

Groups and Rings

Carter Aitken

2025-05-05

Abstract

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

Contents

1	Operations on Sets	3
1.1	K-Ary Operations	3
	<i>Definition:</i> Binary Operations	3
1.2	Associative Operations	4
	<i>Definition:</i> (Informal) Bracketing	4
	<i>Definition:</i> Bracketing	4
	<i>Notation:</i> Associativity makes Brackets Pointless	5
	<i>Definition:</i> Commutative	5
	<i>Definition:</i> Identity	6
	<i>Lemma:</i> Uniqueness of Identity	6
	<i>Definition:</i> Inverse	6
	<i>Lemma:</i> Associativity implies Uniqueness of Inverses	6
	<i>Notation:</i> Inverse	7
	<i>Lemma:</i> Properties of the Inverse	8
	<i>Lemma:</i> Cancellation Property	8
2	Groups	9
2.1	Definitions	9
	<i>Definition:</i> Group	9
	<i>Notation:</i> Multiplicative Notation	9
	<i>Definition:</i> Abelian Group	9
	<i>Definition:</i> Permutation Group	10
	<i>Definition:</i> Order	10
	<i>Notation:</i> General Linear Group	10

2.2	Dihedral Groups	11
	<i>Definition:</i> N-Gon	11
	<i>Definition:</i> An N-Gon Symmetry	11
	<i>Definition:</i> Dihedral Group	11
	<i>Lemma:</i> Dihedral GROUP	11
	<i>Definition:</i> Group Power	11
	<i>Definition:</i> Order of an Element	12
	<i>Lemma:</i> Properties of Order	12
	<i>Proposition:</i> Dihedral Group Explicit Classification	12

1 Operations on Sets

1.1 K-Ary Operations

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

In abstract algebra, we're interested 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 $b : X \times X \rightarrow X$.

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 $f : \underbrace{X \times \cdots \times X}_k \rightarrow X$.

$x \mapsto \frac{1}{x}$ 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. $- : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ isn't associative. Neither is $\div : \mathbb{Q}^\times \times \mathbb{Q}^\times \rightarrow \mathbb{Q}^\times$. Function composition is associative.

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

$$a_1 \boxtimes \dots \boxtimes a_n \text{ s/t the expression can be evaluated}$$

