Subgroups

In response to student homework and presentations during this week, I pointed out that the group axioms (associativity, existence of identity, and existence of inverse) are the minimum requirements needed to have left and right cancellation. This is really the main point of groups.

Proposition. *If $a, b, c \in G$ then we can cancel on the left or right.*

- $ab = ac \iff b = c$
- $ba = ca \iff b = c$

Group axioms have ONE JOB: Making left and right cancellation happen. Using this, we can show if and only if relationships among statements as in the following example.

Lemma. *Elements a and b commute if and only if a^{-1} and b commute (i.e. $ab = ba$ if and only if $a^{-1}b = ba^{-1}$).*

Proof. Consider the following string of equivalent statements.

$$\begin{aligned} ab &= ba \\ a^{-1}aba^{-1} &= a^{-1}baa^{-1} \\ e\,ba^{-1} &= a^{-1}b\,e \\ ba^{-1} &= a^{-1}b \end{aligned}$$

□

Definition. A subgroup of a group is a subset which is also a group using the containing set's group operation. We write "$H \subset G$" for "H **subset** of G" and "$H < G$" for "H **subgroup** of G".

Subgroups extend the idea of how integers, rational numbers, and real numbers are related.

Proposition. *Integers is a subgroup of rationals which is a subgroup of reals which is a subgroup of complex.*

$$\begin{array}{ccccccc} (\mathbb{Z},+) & < & (\mathbb{Q},+) & < & (\mathbb{R},+) & < & (\mathbb{C},+) \\ & & (\mathbb{Q}^{\neq 0},\cdot) & < & (\mathbb{R}^{\neq 0},\cdot) & < & (\mathbb{C}^{\neq 0},\cdot) \end{array}$$

To prove that something is a subgroup, you can verify the group axioms. It must have an associative operation, an identity, and inverses.

In practice, there is usually one other step – you must show that the group operation $G \times G \to G$ descends to a well-defined operation $H \times H \to H$. In this case we say the operation is **closed** on H (i.e. it doesn't go outside of H).

Definition. An operation on a set G is **closed** on a subset H if the image of the operation restricted to H is contained in H.

With this language, checking that something is a subgroup usually takes three steps.

Proposition. *A subset $H \subset G$ is a subgroup if the following conditions are satisfied.*

- *The subset is nonempty $H \neq \emptyset$ (usually we show that $e \in H$).*
- *The subset is closed under the group operation (i.e. if $a, b \in H$ then $ab \in H$).*
- *The subset is closed under inverses (i.e. if $a \in H$ then $a^{-1} \in H$).*

Textbooks will often shorten this into a (deceptively) single closure statement ($ab^{-1} \in H \neq \emptyset$). But actually showing that isn't any simpler than the three steps above. So I suggest that we just stick with this.

We've already seen another example of subgroups. Recall that the center of a group is the set of all elements which commute with everything in the group.

Proposition. *The center of a group $Z(G)$ is a subgroup of G.*

Proof. Verify the three conditions given above.

- The identity commutes with all elements ($eg = e = ge$), so $e \in Z(G)$. Thus $Z(G)$ is nonempty.
- If $a, b \in Z(G)$ then for every $g \in G$, we have
$$(ab)g \;=\; abg \;=\; agb \;=\; gab \;=\; g(ab)$$
so $ab \in Z(G)$
- If $a \in Z(G)$ then by the lemma above, $a^{-1} \in Z(G)$ also.

□

Below are some other interesting subgroups. Some were shown in class, others were homework.

Proposition. *If G is abelian then $\{x \in G \mid x^2 = e\}$ is a subgroup.*

Proposition. *If G is abelian then $\{x^2 \mid x \in G\}$ is a subgroup.*

Proposition. *The set of integer powers of 2 is a subgroup of the multiplicative rationals, $\{2^k \mid k \in \mathbb{Z}\} \;<\; \mathbb{Q}^{\neq 0}$.*

Proposition. *The set of multiples of n is a subgroup of the additive integers, $n\mathbb{Z} \;<\; \mathbb{Z}$.*

Proposition. *The set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \setminus \{0\}$ is a subgroup of multiplicative reals $\mathbb{R}^{\neq 0}$.*

Example. Below are some subsets which fail to be subgroups.

