Quotient groups

Let G be a group. We've already discussed one way to create smaller groups from G, which is by looking at subgroups.

Another way is by looking at quotient groups.

Idea/motivation:

Let $\varphi: G \to H$ be a homomorphism.

Def: If $h \in H$, the fiber of φ over h is the set

$$\{ g \in G \mid \varphi(g) = h \} \subseteq G.$$

i.e. the set of elements of G that map to h.

Note: The union of the fibers is all of G (since for $g \in G$, g is in the fiber over $\varphi(g)$), and all the fibers are pairwise disjoint.

i.e. no two fibers intersect, since every element only lies in one fiber.

That is, the fibers of φ form a partition of G.

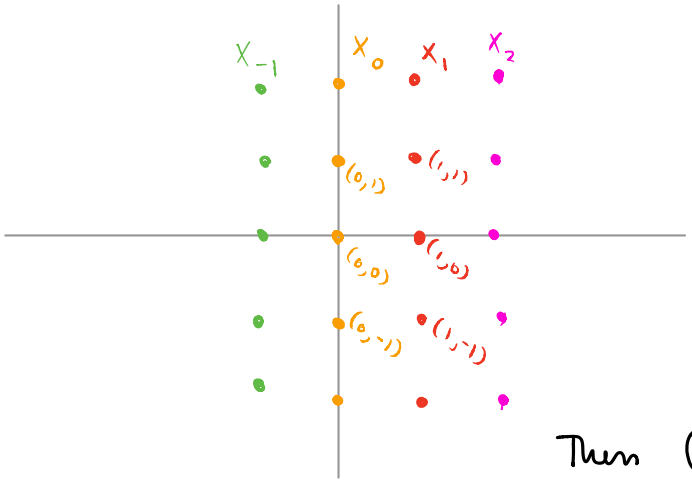
So, for each $h \in \operatorname{im}\varphi$ (the image of φ), denote the fiber over h by X_h. Then we have a natural operation on the fibers given by

$$X_a X_b = X_{ab}.$$

This is a group w/ identity 1 and $(X_a)^{-1} = X_{a^{-1}}$, and it is naturally isomorphic to the image of φ.

This is a quotient group of G. (We will see a formal definition soon).

Ex: Let $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be defined $f(a,b) = a$, i.e. projection onto the first coordinate.



Then $X_a = \{(a,b) \mid b \in \mathbb{Z}\}$
$= \{\ldots, (a,-1), (a,0), (a,1), \ldots\}$

Note, if $(a,b) \in X_a$, $(a',b') \in X_{a'}$
Then $(a,b)+(a',b') = (a+a', b+b') \in X_{a+a'} = X_a X_{a'}$

That is, we can first add representatives, whose fiber is the product of the first two fibers

Ex: Let $n \geq 2$ and $\mathbb{Z}_n$ the cyclic group of order n, gen. by x.

Define $\varphi: \mathbb{Z} \to \mathbb{Z}_n$ by $a \longmapsto x^a$. (Check that φ is a homomorphism)

Then the fiber over x^k is $a \in \mathbb{Z}$ s.t. $a = bn + k$, $b \in \mathbb{Z}$.

i.e. $X_{x^k} = \{ a \in \mathbb{Z} \mid a \equiv k \pmod{n} \}$.

Thus, the quotient group here is $\mathbb{Z}/n\mathbb{Z}$.

Before we continue, let's take a detour to review homomorphisms.

Let $\varphi: G \to H$ be a homomorphism.

Basic properties of φ

- Recall the kernel of φ is

$$\ker \varphi := \{ g \in G \mid \varphi(g) = 1 \}$$

and the image of φ is

$$\operatorname{im} \varphi := \{ \varphi(g) \mid g \in G \}.$$

From the homework, $\ker \varphi \leq G$ and $\operatorname{im} \varphi \leq H$.

- $\varphi(1) = 1$ since $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$, so $\varphi(1)$ must be the identity.

