From last time:

A <u>group</u> is a pair $(G, *)$, where G is a set and $*$ is a binary operation on G, satisfying:

1) $*$ is associative,

(identity element)

2) $\exists e \in G$ s.t. $\forall g \in G$, $e * g = g * e = g$, and

(existence of identity)

(inverse of g)

3) $\forall g \in G$, $\exists h \in g$ s.t. $g * h = h * g = e$.

(existence of inverses)

Examples:

$(\mathbb{Z}, +)$ $(\mathbb{Q}, +)$ $(\mathbb{R}, +)$ $(\mathbb{C}, +)$ $(M_{m,n}(\mathbb{R}), +)$

(groups with "additive" operations)

$(\mathbb{Q} \setminus \{0\}, \cdot)$ $(\mathbb{R} \setminus \{0\}, \cdot)$ $(\mathbb{C} \setminus \{0\}, \cdot)$ $(GL_2(\mathbb{R}), \cdot)$

(groups with "multiplicative" operations)

$(\mathcal{P}(S), \Delta)$

(maybe "multiplicative"?)

Notational conventions:

$(G, *) \longleftrightarrow G$

<u>finite group</u> : $|G| < \infty$ — order of G

group G	additive notation	multiplicative notation
$g * h$	$g + h$	gh
identity e	0	1
inverse of g	$-g$	g^{-1}
$\underbrace{g * g * \cdots * g}_{n\text{-times}}$ $(n \in \mathbb{N})$	$ng = \underbrace{g + g + \cdots + g}_{n\text{-times}}$	$g^n = \underbrace{g \cdot g \cdot \cdots \cdot g}_{n\text{-times}}$
	$0g = 0$	$g^0 = 1$
	$-ng = \underbrace{(-g) + \cdots + (-g)}_{n\text{-times}}$	$g^{-n} = \underbrace{(g^{-1}) \cdot \cdots \cdot (g^{-1})}_{n\text{-times}}$

Basic properties that all groups satisfy

Let G be a group (written multiplicatively).

1) Uniqueness of identity:

If $e, \tilde{e} \in G$ are identity elements, then $e = \tilde{e}$.

Pf: Suppose e and $\tilde{e}$ are identity elements.

Then
$$\begin{aligned} e &= e\tilde{e} && (\tilde{e} \text{ is an identity}) \\ &= \tilde{e} && (e \text{ is an identity}) \quad \blacksquare \end{aligned}$$

2) Uniqueness of inverses:

Suppose $g \in G$. If $h, \tilde{h} \in G$ are inverses of g then $h = \tilde{h}$.

Pf: Suppose h and $\tilde{h}$ are inverses of g.

Then
$$\begin{aligned} h &= eh && (\text{existence of identity}) \\ &= (\tilde{h} g) h && (\tilde{h} \text{ is an inverse of } g) \\ &= \tilde{h}(gh) && (\text{associativity}) \\ &= \tilde{h} e && (h \text{ is an inverse of } g) \\ &= \tilde{h} && (\text{def. of } e) \quad \blacksquare \end{aligned}$$

3) Cancellation laws

If $g, h, a \in G$ satisfy $ag = ah$, or if they satisfy $ga = ha$, then $g = h$.

Pf:

If $ag = ah$ then	If $ga = ha$ then
$a^{-1}(ag) = a^{-1}(ah)$	$(ga)a^{-1} = (ha)a^{-1}$
$\Rightarrow (a^{-1}a)g = (a^{-1}a)h$	$\Rightarrow g(aa^{-1}) = h(aa^{-1})$
$\Rightarrow eg = eh$	$\Rightarrow ge = he$
$\Rightarrow g = h$.	$\Rightarrow g = h$. $\blacksquare$

4) Generalized associativity

$\forall n \in \mathbb{N}$ and $\forall g_1, \dots, g_n \in G$, the value of $g_1 g_2 \cdots g_n$ does not depend on the choice of where to put parenthesis.

(ex: $n=4$, $(g_1g_2)(g_3g_4) = g_1(g_2(g_3g_4)) = (g_1(g_2g_3))g_4 = \cdots$)

Pf: ... (tricky) induction on n... $\blacksquare$

5) If $g, h \in G$ and $gh = e$ then $h = g^{-1}$.

Pf: Only need to check that $hg = e$.

We have that

$$
\begin{aligned}
hg &= e(hg) && \text{(existence of identity)} \\
&= (g^{-1}g)(hg) && \text{(existence of inverses)} \\
&= (g^{-1}(gh))g && \text{(gen. assoc.)} \\
&= (g^{-1}e)g && (gh=e \text{, by assumption}) \\
&= g^{-1}g && \text{(def. of } e) \\
&= e && \text{(def. of } g^{-1})
\end{aligned}
$$

Since $gh = hg = e$, we conclude that $h = g^{-1}$. $\blacksquare$

6) $\forall g \in G$, $(g^{-1})^{-1} = g$.

Pf: By the definition of g^{-1},

$$g(g^{-1}) = (g^{-1})g = e.$$

This implies that $(g^{-1})^{-1} = g$. $\blacksquare$

7) $\forall g,h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.

Pf: Observe that

$$\begin{aligned}(gh)(h^{-1}g^{-1}) &= g(hh^{-1})g^{-1} \quad \text{(gen. assoc.)}\\ &= geg^{-1}\\ &= gg^{-1}\\ &= e.\end{aligned}$$

By property 5, $(gh)^{-1} = h^{-1}g^{-1}$. $\blacksquare$

Note: If G is non-Abelian then it is <u>not true</u> that $\forall g,h \in G$, $(gh)^{-1} = g^{-1}h^{-1}$.

Ex: $G = GL_2(\mathbb{R})$, $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$.

Then: $AB = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}$, $(AB)^{-1} = \begin{pmatrix} \frac{1}{2} & -1 \\ 0 & 1 \end{pmatrix}$

$A^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$, $B^{-1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 1 \end{pmatrix}$, and

$B^{-1}A^{-1} = \begin{pmatrix} \frac{1}{2} & -1 \\ 0 & 1 \end{pmatrix} = (AB)^{-1}$, but

$A^{-1}B^{-1} = \begin{pmatrix} \frac{1}{2} & -2 \\ 0 & 1 \end{pmatrix} \neq (AB)^{-1}$.