Class 17

March 8, 2024

Results from Normal Subgroups

Thm

Every subgroup of an abelian group G is normal.

Pf

Suppose G is abelian with subgroup $H \leq G$. Then $\forall h \in H$, $\forall a \in G$

$$ah = ha$$

Thus

$$aH = \{ah | h \in H\} = \{ha | h \in H\} = Ha$$

so $H \trianglelefteq G$.

Thm

Let G be a group. If $H \trianglelefteq G$ and $K \leq G$ then $HK = \{hk | h \in H, k \in K\} \leq G$

Pf

Let's use the first subgroup test. First, note $e \in H, K$ so $e = ee \in HK$, so HK is nonempty. Let $h_1k_1, h_2k_2 \in HK$. Then we want to show

$$(h_1k_1)(h_2k_2)^{-1} \in HK$$

Using Shoe-Sock:

$$(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2$$

and as $K \leq G$, then $k_1k_2^{-1} = k \in K$ so

$$h_1k_1k_2^{-1}h_2^{-1} = h_1kh_2^{-1}$$

As H is normal, then for each $g \in G$, for each $h \in H$, there exists $h' \in H$ such that

$$gh = h'g$$

As $H \leq G$, then $h_2^{-1} \in H$ so we can use this property, to get

$$h_1kh_2^{-1} = h_1h_3k$$

for some $h_3 \in H$. As $H \leq G$, then $h_1h_3 = h \in H$, thus

$$h_1h_3k = hk \in HK$$

and by the first subgroup test, $HK \leq G$

Lagrange's Theorem

We can determine some important information about the possible subgroups of group G depending on the order of G. Suppose G is a finite group, and G has order n. That is

$$|G| = n$$

If $H \leq G$, then

$$|H| \mid |G|$$

That is n must be divisible by $|H|$. This can be shown by recalling the properties of cosets we proved a couple of classes ago. The cosets formed from H will partition G into equally sized parts, no matter which subgroup H is chosen. As n is a positive integer, this is only possible if n is divisible by $|H|$.

Cor

$$|\langle a \rangle| \mid |G|$$

Recall the element $a \in G$ will always generate a subgroup of G. We say the order of element a is

$$|a| = |\langle a \rangle|$$

As this is a subgroup of G, this implies the order of each element of G must divide the number of elements in G.

Quotient Groups (Factor Groups)

To wrap up our discussion of normal subgroups, we are going to discuss quotient groups. Informally, quotient groups are made of the cosets formed from a normal subgroup of a group G. By grouping elements of G together into these cosets, we can still learn a lot about the underlying structure of G. Formally, let G be a group and let $H \lhd G$. Then the set

$$G/H = \{aH | a \in G\}$$

is a group under the binary operation

$$(aH)(bH) = abH$$

for $a, b \in G$

pf

We will now prove this is a well defined group. First, let's consider the binary operation in question. Using the usual definition of multiplication of cosets:

$$(aH)(bH) = aHbH$$

but, since H is normal

$$aHbH = a(Hb)H = a(bH)H = abHH = abH$$

Thus our product makes sense if we assume H is normal. Furthermore,

$$abH \in G/H$$

as

$$ab \in G$$

Since G is a group and has closure. This gives us a valid binary operation. To show associativity, consider the following for $a, b, c \in G$

$$((aH)(bH))(cH) = (abH)(cH) = (ab)cH$$

as G is a group and has associativity:

$$a(bc)H = (aH)(bcH) = (aH)((bH)(cH))$$

as desired. Now, for the identity element:

$$eH = H \in G/H$$

For any $aH \in G/H$.

$$(H)(aH) = aH = (aH)(H)$$

so H is the identity. For inverse elements, suppose $a \in G$. Then $a^{-1} \in G$, thus

$$(aH)\left(a^{-1}H\right) = aa^{-1}H = eH = H$$

so for any element $aH \in G/H$, $(aH)^{-1} = a^{-1}H$. As all of the necessary conditions are met, we have G/H as a group. Let's look at some examples of quotient groups:

Ex 1

Let $G = (\mathbb{Z}, +)$ and let $5\mathbb{Z} = \{0, \pm 5, \pm 10, \dots\}$. First, let's note that $5\mathbb{Z}$ is a normal subgroup of G as

