18MAA242 Lecture 22

Normal subgroups + Quotients, 2

Last time: a subgroup $H \subset G$ is normal if left & right cosets coincide: $gH = Hg \quad \forall g$

or equivalently $ghg^{-1} \in H \quad \forall g \in G, h \in H$.

We saw: if $H \subset G$ is normal, then the set of cosets G/H is a group: $(g_1 H)(g_2 H) = g_1 g_2 H$.

Homomorphisms + Quotients

Let $\varphi : G \to G'$ be a homomorphism, meaning

$$(*) \quad \varphi(xy) = \varphi(x)\varphi(y) \quad \forall x, y \in G.$$

Definition: Then kernel of φ is the set

$$\mathrm{Ker}(\varphi) = \{ g \in G \mid \varphi(g) = e \}$$

The image of φ is the set

$$\mathrm{Im}(\varphi) = \{ g' \in G' \mid g' = \varphi(g) \text{ for some } g \in G \}$$

Example: If $G = V$ and $G' = V'$ vector spaces and $\varphi: V \to V'$ a linear map, then

$\mathrm{Ker}(\varphi)$ and $\mathrm{Im}(\varphi)$ are exactly as defined in the linear algebra module:

$$\mathrm{Ker}(\varphi) = \{ v \in V \mid \varphi(v) = \underset{\substack{\text{identity element}\\ \text{for } + \text{ in } V'}}{0} \}$$

$$\mathrm{Im}(\varphi) = \{ v' \in V' \mid v' = \varphi(v) \text{ for some } v \in V \}.$$

In that context you know the rank-nullity theorem: $\dim \mathrm{Ker}(\varphi) + \dim \mathrm{Im}(\varphi) = \dim V$.

In fact there is a more general result, valid for all homomorphisms:

Theorem (Homomorphism Theorem):

Let $\varphi: G \to G'$ be a group homomorphism.

Then 1) $\mathrm{Ker}(\varphi)$ is a normal subgroup of G

2) The map $\tilde{\varphi}: G/\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi)$

$$g\,\mathrm{Ker}(\varphi) \mapsto \varphi(g)$$

is an isomorphism.

Sketch Proof:

1) First need to prove $Ker(\varphi)$ and $Im(\varphi)$ are subgroups of G, G' respectively. See the Problem Sheet.

2) Why is $Ker(\varphi)$ normal? For any $g \in G$, $k \in Ker(\varphi)$ we have

$$\varphi(gkg^{-1}) \overset{(*)}{=} \varphi(g)\varphi(k)\varphi(g^{-1})$$
$$= \varphi(g)e'\varphi(g)^{-1}$$
$$= e'.$$

So $gkg^{-1} \in Ker(\varphi)$.

3) Why is $\tilde{\varphi} : G/Ker(\varphi) \longrightarrow Im(\varphi)$ an isomorphism?

First check it is a homomorphism: write K for $Ker(\varphi)$; then we have

$$\tilde{\varphi}((xK)(yK)) = \tilde{\varphi}((xy)K)$$
$$= \varphi(xy) = \varphi(x)\varphi(y)$$
$$= \tilde{\varphi}(xK)\tilde{\varphi}(yK).$$

Surjective: immediate, since any element of $\mathrm{Im}(\tilde{\varphi})$ looks like $\varphi(g)$ (some $g \in G$), and

$$\varphi(g) = \tilde{\varphi}(gK).$$

Injective: if $\tilde{\varphi}(g_1K) = \tilde{\varphi}(g_2K)$

then $\varphi(g_1) = \varphi(g_2)$,

hence $\varphi(g_1^{-1}g_2) = e'$

so $g_1^{-1}g_2 \in K$,

hence $g_1K = g_2K$. ■

So $\tilde{\varphi}$ is indeed an isomorphism:

$$G/_{\mathrm{Ker}(\varphi)} \cong \mathrm{Im}(\varphi).$$

Example: $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$

$$K \longmapsto K \bmod m$$

$\mathrm{Im}(\varphi) = \mathbb{Z}_m$, $\mathrm{Ker}(\varphi) = m\mathbb{Z} = \{mn \mid n \in \mathbb{Z}\}$

So $\mathbb{Z}/_{m\mathbb{Z}} \cong \mathbb{Z}_m$.

What's next? (Non-examinable!)

Simple groups — group-theoretic counterpart of prime numbers.

A group G is simple if its only normal subgroups are $\{e\}$ and G.

By using quotients, every group can be "broken down" into simple groups.

Can we classify simple groups?

This was a major area of research in 20^{th} century pure mathematics.

Solution completed (?) during 1955-2004, spanning more than 10,000 journal pages.

Every finite simple group is isomorphic to one of the following:

- cyclic groups $\mathbb{Z}_p$, p prime
- alternating groups A_n, $n \geq 5$
- groups "of Lie type" (groups of matrices with entries in $\mathbb{Z}_p$)
- 26 "sporadic" groups : the largest is the "Monster" M, with order

$$|M| \approx 8 \times 10^{53} \qquad \text{(Fischer-Griess, 1973)}.$$