Basic properties of groups

Identities & inverses

Prop ① Every group has a unique identity element.

Prop ② Every element in a group has a unique inverse element.

Hint: Associativity is needed.

Prop ③ For any elements $a, b \in G$, the inverse of ab is given by $(ab)^{-1} = b^{-1}a^{-1}$.

(Proof.) Because inverses are unique, we just need to show that $b^{-1}a^{-1}$ satisfies the inverse property for ab.

Indeed:

$$(b^{-1}a^{-1}) \circ (ab) = b^{-1}(a^{-1}a)b = b^{-1}(eb)$$
$$= b^{-1}b = e$$

& $$(ab) \circ (b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1}$$
$$= aa^{-1} = e.$$

∎

Prop ④ Every element of a group is the inverse element of its inverse element: $(a^{-1})^{-1} = a$.

(Proof.) By def'n, $a^{-1}(a^{-1})^{-1} = e$. Left multiplication by a yields $(aa^{-1})(a^{-1})^{-1} = ae$

$$\rightarrow (a^{-1})^{-1} = a.$$

∎

Cancellation

Prop 5 For any fixed $a, b \in G$, there are unique elements $x, y \in G$ such that

$$ax = b \quad \& \quad ya = b.$$

Rmk. This is a proposition about the invertibility of a.

Think of solving $A\vec{x} = \vec{b}$ for $\vec{x}$.

Need both equations b/c we want to post-compose a ($ax = b$) or pre-compose a ($ya = b$).

(Proof.) We'll prove existence & uniquness for sol'ns to $ya = b$.

$ax = b$ is an exercise.

Existence: Let $y = ba^{-1}$.

Then $ya = (ba^{-1})a = b(a^{-1}a)$

$= be = b$ ✓

"suppose"

Uniqueness: $\S$ y_1 & y_2 satisfy $y_1 a = b$ and $y_2 a = b$.

Then $y_1 a = y_2 a$. Right-multiply by a^{-1}:

$$(y_1 a)a^{-1} = (y_2 a)a^{-1} \rightarrow \cdots$$

$$\rightarrow y_1 = y_2.$$

∎

Prop 6 (left cancellation) $\forall\, a, b, c \in G$,

$$ab = ac \implies b = c.$$

Prop 7 (right cancellation) $\forall\, a,b,c \in G$,

$$ba = ca \implies b = c.$$

Notation

For any $a \in G$ and integer $n \geq 1$,

$$a^n := \underbrace{a \circ a \circ \cdots \circ a}_{n \text{ times}}.$$

$$a^0 := e$$

$$a^{-n} := \underbrace{a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}}_{n \text{ times}}$$

Prop 8 $\forall\, a,b \in G$ and any $m,n \in \mathbb{Z}$,

1. $a^m a^n = a^{m+n}$;
2. $(a^m)^n = a^{mn}$;
3. $(ab)^n = (b^{-1}a^{-1})^{-n}$, with $(ab)^n = a^n b^n$ if G is abelian.

Rmk We'll use multiplicative notation for $(\mathbb{Z},+)$ & $(\mathbb{Z}_n,+)$: $\underbrace{a+a+\cdots+a}_{n \text{ times}} = na$

Subgroups

Recall:

$$SO(n) = \{A \in M_n(\mathbb{R}) \mid A^T A = I \text{ ; } \det A = 1\}$$

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}.$$

Notice: $SO(n) \subsetneq GL_n(\mathbb{R})$ and they use the same group operation.

We think of $SO(n)$ as a restricted set of symm.

$GL_n(\mathbb{R})$ preserves v.s. structure of $\mathbb{R}^n$

$SO(n)$ preserves v.s. structure AND oriented Euclidean geometry.

Def. A subgroup of a group $(G, \circ_G)$ is a group $(H, \circ_H)$ s.t. H is a subset of G and $\circ_H$ is the restriction of $\circ_G$. I.e.,

$$a \circ_H b = a \circ_G b, \ \forall \ a, b \in H.$$

Examples

① Two more subgroups of $GL_n(\mathbb{R})$:

$$SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A = 1\}$$

$$O(n) = \{A \in M_n(\mathbb{R}) \mid A^T A = I\}$$

Both preserve v.s. structure, since they're in $GL_n(\mathbb{R})$.

$SL_n(\mathbb{R})$ preserves signed Euclidean volumes of top-dim'l subsets

$O(n)$ preserves inner products $\langle A\vec{v}, A\vec{w}\rangle = \langle \vec{v}, \vec{w}\rangle$.

Notice: $SL_n(\mathbb{R}) \cap O(n) = SO(n)$ is also a subgroup.

2. Recall: $(M_n(\mathbb{R}), \times)$ is <u>not</u> a group.
But $(M_n(\mathbb{R}), +)$ <u>is</u> a group.

<u>Q</u>: Is $GL_n(\mathbb{R}) \subsetneq M_n(\mathbb{R})$ a subgroup?

No. $\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \notin GL_n(\mathbb{R})$.

Also, $\exists\, A, B$ with $\det A, \det B \neq 0$ and $\det(A+B) = 0$.

So $+$ is not <u>closed</u> on $GL_n(\mathbb{R})$.