Lecture 13 Quotient groups and homomorphisms

- Equivalence relation: a relation $\sim$ on a set X which is
  reflexive: $a \sim a$
  symmetric: $a \sim b \Rightarrow b \sim a$
  transitive: $a \sim b$ and $b \sim c \Longrightarrow a \sim c$.

- Partition: A collection Ω of subsets of X which are pairwise disjoint and whose union is all of X.

- For any equivalence relation $\sim$ on X the collection
  $\Omega = \{ [a] \mid a \in X \}$ where $[a] = \{ b \mid a \sim b \}$
  is a partition of X.

<u>Proposition</u>: let G be a group, $H \leq G$ a subgroup.
Define a relation by $a \sim b \Leftrightarrow a^{-1}b \in H$.
Then $a \sim b$ is an equivalence relation and the equivalence classes are the left cosets $\{ aH \mid a \in G \}$

<u>Proof</u>: Reflexive: $a \sim a \Leftrightarrow a^{-1}a \in H$. But $a^{-1}a = e \in H$ since H is a subgroup.

Symmetric $a \sim b$ means $a^{-1}b \in H$. Then $(a^{-1}b)^{-1} = b^{-1}a \in H$ so $b \sim a$

Transitive $a \sim b$ and $b \sim c$ mean $a^{-1}b \in H$ and $b^{-1}c \in H$ then $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$, so $a \sim c$.

Proposition 2.5.3 says $a^{-1}b \in H$ iff $b \in aH$
so $[a] = \{ b \mid a \sim b \} = \{ b \mid a^{-1}b \in H \} = \{ b \mid b \in aH \} = aH$ $\blacksquare$

Notation: We denote by $G/H = \{aH \mid a \in G\}$ the set of left cosets of H in G.

There is a natural surjective function $\pi : G \to G/H$
$\pi(a) = aH$.

We would like to make G/H into a group in such a way that π becomes a homomorphism. This is only possible if H is a normal subgroup of G.

Let $N \leq G$ be a normal subgroup of G. We use the notation $N \triangleleft G$ to indicate that N is normal.

To define a product on $G/N = \{aN \mid a \in G\}$, we would like to define $(aN)(bN) = (ab)N$, but we need to check this is well defined, that it does not depend on how we represent a coset as aN for some $a \in G$:

Proof of well-definedness: Let a, a' be elements of the same coset, so $aN = a'N$, and let b, b' be such that $bN = b'N$.
We must check that $(ab)N = (a'b')N$.
We can write $a = a'n_1$ and $b = b'n_2$ for some $n_1, n_2 \in N$
Then $ab = a'n_1 b'n_2 = a'b'(b')^{-1}n_1 b'n_2$
$= (a'b')\left((b')^{-1}n_1 b'\right)n_2$
but $(b')^{-1}n_1 b' \in N$ because N is normal:
(Normal means $gng^{-1} \in N$ for $n \in N$ and $g \in G$; apply with $g = (b')^{-1}$
So $n = ((b')^{-1}n_1 b')n_2 \in N$, and $ab = a'b'n \in (a'b')N$
Therefore $ab \sim a'b'$ and $abN = (a'b')N$.

Theorem Let $N \trianglelefteq G$ be a normal subgroup. Then $(aN)(bN) = (ab)N$ makes G/N into a group. $\pi: G \to G/N$ $\pi(a) = aN$ is a homomorphism, and $\ker(\pi) = N$.

Proof Associativity: $[(aN)(bN)](cN) = ((ab)N)(cN) = ((ab)c)N$
$= (a(bc))N = (aN)((bc)N) = (aN)[(bN)(cN)]$

Identity: $\left.\begin{array}{l} N aN = (eN)(aN) = (ea)N = aN \\ aN \cdot N = (aN)(eN) = (ae)N = aN \end{array}\right\}$ so $N = eN$ is identity

Inverse: $\left.\begin{array}{l} (a^{-1}N)(aN) = (a^{-1}a)N = eN = N \\ (aN)(a^{-1}N) = (aa^{-1})N = eN = N \end{array}\right\}$ so $(aN)^{-1} = a^{-1}N$

π is homomorphism: $\left.\begin{array}{l} \pi(ab) = (ab)N \\ \pi(a)\pi(b) = (aN)(bN) = (ab)N \end{array}\right\}$ Indeed equal.

$\ker(\pi) = \{a \in G \mid \pi(a) = N\} = \{a \mid aN = N\} = \{a \mid a \in N\} = N$

Remark: The binary operation $(aN)(bN) = (ab)N$ is the only possible one that could make $\pi: G \to G/N$ $\pi(a) = aN$ into a group homomorphism.

We call G/N the <u>quotient group</u> of G by N, and read it "G mod N". We call $\pi: G \to G/N$ the <u>quotient homomorphism</u>.

Example $\langle n \rangle = n\mathbb{Z} \subseteq \mathbb{Z}$ is a subgroup. It is normal because $\mathbb{Z}$ is abelian. Then $\mathbb{Z}/\langle n \rangle = \{[k]_n \mid k \in \mathbb{Z}\}$, where $[k]_n = \{k + qn \mid q \in \mathbb{Z}\}$ is the congruence class of k mod n.
So $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$, and $\pi: \mathbb{Z} \to \mathbb{Z}_n$, $k \mapsto [k]_n$ is the quotient homomorphism.

Example $\mathbb{Z} \subseteq \mathbb{R}$ is a subgroup, normal since $\mathbb{R}$ is abelian. We can thus form $\mathbb{R}/\mathbb{Z}$. How should we think about this.

