- associative
- identity element exists
- every elt has an inverse

Basic Theorems about Groups

There is only one identity element

Can a group G have more than one identity element? The axioms say that there is an element e so that $eg = ge = g$ for all $g \in G$. Could there be two elements e_1 and e_2, both of which act like identity elements?

Proposition: Let G be a group. Then G has exactly one identity element.

Our strategy: we will suppose there are two elements that act like the identity. We will prove they are equal.

Proof: Step by step:

- Suppose that e_1 and e_2 both have the property that $e_i g = g e_i = g$ for all $g \in G$ and $i = 1, 2$.

  $e_1 g = g e_1 = g$ for all g

  $e_2 g = g e_2 = g$ for all g
- Since $ge_1 = g$ for all g, (let $g = e_2$) we have $e_2 e_1 = e_2$.
- Since $e_2 g = g$ for all g, ($g = e_1$) we have $e_2 e_1 = e_1$.
- Therefore $e_1 = e_2$.

Each element has exactly one inverse.

The axioms say that, for every $g \in G$, there is an $h \in G$ so that $hg = gh = e$ where e is the identity element. Could there be two elements h_1 and h_2 so that $h_1g = gh_1 = h_2g = gh_2 = e$?

Proposition: Let G be a group and $g \in G$ be an element. Then there is exactly one inverse element h such that $hg = gh = e$.

$g \in G$

g^{-1}

Our strategy, as before, will be to assume there are two elements that act like this, and prove they are equal.

Proof: Step by step:

- Suppose that $g \in G$ and h_1 and h_2 have the properties $h_1g = gh_1 = e$ and $h_2g = gh_2 = e$.
- Look at $(h_1g)h_2 = eh_2 = h_2$ and $(h_1g)h_2 = h_1(gh_2) = h_1e = h_1$.
- By the associativity property, $h_2 = (h_1g)h_2 = h_1(gh_2) = h_1$.

g $\quad g^{-1}$ = unique mult. inverse to g

Equations in groups

Suppose that h and g are elements of a group G. We can ask if there is an x such that $hx = g$ – in other words, does this equation have a solution?

↑ solve $hx=g$ for x.

$hx=g$
$x = g/h$

Proposition: Let g and h be elements of a group G. The equation $hx = g$ always has a (unique) solution. So does $xh = g$.

Proof: Multiply both sides of the equation $hx = g$ *on the left* by h^{-1}:

$hx = g$

$$h^{-1}(hx) = h^{-1}g.$$

Since $h^{-1}(hx) = (h^{-1}h)x = ex = x$, we have the solution $x = h^{-1}g$.

For the second equation, multiply by h^{-1} *on the right*:

$$(xh)h^{-1} = x(hh^{-1}) = xe = x = gh^{-1}$$

Exponents

If g is an element of a group G, we let $g^n = \overbrace{ggg\cdots g}^{n}$ be the result of multiplying g by itself n times. This makes sense because of the associative law.

$g^n = \overbrace{g \cdot g \cdots g}^{n \text{ times}}$

We let $g^{-n} = (g^{-1})^n$.

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

Proposition: The following rules of exponents hold:

- $g^n g^m = g^{n+m}$ for all $n, m \in \mathbb{Z}$.
- $\underline{(gh)^{-1} = h^{-1}g^{-1}}$
- *If G is abelian* then $(gh)^n = g^n h^n$. If G is not abelian, this is *not true* in general.

$g^{-3} \cdot g^5 = g^{-1}g^{-1}\underbrace{g^{-1}g}gggg$
$= \underbrace{g^{-1}\underbrace{g^{-1}\cancel{e}g}g}gg$
$= g^2$

$(gh)^{-1}gh = e$

$h^{-1}g^{-1} \cdot gh = h^{-1}(g^{-1}g)h = h^{-1}eh = h^{-1}h = e$

$h^{-1}g^{-1}$ is the inverse of gh.

$\overline{(gh)^{-1} = h^{-1}g^{-1}}.$

$(gh)^n = g^n h^n$ If ~~g~~ G is abelian.

$(gh)^n = \underbrace{ghghgh\cdots gh}_{n \text{ times}} = g^n h^n.$ using $gh = hg$.