# MATH 3311, FALL 2025: LECTURE 14, SEPTEMBER 29

Video: `https://youtu.be/anbBkE7HBWQ`
Recall from last time:

**Proposition 1.** *If $f : G \to G'$ is a homomorphism of groups, then $\ker f \trianglelefteq G$ is a normal subgroup and there is a natural bijection*

$$G/\ker f \xrightarrow{\simeq} \mathrm{im}\, f$$

*which carries each left coset $g(\ker f)$ to $g \cdot e = f(g)e = f(g)$.*

*Remark* 1. Note that $\mathrm{im}\, f$ is a subgroup of $G'$ and so in particular is a group. This means that the above natural bijection also equips the set of cosets $G/\ker f$ with the structure of a *group*. In fact, since $f(g_1)f(g_2) = f(g_1g_2)$, the group structure is determined by the formula

$$g_1(\ker f) \cdot g_2(\ker f) = g_1g_2(\ker f).$$

This formula isn't always well-defined.

*Example* 1. Take $G = S_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ and $H = \langle\tau\rangle = \{e, \tau\}$.
Consider the 'product'

$$\sigma H \cdot \sigma^2 H = \sigma^3 H = eH = H.$$

If we instead wrote the first term as $\sigma\tau H$, then we would get

$$\sigma\tau H \cdot \sigma^2 H = \sigma\tau\sigma^2 H = \sigma^2\tau H = \sigma^2 H \neq H.$$

Here, we have used the formula $\tau\sigma^2 = \sigma\tau$, which is valid in $S_3 = D_6$.

Therefore, depending on *how* we write down the coset $\sigma H = \sigma\tau H$, we get *different* answers for the possible product. This shows that the operation is not well-defined.

The difference between this and the case of a kernel is that the latter is always normal, while $H = \langle\tau\rangle \leq S_3$ is *not*:

$$\sigma\tau\sigma^{-1} = \sigma\tau\sigma^2 = \sigma\sigma\tau = \sigma^2\tau \notin H.$$

But normality fixes everything.

**Proposition 2.** *Suppose that $H \trianglelefteq G$ is a normal subgroup. Then:*

1. *The operation*

$$\begin{aligned} G/H \times G/H &\to G/H \\ (g_1H, g_2H) &\mapsto g_1g_2H \end{aligned}$$

*is well-defined.*

2. *This operation equips $G/H$ with the structure of a group with identity given by the coset $H$.*
3. *The function*

$$\begin{aligned} \pi : G &\to G/H \\ g &\mapsto gH \end{aligned}$$

*is a surjective homomorphism.*

*Proof.* Suppose that we have $h \in H$. Then we have $g_1H = g_1hH$ and $g_2H = g_2hH$. We have:

$$(g_1H)(g_2hH) = g_1g_2hH = g_1g_2H;$$

$$\begin{aligned}(g_1hH)(g_2H) &= g_1hg_2H \\ &= g_1(g_2g_2^{-1})hg_2H \\ &= g_1g_2(g_2^{-1}hg_2)H \\ &= g_1g_2H.\end{aligned}$$

Here in the last equality we have used the fact that $g_2^{-1}hg_2 \in H$ by the normality of $H$.

Thus, no matter how we represent our cosets our answer in the end is the same: $g_1g_2H$. This shows well-definedness.

To see that this equips $G/H$ with the structure of a group, we need to check:

(1) (Identity) $H \cdot gH = eH \cdot gH = egH = gH$.
(2) (Associativity)
$$g_1H(g_2H \cdot g_3H) = g_1H \cdot g_2g_3H = g_1(g_2g_3)H = (g_1g_2)g_3H = g_1g_2H \cdot g_3H = (g_1H \cdot g_2H) \cdot g_3H.$$
(3) (Inverses) $g^{-1}H \cdot gH = g^{-1}gH = eH = H$.

Finally, the fact that $\pi : G \to G/H$ is a surjection is clear, and that it is a homomorphism is just:

$$\pi(g_1)\pi(g_2) = g_1H \cdot g_2H = g_1g_2H = \pi(g_1g_2).$$

$\square$

*Remark* 2. The proof of (1) above shows that, in order for the group operation on $G/H$ to be well-defined, we must have $g_2^{-1}hg_2 \in H$ for all $g_2 \in G$ and $h \in H$. This is of course just saying that $H$ is normal. In other words, normality is both *necessary* and *sufficient* for the group operation on $G/H$ to be well-defined.

**Definition 1.** If $H \trianglelefteq G$ is a normal subgroup, the set $G/H$ equipped with the group operation above is called **the quotient of** $G$ **by** $H$, and the homomorphism $\pi : G \xrightarrow{g \mapsto gH} G/H$ is called the **quotient homomorphism**.

*Example* 2. In H@ 5, it is shown that any subgroup of an abelian group is normal.

In particular, $n\mathbb{Z} \leq \mathbb{Z}$ is normal. Here, the quotient group $\mathbb{Z}/n\mathbb{Z}$ is just what we already know, and the quotient homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is the function carrying each integer $a$ to $a (\mathrm{mod}\ n) = a + n\mathbb{Z}$.