- The set of nonzero integers isn't a subgroup of rationals (under multiplication), because it doesn't contain (multiplicative) inverses.
- The set of irrationals isn't a subgroup of the set of reals (under multiplication), because $\sqrt{2} \cdot \sqrt{2} = 2$ which isn't irrational.
- The set of nonnegative integers $\mathbb{Z}^{\geq 0}$ isn't a subgroup of the integers (under addition) because it isn't closed under inverses.
- The set of odd integers isn't a subgroup of integers (under addition) since $1 + 1 = 2$.
- The set of real numbers in the interval $(-1, 1)$ isn't a subgroup of $\mathbb{R}$ (under addition) since $0.9 + 0.9 \;=\; 1.8 \;>\; 1$.

Subgroup behaves well with intersection, but badly with union. We'll discuss how to "fix" this later...

Proposition. *If $H_1, H_2 < G$ then $H_1 \cap H_2 < G$ also!*

Homework: Show that $4\mathbb{Z} \cup 6\mathbb{Z}$ is not a subgroup of $\mathbb{Z}$.

Given an element $g \in G$, the **conjugate** of H by g is $gHg^{-1} = \left\{ghg^{-1} \mid h \in H\right\}$. Subgroup also behaves well with conjugation. This will be important later!

Proposition. *If $H < G$ and $g \in G$, then $gHg^{-1} < G$ also!*

Proof. Verify nonempty, closed under product, closed under inverse.

(Nonempty.) If H is a group then $e \in H$, so $e = geg^{-1} \in gHg^{-1}$.
(Product.) $(gh_1g^{-1})\,(gh_2g^{-1}) = g(h_1h_2)g^{-1} \in gHg^{-1}$.
(Inverse.) $(ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$.

□

I wanted to end the week with the following cool application of subgroups.

Definition. The **order** of a group, $|G|$, is the number of elements in the underlying set.

Knowing the order of a group is powerful. For example

Proposition. *If a group has finite, even order then it contains an element $g \neq e$ with $g^2 = e$.*

Proof. Suppose by way of contradiction that G has finite, even order but contains no elements $g \neq e$ with $g^2 = e$. Then every element aside from e is distinct from its inverse. Partition the group into sets $\{e\}$ and $\{g, g^{-1}\}$. Together, these sets contain an odd number of elements, contradicting the claim that G has even order. □

But knowing the order of a group isn't enough to completely distinguish it!

Definition. The **product** of two groups is $H \times G$ with operation $(h_1, g_1) \circ_\times (h_2, g_2) = (h_1 \circ_H h_2,\ g_1 \circ_G g_2)$.

Proposition. *This defines a group.*

Consider the two groups $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$. Both of these groups have 9 elements. But they are different groups! How do we know???

Proposition. *$\mathbb{Z}_9$ has **only one** proper nontrival subgroup. $\mathbb{Z}_3 \times \mathbb{Z}_3$ has **two** proper nontrivial subgroups.*

Recall that $\{e\} < G$ for all groups. This is the **trivial** subgroup. If a subgroup $H < G$ is neither $\{e\}$ nor G itself, then we say it is a proper nontrivial subgroup.

Preview. Next week we will discuss cyclic subgroups! Cyclic subgroups are the subgroups *generated* by a single element. Their universal property is that they are the **smallest** subgroup containing a given element.

Definition. The **cyclic subgroup** defined by an element $a \in G$ is $\langle a \rangle = \{\dots, a^{-1}, e, a, a^2, a^3, \dots\}$

Proposition. *If $H < G$ and $a \in H$, then $\langle a \rangle < H$.*

Definition. The **order** of an element is $|a| = \big|\langle a \rangle\big|$.

Proposition. *If $|a| = n$ is a finite number, then n is the smallest integer with $a^n = e$.*