Groups and Rings

Carter Aitken

2025-05-05

Abstract

We're studying abstract algebra, specifically groups and rings.

Contents

1 Operations on Sets

1.1 K-Ary Operations

- $\mathbb{N}$ $+, \cdot$
- $\mathbb{Z}$ $+, \cdot, -$
- $\mathbb{Q}$ $+, \cdot, -$
- $\mathbb{R}$ $+, \cdot, -$
- $\mathbb{C}$ $+, \cdot, -, x \mapsto \overline{x}, x \mapsto \sqrt{x}$
- (Vectors) $+$, (scalarmul)
- (Matricies) $+$, (scalarmul), (matrixmul)
- (polynomials) $+, \cdot$

In abstract algebra, we're iinterested in what notions of "numbers" exists.

The different "types" of numbers really are distinguished by the operations on them. In this class we'll stick with operating on sets.

Definition 1.1: Binary Operations. *A **binary operation** on a set X is a function $b : X \times X \to X$.*

Note: we often write binary operators inline (like in Haskell).

We could use $+, \cdot, \times, \div, \otimes, \boxtimes, \oplus, \boxplus, \diamond$

`FIND \gop in the .tex file to change the operator used.`
`/\\newcommand{\\gop}`

Definition 1.2. *a **k-ary operator** on X is a func $f : \underbrace{X \times \cdots \times X}_{k} \to X$.*

$x \mapsto \frac{1}{x}$ on $\mathbb{Q}$ isn't a unary operation b/c $\frac{1}{0}$ isn't defined.
$\mathbb{Q}^\times = \{x \in \mathbb{Q} : x \neq 0\}$ does have the reciprocal as a binary operator, but not minus.

1.2 Associative Operations

Definition 1.3. *a binary operator $\boxtimes$ on X is **associative** if*

$$x \boxtimes (y \boxtimes z) = (x \boxtimes y) \boxtimes z, \quad \forall x, y, z \in X$$

$+, \cdot$ on $\mathbb{N}, \mathbb{Z}$ are associative. $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ isn't associative. Neither is $\div : \mathbb{Q}^\times \times \mathbb{Q}^\times \to \mathbb{Q}^\times$. Function composition is associative.

Definition 1.4: (Informal) Bracketing. *Let $\boxtimes$ be a bin operator on a set X. A **bracketing** of a seq $a_1, \ldots, a_n \in X$ is a way of inserting brackets into*

$a_1 \boxtimes \cdots \boxtimes a_n$ s/t the expression can be evaluated

Definition 1.5: Bracketing. *A **bracket** of $a_1, \ldots, a_n$ is*

$n = 1$: (word) a_1

$n > 1$: $(w_1 \boxtimes w_2)$ *where*

$w_1 \leftarrow$ (bracket) *of* $a_1, \ldots a_k$

$w_2 \leftarrow$ (bracket) *of* $a_{k+1}, \ldots, a_n$

```
data Bracket t = Number t | Branch (Bracket t) (Bracket t)
evalBracket :: (t -> t -> t) -> Bracket t -> t
evalBracket fn aseq =
  case aseq of
    Number x             -> x
    Branch left' right' -> fn (evalBracket fn left')
                              (evalBracket fn right')
```

Proposition 1.1. *a binary operation $\boxtimes$ on X is associative **iff** for every seq $a_1, \ldots, a_n$, $n \geq 1$, every bracketing of $a_1, \ldots a_n$ evaluates to the same elem of X.*

Proof. ($\Longleftarrow$) Take $n = 3$. Then

$$(a \boxtimes b) \boxtimes c = a \boxtimes (b \boxtimes c),\ \forall a, b, c \in X$$

($\Longrightarrow$) Proof by induction.
Base Case: $n = 1$. Every bracketing of a word evaluates to that same word.
Assume proposition is true for $n < k$, where $k > 1$. Let $a_1, \cdots, a_k \in X$. If w is a bracketing of $a_1, \ldots, a_k$ then $w = (w_1 \boxtimes w_2)$, where w_1 is a bracketing of $a_1, \ldots, a_l$ and w_2 is a bracketing of $a_{l+1}, \ldots, a_k$.

$$w_1 = (\cdots (a_1 \boxtimes a_2) \boxtimes \cdots) \boxtimes a_l$$

$$w_2 = (a_{l+1} \boxtimes (\cdots (a_{k-1} \boxtimes a_k) \cdots))$$

$$\begin{aligned} w &\overset{\text{in } X}{=} w_1 \boxtimes w_2 \\ &= (A \boxtimes a_l) \boxtimes w_2 \\ &= A \boxtimes (a_l \boxtimes w_2) \text{ by assoc.} \\ \cdots &= a_1 \boxtimes (\cdots (a_{k-1} \boxtimes a_k) \cdots) \end{aligned}$$

