What is a group?

Tuesday, June 29, 2021 3:29 PM

Group theory is (mostly) about symmetries of objects. In some interesting examples in geometry, combinatorics, or even chemistry, knowing the symmetries uniquely determine the object. One can say that at a meta-level, the whole mathematics (and in general sciences) is about finding patterns as we want to reduce the amount of data that we need to store. (Lowering the complexity of the objects that we are studying.)

We start with an axiomatic definition of groups, and then give the relation with symmetries.

<u>Def.</u> Suppose G is a non-empty set and $(g_1, g_2) \mapsto g_1 \cdot g_2$ is an operator on G (that means it is a function from $G \times G$ to G). We say $(G, \cdot)$ (or simply G) is a group if the following properties hold.

(Associative) $\forall g_1, g_2, g_3 \in G,\quad g_1 \cdot (g_2 \cdot g_3) = (g_1 \cdot g_2) \cdot g_3$

(Neutral element) $\exists\ e \in G,\ \forall g \in G,\quad g \cdot e = e \cdot g = g$

(Inverse) $\forall g \in G,\ \exists g' \in G,\ g \cdot g' = g' \cdot g = e$ where e is a neutral

Examples for groups based on numbers

Tuesday, June 29, 2021 3:29 PM

element.

We have already seen some examples of groups.

<u>Ex.</u> $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, and $(\mathbb{C},+)$ are groups.

<u>Solution.</u> $+$ is associative.

- 0 is in all of these sets and, for every x in $\mathbb{C}$,

  $x+0=0+x=x$, and so 0 is a neutral element of all these sets under addition.

- First notice that every complex number x has an addive inverse: $x+(-x)=(-x)+x=0$. Next we point out that all these sets are closed under taking negative.

<u>Ex.</u> $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$, and $(\mathbb{C}\setminus\{0\},\cdot)$ are groups.

<u>Solution.</u> $\cdot$ is associative.

- 1 is in all of these sets and, for every x in $\mathbb{C}\setminus\{0\}$,

  $x\cdot 1=1\cdot x=x$, and so 1 is a neutral element of all these sets under multiplication.

- First notice that every non-zero complex number z has a

Examples for groups based on numbers

Tuesday, June 29, 2021 3:29 PM

multiplicative inverse that we denote by z^{-1}:

$$z \cdot z^{-1} = z^{-1} \cdot z = 1.$$

Next we notice that, if $x \in \mathbb{R} \setminus \{0\}$, then $x^{-1} \in \mathbb{R} \setminus \{0\}$; and if $x = \frac{m}{n} \in \mathbb{Q} \setminus \{0\}$ with $m, n \in \mathbb{Z} \setminus \{0\}$, then $x^{-1} = \frac{n}{m} \in \mathbb{Q} \setminus \{0\}$.

<u>Ex.</u> $(\mathbb{Z} \setminus \{0\}, \cdot)$, $(\mathbb{Z}^{\geq 0}, +)$ are not groups.

<u>Solution.</u> . $\mathbb{Z} \setminus \{0\}$ has a unique neutral element under $\cdot$, and that element is 1. This is the case because, if e is a neutral element of $\mathbb{Z} \setminus \{0\}$ under $\cdot$, then

$1 \cdot e = 1$ which implies that $e = 1$. Now we argue that $2 \in \mathbb{Z} \setminus \{0\}$ does not have an inverse in $\mathbb{Z} \setminus \{0\}$. If 2 has an inverse in $\mathbb{Z} \setminus \{0\}$, then $2x =$ a neutral element of $(\mathbb{Z} \setminus \{0\}, \cdot)$. This implies $2x = 1$ for some $x \in \mathbb{Z} \setminus \{0\}$, which is a contradiction as the left hand side is even and the right hand side is odd!

. $\mathbb{Z}^{\geq 0}$ has a unique neutral element under addition and that is 0. That is the case because, if e is a neutral element of $(\mathbb{Z}^{\geq 0}, +)$, then $e+0=0$, which implies that $e=0$. Now we show that 1 does not an inverse with respect to addition in $\mathbb{Z}^{\geq 0}$. If it does have an inverse, then there is $x \in \mathbb{Z}^{\geq 0}$ such that $x+1 =$ a neutral element of $\mathbb{Z}^{\geq 0}$. Since 0 is the only neutral element of $(\mathbb{Z}^{\geq 0}, +)$, we deduce that $x+1=0$ for some $x \in \mathbb{Z}^{\geq 0}$. This is a contradiction as the left hand side is at least 1, and $1>0$. ∎

Ex. For every integer $n \geq 2$, $(\mathbb{Z}_n, +)$ is a group.