1. $5\mathbb{Z} \subseteq \mathbb{Z}$

2. From subgroup test 1, if $a, b \in 5\mathbb{Z}$, then $a = 5n, b = 5m$ for some $m, n \in \mathbb{Z}$, thus

$$a - b = 5n - 5m = 5(n - m) \in 5\mathbb{Z}$$

as $n - m \in \mathbb{Z}$. This means $5\mathbb{Z} \leq G$

3. As G is abelian, each of its subgroups are normal, thus $5\mathbb{Z} \lhd G$.

The resulting quotient group is

$$\mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$$

When combining two elements of $\mathbb{Z}/5\mathbb{Z}$, we will use addition, as this is the binary operation of $\mathbb{Z}$. For example,

$$1 + 5\mathbb{Z} + 3 + 5\mathbb{Z} = 1 + 3 + 5\mathbb{Z} + 5\mathbb{Z} = 4 + 5\mathbb{Z}$$

and

$$3 + 5\mathbb{Z} + 3 + 5\mathbb{Z} = 6 + 5\mathbb{Z} = 1 + 5 + 5\mathbb{Z} = 1 + 5\mathbb{Z}$$

In fact, $\mathbb{Z}/5\mathbb{Z} \approx \mathbb{Z}_5$. This can be shown by using the isomorphism $\phi : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}_5$ such that $\phi(a + 5\mathbb{Z}) = a$. In fact, we can make the more general claim

$$\mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}_n$$

Ex 2

Suppose $G = U(11)$. Recall, this is the set of integers $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ under multiplication mod 11. We can take the subgroup

$$H = \langle 3 \rangle = \{1, 3, 9, 5, 4\}$$

Note that H is a subgroup, since it is generated by an element in G and H is normal as it is a subgroup of an abelian group. The quotient group

$$U(11) / \langle 3 \rangle = \{\langle 3 \rangle, 2\langle 3 \rangle\}$$

where $2\langle 3 \rangle = \{2, 6, 7, 10, 8\}$. As this is a group with two elements, then $G/H \approx C_2$. In fact, we can show

$$\langle 3 \rangle \langle 3 \rangle = \langle 3 \rangle$$

$$\langle 3 \rangle 2\langle 3 \rangle = 2\langle 3 \rangle$$

$$2\langle 3 \rangle 2\langle 3 \rangle = 4\langle 3 \rangle = \langle 3 \rangle$$

So, we can take the isomorphism $\phi : U(11) / \langle 3 \rangle \to C_2$ such that $\phi(x) = \begin{cases} 0 & \text{if } x = \langle 3 \rangle \\ 1 & \text{otherwise} \end{cases}$.

Note

Lagrange's theorem also tells us that $|G/H| = |G| / |H|$. This is because each coset of H is equally sized, so we can find the number of cosets by dividing the number of elements of G by the number of elements in H.

Thm

This next theorem generalizes the above result. Let G be a group, and let $Z(G)$ be the center of G. Then

$$G/Z(G) \approx \mathrm{Inn}(G)$$

pf

To prove this, consider the mapping $T : G/Z(G) \to \mathrm{Inn}(G)$ given by $T(gZ(G)) = \phi_g$ where $\phi_g = gxg^{-1}$. First, let's show that this mapping is well defined. We need to make sure each input maps to a single output. If $gZ(G) = hZ(G)$, we need to show $\phi_g = \phi_h$. From

$$gZ(G) = hZ(G)$$

$$h^{-1}gZ(G) = Z(G)$$

thus $h^{-1}g \in Z(G)$. In other words:

$$h^{-1}gx = xh^{-1}g$$

$$gx = hxh^{-1}g$$

$$\phi_g = gxg^{-1} = hxh^{-1} = \phi_h$$

as desired. Now, we will show that T is one-to-one. To do so, suppose $\phi_g = \phi_h$. Then

$$\phi_g = gxg^{-1} = hxh^{-1} = \phi_h$$

thus

$$h^{-1}gxg^{-1} = xh^{-1}$$

$$h^{-1}gx = xh^{-1}g$$

Thus

$$h^{-1}g \in Z(G)$$

so

$$h^{-1}gZ(G) = Z(G)$$

$$gZ(G) = hZ(G)$$

so T is one-to-one, as $T(gZ(G)) = \phi_g = \phi_h = T(hZ(G))$ implies $gZ(G) = hZ(G)$. Now, to show this mapping is onto. Recall $\mathrm{Inn}(G) = \{\phi_g | g \in G\}$. Let $g \in G$. Then

$$\phi_g = gxg^{-1} = T(gZ(G))$$

and as $gZ(G) \in G/Z(G)$, T is onto. Finally, we need to show T is a homomorphism. Let $g, h \in G$. Then $gZ(G), hZ(G) \in G/Z(G)$ such that

$$T(gZ(G)\,hZ(G)) = T(ghZ(G)) = \phi_{gh} = ghx(gh)^{-1}$$

$$= ghxh^{-1}g^{-1} = g\phi_h g^{-1} = \phi_g \circ \phi_h = T(gZ(G))\,T(hZ(G))$$

as desired. As T is an isomorphism and is a homomorphism, then $G/Z(G) \approx \mathrm{Inn}(G)$.