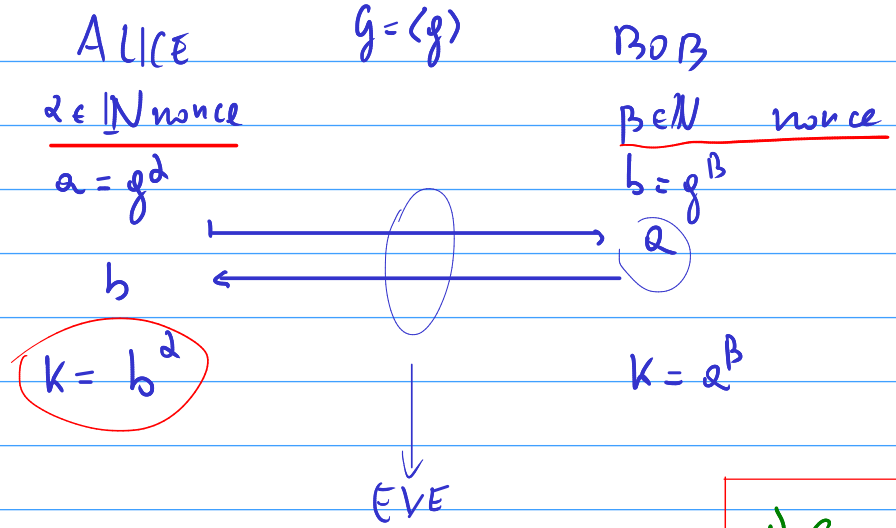
Diffie-Hellman



Def: Un nonce è un numero casuale che viene utilizzato una ed una sola volta.

pfs → perfect forward secrecy.

1) Eve può indovinare $K = g^{ab}$ dati $a = g^a$, $b = g^b$?

DHP = Diffie Hellman problem.

2) DATO $a = g^a$, può EVE calcolare $a = DLOG_g\, a$?

DLOGP = Discrete Logarithm problem.

(2) ⇒ (1) ma non è un se e solo se.

1) Eve vede a e b
2) calcola a da a = DLOG
3) calcola $K = b^a$ DHP

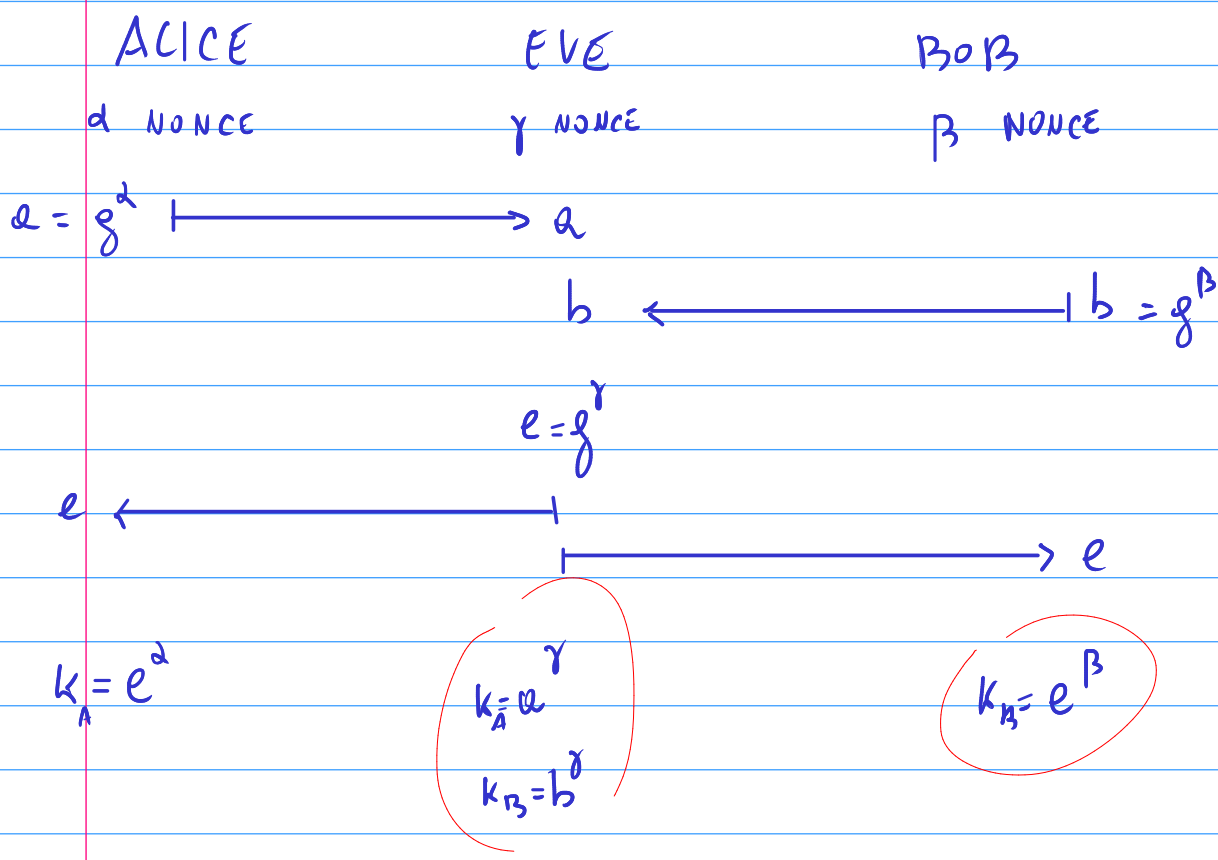
3) Eve sa prevedere i nonce usati da ALICE e BOB?