(1 = identity in G; 1 = identity in H)

- If $g \in G$, $\varphi(g)^{-1} = \varphi(g^{-1})$:

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1) = 1, \text{ so } \varphi(g^{-1}) = \varphi(g)^{-1}.$$

- If $g \in G$, $\varphi(g^n) = \varphi(g)^n$, for $n \in \mathbb{Z}$.

This follows by induction for $n \geq 1$.

$n = 1$ is clear. Assume true for $n-1$.

Then $\varphi(g^n) = \varphi(g^{n-1} g) = \varphi(g^{n-1})\varphi(g) = \varphi(g)^{n-1}\varphi(g) = \varphi(g)^n$.

By the previous property, it holds for negative n as well.

Now we return to quotient groups:

Def: Let $\varphi: G \to H$ be a homomorphism with kernel K. The quotient group G/K is the group whose elements are the fibers of φ (over its image). If X_a is the fiber above a, X_b the fiber above b, then $X_a X_b = X_{ab}$, the fiber above ab.

Note: Why is the kernel K relevant here? K is the fiber over 1, so it is the identity in G/K. In fact, we'll see that all other elts of G/K are "translates" of K.

e.g. in $\mathbb{Z}/n\mathbb{Z}$, the kernel was $n\mathbb{Z}$, and the other fibers are of the form $a + n\mathbb{Z}$.

More precisely:

Thm: Let $\varphi: G \to H$ be a homomorphism w/ kernel K. Let $X \in G/K$ be the fiber above a. i.e. $X = \varphi^{-1}(a) = \{g \in G \mid \varphi(g) = a\}$.
Then for any $u \in X$, $X = \{uk \mid k \in K\} = \{ku \mid k \in K\}$.
(Note that this means for any other $u' \in X$, $\{uk \mid k \in K\} = \{u'k \mid k \in K\}$)

Pf: If $x \in X$, then $\varphi(x) = a = \varphi(u)$

$$\Rightarrow 1 = \varphi(u)^{-1}\varphi(x) = \varphi(u^{-1}x)$$

so $u^{-1}x \in K$, and $x = u(u^{-1}x)$, so $x \in \{uk \mid k \in K\}$.
($u^{-1}x$ in K)

Conversely, if $x \in \{uk \mid k \in K\}$, Then $x = uk$, some $k \in K$,

so $\varphi(x) = \varphi(uk) = \varphi(u)\varphi(k) = a \cdot 1 = a$, so $x \in X$.

Thus $X = \{uk \mid k \in K\}$. Similar reasoning shows that it's also equal to $\{ku \mid k \in K\}$ □

We can define sets of the form $\{uk \mid k \in K\}$ for <u>any</u> subgroup $K \leq G$, not just kernels of homomorphisms:

Def: Let $N \leq G$, $g \in G$. Define

$$gN := \{gn \mid n \in N\} \quad \text{and} \quad Ng := \{ng \mid n \in N\},$$

called, respectively, a <u>left coset</u> and a <u>right coset</u> of N in G. Any element of a coset is a <u>representative</u> for the coset.

(If G is an additive group, we'll write $g+N$ and $N+g$ for left and right cosets)

Ex: 1.) For $n\mathbb{Z} \leq \mathbb{Z}$, the cosets are $\{\underbrace{0+n\mathbb{Z}}_{n\mathbb{Z}}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}\}$

2.) For $\langle r \rangle \leq D_8$, the coset $s\langle r \rangle = \{s, sr, sr^2, sr^3\}$.

$$sr\langle r \rangle = \{sr, sr^2, sr^3, s\} = s\langle r \rangle.$$

In fact, we'll see that if $h \in gN$, then $hN = gN$. i.e. any representative gives the same coset.

We've seen that elements of a quotient group (i.e. fibers) are also cosets of the corresponding kernel. In fact, we can show that we can multiply cosets exactly how we expect:

Theorem: Let G be a group, and K be the kernel of some homomorphism $\varphi: G \to H$. Then the set of left cosets of H form a group w/ operation

$$(uK)\cdot(vK) = (uv)K,$$

and this defines the same group as G/K.

