MA294 Lecture

Timothy Kohl

Boston University

July 7, 2025

Going back to C_6 and $\mathbb{Z}_6$ which we demonstrated were isomorphic, we note that if $G_1 \cong G_2$ for two (finite) groups then we obviously must have that $|G_1| = |G_2|$.

But does $|G_1| = |G_2|$ imply that $G_1 \cong G_2$?

The answer is most definitely *no* as the example of $\mathbb{Z}_4$ and $V = \mathbb{Z}_2 \times \mathbb{Z}_2$ demonstrates.

But how do we *know* that they aren't isomorphic?

Here is a small but important fact:

Lemma

If $\beta : G_1 \to G_2$ is an isomorphism of groups then $\beta(e_1) = e_2$ where e_1 is the identity of G_1 and e_2 is the identity of G_2.

The reason for this is that for $g \in G_1$ we have $\beta(g * e_1) = \beta(g) * \beta(e_1)$ but $\beta(g * e_1) = \beta(g)$ since e_1 is the identity of G_1.
But if we call $\beta(g) = z$ and $\beta(e_1) = w$ then we have

$$z = z * w$$

in G_2, and if we multiply both sides on the left by z^{-1} we get

$$z^{-1} * z = z^{-1} * z * w$$
$$\downarrow$$
$$e_2 = w$$

i.e. $\beta(e_1) = e_2$.

Lemma

If $\beta : G_1 \to G_2$ is an isomorphism of groups, then for each $x \in G_1$, it follows that $|x| = |\beta(x)|$.

Suppose $|x| = m$ and $|\beta(x)| = n$ where $n < m$ then this says $\beta(x)^n = e_2$ where e_2 is the identity in G_2.
But $\beta(x)^n = \beta(x^n)$ and so $\beta(x^n) = e_2$.
But since β is 1-1 and $\beta(e_1) = e_2$ then we must have $x^n = e_1$.

But recall, $|x| = m$ and $n < m$ and so $x^n = e_1$ is impossible, since by definition of order, m is the smallest power of x which is the identity.
So we cannot have $|\beta(x)| < |x|$, and similarly we can show that we also cannot have $|x| < |\beta(x)|$.
So we conclude that we must have $|x| = |\beta(x)|$.

So, going back to $\mathbb{Z}_4$ vs. $\mathbb{Z}_2 \times \mathbb{Z}_2$, if there *were* an isomorphism $\beta : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ then $\beta(1)$ would be an element of order 4 in $\mathbb{Z}_2 \times \mathbb{Z}_2$, which doesn't exist!

Another consequence of the isomorphism definition is that, even if $|G_1| = |G_2|$, if G_1 is abelian, but G_2 is not, then there is no isomorphism $\beta : G_1 \to G_2$.

As such, $\mathbb{Z}_6$ is definitely not isomorphic to D_3.

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 $z^{-1} z g = z^{-1} g z$ namely $g = z^{-1} g z$ and so $g z^{-1} = z^{-1} g z z^{-1}$, that is $g z^{-1} = z^{-1} g$.

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

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

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

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 $4 + H = \{\ldots, -5, -2, 1, 4, 7, 10, 14, \ldots\}$ 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. □

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 $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$.

Proof.

Suppose $g_1H \cap g_2H \neq \emptyset$ then there exists some x in the intersection. So $x = g_1h_1$ and $x = g_2h_2$, i.e. $g_1h_1 = g_2h_2$ so $g_1 = g_2h_2h_1^{-1}$.
Now, if $g_1k \in g_1H$ then $g_1k = g_2h_2h_1^{-1}k = g_2(h_2h_1^{-1}k)$ where $h_2h_1^{-1}k \in H$. (Why?)
This implies that $g_1k \in g_2H$ and so $g_1H \subseteq g_2H$.
Similarly, $g_1h_1 = g_2h_2$ implies that $g_2 = g_1h_1h_2^{-1}$ and so if $g_2t \in g_2H$ (i.e. $t \in H$) then $g_2t = g_1h_1h_2^{-1}t = g_1(h_1h_2^{-1}t)$ where $h_1h_2^{-1}t \in H$, which means $g_2t = g_1h_1h_2^{-1}t \in g_1H$, thus $g_2H \subseteq g_1H$.

Thus $g_1H = g_2H$ □

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 subgroup, which, as we'll see, is an important fact.