↓

ANALISI SUL TEMPO NECESSARIO PER CALCOLARE $g^a = a$ e $g^b = b$.

Che cosa è stato trasmesso/negoziato fra ALICE e BOB?

(MAN) IN THE MIDDLE.

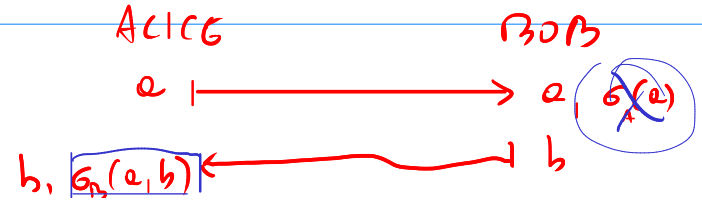


→ STS = Station to Station

Vogliamo un protocollo in cui una chiave k è ACCETTATA se e solo se entrambi i partecipanti possono garantire che

1) la controparte sia chi dice di essere
2) la controparte abbia ricevuto i dati trasmessi per la negoziazione.
3) la controparte possa generare la chiave k a partire dai dati trasmessi.

NON STS.



$\sigma_A(a,b)$ ⟼ $\sigma_A(a,b)$

STS

ALICE

α NONCE

$a = g^{\alpha}$

BOB

β NONCE

$b = g^{\beta}$

a ⟼ a

$K = a^{\beta}$

$b, \mathcal{E}_K(\sigma_B)$ ⟵ $b, \mathcal{E}_K(\sigma_B(a,b))$

$K = b^{\alpha}$

$\mathcal{D}_K(\mathcal{E}_K(\sigma_B(a,b))) =$

$= \sigma_B(a,b)$

e verifica la firma di BOB

$\mathcal{E}_K(\sigma_A(a,b))$ ⟼ $\mathcal{E}_K(\sigma_A(a,b))$

verifica la firma di ALICE in $\mathcal{D}_K(\mathcal{E}_K(\sigma_A(a,b)))$.

N.B MAI FIRMARE IN BIANCO.

Supponiamo di avere un criptosistema (RSA) A CHIAVE PUBBLICA IN CUI LA FIRMA CORRISPONDE ALLA DECODIFICA E VALE UNA PROPRIETÁ OMOMORFICA

DEL TIPO

$$\mathcal{E}_K(\alpha) \cdot \mathcal{E}_K(\beta) = \mathcal{E}_K(\alpha\beta)$$

