MA294 Lecture

Timothy Kohl

Boston University

February 20, 2024

Subgroups

Definition

A subset $H \subseteq G$ (for G a group) is a subgroup if H itself is a group with respect to the same group operation it inherits from G.
Notation: If so, then we write $H \leq G$.

Example: $G = \mathbb{Z}$ and let $H = \langle 2 \rangle = 2\mathbb{Z} = \{\textit{even integers}\} = \{2n \mid n \in \mathbb{Z}\}$

Observe this *is* a subgroup since $2m + 2n = 2(m+n)$ so it's closed, and $0 = 2 \cdot 0 \in H$, and for $2m \in H$ we note that $-2m = 2(-m) \in H$ so H is indeed a group in and of itself.

Note, we do not need to check that the group operation in H is associative since it's contained in a group (namely G) which is already associative.

Example:

$$G = D_3 = \{r_0, r_{120}, r_{240}, f_1, f_2, f_3\}$$
$$H = \langle r_{120} \rangle = \{r_0, r_{120}, r_{240}\}$$

H is a subgroup since the composition of two rotations is a rotation so H is closed, and the identity $r_0 \in H$, and $r_{120}^{-1} = r_{240}$ (and symmetrically $r_{240}^{-1} = r_{120}$) so H contains inverses for all its elements.

Similarly $K = \langle f_1 \rangle = \{r_0, f_1\}$ is a subgroup since $f_1 \circ f_1 = r_0$ and $r_0 \in K$ and $f_1^{-1} = f_1$ so K contains inverses etc.

Note, not all subsets of a group G are subgroups, for example

$$\tilde{H} = \{r_0, r_{120}.r_{240}, f_1\}$$

is not a subgroup since $r_{120} \circ f_1 = f_3 \notin \tilde{H}$.

i.e. $\tilde{H}$ is not closed.

Verifying that $H \subseteq G$ is a subgroup can be simplified.

Subgroup Test

$H \subseteq G$ is a subgroup if
(i) $a, b \in H$ implies $ab \in H$ (closure)
(ii) $a \in H$ implies $a^{-1} \in H$

We note that associativity does not need to be checked, and (i) and (ii) imply that H contains the identity. (Why? - Exercise)

An application of this test is the following basic class of examples of subgroups.

Definition

If $x \in G$ and if $|x| = m$ then $H = \langle x \rangle = \{e, x, x^2, \ldots, x^{m-1}\}$ is the *cyclic subgroup generated by* x which *is* a subgroup of G.

If x has infinite order then $H = \langle x \rangle = \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\}$ is also a subgroup of G.

Why is this always a subgroup?

If $x^i, x^j \in H$ then $x^i x^j = x^{i+j} \in H$ and $x^i \in H$ implies $x^{-i} \in H$ since H consists of all powers of x so it must contain x^{-i}.

A more advanced example of where this test is used is for subgroups which are defined by a *property* that determines whether an element is in the subgoup or not, rather than an explicit list of elements.

The following example is interesting, especially in light of the fact that there are groups which are non-abelian.

Definition

For G a group, the *center* of a group is

$$Z(G) = \{z \in G \mid zg = gz \text{ for all } g \in G\}$$

which is the set of those elements of G which commute with *every* element of G.

Why is $Z(G)$ a subgroup?

Well, if $z_1, z_2 \in Z(G)$ then we wish to show $z_1 z_2 \in Z(G)$.

If $g \in G$ then $z_1 z_2 g = z_1(z_2 g) = z_1(g z_2) = (z_1 g) z_2 = (g z_1) z_2 = g z_1 z_2$ and so, indeed, $z_1 z_2 \in Z(G)$.

If now $z \in Z(G)$ and $g \in G$ then $zg = gz$ so $z^{-1}zg = z^{-1}gz$ namely $g = z^{-1}gz$ and so $gz^{-1} = z^{-1}gzz^{-1}$, that is $gz^{-1} = z^{-1}g$.

