Prop: $(G, \cdot)$ gruppo, H e K 2 sottogruppi allora $H \cap K$ é un sottogruppo.

oss: in generale, l'unione di sottogruppi non é un sottogruppo:

(contro)es: In $(\mathbb{Z}, +)$, $3\mathbb{Z}$ e $7\mathbb{Z}$

$3\mathbb{Z} \cup 7\mathbb{Z} = H$

$7 \in 7\mathbb{Z} \Longrightarrow 7 \in H$

$3 \in 3\mathbb{Z} \Longrightarrow 3 \in H$

ma: $7-3=4 \notin H$

quindi H non é un sottogruppo

Def: G gruppo, H e K due sottogruppi. Si dice SOTTOGRUPPO UNIONE di H e K, e si denota con $H \vee K$, il minimo sottogruppo di G che contiene sia H che K:

$$H \vee K = \bigcap_{\substack{L < G \\ L \supseteq H \cup K}} L$$

Prop: G gruppo, H e K sottogruppi:

$$H \vee K = \{ h_1 k_1 h_2 k_2 \dots h_n k_n \mid h_i \in H, k_i \in K \}$$

Corollario: se G é abeliano:

$$H \vee K = \{ hk \mid h \in H, k \in K \} \quad \text{(notazione moltiplicativa)}$$

[similmente, usando la notazione additiva:
$$H \vee K = \{ h+k \mid h \in H, k \in K \}$$
]

dim. coroll:

G abeliano $\Longrightarrow$ $h_1k_1h_2k_2\cdots h_nk_n$
$= (h_1h_2\cdots h_n)(k_1k_2\cdots k_n) = hk$ #

dim. prop: $H \vee K = \bigcap_{\substack{L<G \\ L \supseteq H \cup K}} L$

$S = \{ h_1k_1h_2k_2\cdots h_nk_n \mid h_i \in H,\ k_i \in K \}$

prop: $H \vee K = S$

$\supseteq$

questa inclusione è immediata perché $H \vee K$ è un sottogruppo che contiene tutti gli elt. di H e tutti gli elt. di K $\Longrightarrow$ contiene tutti i loro prodotti
$\Longrightarrow$ contiene S.

$\subseteq$ osserviamo che S contiene $H \cup K$:

$\forall h \in H$, $\quad h = \underset{\substack{\cap \\ H}}{h} \cdot \underset{\substack{\cap \\ K}}{1_G} \in S$

$\forall k \in K$, $\quad k = \underset{\substack{\cap \\ H}}{1_G} \cdot \underset{\substack{\cap \\ K}}{k} \in S$

quindi se dimostriamo che S è un sottogruppo, per definizione conterrà $H \vee K$, che è quello che vogliamo.

Usiamo il criterio: prendiamo $x, y \in S$ e mostriamo che $xy^{-1} \in S$.

$$x = h_1 k_1 h_2 k_2 \cdots h_n k_n \qquad h_i \in H \quad k_i \in K$$
$$y = \alpha_1 \beta_1 \alpha_2 \beta_2 \cdots \alpha_m \beta_m \qquad \alpha_i \in H \quad \beta_i \in K$$

$$xy^{-1} = (h_1 k_1 \cdots h_n k_n)(\alpha_1 \beta_1 \cdots \alpha_m \beta_m)^{-1}$$
$$= (h_1 k_1 \cdots h_n \underbrace{k_n)(\beta_m^{-1}}_{\in K} \alpha_m^{-1} \beta_{m-1}^{-1} \cdots \beta_1^{-1} \alpha_1^{-1})$$

$k_n \beta_m^{-1} = \gamma$

$$= h_1 k_1 h_2 k_2 \cdots h_n \gamma \alpha_m^{-1} \beta_{m-1}^{-1} \cdots \beta_1^{-1} \alpha_1^{-1} \cdot 1_G \in S$$

$\#$

__Def:__ Siano G un gruppo e $A \subseteq G$ un suo sottoinsieme. Il SOTTOGRUPPO GENERATO DA A è il più piccolo sottogruppo che contiene A, e si denota $\langle A \rangle$:

$$\langle A \rangle = \bigcap_{\substack{H < G \\ H \supseteq A}} H$$

__oss./esercizio:__ $A = \{x\} \qquad \langle \{x\} \rangle = \langle x \rangle$

$f : G \longrightarrow H$ omomorfismo

$$f(xy) = f(x)f(y)$$

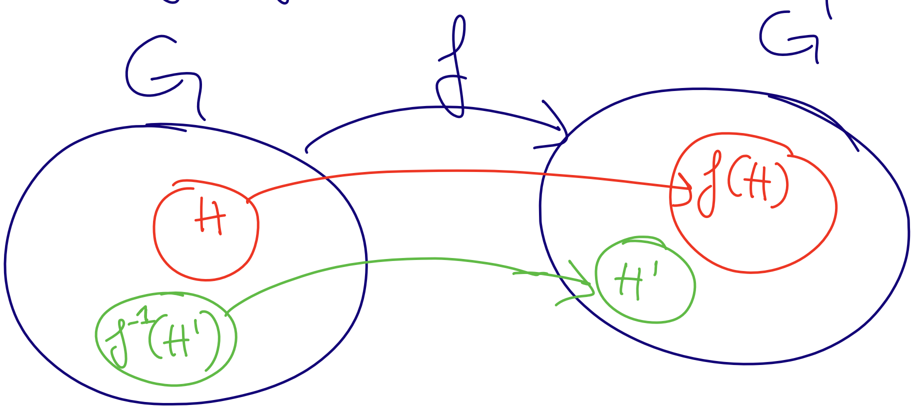
Prop: Sia $f : G \longrightarrow G'$ omomorfismo.
Se $H < G$ sottogruppo, $f(H) < G'$ sottogruppo.

