

Proposition: (Kernels are normal) Let

G, H be groups and

$\varphi: G \rightarrow H$ a homomorphism.

Then $\ker(\varphi) \triangleleft G$.

proof: We already know $\ker(\varphi) \subseteq G$.

We need to show

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

$\forall x \in G$.

Take $y \in \ker(\varphi)$, consider

$$x \cdot y \cdot x^{-1} \text{ for } x \in G.$$

Then

$$\varphi(xy \cdot x^{-1})$$

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

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

$$= \varphi(x) \cdot \underbrace{e_H}_{\text{since } y \in \ker(\varphi)} \cdot \varphi(x)^{-1}$$

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

$$= e_H$$

$$\Rightarrow xyx^{-1} \in \ker(\varphi)$$

$$\text{and } x \in G, y \in \ker(\varphi).$$

So we have

$$x \ker(\varrho) x^{-1} \subseteq \ker(\varrho)$$

We want to show

$$\ker(\varrho) \subseteq x \ker(\varrho) x^{-1}$$

Let $y \in \ker(\varrho)$. Then

$$y = (\underbrace{x \cdot x^{-1}}_{e_6}) \cdot y \cdot (\underbrace{x \cdot x^{-1}}_{e_6})$$

$$= x \cdot (x^{-1} \cdot y \cdot x) \cdot x^{-1}$$

From the first direction, since

$$y \in \ker(\varrho),$$

$$x' \cdot y \cdot x \in \ker(\varphi)$$

$$\text{Set } k = x^{-1} \cdot y \cdot x$$

Then

$$y = x \cdot k \cdot x^{-1} \in x \ker(\varphi) x^{-1}$$

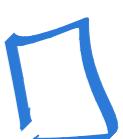
$$\Rightarrow \ker(\varphi) \subseteq x \ker(\varphi) x^{-1}$$

Therefore, we have the desired

$$\text{equality } \ker(\varphi) = x \ker(\varphi) x^{-1}$$

$\forall x \in G$, and so

$$\ker(\varphi) \triangleleft G$$



Remark: The converse of the previous proposition is also true!

Namely, $H \triangleleft G$ if
and only if \exists a group
 K and a homomorphism
 $\varphi: G \rightarrow K$ with $H = \ker(\varphi)$.

But the converse requires
more machinery to prove...

Caution: If $H \trianglelefteq G$ and

$x H x^{-1} = x$ for some

$x \in G$, it does **NOT**

follow that $xyx^{-1} = y$

for all $y \in H$.

Example: $G = S_3$, $H = \langle (123) \rangle$.

Then in fact,

$H \trianglelefteq G$, so

$x H x^{-1} = x \quad \forall x \in G$.

But if $x = (12)$,

$$(18)(123)(12)^{-1}$$

$$= (12)(123)(12)$$

$$= (132) \neq (123)$$

Nevertheless, $(132) \in H$, since

$$(132) = (123)^{-1}.$$

Back to Symmetric Groups

Recall: (S_n and cycle notation)

$S_n =$ all bijections on an n -element set, with the group operation of function composition

We use cycle notation to

describe elements of S_n , where

$(x_1 x_2 \cdots x_k)$ represents

a cycle for $k \leq n$ and

$\{x_1, x_2, \dots, x_n\}$ distinct elements of the n -element set -

Lemma: (transposition decomposition) Let $\alpha \in S_n$. Then every $\sigma \in S_n$ can be expressed as a product of transpositions, where a transposition is a cycle of length 2:

$$(x_1 x_2), \text{ with } x_1, x_2 \in \{1, 2, \dots, n\}, \\ x_1 \neq x_2$$

proof: Recall that every $\sigma \in S_n$ is the product of disjoint cycles.

Therefore, it suffices to prove
the result when σ is a
cycle.

Fix $n \in \mathbb{N}$. We will induct
on the length of the
cycle σ . Let k be the
length of a cycle in S_n , $\sigma \in S_n$.

$$\underline{k=1} \quad \sigma = \text{identity}$$

$$\sigma = (12)(12) = \text{identity}$$

is a product of transpositions.

$k=2$ σ itself is a transposition!

$k=3$ $\sigma = (x_1 \ x_2 \ x_3)$

$$\sigma = (x_1 \ x_2) (x_2 \ x_3) \checkmark$$

$k=4$ $\sigma = (x_1 \ x_2 \ x_3 \ x_4)$

$$\sigma = (x_1 \ x_2) (x_2 \ x_3 \ x_4) \checkmark$$

by the $k=3$

case, $(x_2 \ x_3 \ x_4)$

is a product of
transpositions.

General k

Suppose we know that

for any cycle of length

$k-1$ for $k \in \mathbb{N}, k \geq 5$,

the cycle may be expressed

as a product of transpositions.

Then let

$\sigma = (x_1 x_2 \cdots x_n)$ be

a cycle of length k in S_n .

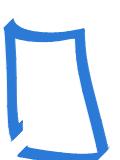
$$\sigma = (x_1 x_2) (\underbrace{x_2 x_3 \cdots x_n}_{\text{length } k-1 \text{ cycle}}) \checkmark$$

By induction,
 $(x_2 x_3 \cdots x_k)$ can be
expressed as a product
of transpositions, and

$$\text{so } \sigma = (x_1 x_2) (x_2 x_3 \cdots x_k)$$

can also be expressed as a
product of transpositions.

Note: $(x_1 x_2 x_3 \cdots x_k)$
 $= (x_1 x_2) (x_2 x_3) (x_3 x_4) \cdots (x_{k-1} x_k)$



Definition: (sign on S_n , notation) If

$\sigma \in S_n$, define the sign

of σ , denoted by $\varepsilon(\sigma)$,

to be

$$\varepsilon(\sigma) = \begin{cases} 1, & \text{if } \sigma \text{ can be expressed as a product} \\ & \text{of an even number of} \\ & \text{transpositions} \\ -1, & \text{if } \sigma \text{ can be expressed as a} \\ & \text{product of an odd number} \\ & \text{of transpositions} \end{cases}$$

Observe that, under multiplication,

$\{1, -1\}$ is isomorphic to \mathbb{Z}_2 .

If $\varepsilon(\sigma) = 1$, we say σ is

even. If $\varepsilon(\sigma) = -1$, we say σ

is **odd**.

ε is a homomorphism since \forall

$\sigma, \tau \in S_n$, if

(i) σ and τ are both even,

then $\sigma\tau$ can be expressed as

a product of an **even** number
of transpositions, so

$$1 = \varepsilon(\sigma\tau) = \varepsilon(\sigma) \cdot \varepsilon(\tau) = 1 \cdot 1$$

2) σ and τ are both odd,
then $\sigma\tau$ can be expressed
as a product of an even
number of transpositions,

so

$$1 = \varepsilon(\sigma\tau) = \varepsilon(\sigma) \varepsilon(\tau) = (-1) \cdot (-1)$$

3) one of σ or τ is even
and the other is odd, then
 $\sigma\tau$ can be expressed as
a product of an odd
number of transpositions, so

$$-\mathbb{1} = \varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau) = \mathbb{1} \cdot (-1)$$

Big \mathcal{Q} : Is ε well-defined?