Groups

A *group* $\langle G, * \rangle$ is a set G closed under a binary operation $*$ such that

1.) $(a*b)*c = a*(b*c) \quad \forall\, a,b,c \in G$ (associativity)

2.) $\exists$ an element $e \in G$ s.t. $\forall\, x \in G$

$$e * x = x * e = x$$

(e is called the *identity element*)

3.) $\forall\, a \in G\ \exists\, a^{-1} \in G$ s.t. $a * a^{-1} = a^{-1} * a = e$.

(a^{-1} is called an *inverse* of a)

Ex: $\langle \mathbb{Z}, + \rangle$ is a group: $(a+b)+c = a+(b+c)$, so it's associative.

$0 + a = a + 0 = a\ \forall\, a \in \mathbb{Z}$, and $a + (-a) = (-a) + a = 0\ \forall\, a \in \mathbb{Z}$.

However, $\langle \mathbb{Z}_+, + \rangle$ is not a group. $*$ is associative, but $e + a > a\ \forall\, e, a \in \mathbb{Z}_+$. i.e. there is no identity element.

Ex: $\langle \mathbb{Q} - \{0\}, \cdot \rangle$ is a group (1 is the identity).

$\langle \mathbb{Z} - \{0\}, \cdot \rangle$ is not a group: it has 1 as an identity, but there is no $a \in \mathbb{Z} - \{0\}$ s.t. $2 \cdot a = 1$.

Ex: $\langle \{f : \mathbb{R} \to \mathbb{R}\}, + \rangle$ is a group w/ identity $f(x) = 0$.

However, this is not a group w/ operations $\cdot$ or $\circ$ (HW problem)

EX: Let $n \in \mathbb{Z}_+$. Define $\mathbb{Z}_n = \langle \{0, 1, \dots, n-1\}, + \rangle$, where $+$ is addition "modulo" n, i.e. $a + b =$ the remainder of $a+b \in \mathbb{Z}$ when dividing by n.

So $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ and the $+$ table is

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Def: If $\langle G, * \rangle$ is a group, then G is <u>abelian</u> if $*$ is commutative.

Basic Properties of groups

Theorem: If $\langle G, * \rangle$ is a group and $a, b, c \in G$, then

if $a * b = a * c$ then $b = c$, and if $b * a = c * a$ then $b = c$.

Proof: Assume $a * b = a * c$. Then $\exists\, a^{-1} \in G$ s.t. $a^{-1} * a = e$.

Thus $a^{-1} * (a * b) = a^{-1} * (a * c)$

$\Rightarrow (a^{-1} * a) * b = (a^{-1} * a) * c$

$\Rightarrow e * b = e * c \Rightarrow b = c$.

Similarly, by a symmetric argument, from $b * a = c * a$ we can deduce $b = c$. $\square$

Theorem: If $\langle G, * \rangle$ is a group and $a, b \in G$, then $\exists$ a unique $x \in G$ s.t. $a * x = b$, and a unique $y \in G$ s.t. $y * a = b$.

Proof: Let $a, b \in G$. Let $a^{-1} \in G$ s.t. $a^{-1} * a = a * a^{-1} = e$.

Define $x = a^{-1} * b$. Then
$$\begin{aligned} a * x &= a * (a^{-1} * b) \\ &= (a * a^{-1}) * b \\ &= e * b = b. \end{aligned}$$

Thus, such an element exists. Now we show it's unique.

Suppose $a * c = b$. Then $a * c = a * x \Rightarrow c = x$, so x is unique.

A similar argument shows that the second part of the statement holds. $\square$

Cor: If e is an identity of $\langle G, * \rangle$, then e is the unique identity.

Pf: $\exists$ unique x, y s.t. $a * x = a$ and $y * a = a$, so $x = e = y$. $\square$

Cor: If $x \in G$, then x has a unique inverse x^{-1}, and if $x * c = e$ or $c * x = e$, then $c = x^{-1}$.

Cor: $(a * b)^{-1} = b^{-1} * a^{-1}$

Pf:
$$\begin{aligned} (a * b) * (b^{-1} * a^{-1}) &= ((a * b) * b^{-1}) * a^{-1} \\ &= (a * (b * b^{-1})) * a^{-1} \\ &= (a * e) * a^{-1} \\ &= a * a^{-1} = e. \end{aligned}$$

Thus, since inverses are unique, $(a * b)^{-1} = (b^{-1} * a^{-1})$

Ex: Let $G = \{e, a, b\}$. What are the possible groups w/ G as the underlying set?

e is the unique identity, so we need to find

$a*a$, $a*b$, $b*a$, and $b*b$.

If $a*b=a$, then $b=e$, which isn't the case.
similarly, $a*b \neq b$, and $b*a \neq a$ or b. Thus $a*b=e$, $b*a=e$.

$a^2 = a*a \neq a$ (since $a \neq e$) and $a^2 \neq e$ (since $a \neq b = a^{-1}$)
Thus $a^2 = b$, and, similarly $b^2 = a$, so the table becomes

$$\begin{array}{c|ccc} & e & a & b \\ \hline e & e & a & b \\ a & a & b & e \\ b & b & e & a \end{array}$$

can
Check that this is in fact a group (relabel $e=0$, $a=1$, $b=2$, and this becomes $\mathbb{Z}_3$). In fact, this is the only group w/ 3 elements "up to isomorphism" (we will see what this means later).

Def: The order of a group G, $|G|$, is the cardinality of G.
If $a \in G$, then the order of a, $|a|$, is the smallest $n \in \mathbb{Z}_+$ s.t. $a^n = e$. If $a^n \neq e$ $\forall n$, then $|a| = \infty$.

Example: • $e^1 = e$, so $|e| = 1$.

• In $\mathbb{Z}_3$, $|0| = 1$,
$1+1+1=0$, so $|1|=3$, and $2+2=1$, $1+2=0$, so $|2|=3$.

- In $\langle \mathbb{Z}, + \rangle$, $\forall\ n \in \mathbb{Z}$ s.t. $n \neq 0$, $|n| = \infty$.