Lagrange's Theorem

Theorem

If G is a finite group and $H \leq G$ then $|H| \mid |G|$.

Proof.

We've already established most of the important facts.

We know that with respect to H, there exists elements of G, $g_1, \ldots, g_r$ such that

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

where each coset is disjoint from the others, and so

$$|G| = |g_1 H| + |g_2 H| + \cdots + |g_r H|$$

and the proof is finished by recalling the other fact we noted, which is that $|g_i H| = |H|$ for each g_i and so $|G| = r|H|$, that is $|H| \mid |G|$. □

One other point to mention about cosets is related to notation.

Definition

If $H \leq G$ then the number of distinct cosets of H in G is the index of H in G and is denoted $[G : H]$.

We note, that if G is finite, then Lagrange's theorem implies that $[G : H] = \frac{|G|}{|H|}$.

We note, for reference, that $[G : H]$ also makes sense for infinite groups.

Consider $G = \mathbb{Z}$ and $H = 2\mathbb{Z} \leq G$, namely $H = \{\dots, -4, -2, 0, 2, 4, \dots\}$ and start with the trivial coset

$$0 + H = \{\dots, -4, -2, 0, 2, 4, \dots\} \text{ (all even integers!)}$$

and since this is not all of $\mathbb{Z}$ we pick an element not in H, say 1 and consider the coset

$$1 + H = \{\dots, -3, -1, 1, 3, 5 \dots\} \text{ (all odd integers!!)}$$

and we realize that there are no other elements not already accounted for, so we're done and we can write

$$\mathbb{Z} = (0 + H) \cup (1 + H) \text{ i.e. the union of the even and odd integers}$$

so $[\mathbb{Z} : 2\mathbb{Z}] = 2$.

Exericse: What is $[\mathbb{Z} : m\mathbb{Z}]$ where $m\mathbb{Z} = \langle m \rangle$?

One other thing to note is that everything we say about left cosets, holds for right cosets as well, so there's no particular 'preference' for left cosets over right cosets.

That is, the number of left cosets of a subgroup $H \leq G$ is the same as the number of right cosets, and a group can be partitioned into a disjoint union of right cosets.

The only point to reiterate is that for a given subgroup, $H \leq G$ it need not be the case that $gH = Hg$.

Here is one of the first applications of Lagrange's theorem, and what is kind of extraordinary is how simple the proof is, considering the depth of the statement being proved.

We have seen that, for example, there are two groups with 4 elements, for example $\mathbb{Z}_4$ and $V = \mathbb{Z}_2 \times \mathbb{Z}_2$ and a general question that's important in group theory is:

How many distinct groups are there of a given order (size)?

where by distinct, we mean not isomorphic, for example $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$.

For $|G| = 4$ for example, it turns out that there are only 2 non-isomorphic groups, namely $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ but, in general, it gets harder to figure out the number of different groups of order (size) n as n gets larger.

We can say this however.

Theorem

If $|G| = p$ for p a prime number, then $G \cong C_p$. (where $C_p \cong \mathbb{Z}_p$)

Proof.

Let $x \in G$ and consider $H = \langle x \rangle \leq G$.

If $x = e$ then $|H| = 1$ of course. If $x \neq e$ then $|H| > 1$ but, by Lagrange's theorem, $|H| \big| |G|$.

However, since $|G| = p$ then, since $|H| > 1$ we must have $|H| = p$, so that $H = \{e, x, x^2, \ldots, x^{p-1}\}$.

But $|H| = |G| = p$ and H is a subset of G, which means $H = G$, but this means $G = \langle x \rangle$ and so $G \cong C_p$, the cyclic group of order p. $\square$

This is somewhat extraordinary since it implies, for example that there is exactly 1 group of order 127, but, in contrast, it is known that there are 2328 groups of order 128!

Again, the number of distinct groups of a given size is, in fact, an open problem in group theory.

One of the other facts we can infer from looking at the proof of the above theorem is this.

Proposition

If G is a finite group, say $|G| = n$ then for $x \in G$, one has $|x| \big| n$. (i.e. $|x| \big| |G|$)

Why?

Quite simply, if $x \in G$, then x gives rise to the subgroup $H = \langle x \rangle = \{e, x, \ldots, x^{m-1}\}$ for some m where $|x| = m = |H|$, so by Lagrange's theorem, $m|n$.