Groups

Carmen M. Wright, Ph.D.

Jackson State University

Spring 2017

Definition of a group

We say that $\langle G, *\rangle$ is a **group** if the following conditions are satisfied:

- Closure: $\forall x, y \in G$, $x * y \in G$.
- Associativity: $\forall x, y, z \in G$, $x * (y * z) = (x * y) * z$.
- Identity (unique): $\exists e \in G$ $\forall x \in G$, $x * e = x = e * x$.
- Inverses (for each element): $\forall x \in G$ $\exists y \in G$ s.t. $x * y = e = y * x$

Note: The two most common operations are “multiplication” and “addition”. General statements about groups are always phrased in multiplicative notation.

Shorthand

For convenience we drop the $*$:
CAIIn

- C: $gh \in G$
- A: $(gh)k = g(hk)$
- I: $ge = g = eg$
- In: $gg' = e = g'g$

	multiplicative notation	additive notation
operation	gh	$g + h$
inverse	g^{-1}	$-g$
most common identity	“1”	“0”

Examples

(a) $\langle \mathbb{R}, + \rangle$ is a group.

(b) $(\mathbb{R}, \cdot)$ is *not* a group, but

(c) $\langle \mathbb{R}^\times, \cdot \rangle$ *is* a group.

(d) General linear group (matrix mult.) is a group:
$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$

(e) Special linear group (matrix mult.) is a group:
$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\}$

Exercises: More examples on *Operations Worksheet*

Function example 1

Set of real-valued functions having as domain the set $\mathbb{R}$ of all real numbers:

$$\mathcal{F}(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R}\}$$

Suppose we have $(\mathcal{F}(\mathbb{R}), +)$. For $f, g \in \mathcal{F}(\mathbb{R})$, we define $f + g$ by how it acts on elements of the domain:

$$(f + g)(x) := f(x) + g(x)$$

- Closure: Let $f, g \in \mathcal{F}(\mathbb{R})$. Let $x \in \mathbb{R}$ be in the domain. Then $(f+g)(x) = \underbrace{f(x)}_{\in\mathbb{R}} + \underbrace{g(x)}_{\in\mathbb{R}} \in \mathbb{R}$
- Associativity: Let $f, g, h \in \mathcal{F}(\mathbb{R})$. Is $(f+g)+h = f+(g+h)$?

$$\begin{aligned}
[(f+g)+h](x) &= (f+g)(x) + h(x) \\
&= f(x) + g(x) + h(x) \\
&= f(x) + (g+h)(x) \\
&= [f+(g+h)](x)
\end{aligned}$$

- Identity: The zero function, $\mathcal{O}(x) = 0$, $f + \wr = f = \wr + f$:

$$(f + \mathcal{O})(x) = f(x) + \underbrace{\mathcal{O}(x)}_{=0} = f(x) = \underbrace{\mathcal{O}(x)}_{=0} + f(x) = (\mathcal{O} + f)(x)$$

- Inverses: Let $f \in \mathcal{F}(\mathbb{R})$. Then $-f$ is its inverse, defined as $(-f)(x) := -f(x)$.

$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) + (-f(x)) = 0 = \mathcal{O}(x)$$

$$((-f) + f)(x) = (-f)(x) + f(x) = (-f(x)) + f(x) = 0 = \mathcal{O}(x)$$

$$\Longrightarrow f + (-f) = \mathcal{O} = (-f) + f$$

Function example 2

$\mathcal{F}(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R}\}$, now with function composition:

$$(f \circ g)(x) := f(g(x))$$

- Closure: $\mathbb{R}$ is domain for all functions, nothing undefined, so $f \circ g : \mathbb{R} \to \mathbb{R}$
- Associativity: $(f \circ g) \circ h = f \circ (g \circ h)$

$$[(f \circ g) \circ h](x) = (f \circ g)(h(x)) = f(g(h(x)))$$

$$[f \circ (g \circ h)](x) = f((g \circ h)(x)) = f(g(h(x)))$$

- Identity: $id(x) = x \quad \Rightarrow \quad f \circ id = f = id \circ f$
- Inverses: no, only bijective functions are invertible

Commutativity

Let A be a set with operation $*$. Then $*$ is *commutative* on A if

$$\forall a, b \in A, \quad a * b = b * a.$$

Abelian group

We say that a group is an **abelian** group if its operation is commutative.