ALICE

Codifica

$\mathcal{E} = \mathcal{E}_{K_B}(m)$

per bob

BOB

EVE

$\longrightarrow$ intercetta

c

$\longmapsto$ c

è convinto

BOB A

FIRMARE c

m $\longleftarrow$ $\mathcal{D}_K(\mathcal{E})$

c

$\mathcal{E}_{K_B}("2") = \mathcal{E}$

$c' = \mathcal{E}c \longmapsto$

$\mathcal{D}(\mathcal{E}) \cdot \mathcal{D}(c)$

$\mathcal{D}_K("2")m \longleftarrow$

$"2" \longmapsto \mathcal{D}_K(2)$

$\mathcal{D}_K("2") \longleftarrow$

DH è basato sulla difficoltà di DLOG come prerequisito

→ Gruppi, sottogruppi e gruppi ciclici

$(G, \circ)$ gruppo

1) $\exists\, 1 \in G : \; 1 \cdot g = g \cdot 1 = g \quad \forall g \in G$

2) $\forall g \in G \; \exists\, g^{-1} \in G : \; g \cdot g^{-1} = 1$

3) $\forall g, h, m \in G : \; g \cdot (h \cdot m) = (g \cdot h) \cdot m$

$H \subseteq G$ sottogruppo di G se $H \subseteq G$ e valgono 1, 2, 3 in H (ristrette e rivolte rispetto l'op. di G ad H)

proprietà di chiusura

$$H \subseteq G \iff \forall h, m \in H, \; h^{-1} \cdot m \in H$$

1) $1 = h^{-1} \cdot h \in H$ 2) $h^{-1} \cdot 1 = h^{-1} \in H$

3) $\forall h, m \in H \quad (h^{-1})^{-1} m = hm \in H$

Teorema (Lagrange): Sia G un gruppo $|G| = n < \infty$ ed $H \leq G$ sottogruppo $\Rightarrow$

$$|H| \mid n$$

↖ divide

Esempio

$|G| = 10 \Rightarrow$ $H \leq G$

$$|H| \in \{1, 2, 5, 10\}$$

N.B: $\{1\} \leq G$, $G \leq G$ } sottogruppi banali

DIM: Sia $H \leq G$.

$\forall g \in G$ definiamo la classe destra di H (associata a g) l'insieme $gH = \{gh \mid h \in H\}$.

oss 1) $|gH| = |H|$

2) $R(G:H) = \{gH \mid g \in G\}$.

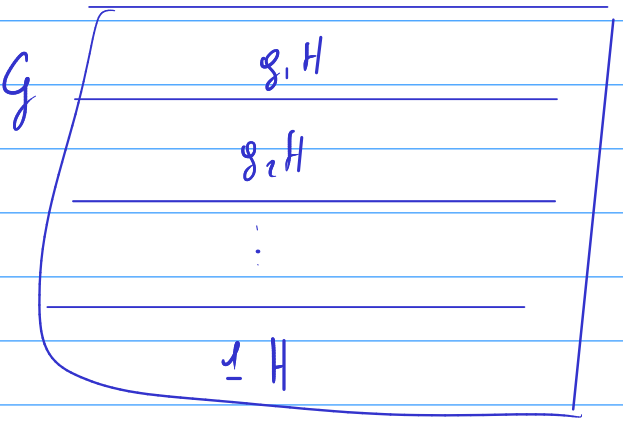
è una partizione di G

$\Rightarrow \forall\ gH, g'H$ laterali dx

$$gH \cap g'H = \emptyset \quad \text{oppure} \quad gH = g'H$$

Idea di dim: Noi stiamo asserendo che G si decompone in tanti pezzi disgiunti ognuno dei quali ha $|H|$ elementi

$\Rightarrow |G| = |H| \cdot t$



DIMOSTRAZIONE

1) $|gH| = |H|$ infatti la funzione $\varphi : \begin{cases} gH \to H \\ x \to g^{-1}x \end{cases}$

è l'inversa della funzione $\psi : \begin{cases} H \to gH \\ x \to gx \end{cases}$

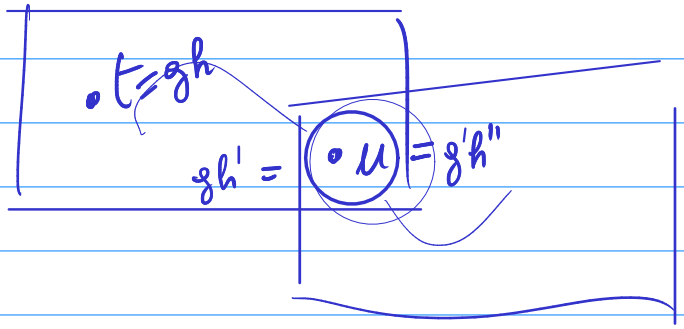
$\Rightarrow \varphi$ e ψ sono biiezioni $\to$ fine.