That is, $z \in Z(G)$ implies $z^{-1} \in Z(G)$.

So what does $Z(G)$ look like?

For abelian groups G, if you look at the definition it's pretty clear that $Z(G) = G$.

In contrast, $Z(D_3) = \{r_0\}$ (i.e. just the identity) which can happen, although for other non-abelian groups, G, it turns out that $Z(G)$ is a *proper* subgroup, neither $\{e\}$ nor all of G.

As we shall see, the nature of the subgroups of a group is very important to ones understanding of the group itself.

Coset and LaGrange's Theorem

One of the key result in (finite) group theory centers around the relationship between a given group and its subgroups.

Definition

Let H be a subgroup of a (finite) group G and for $g \in G$

- the left coset $gH = \{gh \mid h \in H\}$
- the right coset $Hg = \{hg \mid h \in H\}$

So if $H = \{h_1, \ldots, h_m\}$ for example, then $gH = \{gh_1, \ldots, gh_m\}$ and $Hg = \{h_1 g, \ldots, h_m g\}$.

Example: Let $G = D_3$ and $H = \langle r_{120} \rangle = \{r_0, r_{120}, r_{240}\}$.

$$\begin{aligned} f_1 H &= \{f_1 \circ r_0, f_1 \circ r_{120}, f_1 \circ r_{240}\} \\ &= \{f_1, f_2, f_3\} \end{aligned}$$

or, if $K = \langle f_1 \rangle = \{r_0, f_1\}$ then

$$\begin{aligned} r_{120} K &= \{r_{120} \circ r_0, r_{120} \circ f_1\} \\ &= \{r_{120}, f_3\} \end{aligned}$$

and, in contrast

$$\begin{aligned} K r_{120} &= \{r_0 \circ r_{120}, f_1 \circ r_{120}\} \\ &= \{r_{120}, f_2\} \end{aligned}$$

which shows that we can't expect $gH = Hg$ necessarily.

Important Obervations

- gH and Hg are not necessarily equal.
- gH and Hg are both subsets of G, but generally *not* subgroups.
- In fact, gH is a subgroup only if $g \in H$, in which case $gH = H$.

Notation Alert: If G is an 'additive' group like $\mathbb{Z}$ or $\mathbb{Z}_m$ then we use additive notation for the cosets.

For example: Consider $(\mathbb{Z}, +)$ and let $H = 3\mathbb{Z} = \langle 3 \rangle$ so that

$$H = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$$

where now, for example $1 + H = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$.

This example can be used to demonstrate another interesting fact, namely that $g_1 H = g_2 H$ (or $g_1 + H = g_2 + H$) even if $g_1 \neq g_2$.

Observe for $H = 3\mathbb{Z}$ above that $4 + H = \{\dots, -5, -2, 1, 4, 7, 10, 14, \dots\}$ which is the same as $1 + H$.

Why?(We'll get back to this question soon.)

Our goal is to show an important relationship between the size of a group, and the size of any subgroup.

Proposition

For $H \leq G$ a subgroup, and $g \in G$ one has that $|gH| = |H|$ and $|Hg| = |H|$.

Proof.

Define $f : H \to gH$ by $f(h) = gh$ and observe that if $f(x) = f(y)$ then $gx = gy$ which implies that $g^{-1}gx = g^{-1}gy$, that is, $x = y$ so f is 1-1.

And if $gz \in gH$ then it's pretty clear that $gz = f(z)$ so f is onto, and therefore a bijection, and so the cardinality of the domain and range are the same, i.e. $|H| = |gH|$, and a similar argument shows that $|H| = |Hg|$ too. $\square$

Going further into the study of cosets, we have the following.

Proposition

If $H \leq G$ is a subgroup, then for $g_1, g_2 \in G$, either $g_1 H = g_2 H$ or $g_1 H \cap g_2 H = \emptyset$.

