

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

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

- ➊ Addition and multiplication of real numbers are examples of binary operators; these operators are commutative and associative.
- ➋ 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.
- ➌ Usually binary operators are expressed in *infix notation*; that is, the operator is in between its arguments.
- ➍ For example, we write $1 + 107 = 108$, not $+(1, 107) = 108$.
- ➎ 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 \mathbb{R} . Since $x + 0 = x$ for all real x , the identity element 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 \mathbb{R} to \mathbb{R} . The function $x \in \mathbb{R} \mapsto x$ is the identity element 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 elements 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.

Famous fields

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

- Ⓐ $(\mathbb{R}, +, \times)$ is the real field.
- Ⓑ $(\mathbb{Q}, +, \times)$ is the rational field. Certainly the sum and product of rational numbers is a rational number so indeed, $+: \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ and similarly for \times . The other required conditions are “inherited” from the properties of the real field.
- Ⓒ $(\mathbb{Z}, +, \times)$ isn't a field because, for example, there is no $x \in \mathbb{Z}$ 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

- Ⓐ If $a, b \in P$, we have $a + b \in P$,
- Ⓑ If $a, b \in P$, we have $a \times b \in P$,
- Ⓒ For all $a \in \mathcal{F}$ exactly one of the following is true: (i) $a \in P$, (ii) $-a \in P$, (iii) $a = 0$.