In particular this operation is well-defined so that if $u' \in uK$ and $v' \in vK$ s.t. $uK = u'K$ and $vK = v'K$, then $(uv)K = (u'v')K$.

Pf: Let $X, Y \in G/K$ and $Z = XY$ in G/K. We showed already that these are left cosets of K.

Let $X = \varphi^{-1}(a)$, $Y = \varphi^{-1}(b)$. Then $Z = \varphi^{-1}(ab)$, by definition.

We want to show that the operation defined on cosets gives the same result.

Let $x \in X$ and $y \in Y$ be arbitrary elts of the fibers, so

$$X = xK, \quad Y = yK.$$

We need to show that $(xy)K = Z$. i.e. that $xy \in Z$.

$\varphi(xy) = \varphi(x)\varphi(y) = ab$, so $xy \in Z \Rightarrow (xy)K = Z$.

Note that this didn't depend on the representatives we chose, which shows the operation is well-defined. □

Remark: We could've replaced "left coset" w/ "right coset" in the theorem.

Ex:

1.) If G is any group and $\varphi: G \to H$ is an isomorphism, then $\ker\varphi = 1$, and the fibers of φ are the singleton subsets of G, so $G/1 \cong G$.

2.) If $\psi: G \to 1$ is the trivial homomorphism, then $\ker\psi = G$, so G/G is a single element group, i.e. 1.

We've now shown how to define G/K if K is the kernel of some homomorphism. However, we showed that you can define the multiplication in the group w/out using the homomorphism at all. i.e. $(aK)(bK) = abK$. This raises a natural question:

Question: If $H \leq G$, can we define the quotient group G/H?

Answer: In general, no!! We will see why soon. In fact, we'll

show that the group operation on G/H is well-defined if and only if H is the kernel of a homomorphism. We'll soon give a criterion to determine when H is a kernel.

First, we'll show that for any subgroup, the following holds:

Prop: Let $N \leq G$. The set of left cosets of N in G form a partition of G.

Pf: For any $g \in G$, $g \in gN$, since $1 \in N$. Thus, the union of cosets is all of G.

Suppose $uN \neq vN$. WLOG, let $un \in uN$ but not in vN.

We want to show $uN \cap vN = \emptyset$. For the sake of contradiction, assume $g \in uN \cap vN$, then $g = ua = vb$

$\Rightarrow$ $un = uaa^{-1}b = vba^{-1}b \in vN$, a contradiction. Thus, the cosets form a partition. $\square$

Note: This means that u and v are in the same coset $\iff uN = vN \iff u = vn$, some $n \in N \iff v^{-1}u \in N$.

Prop: Let G be a group and $N \leq G$.

1.) The operation on left cosets $uN \cdot vN = uvN$ is well-defined if and only if $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$.

2.) If the above operation is well-defined, then the cosets form a group, w/ identity $1N = 1$, and $(gN)^{-1} = g^{-1}N$.

Pf: 1.) First assume it's well-defined. i.e. if $uN = u'N$ and $vN = v'N$ then $uvN = u'v'N$.

Let $g \in G$, $n \in N$. Then $1, n \in N$, so $1g^{-1}N = ng^{-1}N$

$$\Rightarrow gg^{-1}N = gng^{-1}N$$

$$\Rightarrow N = gng^{-1}N \Rightarrow gng^{-1} \in N.$$

Now we prove the converse. Assume $gng^{-1} \in N \ \forall \ n \in N, g \in G$.

Suppose $u, u' \in uN$ (i.e. $uN = u'N$) and $v, v' \in vN$.

We need to show $u'v' \in uvN$. For some $n, m \in N$, we have

$u'v' = (um)(vn) = uvv^{-1}mvn = uv(v^{-1}mv)n$.

$v^{-1}mv \in N$, $n \in N$, so $uv(v^{-1}mv)n \in uvN$, as desired.