dim: usiamo il criterio:
Siano x' e $y' \in f(H)$
dobbiamo mostrare che $x'(y')^{-1} \in f(H)$.

$$\left.\begin{array}{l} \exists\, x \in H \text{ t.c. } x' = f(x) \\ \exists\, y \in H \text{ t.c. } y' = f(y) \end{array}\right] \Longrightarrow xy^{-1} \in H$$

$$\boxed{f(xy^{-1})} = f(x)\, f(y^{-1}) = f(x)\, f(y)^{-1}$$
$$= \boxed{x' \cdot (y')^{-1}} \in f(H) \quad \#$$

Corollario: $f : G \longrightarrow G'$ omomorfismo.
Allora $\mathrm{Im}(f) = f(G)$ è un sottogruppo di G'.



Prop [esercizio]: Sia $f : G \longrightarrow G'$ omomorfismo, e sia $H' < G'$ sottogruppo. La retroimmagine $f^{-1}(H') < G$ è un sottogruppo.

Def: Sia $f: G \to G'$ omomorfismo.
Il NUCLEO di f, denotato con $\ker(f)$ è l'insieme delle retroimmagini dell'elem. neutro di G':

$$\ker(f) = f^{-1}(\{1_{G'}\}) = \{x \in G \mid f(x) = 1_{G'}\}$$

[notazione additiva: $\ker(f) = \{x \in G \mid f(x) = 0_{G'}\}$]

Corollario: $\ker(f) < G$ è un sottogruppo.

Prop: $f: G \to G'$ omomorfismo. Allora:

(i) f è un epimorfismo $\iff \mathrm{Im}(f) = G'$

(ii) f è un monomorfismo $\iff \ker(f) = \{1_G\}$

dim: (i) ✓

(ii) $(\Longrightarrow)$ Sia f mono, e sia $x \in \ker(f)$

$\Longrightarrow \underline{f(x)} = 1_{G'} = \underline{f(1_G)} \Longrightarrow x = 1_G$ ✓

$(\Longleftarrow)$ supponiamo $\ker(f) = \{1_G\}$ e siano $x, y \in G$ t.c. $f(x) = f(y)$.

Allora: $f(x) = f(y) \iff f(x)f(y)^{-1} = f(y)f(y)^{-1}$

$$\boxed{f(xy^{-1}) = 1_{G'}}$$

$\Longrightarrow xy^{-1} \in \ker(f) = \{1_G\}$

$\Longrightarrow xy^{-1} = 1_G \Longrightarrow xy^{-1}y = 1_G \cdot y \Longrightarrow x = y$ ✓

#

GRUPPO SIMMETRICO S_n

$I_n = \{1, 2, 3, \dots, n\}$

Def: Una biezione di I_n in se stesso é detta PERMUTAZIONE. L'insieme di tutte le permutazioni é un gruppo rispetto alla composizione, detto GRUPPO SIMMETRICO DI ORDINE n e denotato S_n.

S_n ha $n!$ elementi.

notazione:
$$S_n \ni \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

es:
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

$\sigma : I_5 \longrightarrow I_5$

$1 \longmapsto 3$
$2 \longmapsto 4$
$3 \longmapsto 5$
$4 \longmapsto 1$
$5 \longmapsto 2$

1 3 5 2 4 1

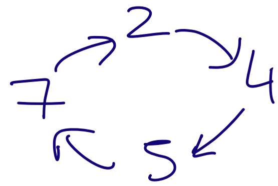
$(1\,3\,5\,2\,4)$

es:
$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 4 & 1 & 7 & 6 \end{pmatrix}$$

1 3 5

$(1\,3\,5)\cancel{(2)(4)}(6\,7) = (1\,3\,5)(6\,7)$

es: $(2457)(18)$



$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 4 & 3 & 5 & 7 & 6 & 2 & 1 \end{pmatrix}$$

Def: Dati $a_1, \dots, a_k \in I_n$ indichiamo con $(a_1\, a_2 \dots a_k)$ la permutazione σ t.c.

$$\begin{cases} \sigma(a_i) = a_{i+1} & \text{per } i = 1 \dots k-1 \\ \sigma(a_k) = a_1 \end{cases}$$

e che lascia invariati tutti gli altri elt. di I_n.
Tale permutazione é detta CICLO DI LUNGHEZZA K.

- Due cicli sono detti DISGIUNTI se tali sono gli insiemi degli elt. da loro permutati.
- Un ciclo di lunghezza 2 é detto TRASPOSIZIONE.