Recall the group $\mathcal{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ of unit complex numbers.
any $z \in \mathcal{U}$ is of the form $z = e^{i\theta}$ for some $\theta \in \mathbb{R}$.
There is a homomorphism $\varphi : \mathbb{R} \to \mathcal{U}$ $\varphi(t) = e^{2\pi i t}$
$\varphi(s+t) = e^{2\pi i (s+t)} = e^{2\pi i s} e^{2\pi i t} = \varphi(s)\varphi(t)$.
This homomorphism is surjective, and its kernel is
$\ker(\varphi) = \{t \in \mathbb{R} \mid e^{2\pi i t} = 1\} = \{t \in \mathbb{R} \mid 2\pi i t = 2\pi i k \text{ for } k \in \mathbb{Z}\}$
$= \mathbb{Z}$.

On the other hand, $\pi : \mathbb{R} \to \mathbb{R}/\mathbb{Z}$ is another surjective homomorphism whose kernel is $\mathbb{Z}$.

In fact, $\mathbb{R}/\mathbb{Z}$ is isomorphic to $\mathcal{U}$:
Define $\overline{\varphi} : \mathbb{R}/\mathbb{Z} \to \mathcal{U}$ $\overline{\varphi}(t+\mathbb{Z}) = e^{2\pi i t}$

Well-defined? If $t + \mathbb{Z} = t' + \mathbb{Z}$ then $t' = t + n$, $n \in \mathbb{Z}$.
so $e^{2\pi i t'} = e^{2\pi i t} e^{2\pi i n} = e^{2\pi i t} \cdot 1 = e^{2\pi i t}$, so yes.

Homomorphism? $\overline{\varphi}((s+\mathbb{Z}) + (t+\mathbb{Z})) = \overline{\varphi}((s+t)+\mathbb{Z}) = e^{2\pi i (s+t)} = e^{2\pi i s} e^{2\pi i t}$
$\overline{\varphi}(s+\mathbb{Z})\overline{\varphi}(t+\mathbb{Z}) = e^{2\pi i s} e^{2\pi i t}$ so yes.

Surjective? Yes since each $z \in \mathcal{U}$ is $e^{2\pi i t}$ for some $t \in \mathbb{R}$.
Injective? If $\overline{\varphi}(s+\mathbb{Z}) = \overline{\varphi}(t+\mathbb{Z})$, then $e^{2\pi i s} = e^{2\pi i t}$
then $e^{2\pi i (s-t)} = 1$, so $s - t \in \mathbb{Z}$. then $s + \mathbb{Z} = t + \mathbb{Z}$,
so s and t represent the same element of $\mathbb{R}/\mathbb{Z}$.
So $\overline{\varphi} : \mathbb{R}/\mathbb{Z} \to \mathcal{U}$ is an isomorphism.

Observe that among
$$\begin{tikzcd} \mathbb{R} \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \mathcal{U} \\ \mathbb{R}/\mathbb{Z} \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd}$$
we have the relation $\overline{\varphi} \circ \pi = \varphi$

Quotient group isomorphism theorem

We can generalize the example $\mathbb{R}/\mathbb{Z} \cong U = \{e^{2\pi i t} \mid t \in \mathbb{R}\}$ as follows:

<u>Theorem 2.7.6</u>: Let $\varphi : G \to \overline{G}$ be a surjective homomorphism of groups. Let $N = \ker(\varphi)$. Let G/N be the quotient group, and let $\pi : G \to G/N$ be the quotient homomorphism.
Then: $\overline{G}$ is isomorphic to G/N.
More precisely, there is a unique isomorphism $\tilde{\varphi} : G/N \to \overline{G}$ satisfying $\tilde{\varphi} \circ \pi = \varphi$;

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \overline{G} \\ G/N \arrow[ur, "\tilde{\varphi}"'] & \end{tikzcd}$$

<u>Proof</u>: Want to define $\tilde{\varphi} : G/N \to \overline{G}$ by $\tilde{\varphi}(aN) = \varphi(a)$
Need to show this is well defined:
$aN = a'N \Rightarrow a' = an$ for some $n \in N$
$\Rightarrow \varphi(a') = \varphi(an) = \varphi(a)\varphi(n) = \varphi(a)e = \varphi(a)$
so $\tilde{\varphi}(aN) = \varphi(a) = \varphi(a') = \tilde{\varphi}(a'N)$,
and the definition is consistent.

Homomorphism? $\tilde{\varphi}((aN)(bN)) = \tilde{\varphi}((ab)N) = \varphi(ab)$
$= \varphi(a)\varphi(b) = \tilde{\varphi}(aN)\tilde{\varphi}(bN)$ Yes!

Surjective? If $g \in \overline{G}$, $g = \varphi(a)$ for some $a \in G$ since φ is surjective, so $g = \tilde{\varphi}(aN)$ as well, so Yes!

Injective? Recall homomorphism is injective iff kernel is trivial.
$\ker(\tilde{\varphi}) = \{aN \mid \tilde{\varphi}(aN) = e\} = \{aN \mid \varphi(a) = e\}$
$= \{aN \mid a \in \ker\varphi\} = \{aN \mid a \in N\}$
$= \{N\}$ this is the identity element of G/N, so Yes!

Lastly we check $\tilde{\varphi} \circ \pi = \varphi$: $(\tilde{\varphi} \circ \pi)(a) = \tilde{\varphi}(\pi(a))$
$= \tilde{\varphi}(aN) = \varphi(a)$, so Yes! $\blacksquare$

This theorem says that there is an intimate connection between quotient groups and surjective homomorphisms.