Abelian group examples

- $\langle \mathbb{R}, + \rangle$
- $\langle \mathbb{R}^*, \cdot \rangle$
- $\mathbb{Z}_n$ (add.)
- $U(n)$ (mult.)

Non-abelian group examples

- most groups involving matrix multiplication (e.g. $GL_2(\mathbb{R})$, $SL_2(\mathbb{R})$)
- most groups involving function composition: $f \circ g \neq g \circ f$

Subgroups

Simply put: Let G be a group.
H is a subset of G & H is a group → H is a subgroup

Subgroups

Let G be a group and H a subset of G. Then H is said to be a subgroup if the following conditions hold:

- H contains the identity of G, i.e. $e_G \in H$
- If $a, b \in H$, then $ab \in H$.
- If $a \in H$, then $a^{-1} \in H$.

*Associativity is inherited from G, no need to prove it

Notation: $H \leq G$

Subgroups: Examples

- $\mathbb{Z} \leq \mathbb{R}$ as add. groups: $\langle \mathbb{Z}, + \rangle \leq \langle \mathbb{R}, + \rangle$
- $\mathbb{Q}^* \leq \mathbb{R}^*$ as mult. groups: $\langle \mathbb{Q}^*, \cdot \rangle \leq \langle \mathbb{R}^*, \cdot \rangle$
- $SL_2(\mathbb{R}) \leq GL_2(\mathbb{R})$ under matrix mult.

Uniqueness

- The identity of a group is unique.
- Inverse elements are unique. An element has one and only one inverse. In some cases its inverse is itself.

Cancellation law

Theorem

Theorem 1: If G is a group and a, b, c are elements of G, then

- $ab = ac$ *implies* $b = c$, *and*
- $ba = ca$ *implies* $b = c$.

Note that $ab = ca$ does *not* imply $b = c$. Why not?

Inverses

Theorem

Theorem 2: If G is a group and a, b are elements of G, then

$$ab = e \text{ implies } a = b^{-1} \text{ and } b = a^{-1}.$$

Computing inverses

Theorem

Theorem 3: If G is a group and a, b are elements of G, then

- $(ab)^{-1} = b^{-1}a^{-1}$ *and*
- $(a^{-1})^{-1} = a.$

Associative law

Parentheses are redundant:

$$a(bc)d = ab(cd) = (ab)(cd) = (ab)cd = abcd$$

Combined with inverse property:

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}$$

Exponential notation, $n \in \mathbb{Z}^+$:

$$a^n = \underbrace{aa \cdots a}_{n \ \text{factors}}$$

$$a^{-n} = (a^{-1})^n = (a^n)^{-1}$$

Exponent laws

$g, h \in G,\ n, m \in \mathbb{Z},$

1. $g^n g^m = g^{n+m}$
2. $(g^n)^m = g^{nm}$
3. If $gh = hg$, then $(gh)^n = g^n h^n$.

Summary of some properties: For any $g \in G$,

1. $e^{-1} = e$
2. $(g^{-1})^{-1} = g$
3. $(gh)^{-1} = h^{-1}g^{-1}$
4. $(g^n)^{-1} = (g^{-1})^n$ for all $n \geq 0$

Note: $g^{-k} = (g^{-1})^k = (g^k)^{-1}$ for $k \geq 1$

Order of a group: If G is a finite group, the number of elements in G is called the *order* of G, commonly denoted as

$$|G|$$