// ALTERNATIVAMENTE Lim. che ψ è suriettiva e iniettiva $\Rightarrow$ suriettiva per def. di gH, Iniettiva. perché se $gx = gy \Rightarrow g^{-1}(gx) = g^{-1}(gy)$

$\Rightarrow x = y$ D //

// OGNI CATERALE HA LO STESSO NUMERO DI ELEMENTI $\rightarrow$

2) gH



supponiamo $gH \cap g'H \ni u \Rightarrow$ DOSTRIAMO

$\neq \emptyset$ $gH = g'H$

Sia $t \in gH \Rightarrow \exists\, h \in H$ tale che

$t = gh$

ma anche $u = gh' = g'h''$ con

$h', h'' \in H$

mostriamo che $t = g' h'''$ con $h''' \in H$

$$u = g h' = g' h'' \Rightarrow \boxed{g = g' h'' h'^{-1}}$$

$$\Rightarrow t = gh = (g' h'' h'^{-1}) h =$$

$$= g' \underbrace{(h'' h'^{-1} h)}_{\in H} = g' h''' \Rightarrow$$

$$\Rightarrow t \in g'H \Rightarrow gH \subseteq g'H$$

il viceversa è analogo. □

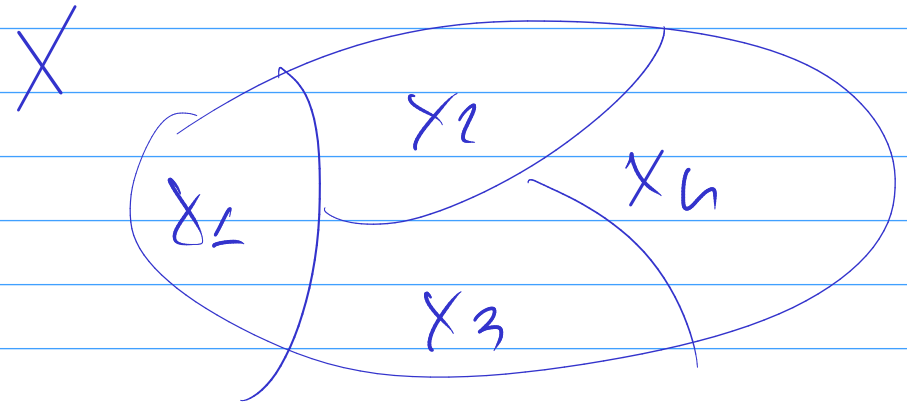
In particolare se $|G| = p$, p primo

$\Rightarrow$ (gli unici sottogruppi di G sono quelli banali)

Oss: Se $H \leq G$ sottogruppo $\Rightarrow$

$\Rightarrow H$ induce una partizione su G.

MA OGNI VOLTA CHE SI HA UNA PARTIZIONE SI HA ANCHE UNA relazione di equivalenza.



$x \sim y \iff x, y \in X_i$

→ OGNI SOTTOGRUPPO DEFINISCE UN INSIEME QUOZIENTE DI G.

QUANDO QUESTO INSIEME È DOTATO IN MODO "NATURALE" DI UNA STRUTTURA DI GRUPPO?

Sottogruppo normale

$H \trianglelefteq G$

sottogruppo normale di G

se $\boxed{H = gHg^{-1} \quad \forall g \in G}$

ove $gHg^{-1} = \{ ghg^{-1} \mid h \in H \}$.

ALTERNATIVAMENTE se $\boxed{Hg = gH \ \forall g \in G}$

Oss: Se G è commutativo $\Rightarrow H \subseteq G$ implica $H \trianglelefteq G$. In generale per G non commutativo $\exists$ sottogruppi non normali.