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

$$\begin{aligned} n = 1 &: (\text{word}) a_1 \\ n > 1 &: (w_1 \boxtimes w_2) \text{ where} \\ &w_1 \leftarrow (\text{bracket}) \text{ of } a_1, \dots, a_k \\ &w_2 \leftarrow (\text{bracket}) \text{ of } a_{k+1}, \dots, a_n \end{aligned}$$

```
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 $a_1, \dots, a_n, n \geq 1$, every bracketing of a_1, \dots, a_n evaluates to the same elem of X .

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

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

(\Rightarrow) 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 $a_1, \dots, a_k \in X$. If w is a bracketing of a_1, \dots, a_k then $w = (w_1 \boxtimes w_2)$, where w_1 is a bracketing of a_1, \dots, a_l and w_2 is a bracketing of a_{l+1}, \dots, a_k .

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

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

$$w \stackrel{\text{in } X}{=} w_1 \boxtimes w_2$$

$$= (A \boxtimes a_l) \boxtimes w_2$$

$$= A \boxtimes (a_l \boxtimes w_2) \text{ by assoc.}$$

$$\dots = a_1 \boxtimes (\dots (a_{k-1} \boxtimes a_k) \dots)$$

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

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. $(\boxtimes) : X \times X \rightarrow X$ 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 $M_{n \times m} \leftarrow (\text{comm})$. (matrix mul) on $M_n \not\leftarrow (\text{comm})$.

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 $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \dots$. 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: Associativity 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 invertible elements.

$(\mathbb{Z}, +)$ has every element invertible.

(\mathbb{Z}, \cdot) has only $\{\pm 1\}$ as invertible.

(\mathbb{Q}, \cdot) has \mathbb{Q}^\times as invertible.

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

Lemma 1.3: Properties of the Inverse. Let $(\boxtimes) \leftarrow (\text{assoc})$ 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 $b \leftarrow (\text{invertable}) \implies (a \boxtimes b)^{-1} = b^{-1} \boxtimes a^{-1}$

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) .

$$a \boxtimes x = e$$

$$y \boxtimes a = e$$

$$\implies x = a_R^{-1}$$

$$\implies y = a_L^{-1}$$

$$(\boxtimes) \leftarrow (\text{assoc}) \implies a_R^{-1} = a_L^{-1} = a^{-1}$$

$$\implies a \text{ is invertable}$$

□

Lemma 1.4: Cancellation Property. Let \boxtimes be an assoc bin op on X w/ id e .

If it has a left inverse and $a \boxtimes u = a \boxtimes v \implies u = v$. Vice Versa.

Proof. It should be taken as an axiom. □

2 Groups

2.1 Definitions

Definition 2.1: Group. a group is a pair (G, \boxtimes) where G is a set and \boxtimes is an assoc bin op on G , w/ and id e , s/t every elem of G is invertable.

Notation 2.1: Multiplicative Notation. if the op is clear, we'll usually just write G instead of (G, \boxtimes) .

We often use (\cdot) as the default symbol for the operation on a group, or even just writing $g \cdot h = gh$. The identity can be denoted by $e, e_G, 1, 1_G$. We use a^{-1} for the inverse of a . This is called **multiplicative notation**.

Definition 2.2: Abelian Group. A group (G, \boxtimes) is **abelian** if \boxtimes is abelian (commutative).

For abelian groups, we often use additive notation.

$(+)$, $\text{id} \leftarrow 0$ or 0_G , $\text{inv}(a) = a$.

1. \mathbb{Z}^+ is an abelian group (under $+$).

$$(+) \leftarrow (\text{assoc}), \text{inv}(a) = -a, \text{id}(+) = 0, + \leftarrow (\text{bin op})$$

Note that this is true for $\mathbb{Q}^+ = (\mathbb{Q}, +)$, \mathbb{R}^+ .

2. \mathbb{Z} isn't a group; every element in \mathbb{Z} isn't invertable under (\cdot)
3. We know that $|\mathbb{Z}| = |\mathbb{Q}|$. Let $\phi \leftarrow (\text{bij}) : \mathbb{Z} \rightarrow \mathbb{Q}$. Define an operator on \mathbb{Z} by $a \boxtimes b = \phi^{-1}(\phi(a) + \phi(b))$. (\mathbb{Z}, \boxtimes) is an (abelian) group. (**Ex:** $1 \boxtimes 2 = 8$)

Lemma 2.1. Let $\boxtimes \leftarrow (\text{assoc, bin op on } M, \text{id} \leftarrow e)$, $G := \{g \in M : g \leftarrow (\text{invertable wrt } \boxtimes)\}$. Then G is a group w/ $g \cdot h := g \boxtimes h$.

Proof. Hmk. □

The smallest possible group is called the trivial group, and it has one element, $\{e\}$, $ee = e$.

1. invertability
2. identity
3. closure of (\boxtimes)
4. assoc of (\boxtimes) .

$$\mathbb{Q}^\times = \{a \in \mathbb{Q} : a \neq 0\}$$