Hence any 2 bracketings of $a_1, \ldots, a_k$ evaluate to $a_1 \boxtimes (\cdots (a_{k-1} \boxtimes x_k) \cdots)$. By induction, the prop holds. □

Notation 1.1: Associativity makes Brackets Pointless. *Since $\boxtimes$ is associative, brackets become redundant.* $a \boxtimes b \boxtimes c := a \boxtimes (b \boxtimes c)$

Definition 1.6: Commutative. $(\boxtimes) : X \times X \to X$ *is* ***commutative*** *(or "abelian") if*

$$a \boxtimes b = b \boxtimes a, \forall a, b \in X$$

$+, \cdot$ on $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}$ are commutative.

$+$ on $M_{n \times m} \leftarrow$ (comm). (matrix mul) on $M_n \not\leftarrow$ (comm).

We're much more focused on associative operators as opposed to commutative.
We cover 2 Topics:

1. **Group Theory:** a single associative op w/ some additional properties
2. **Ring Theory:** 2 associative op that behave "like" $+$ & $\cdot$.

Definition 1.7: Identity. *An identity for a given bin op $\boxtimes$ is a element $e \in X$ s/t $e \boxtimes x = x \boxtimes e = x$, $\forall x \in X$.*

0 is an identity for $+$ on $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \cdots$. 1 is an identity for $\cdot$ on $\mathbb{Q}$

Lemma 1.1: Uniqueness of Identity. *If e and e' are identities for $\boxtimes$ on X, then $e = e'$.*

Proof. $e = e \boxtimes e' = e'$ □

Definition 1.8: Inverse. *let $\boxtimes$ be a bin op on X with iden e. Let $x \in X$. $y \in X$ is a*

1. ***left inverse*** *for X if $y \boxtimes x = e$,*
2. ***right inverse*** *for X if $x \boxtimes y = e$,*
3. *and an* ***inverse*** *for X if $x \boxtimes y = e = y \boxtimes x$.*

Lemma 1.2: Associtivity implies Uniqueness of Inverses. *Suppose we have $(\boxtimes) \leftarrow (\text{assoc})$. If y_L and y_R are left and right inverses of x, then $y_L = y_R$.*

Proof.

$$\begin{aligned}(y_L \boxtimes x) \boxtimes y_R &= e \boxtimes y_R \\ &= y_R \\ (y_L \boxtimes x) \boxtimes y_R &= y_L \boxtimes (x \boxtimes y_R) \quad (\text{by assoc}) \\ &= y_L \boxtimes e \\ &= y_L\end{aligned}$$

□

Consequences: x is invertable **iff** it has a left and right inverse.

Note: is is possible to be left invertable but not right invertable, and vice verse.

$\mathbb{N} = \{1, 2, \dots\}, +$ has no invertable elements.
$(\mathbb{Z}, +)$ has every element invertable.
$(\mathbb{Z}, \cdot)$ has only $\{\pm 1\}$ as invertable.
$(\mathbb{Q}, \cdot)$ has $\mathbb{Q}^\times$ as invertable.

Notation 1.2: Inverse. *if x is inivertable, and has a uni inv, then we denote it x^{-1}.*

Lemma 1.3: Properties of the Inverse. *Let* $(\boxtimes) \leftarrow$ (assoc) *w/ id* e.

1. e *is invertable,* $e^{-1} = e$.

   Proof. $e \boxtimes e = e$ □

2. *if* a *is invertable, then so is* a^{-1} *and* $(a^{-1})^{-1} = a$.

3. *if* a *and* $b \leftarrow$ (invertable) $\implies (a \boxtimes b)^{-1} = b^{-1} \boxtimes a^{-1}$

   Proof. $a \boxtimes b \boxtimes b^{-1} \boxtimes a^{-1} = a \boxtimes e \boxtimes a^{-1} = e$ Similiar in reverse. □

4. a *is invertable* ***iff***

$$a \boxtimes x = b$$
$$y \boxtimes a = b$$

   both have uniq sols $\forall b \in X$.

   Proof. ($\implies$) Assume a is invertable. Then

$$x = a^{-1} \boxtimes b$$
$$y = b \boxtimes a^{-1}$$

   ($\impliedby$) Assume the system has a uni X and Y, $\forall B \in X$. Let $b = e$, where e is the identity of $(X, \boxtimes)$.

$$\begin{aligned} a \boxtimes x &= e \\ y \boxtimes a &= e \\ \implies x &= a_R^{-1} \\ \implies y &= a_L^{-1} \\ (\boxtimes) \leftarrow (\text{assoc}) \implies a_R^{-1} &= a_L^{-1} = a^{-1} \\ \implies a &\text{ is invertable} \end{aligned}$$

   □