Solution. We have already discussed all the group properties.

Ex. For every integer $n \geq 2$, $(\mathbb{Z}_n^{\times}, \cdot)$ is a group.

Solution. We have already checked all the conditions. ∎

Ex. Suppose n is an integer which is at least 2. Then $(\mathbb{Z}_n \setminus \{[0]_n\}, \cdot)$ is a group if and only if n is prime.

Solution. $(\Leftarrow)$ If n is prime, then $\mathbb{Z}_n^{\times} = \mathbb{Z}_n \setminus \{[0]_n\}$; and the claim follows from the previous example.

$(\Rightarrow)$ We show the contrapositive. If $n \geq 2$ is not prime, then

then $n=dd'$ for some integers d,d' in the interval $(1..n)$. Then $[d]_n, [d']_n \in \mathbb{Z}_n \setminus \{[0]_n\}$ and

$$[d]_n \cdot [d']_n = [n]_n = [0]_n.$$

Hence $\cdot$ is not an operator on $\mathbb{Z}_n \setminus \{[0]_n\}$. ∎

In some of the examples, we showed the uniqueness of a neutral element when it exists. Next we show this property in a general setting.

Lemma. Suppose G is a non-empty set, and $(g_1, g_2) \mapsto g_1 \cdot g_2$ is an operation. Suppose $e, e' \in G$ are neutral elements of $\cdot$. Then $e=e'$. In particular, in a group, there is a unique neutral element.

Pf. Since e is a neutral element, $e \cdot e' = e'$. Because e' is a neutral element, $e \cdot e' = e$. Altogether we have

$$e' = e \cdot e' = e.$$ ∎

Next we show the uniqueness of inverse in a group.

Lemma. Suppose $(G, \cdot)$ is a group. Then every element g

has a unique inverse. That means if g_1, g_2 are inverses of g, then $g_1 = g_2$. (By inverse we mean the following: let e_G be the unique neutral element of $(G, \cdot)$. Then saying that g_i is an inverse of g means

$$g_i \cdot g = g \cdot g_i = e_G\ .)$$

Pf. Here is the nice argument and as you can observe we only need to assume that $g_1 \cdot g = e_G$ and $g \cdot g_2 = e_G$.

$$\begin{aligned} g_1 &= g_1 \cdot e_G && (e_G \text{ is the neutral element}) \\ &= g_1 \cdot (g \cdot g_2) \\ &= (g_1 \cdot g) \cdot g_2 && (\text{associative}) \\ &= e_G \cdot g_2 \\ &= g_2 && (e_G \text{ is the neutral element}) \ \blacksquare \end{aligned}$$

The inverse of $g \in G$ in a multiplicative notation is denoted by g^{-1}. When we are working with an additive notation $(G, +)$, the neutral element is denoted by 0 and the inverse of $g \in G$ is denoted by $-g$.

Basic properties of groups

Tuesday, June 29, 2021 3:29 PM

Lemma. Suppose $(G,\cdot)$ is a group. Then for every g,h in G, we have $(g\cdot h)^{-1} = h^{-1}\cdot g^{-1}$.

Pf. Since inverse of an element is unique, it is enough to check that $(g\cdot h)\cdot(h^{-1}\cdot g^{-1}) = (h^{-1}\cdot g^{-1})\cdot(g\cdot h) = e_G$.

$$
\begin{aligned}
(g\cdot h)\cdot(h^{-1}\cdot g^{-1}) &= g\cdot(h\cdot h^{-1})\cdot g^{-1} && \text{(associative)}\\
&= (g\cdot e_G)\cdot g^{-1}\\
&= g\cdot g^{-1} = e_G && \text{(neutral element)}
\end{aligned}
$$

Similarly $(h^{-1}\cdot g^{-1})\cdot(g\cdot h) = h^{-1}\cdot(g^{-1}\cdot g)\cdot h = h^{-1}\cdot e_G\cdot h$
$$= h^{-1}\cdot h = e_G. \qquad \blacksquare$$

Lemma. For every $g\in G$, $(g^{-1})^{-1} = g$.

