F is commutative provided

$$(\forall a, b \in S)(F(a, b) = F(b, a)).$$

It is associative provided

$$(\forall a, b, c \in S)(F(a, F(b, c)) = F(F(a, b), c)).$$

It has an *left identity element* provided

$$(\exists\ \theta \in S)((\forall a \in S)(F(\theta, a) = a).$$

And it has an *right identity element* provided

$$(\exists\ \theta \in S)((\forall a \in S)(F(a, \theta) = a).$$

1. Addition and multiplication of real numbers are examples of binary operators; these operators are commutative and associative.
2. In this context, binary means that the function takes *two* members of the same set; the use of binary has nothing to do with base two representation of a number.
3. Usually binary operators are expressed in *infix notation*; that is, the operator is in between its arguments.
4. For example, we write $1 + 107 = 108$, not $+(1, 107) = 108$.
5. For a commutative binary operator, every right identity element is a left identity element; so we'll call them collectively an identity element.

Examples

(a) Addition $+$ is a binary operator on R. Since $x + 0 = x$ for all real x, the unit for addition is zero. Further we know that addition is commutative and associative.

(b) Function composition $\circ$ is a binary operator on the set of functions from R to R. The function $x \in \mathrm{R} \mapsto x$ is the unit for function composition . Function composition is associative, but not commutative.

Unique elements

Theorem

Let S be a set and let F be a commutative binary operator on S. Then F has at most one identity element.

Proof

Let θ and θ' be identity element. for F. We'll show that $\theta = \theta'$. We have

$$\begin{aligned} \theta &= F(\theta', \theta), && \text{(because } \theta \text{ is an identity element.)} \\ &= F(\theta, \theta'), && \text{(because } F \text{ is commutative)} \\ &= \theta'. && \text{(because } \theta' \text{ is an identity element.)} \end{aligned}$$

So $\theta = \theta'$.

Fields

We would like to capture the important features of the real numbers and give all such structures a name. This object is a *field*.

Definition

A field is an ordered triple $(\mathcal{F}, +, \times)$ where $\mathcal{F}$ is a set and both $+$ and $\times$ are commutative and associative binary operators on $\mathcal{F}$ that have identity elements; the identity element for $+$ is 0 and the identity element for $\times$ is 1.

1. For all $a, b, c \in \mathcal{F}$, we have $a \times (b + c) = a \times b + a \times c$.
2. For all $a \in \mathcal{F}$ there is $-a \in \mathcal{F}$ such that $a + -a = 0$.
3. For all $a \in \mathcal{F}_{\neq 0}$ there is $a^{-1} \in \mathcal{F}$ such that $aa^{-1} = 1$.

1. We say that $-a$ is an additive inverse of a.
2. We say that a^{-1} is a multiplicative inverse of a.

Unique inverses

Theorem

Let $(\mathcal{F}, +, \times)$ be a field. The additive and multiplicative inverses are unique.

Proof

Let $a \in \mathcal{F}$ and suppose $a + b = 0$ and $a + b' = 0$. We'll show that $b = b'$. We have

$$\begin{aligned} b &= b + 0, \\ &= b + (a + b'), \\ &= (b + a) + b', \\ &= (a + b) + b', \\ &= 0 + b', \\ &= b'. \end{aligned}$$

The proof for the multiplicative inverse is similar and left as an exercise for the willing.

Why is the product of negative numbers positive?

Theorem

Let $(\mathcal{F}, +, \times)$ be a field. For all $a, b \in \mathcal{F}$, we have

1. $0a = a0 = 0.$
2. $a(-b) = (-a)b = -(ab)$
3. $-(-a) = a$
4. $(-a)(-b) = ab$

The last is the most mysterious for grade school students. A proof follows from replacing $a \to -a$ in $a(-b) = (-a)b$ and using $-(-a) = a$.

Let's prove $a(-b) = (-a)b = -(ab)$.

Proof

Let $(\mathcal{F}, +, \times)$ be a field. For all $a, b \in \mathcal{F}$, we have

$$0 = a0 = a(b + -b) = ab + a(-b).$$

So $-(ab) = a(-b)$. Interchanging a and b and using commutivity gives $-(ab) = (-a)b$.

Famous fields

Let $+$ and $\times$ be ordinary number addition and multiplication, respectively. Then

1. $(R, +, \times)$ is the real field.
2. $(Q, +, \times)$ is the rational field. Certainly the sum and product of rational numbers is a rational number so indeed, $+ : Q \times Q \to Q$ and similarly for $\times$. The other required conditions are "inherited" from the properties of the real field.
3. $(Z, +, \times)$ isn't a field because, for example, there is no $x \in Z$ such that $2x = 1$.

Ordered Fields

Definition

A field $(\mathcal{F}, +, \times)$ is ordered provided there is a subset P of $\mathcal{F}$ such that

a. If $a, b \in P$, we have $a + b \in P$,
b. If $a, b \in P$, we have $a \times b \in P$,
c. For all $a \in \mathcal{F}$ exactly one of the following is true: (i) $a \in P$, (ii) $-a \in P$, (iii) $a = 0$.
d. $[b - a \in P] \equiv [a < b]$.
e. $[a \leq b] \equiv [a < b \vee a = b]$.

Assume the reals

We will assume that there is a set R with members called *real numbers* along with functions $+ : \mathsf{R} \times \mathsf{R} \to \mathsf{R}$ and $\times : \mathsf{R} \times \mathsf{R} \to \mathsf{R}$. Further we'll assume that this field is ordered by the positive numbers.

Theorem

Let $(\mathcal{F}, +, \times)$ be an ordered field. For all $a, b, c \in \mathcal{F}$ we have

(a) $a < b \implies a + c < b + c$.

(b) $a < b \wedge b < c \implies a < c$.

(c) $a < b \wedge c > 0 \implies ac < bc$.

(d) $a < b \wedge c < 0 \implies ac > bc$.

(e) $a \neq 0 \implies a^2 > 0$.