Lecture 13 Constructing groups

External direct product

Let G_1 and G_2 be two groups.

We define a binary operation on $G_1 \times G_2$ by setting

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2)$$

where $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$

$G_1 \times G_2$ is a group under this binary operation.

The identity element is $(1_{G_1}, 1_{G_2})$.

The inverse of (x, y) is (x^{-1}, y^{-1}).

This group is denoted by $G_1 \times G_2$ or $G_1 \oplus G_2$.

Example

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} = \{(\bar{0},\bar{0}), (\bar{1},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{1}), (\bar{0},\bar{2}), (\bar{1},\bar{2})\}$$

Exercise: Check that $\operatorname{ord}(\bar{1},\bar{1}) = 6$.

Thus, this is a cyclic group of order 6.

Thus $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$.

Example

Exercise: $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is a group of order 4. Check that it has no element of order 4. So, this group is not cyclic.

Group homomorphisms

Let G and H be groups.

A group homomorphism from G to H is a function $\varphi : G \to H$ such that

$$\varphi(g_1 g_2) = \varphi(g_1) \cdot \varphi(g_2)$$

for $g_1, g_2 \in G$.

Example

1) Any group isomorphism is a group homomorphism.
2) Let m be a positive integer. The function $f: \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ defined by $f(n) = n + m\mathbb{Z}$ is a group homomorphism.

3) $G = \mathbb{R}^{\times}$ (group of non-zero real numbers under multiplication)

$H = (\mathbb{R}_{>0}, \times)$

(group of <u>positive</u> real numbers under multiplication).

Let $f : G \longrightarrow H$ be given by $f(x) = |x|$. This is a homomorphism

Easy results

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

(1) $\varphi(1_G) = 1_H$.

Proof: $\varphi(1_G) = \varphi(1_G \cdot 1_G) = \varphi(1_G) \cdot \varphi(1_G)$

So $\varphi(1_G) = 1_H$. //

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

<u>Proof</u>: $\varphi(x^{-1}) \cdot \varphi(x) = \varphi(x \cdot x^{-1})$

$= \varphi(1_G) = 1_H$

So $\varphi(x^{-1}) = \varphi(x)^{-1}$ //

Kernel and image

Definition: Let $\varphi : G \to H$ be a group homomorphism. The **kernel of φ**, denoted by $\ker(\varphi)$ is defined as

$$\ker(\varphi) = \{ g \mid g \in G,\ \varphi(g) = 1_H \}.$$

The <u>image of φ</u>, denoted by $\mathrm{im}(\varphi)$ is

$$\mathrm{im}(\varphi) = \{h \mid h \in H,\ h = \varphi(g) \text{ for some } g \in G\}$$

<u>Easy exercise</u>: $\mathrm{Ker}(\varphi)$ is a subgroup of G. $\mathrm{Im}(\varphi)$ is a subgroup of H.

Example

Let $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$, given by $\varphi(n) = n + m\mathbb{Z}$.

Then, $\ker(\varphi) = m\mathbb{Z}$.

Example

$\varphi : \mathbb{R}^{\times} \longrightarrow \mathbb{R}^{\times}$

$\varphi(x) = x^2$. Then, φ is a homomorphism. $\ker(\varphi) = \{1, -1\}$.

$\mathrm{Im}(\varphi) = (\mathbb{R}_{>0}, \times)$.

A generalization

We have seen that the set of cosets of $m\mathbb{Z}$ in $\mathbb{Z}$ forms a group.

Can this work for any group G and subgroup $H \leq G$?

Let G be a group and $H \subseteq G$ a subgroup.
We want to define a binary operation on G/H by mapping (g_1H, g_2H) to g_1g_2H. Does this work?

Obstacle:

Suppose g_1' and g_2' are such that $g_1 H = g_1' H$ and $g_2 H = g_2' H$.

By our proposed definition $g_1' H \cdot g_2' H$ should be $g_1' g_2' H$.

So, we must have

$g_1 g_2 H = g_1' g_2' H$ whenever $g_1 H = g_1' H$ and $g_2 H = g_2' H$.

Recall: When is $xH = yH$?
This happens if and only if $y \in xH$, i.e. $y = xh$ for some $h \in H$.

So, if $g_1' = g_1 h_1$ and $g_2' = g_2 h_2$ for some $h_1, h_2 \in H$, we would like to have

$$g_1 h_1 g_2 h_2 = g_1 g_2 h \quad \text{for some } h \in H.$$

This happens if and only if

$$(g_1 h_1 g_2 h_2)^{-1} g_1 g_2 \in H .$$

$$(g_1 h_1 g_2 h_2)^{-1} g_1 g_2 = (h_2^{-1} g_2^{-1} h_1^{-1} g_1^{-1}) g_1 g_2$$
$$= h_2^{-1} (g_2^{-1} h_1^{-1} g_2)$$

This element is in H

$\Longleftrightarrow \quad g_2 h_1 g_2^{-1} \in H.$

We need this to happen for any choice of $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

Normal subgroups

Let G be a group and let H be a subgroup of G. We say that H is a normal subgroup if $gHg^{-1} \subseteq H$ for all $g \in G$.