$$\mathbb{R}^\times = \{a \in \mathbb{R} : a \neq 0\}$$

Both are groups under multiplication (bad notation considering \mathbb{R}^+ is a group but \mathbb{Q}^\times is a set. I assume \mathbb{Q}^\times is a group, equal to $(\mathbb{Q}^\times, (\cdot))$).

Corollary 2.1. *Let X be a set, and let S_X be the set of functions $\{f : X \rightarrow X : f \leftarrow (\text{invertable})\} = \{f \in \text{Fun}(X, X) : f \leftarrow (\text{inv})\}$. Then S_X is a group under function composition.*

Definition 2.3: Permutation Group. $X := \{1, \dots, n\}$. S_X is called the permutation group of rank n , and is denoted S_n .

$$\Sigma := \{\sigma \in \text{Fun}(X, X) : \sigma \leftarrow (\text{bij})\}$$

$$S_X := (\Sigma, \circ)$$

Definition 2.4: Order. *The order of a group $G = (E, \boxtimes)$ is $|G| = |E|$, where E is finite. If E is infinite, we'll say $|G| = +\infty$.*

$$|S_n| = |(\Sigma, \circ)| = n!$$

$$(M, \boxtimes) \leftarrow (\text{monoid}) \implies (M|_{(\text{inv})}, \boxtimes) \leftarrow (\text{group})$$

Example of above. $M_n\mathbb{F} := M_{n \times n}(\mathbb{F})$.
 $(M_n\mathbb{F}, \cdot) \leftarrow (\text{monoid})$, so $(M_n\mathbb{F}|_{(\text{inv})}, \cdot) \leftarrow (\text{group})$

Notation 2.2: General Linear Group. $(M_n\mathbb{F}|_{(\text{int})}, \cdot)$ is called the **general linear group** (over \mathbb{F}), denoted

$$\text{GL}_n\mathbb{F}$$

2.2 Dihedral Groups

Definition 2.5: N-Gon. Let $\mathbb{P}_n : n \geq 3$ denote the regular n -gon, with vertices

$$v_k = \left(\cos \frac{2\pi k}{n}, \sin \frac{2\pi k}{n} \right) : 0 \leq k \leq n \text{ noting } v_n = v_0$$

Definition 2.6: An N-Gon Symmetry. A *symmetry of the n -gon* is an elem $T \in \text{GL}_2\mathbb{R}$ s/t $T(\mathbb{P}_n) = \mathbb{P}_n$

Definition 2.7: Dihedral Group. The set of symmetries of \mathbb{P}_n is called the *dihedral group of rank n* , denoted D_{2n} .

Lemma 2.2: Dihedral GROUP. D_{2n} is a group under matrix multiplication.

Proof. Later, in section subgroups. □

What are the elems of D_{2n} ? $\text{Id}(D_{2n}) = I_2$.

Rotation s by $\frac{2\pi}{n}$ radians are elems, and $s(v_i) = v_{i+1}$, $\forall i = 0, \dots, n-1$.

Reflection along the x axis is an elem, so $r(v_i) = v_{n-i}$.

Definition 2.8: Group Power.

$$g^n := \underbrace{g \cdot g \cdots g}_n, \quad n \geq 0.$$

$$g^{-n} := \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_n$$

$$g^0 := e = \text{Id}(G).$$

Note. $g^{-n} = (g^{-1})^n$ and $g^{-n}g^n = e$ Prove the following:

$$g^n g^m = g^{n+m}$$

$$(g^n)^m = g^{nm}$$

All this also has additive notation. $ng = g + \cdots + g$ and $(-n)g = \underbrace{(-g) + \cdots + (-g)}_n$

Note.

$$(gh)^n \neq g^n h^n$$

Definition 2.9: Order of an Element. The **order** $g \in G$ is denoted

$$|g| := \min(\{k \geq 1 : g^k = e\} \cup \{+\infty\})$$

Example: $|e| = 1, |g| = 1 \iff g = e.$ $\mathbb{Z}^+, |1| = +\infty.$ $(\mathbb{Z}/n\mathbb{Z}, +) \quad |[1]| = n \text{ b/c } n \cdot [1] = 0$

Lemma 2.3: Properties of Order. 1. $g^n = e \implies g^{n-1} \cdot g = e \implies g^{n-1} = g^{-1}$

$$2. \quad g^n = e \iff (g^n)^{-1} = e \\ \implies |g^{-1}| = |g|$$

Example

$$-[1] = (n-1)[1] = [n-1]$$

Back to dihedral groups.

$$D_{2n}, |s| = n \equiv s^n(\mathbb{P}_n) = \mathbb{P}_n. \quad |r| = 2 \equiv r^2(\mathbb{P}_n) = \mathbb{P}_n.$$

So $e, s, s^2, \dots, s^{n-1} \in D_{2n}$, and $r, sr, s^2r, \dots, s^{n-1}r \in D_{2n}$.

Proposition 2.1: Dihedral Group Explicit Classification. $D_{2n} = \{s^i : 0 \leq i < n\} \cup \{s^i r : 0 \leq i < n\}$ and $|D_{2n}| = 2n$

Proof. $S, T \in D_{2n}$. So S, T are linear operations. So if

$$S(v_0) = T(v_0)$$

$$S(v_1) = T(v_1)$$

$$\implies S = T$$

following if we treat v_0, v_1 as basic vectors.

Claim 2: $T \in D_{2n} \implies$

$$(T(v_0), T(v_1)) \in \{(v_i, v_{i+1}) : 0 \leq i \leq n-1\} \cup \{(v_{i+1}, v_i) : 0 \leq i \leq n-1\} =: V$$

Proof. v_0, v_1 have to be sent to adj vertices (by picture lol, although we could use a "convexity" argument).

$$(s^i(v_0), s^i(v_1)) = (v_i, v_{i+1}) \quad (r(v_0), r(v_1)) = (v_0, v_{n-1})$$

$$(s^i r(v_0), s^i r(v_1)) = (s^i(v_0), s^i(v_{n-1})) \quad (v_i, v_{i-1})$$

□

Claim 3: $\phi : D_{2n} \rightarrow V : \phi(T) = (T(v_0), T(v_1))$ is a bijection. By claim 1, it's a injection, and by the calculation above, it's a surjection. Finally, $2n = |V|$ and $D_{2n} = |V| \implies 2n = |D_{2n}|$.

So $\{s^i : 0 \leq i \leq n-1\} \cup \{s^i r : 0 \leq i \leq n-1\} = D_{2n}$.

Also $rs(v_0) = r(v_1) = v_{n-1}$, $rs(v_1) = v_{n-2}$ so $rs = s^{n-1}r = s^{-1}r$.

□