Teorema G gruppo $H \trianglelefteq G \Rightarrow$

G/H è dotato di una struttura di gruppo quoziente

ove $\boxed{(g_1 H) \cdot (g_2 H) := (g_1 g_2) H}$

e l'identità è data da $1 \cdot H = H$

DIM: $t \in g_1 H$, $s \in g_2 H$

mostriamo che $(t \cdot s) \in (g_1 g_2) H$

$\Rightarrow \quad t = g_1 h_1 \qquad s = g_2 h_2$

$\Rightarrow \quad ts = g_1 h_1 g_2 h_2$

ma $\quad Hg_2 = g_2 H$ perché $H \trianglelefteq G$

$\Rightarrow \quad h_1 g_2 = g_2 h_1' \Rightarrow$

$= ts = g_1 g_2 h_1' h_2 \in (g_1 g_2) H$

$\forall\, gH \in G/H \quad (1 \cdot H) \cdot (gH) = (1g)H =$

$= gH = (g1)H$

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

$\forall\, gH \in G/H \;\exists\; g^{-1}H \in G/H$ e

$(gH) \cdot (g^{-1}H) = (gg^{-1})H = 1H = H$

$\forall\, aH, bH, cH \in G/H \quad ((aH) \cdot (bH)) \cdot cH =$

$$= (ab)H \cdot cH =$$

$$= ((ab)c)H = (a(bc))H$$

$$= (aH)\cdot((bH)\cdot(cH))$$ □

N.B Se G commutativo G/H commutativo. Se G non commutativo G/H può essere commutativo o no.

Esempio $(\mathbb{Z}, +)$ gruppo commutativo

$n \in \mathbb{N}$ $\quad n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$.

OSS $(n\mathbb{Z}, +)$ è un sottogruppo.

$$n\mathbb{Z} \trianglelefteq \mathbb{Z}$$

perché $\mathbb{Z}$ è commutativo

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \qquad a = b \bmod n \iff a - b \in n\mathbb{Z}$$

$\Leftrightarrow \quad \alpha \in \beta + \mathbb{Z}_n$

Ora

$\mathbb{Z}/n\mathbb{Z}$ gli elementi sono classi del tipo

$$\alpha + n\mathbb{Z}$$

e $(\alpha + n\mathbb{Z}) + (\beta + n\mathbb{Z}) =$

$$= (\alpha + \beta) + n\mathbb{Z}$$

N.B in $\mathbb{Z}_n$ il DLOG è molto facile da calcolare.

$$DLOG_{1+\mathbb{Z}_n}(\alpha + \mathbb{Z}_n) = \alpha \% n$$

$n = 7 \qquad \mathbb{Z}_n = \langle 1 \rangle$

$$52 + \mathbb{Z}_n \qquad 52 \% 7 = 3$$

OSSERVAZIONE IMPORTANTE.

Tutti i gruppi ciclici finiti sono isomorfi a $(\mathbb{Z}_n, +)$ ove $n = |G|$

$$(g^\alpha)(g^\beta) = g^{\alpha+\beta}$$

Gruppi ciclici

Sia G un gruppo e $g \in G$. Si dice ordine di g $o(g)$ il più piccolo naturale n tale che $g^n = 1$ oppure se tale n non esiste ∞.

Es. su $(\mathbb{R}^*, \cdot)$ -1 ha ordine 2

su $(\mathbb{C}^*, \cdot)$ $\eta_k = e^{2i\pi/k}$

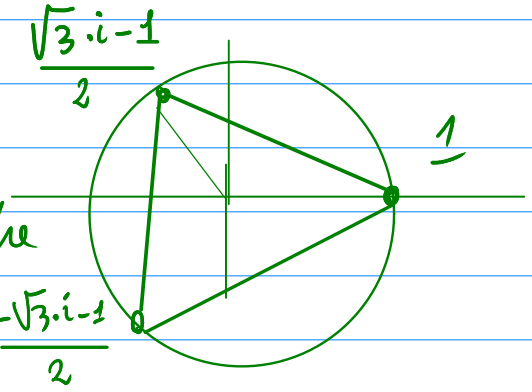
$\eta_k^k = e^{i\pi} = 1 \qquad \forall\, 0 < h \leq k-1 \quad \eta_k^h \neq 1$

Se prendiamo $k = 1$

$$e^{2i\pi} = 1$$

$k = 2 \qquad e^{i\pi} = -1 \qquad \langle e^{i\pi} \rangle = \{-1, +1\}.$

$k = 3$



radici cubiche di 1

Teorema: Se $g \in G$, $o(g) = n \Rightarrow$

$= \{1 = g^n, g, g^2 \text{---} g^{n-1}\}$ è un sottogruppo di G.