Proof.

Suppose $g_1 H \cap g_2 H \neq \emptyset$ then there exists some x in the intersection. So $x = g_1 h_1$ and $x = g_2 h_2$, i.e. $g_1 h_1 = g_2 h_2$ so $g_1 = g_2 h_2 h_1^{-1}$.
Now, if $g_1 k \in g_1 H$ then $g_1 k = g_2 h_2 h_1^{-1} k = g_2(h_2 h_1^{-1} k)$ where $h_2 h_1^{-1} k \in H$. (Why?)
This implies that $g_1 k \in g_2 H$ and so $g_1 H \subseteq g_2 H$.
Similarly, $g_1 h_1 = g_2 h_2$ implies that $g_2 = g_1 h_1 h_2^{-1}$ and so if $g_2 t \in g_2 H$ (i.e. $t \in H$) then $g_2 t = g_1 h_1 h_2^{-1} t = g_1(h_1 h_2^{-1} t)$ where $h_1 h_2^{-1} t \in H$, which means $g_2 t = g_1 h_1 h_2^{-1} t \in g_1 H$, thus $g_2 H \subseteq g_1 H$.

Thus $g_1 H = g_2 H$ □

Note, if $H \leq G$ and $e \in G$ is the identity, then $eH = H$ since if $H = \{h_1, h_2, \ldots h_m\}$ then $eH = \{eh_1, eh_2, \ldots, eh_m\} = \{h_1, \ldots, h_m\}$.

And, in general, $gH = H$ if and only if $g \in H$. Exercise!

Lastly, for $H \leq G$, one has $g \in gH$ since if $H = \{h_1, \ldots, h_m\}$ then, assuming $h_1 = e$ we have $gH = \{gh_1, \ldots, gh_m\}$ where now, $gh_1 = ge = g$.

This last observation may seem somewhat trivial, but it highlights the fact that, with respect to a given subgroup $H \leq G$, every element $g \in G$ lies in *at least one* coset of H.

And even though it may be that $g_1H = g_2H$ the elements of G are such that every element of G lies in *exactly one* coset of H in G.

What this implies is that, if G is finite, then for $H \leq G$ one has some elements (called coset representatives) $g_1, \ldots, g_r$ such that

$$G = g_1 H \cup g_2 H \cup \cdots \cup g_r H$$

where each coset above is distinct, i.e. $g_i H \cap g_j H = \emptyset$ for $i \neq j$.

Note, we can assume that $g_1 = e$ since one of the cosets must be the 'trivial' coset, namely H itself, i.e. $eH = H$.

So G can be partitioned into a union of disjoint cosets.

This has important implications for finite groups.

Example: $D_3 = \{r_0, r_{120}, r_{240}, f_1, f_2, f_3\}$ and $H = \{r_0, r_{120}, r_{240}\}$.

The first coset to consider is the trivial coset

$$r_0 H = \{r_0 \circ r_0, r_0 \circ r_{120}, r_0 \circ r_{240}\} = \{r_0, r_{120}, r_{240}\}$$

Since this is clearly not all of D_3, we look for an element of D_3 *not* in H, say f_1 and look at what coset we get.

$$f_1 H = \{f_1 \circ r_0, f_1 \circ r_{120}, f_1 \circ r_{240}\} = \{f_1, f_2, f_3\}$$

and then we see that $r_0 H \cup f_1 H = D_3$ so we are done, i.e. there are no other cosets to make which are disjoint from these two.

Similarly, if $K = \{r_0, f_1\}$ then we can show that

$$D_3 = r_0K \cup r_{120}K \cup r_{240}K$$

where $r_0K = K$, $r_{120}K = \{r_{120}, f_3\}$ and $r_{240}K = \{r_{240}, f_2\}$.

We note the fact (observed earlier) that the size of each coset is the same as the size of the group, which, as we'll see, is an important fact.