**Thm.** Let $G$ be a group and $a \in G$. Then $a$ has a unique inverse, i.e. there is only one element $b \in G$ s.t. $ab = ba = e$.

proof: Sps $b_1$ and $b_2$ are both inverses of $a$. (NTS: $b_1 = b_2$.)

Since both are inverses, $ab_1 = ab_2$.

Mult by sides on left by $b_1$ gives $\underbrace{b_1 a}_{e} b_1 = \underbrace{b_1 a}_{e} b_2$

which implies $b_1 = b_2$. ✓

* Since $a$ has only one inverse, we can unambiguously denote it $a^{-1}$.

**Thm** (Socks-Shoes) Sps $a, b$ elts of a group $G$.

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

proof: Multiply $ab$ by $b^{-1} a^{-1}$:

$$(b^{-1} a^{-1})(ab) = b^{-1} \underbrace{a^{-1} a}_{e} b$$
$$= b^{-1} b$$
$$= e.$$

So yes: $(ab)^{-1} = b^{-1} a^{-1}$.

To check if $x$ is an inverse of $g$ in group, check: does $xg = e$? If so: yes, $x = g^{-1}$

**Notation:** Sps $a \in G$.

- $\underbrace{aaa \cdots a}_{\text{a mult by itself n times}} = a^n$ $\quad n \in \mathbb{Z}, n > 0$.

- $a^0 = e$ (convention)

we don't write $\frac{1}{a}$

- Sps $n \in \mathbb{Z}, n < 0$. Then $a^n$ means $(a^{-1})^{|n|}$

e.g. $a^{-2} = (a^{-1})^2 = a^{-1}a^{-1}$.

With this, we can regroup:

$$g^{np} = (g^n)^p = (g^p)^n$$

But CAREFUL: In general, $(gh)^n \neq g^n h^n$

$\underbrace{ghgh \cdots gh}_{n \text{ times}}$ $\quad \underbrace{gg \cdots g}_{n \text{ times}}\underbrace{hh \cdots h}_{n \text{ times}}$

(unless: $gh = hg$)

Finally, if $G$ is an additive group (e.g. $\mathbb{Z}$ or $\mathbb{Z}_n$),

we often write $ab$ as $a+b$ and

$c^{-1}$ as $-c$ because it's more natural.

e.g. $ab^2a^{-1}c$ would be written $a+\underbrace{2b}_{b+b}-a+c$.