Dim:

$1 \in \{g^n\ g \text{---} g^{n-1}\}.$

$g^\alpha, g^\beta \in \{g^n\ g \text{---} g^{n-1}\}.$

$$\Rightarrow g^{\alpha+\beta} = g^{tn+r} = (g^n)^t \cdot g^r =$$

dividendo $(\alpha+\beta)$ per n e prendendo il resto $0 < r \leq n-1$

$$= 1^t \cdot g^r = g^r \in G$$

supponiamo $g^\alpha \in \{1, g, g^2, \dots, g^{n-1}\}$

se $\alpha = 0 \Rightarrow g^\alpha = 1 \Rightarrow g^{-\alpha} = 1 \in G$

se $1 \leq \alpha \leq n-1 \Rightarrow$ pongo $\beta = n-\alpha$

e considero che $1 \leq \beta \leq n-1$

$$g^\beta \in \{g^0 = 1, g, \dots, g^{n-1}\}.$$

$$g^\beta \cdot g^\alpha = g^{n-\alpha} \cdot g^\alpha = g^n = 1$$

$$\Rightarrow g^\beta = (g^\alpha)^{-1}$$

$$\{g^0 = g^n = 1, g, \dots, g^{n-1}\} \leq G$$

OSS $o(g) \mid |G|$ se $|G| = n < \infty$

perché $o(g) = |\langle g \rangle|$

se $|G| = p$ primo $\Rightarrow \langle g \rangle = \{1\}$ o $\langle g \rangle = G$ $\forall g \in G$

$\langle g \rangle \cong \mathbb{Z}_n$ ove

$$\psi : \begin{cases} \mathbb{Z}_n \to \langle g \rangle \\ k + n\mathbb{Z} \to g^k \end{cases}$$ isomorfismo.

OMOMORFISMI ED ISOMORFISMI

ψ è un omomorfismo di gruppi se G, H gruppi

$$\psi : G \to H$$

$\Leftrightarrow$ $\boxed{\forall g, h \in G. \quad \psi(g^{-1}h) = \psi(g)^{-1}\psi(h)}$

ψ è un isomorfismo se

ψ omomorfismo e biiettivo.

□

$\ker \psi := \{ g \in G \mid \psi(g) = 1 \}$.

N.B: Se $g \in G$ $\Rightarrow \exists$ sempre un omomorfismo.

$$\varphi_g : \begin{cases} \mathbb{Z} \longrightarrow G \\ n \longrightarrow g^n \end{cases}$$

$$m+n \longmapsto g^{m+n} = g^m \cdot g^n$$

$$\ker(\varphi_g) = \{ m \in \mathbb{Z} \mid \varphi_g(m) = 1 \}.$$

Es. 1) $\ker(\varphi_g) \trianglelefteq \mathbb{Z}$

2) Se $o(g) = \infty \Rightarrow \ker(\varphi_g) = \{0\}$.

3) Se $o(g) = n \Rightarrow \ker(\varphi_g) = n\mathbb{Z}$

$$g^{o(g)} = 1 \Rightarrow g^n = 1$$

$$\Rightarrow g^{2n} = 1$$

4) $$\frac{\mathbb{Z}}{\ker(\varphi_g)} = \frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathrm{Im}(\varphi_g) = \langle g \rangle.$$

5) $\boxed{\mathbb{Z}_n \cong \langle g \rangle}$

Teorema di omomorfismo: $\varphi : G \to H$ omomorfismo. $\Rightarrow$

$$\boxed{G/\ker\varphi \cong \mathrm{Im}(\varphi)}$$

DIM

1) $\ker\varphi \trianglelefteq G$

infatti se $g \in G$, $k \in \ker\varphi$

$$\Rightarrow \varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1}$$

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

$$\Rightarrow g(\ker\varphi)g^{-1} = \ker\varphi.$$

2) Suriettività $\Rightarrow$ OVVIA (ogni funzione è suriettiva sulla sua immagine!).

INIETTIVITÀ: Supponiamo $\varphi(h) = \varphi(g)$

mostriamo che $h \in g\ker\varphi$

quindi in particolare

$$\varphi(h\ker\varphi) = \varphi(g\ker\varphi)$$

$$\Leftrightarrow h\ker\varphi = g\ker\varphi.$$

$\varphi(h)=\varphi(g) \Rightarrow$

$$\Rightarrow 1 = \varphi(h)\cdot\varphi(g)^{-1} = \varphi(hg^{-1})$$

$$\Rightarrow hg^{-1} \in \ker\varphi \Rightarrow$$

$$\Rightarrow h \in (\ker\varphi)g =$$

(in quanto $\ker\varphi \trianglelefteq G$)

$$= g(\ker\varphi)$$

perché $(\ker\varphi)g = g(\ker\varphi)$ □