Example

Consider the subgroup H of D_3 defined by $H = \{1, \rho, \rho^2\}$

H is a normal subgroup.

If $g \in H$, clearly $gHg^{-1} \subseteq H$.

If $g \notin H$, g is a reflection.

For any i, $g\rho^i g^{-1}$ is a rotation.

(Do you see why?)

Example

Let G be an abelian group. Then, any subgroup H of G is a normal subgroup.

Non-example

The subgroup $\{1, \tau\}$ of D_3 is not normal as $\rho\tau\rho^{-1} = \rho^2\tau \notin \{1, \tau\}$.

Center of a group

<u>Example</u> For any group G, the set $Z(G) = \{z \mid z \in G,\ zg = gz \text{ for all } g \in G\}$.

$Z(G)$ is a subgroup of G.

If $z \in Z(G)$ and $g \in G$, we have $gzg^{-1} = zgg^{-1} = z \in Z(G)$.

Thus, $Z(G)$ is a normal subgroup.

Basic properties

Proposition 1 Let G be a group and let H be a normal subgroup of G. Then, for any $g \in G$, we have $gHg^{-1} = H$.

Proof

By definition, for any $g \in G$, $g^{-1}H(g^{-1})^{-1} \subseteq H$.

So $g^{-1}Hg \subseteq H$.

So $g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1}$.

So $H \subseteq gHg^{-1}$. But we also have $gHg^{-1} \subseteq H$. So $H = gHg^{-1}$ //

Proposition 2 Let G be a group and $H \subseteq G$ be a normal subgroup. Then, for any $g \in H$, we have

$$gH = Hg.$$

Thus

$$\underset{\text{(left cosets)}}{G/H} = \underset{\text{(right cosets)}}{H\backslash G}$$

<u>Proof</u> Any element of gH is of the form gh for some $h \in H$.

Then, $gh = gh(g^{-1}g) = (ghg^{-1}) \cdot g$.

But $ghg^{-1} \in H$ as H is normal.

So, $(ghg^{-1})g \in Hg$.

Thus $gH \subseteq Hg$.

On the other hand, any element of Hg is of the form hg for some $h \in H$.

But, $hg = g(g^{-1}hg)$.

As $g^{-1}hg \in H$, $hg = g(g^{-1}hg) \in gH$.

So $Hg \subseteq gH$.

Thus $gH = Hg$. //

Quotient group (factor group)

Let G be a group and let $H \subseteq G$ be a normal subgroup. We define a binary operation

$$G/H \times G/H \longrightarrow G/H$$

by mapping $(g_1 H, g_2 H)$ to $g_1 g_2 H$.

This definition does not depend on the choice of g_1 and g_2 as representatives of the cosets $g_1 H$ and $g_2 H$.

Indeed, if $g_1' H = g H$ and $g_2' H = g_2 H$, $g_1' = g_1 h_1$ and $g_2' = g_2 h_2$ where $h_1, h_2 \in G$.

$$g_1h_1g_2h_2 = g_1(g_2g_2^{-1})h_1g_2h_2$$
$$= g_1g_2(g_2^{-1}h_1g_2)h_2$$

As $g_2^{-1}h_1g_2 \in H$ (since H is normal), $g_1h_1g_2h_2 \in g_1g_2H$.

So $g_1'g_2' \in g_1g_2H$.

So $g_1'g_2'H = g_1g_2H$.

<u>Claim</u> With this operation, G/H is a group.

<u>Proof:</u>

<u>Identity</u>: H is the identity.

Indeed, $H \cdot gH = (1H) \cdot (gH)$

$= (1 \cdot g)H = gH.$

Similarly, $gH \cdot H = gH.$

Inverses $gH \cdot g^{-1}H = gg^{-1}H = H$.

Similarly, $g^{-1}H \cdot gH = g^{-1}gH = H$.

So $g^{-1}H$ is the inverse of gH.

Associativity

$$(g_1H \cdot g_2H) \cdot g_3H = ((g_1g_2) \cdot H) \cdot g_3H$$

$$= (g_1g_2) \cdot g_3H = g_1(g_2g_3)H$$

$$= g_1H \cdot g_2g_3H = g_1H(g_2H \cdot g_3H).$$

The set G/H with this binary operation is called the <u>factor group</u> or <u>quotient group</u> <u>of G by H.</u>

Theorem: Let $\varphi : G \longrightarrow H$ be a group homomorphism. Then $\ker(\varphi)$ is a normal subgroup of G.

Proof: Let $x \in \ker(\varphi)$ and $g \in G$. Then $\varphi(g x g^{-1}) = \varphi(g) \cdot \varphi(x) \cdot \varphi(g^{-1})$

$$= \varphi(g)\cdot 1_H \cdot \varphi(g^{-1})$$
$$= 1_H$$

So $gxg^{-1} \in \ker(\varphi)$ for all $x \in \ker(\varphi)$.

Thus, $\ker(\varphi)$ is a normal subgroup of G. //