GRUPPI (V PARTE)

$(G,\cdot)$ gruppo . $g \in G$ fissato.

Consideriamo la funzione $\varepsilon : (\mathbb{Z},+) \longrightarrow \langle g \rangle$ è un epimorfismo
$k \longmapsto g^k$

Infatti: $\varepsilon(r+s) = g^{r+s} = g^r \cdot g^s = \varepsilon(r)\cdot\varepsilon(s) \Rightarrow \varepsilon$ è un omomorfismo
$\forall x \in \langle g \rangle \quad x = g^k$ per qualche $k \in \mathbb{Z}$, ma allora $x = \varepsilon(k) \Rightarrow \varepsilon$ suriettiva.

Possono presentarsi due casi:

indica isomorfismo

1) ε è anche iniettiva $\Rightarrow \varepsilon$ è un isomorfismo, cioè $(\mathbb{Z},+) \cong (\langle g \rangle, \cdot)$
e le potenze di g sono tutte distinte tra loro $\Rightarrow \langle g \rangle$ è infinito.

2) Se ε non è iniettiva $\Rightarrow \underset{s \neq t}{\exists\, s,t \in \mathbb{Z}}$ t.c. $\varepsilon(s) = \varepsilon(t)$, cioè $g^s = g^t$.

Possiamo supporre $s > t$. Allora moltiplicando a destra per g^{-t}:
$g^s \cdot g^{-t} = g^t \cdot g^{-t} \Rightarrow g^{s-t} = g^{t-t} \Rightarrow g^{s-t} = e_G$ cioè $\exists\, k \in \mathbb{N} \setminus \{0\}$ t.c. $g^k = e_G$

Sia $n = \min\{k \in \mathbb{N} \setminus \{0\} \mid g^k = e_G\}$.

Ora $\forall k \in \mathbb{Z}$, possiamo svolgere la divisione euclidea per n e otteniamo $k = q\cdot n + r$ con $0 \leq r < n$. Allora:

$$g^k = g^{q\cdot n + r} = g^{qn}\cdot g^r = (\underbrace{g^n}_{= e_G})^q \cdot g^r = (e_G)^q \cdot g^r = e_G \cdot g^r = g^r$$

<u>OSS</u>: $g^r = e_G$ se e solo se $r = 0$ (perché $r < n$ ed n è il minimo positivo con quella proprietà)

In conclusione: ci sono solo n potenze distinte di g:

$$\langle g \rangle = \{e_G, g, g^2, \dots, g^{n-1}\}$$

A partire da $g^n (= e_G)$ le potenze si ripetono.

<u>Def</u>: Si dice <u>periodo</u> di g in G l'ordine $|\langle g \rangle| = n$.

<u>OSS</u>:
1) g ha periodo $1 \iff g = e_G$
2) g ha periodo infinito $\Rightarrow \varepsilon$ iniettiva $\Rightarrow \langle g \rangle \cong \mathbb{Z}$
3) Possono esistere elementi di periodo finito dentro gruppi infiniti:
   es. $(\mathbb{Q}^\times, \cdot)$ $\quad -1$ ha periodo 2
4) Se $\langle g \rangle$ è infinito $\Rightarrow g^k$ ha periodo infinito $\forall k \neq 0$
5) Se $|G| = n$ finito, $\underset{\text{sottogruppo}}{\langle g \rangle \leq G} \underset{\text{Lagrange}}{\Longrightarrow} |\langle g \rangle| = d$ deve dividere n, cioè il periodo di g deve essere un divisore di n

Prop: Se $G = \langle g \rangle$, allora qualunque omomorfismo $f : (G, \cdot) \longrightarrow (H, *)$
è completamente determinato da $f(g)$.

Dim: L'immagine di qualunque elemento di G è determinata dall'immagine del generatore (g)
Infatti, se $x \in G \Rightarrow x = g^k$ per qualche $k \in \mathbb{Z}$, ma allora
$f(x) = f(g^k) = f(g)^k$.

Ciò non significa che $f(g)$ possa essere scelta a piacere.

Es. $f : (G, \cdot) \longrightarrow (\mathbb{Z}, +)$ con $|G| = n$, $G = \langle g \rangle$

Allora $n \cdot f(g) = f(g^n) = f(e_G) = 0 \Rightarrow f(g) = 0$

Di conseguenza $f(g^k) = k \cdot f(g) = 0 \quad \forall k \in \mathbb{Z}$

Cioè l'unico omomorfismo $(G, \cdot) \longrightarrow (\mathbb{Z}, +)$ è quello banale, che manda tutto in 0.

Es. $f : (\mathbb{Z}_6, +) \longrightarrow (\mathbb{Z}_4, +) \qquad \mathbb{Z}_6 = \langle \bar{1} \rangle$

allora $6 \cdot f(\bar{1}) = f(6 \cdot \bar{1}) = f(\bar{0}) = \bar{0}$, ma in $\mathbb{Z}_4$ $\quad 6 \cdot f(\bar{1}) = \underbrace{4 \cdot f(\bar{1})}_{= \bar{0}} + 2 \cdot f(\bar{1})$

$\Rightarrow 2 \cdot f(\bar{1}) = \bar{0}$ in $\mathbb{Z}_4 \Rightarrow f(\bar{1})$ può essere $= \bar{0}$
oppure $= \bar{2}$

Prop: Sia $(G,\cdot)$ un gruppo con $|G|=n$ finito $\Rightarrow \forall g\in G \quad g^n = e_G$

Dim: Non è detto che g sia un generatore, però $\langle g\rangle \leq G \overset{\text{Lagrange}}{\Longrightarrow} |\langle g\rangle| = d$ è un divisore di n.

Cioè $\exists k\in\mathbb{Z}$ t.c. $n = dk$, quindi

$$g^n = g^{dk} = (\underbrace{g^d}_{\substack{\shortparallel \\ e_G \text{ perché } d \text{ è il } \underline{\text{periodo}} \text{ di } g}})^k = (e_G)^k = e_G$$

Conseguenza:

Teorema di Eulero: Dati $a\in\mathbb{Z}$, $N\in\mathbb{N}$, $N\geq 2$, $MCD(a,N)=1$.

Allora $\quad a^{\varphi(N)} \equiv 1 \mod N$.

Dim: Consideriamo il gruppo $(\mathbb{Z}_N^\times, \cdot)$ degli elementi invertibili in $\mathbb{Z}_N$ (rispetto alla moltiplicazione).

Sappiamo che $\varphi(N) = |\mathbb{Z}_N^\times|$.

Se $MCD(a,N)=1$, allora $\bar{a}$ è invertibile in $\mathbb{Z}_N$, cioè $\bar{a}\in\mathbb{Z}_N^\times$

Ora, la proposizione precedente ci dice che $\forall \bar{x}\in\mathbb{Z}_N^\times \quad \bar{x}^{|\mathbb{Z}_N^\times|} = \bar{1}$ cioè $\bar{x}^{\varphi(N)} = \bar{1}$

In particolare $\bar{a}^{\varphi(N)} = \bar{1}$ in $\mathbb{Z}_N$, ovvero $a^{\varphi(N)} \equiv 1 \mod N$. $\boxtimes$