Pf. We have that $g^{-1}\cdot g = e_G$. Multiply both sides by $(g^{-1})^{-1}$ from left. Then $(\underbrace{(g^{-1})^{-1}\cdot g^{-1}}_{e_G})\cdot g = (g^{-1})^{-1}\cdot e_G = (g^{-1})^{-1}$.

Hence $e_G\cdot g = (g^{-1})^{-1}$, and so $g = (g^{-1})^{-1}$. $\blacksquare$

Lemma. (Cancellation law) $g\cdot h = g\cdot h' \Rightarrow h = h'$. Similarly $h\cdot g = h'\cdot g \Rightarrow h = h'$.

Pf. $g\cdot h = g\cdot h' \Rightarrow g^{-1}\cdot(g\cdot h) = g^{-1}\cdot(g\cdot h') \Rightarrow (\underbrace{g^{-1}\cdot g}_{e_G})\cdot h = (\underbrace{g^{-1}\cdot g}_{e_G})\cdot h'$

$\Rightarrow h = h'$. The other is similar. $\blacksquare$

Exponents of elements

Tuesday, June 29, 2021 3:29 PM

Suppose $(G,\cdot)$ is a group and $g\in G$. For a positive integer n, we let $g^n := \underbrace{g\cdot\cdots\cdot g}_{n \text{ times}}$. For a negative integer n, we let $g^n := \underbrace{(g^{-1})\cdot\cdots\cdot(g^{-1})}_{-n \text{ times}}$. And we let $g^0 := e_G$ (the neutral element).

Lemma. For $n,m\in\mathbb{Z}$, $(g^n)^m = g^{nm}$.

Pf. We will consider various cases depending on signs of m and n. Suppose m and n are positive. Then

$$(g^n)^m = \underbrace{g^n\cdot\cdots\cdot g^n}_{m \text{ times}} = \underbrace{\overbrace{(g\cdot\cdots\cdot g)}^{n \text{ times}}\cdot\cdots\cdot\overbrace{(g\cdot\cdots\cdot g)}^{n \text{ times}}}_{m \text{ times}} = \overbrace{g\cdot\cdots\cdot g}^{mn \text{ times}} = g^{mn}.$$

$\underline{m>0,\ n<0}$. $(g^n)^m = \underbrace{g^n\cdot\cdots\cdot g^n}_{m \text{ times}} = \underbrace{\overbrace{(g^{-1}\cdot\cdots\cdot g^{-1})}^{-n \text{ times}}\cdot\cdots\cdot\overbrace{(g^{-1}\cdot\cdots\cdot g^{-1})}^{-n \text{ times}}}_{m \text{ times}}$

$$= \underbrace{g^{-1}\cdot\cdots\cdot g^{-1}}_{-mn \text{ times}} = g^{mn}. \text{ (notice that } mn<0)$$

$\underline{m<0,\ n>0}$. $(g^n)^m = \underbrace{(g^n)^{-1}\cdot\cdots\cdot(g^n)^{-1}}_{-m \text{ times}}$

$$= \underbrace{\overbrace{(g\cdot\cdots\cdot g)}^{n \text{ times}}{}^{-1}\cdot\cdots\cdot\overbrace{(g\cdot\cdots\cdot g)}^{n \text{ times}}{}^{-1}}_{-m \text{ times}}$$

By the previous lemma, $\overbrace{(g\cdot\cdots\cdot g)}^{n \text{ times}}{}^{-1} = \overbrace{g^{-1}\cdot\cdots\cdot g^{-1}}^{n \text{ times}}$. (I) Hence

$$(g^n)^m = \underbrace{\overbrace{(g^{-1}\cdot\cdots\cdot g^{-1})}^{n \text{ times}}\cdot\cdots\cdot\overbrace{(g^{-1}\cdot\cdots\cdot g^{-1})}^{n \text{ times}}}_{-m \text{ times}}$$

$$= \underbrace{g^{-1}\cdot\cdots\cdot g^{-1}}_{-mn \text{ times}} = g^{mn}. \quad \text{(Notice that } mn<0)$$

Exponents of elements

Tuesday, June 29, 2021 3:29 PM

<u>$m<0, n<0$</u>. It is easier to work with positive numbers.