2.) If the operation is well-defined, we just need to check the group axioms:

For $g \in G$, $1Ng N = 1gN = gN = gN1N$, so $1N$ is the identity.

$gNg^{-1}N = gg^{-1}N = 1N = g^{-1}gN = g^{-1}NgN$, so gN has inverse $g^{-1}N$.

If $a,b,c \in G_1$, associativity follows from associativity on G. □

So now we have a condition for when G/N is a group. More formally:

Def: gng^{-1} is the conjugate of $n \in N$ by g.

The set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is the conjugate of N by g.

g normalizes N if $gNg^{-1} = N$.

A subgroup $N \leq G$ is normal if every element of G normalizes N, and we write $N \trianglelefteq G$ to denote that N is a normal subgroup of G.

Sometimes it's hard to check $gNg^{-1} = N$, so we can use the following:

Thm: The following are equivalent:

1.) $N \trianglelefteq G$

2.) $gN = Ng \quad \forall \ g \in G$.

3.) $gNg^{-1} \subseteq N \quad \forall \ g \in G$.

Pf: Clearly 1.) $\Rightarrow$ 3.). For the rest, see HW #4.

Now we show that normal subgroups are exactly possible kernels of homomorphisms.

Theorem: $N \leq G$ is normal $\iff$ it is the kernel of a homomorphism.

Pf: If N is the kernel of a homomorphism, then we showed left cosets are the same as right cosets. Thus, the above shows $N \trianglelefteq G$.

Now assume $N \trianglelefteq G$. Then let $H = G/N$, and define

$$\varphi : G \to G/N \text{ by } \varphi(g) = gN$$

By the definition of the operation on G/N, if $g, h \in G$,

$\varphi(gh) = ghN = gNhN = \varphi(g)\varphi(h)$, so this is a homomorphism, and $\varphi(g) = 1N \iff gN = 1N \iff g \in N$, so $\ker \varphi = N$. $\square$

Ex:

1.) Any subgroup of an abelian group is normal since $ghg^{-1} = n \ \forall \ g, n \in G$.

In fact, if $N \leq Z(G)$, then N is normal in G since

every element of N commutes w/ every element of G.

2.) $Z(D_8) = \{1, r^2\}$, so $\langle r^2 \rangle \trianglelefteq D_8$.

The cosets in $D_8/\langle r^2 \rangle$ are the two element sets $\{g, gr^2\}$,

so there are 4 of them. i.e. $|D_8/\langle r^2 \rangle| = 4$.

Which group of order 4 is it isomorphic to?

$r^2 \in \langle r^2 \rangle$, so $|r\langle r^2 \rangle| = 2$ $\quad$ $s^2 = 1 \in \langle r^2 \rangle$, so $|s\langle r^2 \rangle| = 2$.

i.e. 2 distinct elements have order 2, so $D_8/\langle r^2 \rangle \not\cong \mathbb{Z}_4$.

Thus $D_8/\langle r^2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

3.) Let $H = \langle (123) \rangle \leq S_3$. Is $H \trianglelefteq S_3$? On HW: $H \trianglelefteq S_3 \Leftrightarrow N_{S_3}(H) = S_3$.

$(12)(123)(12) = (132) \in H$. Thus $(12) \in N_G(H)$.

$(12) = (12)^{-1}$

We know $\underset{\text{order } 3}{H} \leq \underset{\text{order} > 3}{N_{S_3}(H)} \leq \underset{\text{order } 6}{S_3}$ $\quad$ So $N_{S_3}(H) = S_3 \Rightarrow H \trianglelefteq S_3$.

$|S_3/H| = 2$, so $S_3/H \cong \mathbb{Z}_2$

Ex: (non-normal subgroup) Let $H = \langle (12) \rangle \leq S_3$.

$(13)(12)(13) = (23) \notin H$. Thus $N_{S_3}(H) \neq S_3$ (In fact it is just H), so

$H \ntrianglelefteq S_3$.