So we write $m=-r$ and $n=-s$ where $r,s>0$. Then we have to show $(g^{-r})^{-s}=g^{rs}$. By definition, $g^{-r}=\underbrace{g^{-1}\cdot\dots\cdot g^{-1}}_{r \text{ times}}$.

Hence $(g^{-r})^{-s}=\left[(g^{-1})^{r}\right]^{-s}$. By the case where $n>0$, $m<0$, we deduce $(x^r)^{-s}=x^{-rs}$. Therefore

$$(g^{-r})^{-s}=(g^{-1})^{-rs}=(g^{-1})^{-1}\cdot\dots\cdot(g^{-1})^{-1}, \quad rs \text{ times}.$$

$$=\underbrace{g\cdot\dots\cdot g}_{rs \text{ times}}=g^{rs}$$

<u>$m=0$</u>. $(g^n)^m=e_G$ and $g^{nm}=e_G$ as $m=mn=0$.

<u>$n=0$</u>. $(g^n)^m=e_G^m=e_G$ and $g^{mn}=e_G$ as $mn=0$.

Notice that $e_G\cdot\dots\cdot e_G=e_G$ and $e_G^{-1}=e_G$, and so $e_G^m=e_G$.

So we showed $(g^n)^m=g^{mn}$ for every $m,n\in\mathbb{Z}$. ∎

When we are working with an additive group $(G,+)$ instead of writing g^n we write ng. So in $(G,+)$,

$$ng=\begin{cases} g+\dots+g \ (n \text{ times}) & \text{if } n>0 \\ 0 & \text{if } n=0 \\ (-g)+\dots+(-g) \ (-n \text{ times}) & \text{if } n<0. \end{cases}$$

We have $m(ng)=(mn)g$ for every $m,n\in\mathbb{Z}$.

Exponents of elements

Tuesday, June 29, 2021 3:29 PM

Lemma. For every $m,n\in\mathbb{Z}$, $g^m\cdot g^n=g^{m+n}$.

Pf. We consider various cases depending on the signs of m,n.

Since it is easier to work with positive numbers, each time we write $m=\operatorname{sgn}(m)\,r$ and $n=\operatorname{sgn}(n)\,s$ where $r=|m|$, $s=|n|$.

$m,n>0$. $g^m\cdot g^n=\underbrace{(g\cdot\cdots\cdot g)}_{m\text{ times}}\cdot\underbrace{(g\cdot\cdots\cdot g)}_{n\text{ times}}=\underbrace{g\cdot\cdots\cdot g}_{m+n\text{ times}}=g^{m+n}$.

$m=-r,\ n=s,\ r<s$. By the previous case, $g^{s-r}\cdot g^r=g^s$

$$\Rightarrow g^{s-r}=g^s\cdot(g^r)^{-1}=g^s\cdot g^{-r}.$$

$m=-r,\ n=s,\ r>s$. By the first case, $g^s\cdot g^{r-s}=g^r$.

$$\Rightarrow g^{r-s}=(g^s)^{-1}\cdot g^r \Rightarrow (g^{r-s})^{-1}=((g^s)^{-1}\cdot g^r)^{-1}$$

$$\Rightarrow g^{-(r-s)}=(g^r)^{-1}\cdot((g^s)^{-1})^{-1}\Rightarrow g^{-r+s}=g^{-r}\cdot g^s.$$

$m=0$. $g^m\cdot g^n=e_G\cdot g^n=g^n=g^{m+n}$.

$n=0$. $g^m\cdot g^n=g^m\cdot e_G=g^m=g^{m+n}$.

By the above cases, we obtain the claim when $n\geq 0$, and $m\in\mathbb{Z}$.

$n=-s,\ s>0$. $g^{m-s}\cdot g^s=g^m\Rightarrow g^{m-s}=g^m\cdot(g^s)^{-1}$

$$\Rightarrow g^{m-s}=g^m\cdot g^{-s}.$$

∎