ALGEBRA 1 - 09/12/2020

GRUPPI CICLICI - 2ª PARTE

MEMO G è ciclico $\overset{\Delta}{\iff} \exists\, g \in G : G = \langle g \rangle$

$\forall\, \gamma \in G, \quad E_\gamma := \{ e \in \mathbb{N}_+ \mid \gamma^e = 1_G \} = \{\text{esponenti di } \gamma\}$

$$\omega(\gamma) := \begin{cases} +\infty, & \text{se } E_\gamma = \emptyset \\ \min_{\leq}(E_\gamma), & \text{se } E_\gamma \neq \emptyset \end{cases}$$

Struttura: $G = \langle g \rangle \Rightarrow G = \{ g^z \mid z \in \mathbb{Z} \}$

Classificazione: $G = \langle g \rangle \Rightarrow G \cong (\mathbb{Z}_n ; +)$

con $n = \begin{cases} |G| = \omega(g) & \text{se } \omega(g) < +\infty \\ 0 & \text{se } |G| = \omega(g) = +\infty \end{cases}$

via $\mathbb{Z}_n \longrightarrow G = \langle g \rangle$, $\bar{z} \longmapsto g^z$

Sottogruppi in gruppi ciclici

Proposizione 1: **Hp:** $G = \langle g \rangle$ è ciclico, $H \leq G$

Th: H è ciclico, con $H = \langle g^\eta \rangle$ dove

$$\eta = \begin{cases} 0, & \text{se } E_H = \emptyset \\ \min_{\leq}(E_H), & \text{se } E_H \neq \emptyset \end{cases} \quad \text{con} \quad E_H := \{ e \in \mathbb{N}_+ \mid g^e \in H \}$$

Dim: 1° CASO – $E_H = \emptyset$: $\forall\, h \in H \leq G = \langle g \rangle$, $\Rightarrow$

$\Rightarrow \exists\, z \in \mathbb{Z} : h = g^z$, $\Rightarrow$ anche $g^{-z} = h^{-1} \in H^{-1} = H$ $\Rightarrow$

$\Rightarrow g^z, g^{-z} \in H \Rightarrow$ se $|z| > 0$, $\Rightarrow |z| \in E_H \Rightarrow E_H \neq \emptyset$, ↯

QUINDI è $|z| = 0$, $\Rightarrow z = 0 \Rightarrow h = g^z = g^0 = 1_G \Rightarrow H = \{1_G\} \Rightarrow$

$\Rightarrow H = \{1_G\} = \langle g^0 \rangle$, q.e.d.

2° CASO – $E_H \neq \phi$: $E_H \neq \phi \Rightarrow \exists\, \eta = \min_{\leq}(E)_H : h_0 := g^\eta \in H$

$\Rightarrow \forall\, h \in H \leq G = \langle g \rangle,\ \exists\, z \in \mathbb{Z} : h = g^z$ $\Big) \Longrightarrow$

DIVIDO z per η $\Rightarrow$ $\boxed{z = \eta \cdot q + r}$, $\boxed{0 \leq r < \eta}$

$\Rightarrow h = g^z = g^{\eta q + r} = (g^\eta)^q \cdot g^r = h_0^q \cdot g^r \Rightarrow$

$\Rightarrow g^r = h_0^{-q} \cdot h \in H$ $\Big\}$ $\Rightarrow$ $\begin{cases} 0 < r < \eta := \min(E_H) & \text{(4)} \\ r = 0 \Rightarrow z = \eta \cdot q \Rightarrow \end{cases}$

$0 \leq r < \eta$

$\Rightarrow h = g^z = g^{\eta q} = (g^\eta)^q \in \langle g^\eta \rangle \Rightarrow H = \langle g^\eta \rangle$ q.e.d. □

NOTAZIONE: (1) $\forall$ gruppo G, poniamo

$$\mathcal{S}_G := \{ H \mid H \leq G \} = \{ \text{sottogruppi di } G \}$$

(2) $\forall\, n \in \mathbb{N}_+$, $\mathrm{Div}(n) := \{ d \in \mathbb{N}_+ \mid d \,\delta_{\mathbb{N}}\, n \} = \{ \text{divisori di } n \}$

Teorema 2: **Hp:** $G = \langle g \rangle$ ciclico di ordine finito $n \in \mathbb{N}_+$.

Th: (a) $\forall\, H \leq G$, con $E_H := \{e \in \mathbb{N}_+ \mid g^e \in H\}$ e $\eta := \min(E_H)$, si ha $\boxed{\eta \cdot |H| = |G|}$

(b) $\exists$ biiezione

$$\begin{array}{ccc} \mathcal{S}_G & \xrightarrow{\Phi} & Div(n) \\ H & \longmapsto & |H| \end{array}$$

Dim: $\forall\, H \leq \mathcal{S}_G$, si ha $H = \langle g^\eta \rangle$ per la Proposizione 1

Dividiamo n per η: $n = \eta \cdot q + r$, $0 \leq r < \eta \Rightarrow$

ORA $n = |G| = \omega(g) \Rightarrow g^n = 1 \Rightarrow 1 = g^n = (g^\eta)^q \cdot g^r \Rightarrow$

$\Rightarrow g^r = (g^\eta)^{-q} \in H$, $0 \leq r < \eta := \min(E_H) \Rightarrow r = 0 \Rightarrow$

$\Rightarrow \boxed{n = \eta \cdot q}$ così $\eta \in Div(n)$.

INOLTRE ⊛ $q = n/\eta = \omega(g^\eta) = \omega(\langle g^\eta \rangle) = \omega(H)$

Infatti $(g^\eta)^q = g^{\eta \cdot \frac{n}{\eta}} = g^n = 1$ perché $n = |G| = \omega(g)$

& se $\exists\, k : 0 < k < q$, $(g^\eta)^k = 1$ allora $g^{\eta k} = 1$

con $0 < \eta k < \eta q = n = \omega(g) \Rightarrow$ ↯

ALLORA $n = \eta \cdot q$ diventa $|G| = \eta \cdot |H|$ ⇒ OK per (a).

ORA $|H| = q \mid \eta \cdot q = n \Rightarrow |H| \in Div(n)$, $\forall H \in \mathcal{S}_G$

QUINDI ∃ funzione $\mathcal{S}_G \xrightarrow{\Phi} Div(n)$

$H \longmapsto |H|$

Troviamo ora una funzione $Div(n) \xrightarrow{\Psi} \mathcal{S}_G$ inversa!

Consideriamo $\psi : Div(n) \longrightarrow \mathcal{G}_G$

$$q \longmapsto H_q := \langle g^{n/q} \rangle$$

Allora:

$\phi \circ \psi = id_{Div(n)}$ $\forall\, q \in Div(n)$ si ha

$$(\phi \circ \psi)(q) = \phi(\psi(q)) = \phi\left(\langle g^{n/q} \rangle\right) = \left|\langle g^{n/q} \rangle\right| \overset{\text{per la } \circledast}{=} q \quad \text{(ok)}$$

$\psi \circ \phi = id_{\mathcal{G}_G}$ $\forall\, H \in \mathcal{G}_G$ si ha che $\exists\, \eta : H = \langle g^{\eta} \rangle \overset{(a)}{\Longrightarrow}$

$\overset{(a)}{\Longrightarrow}$ $n = \eta \cdot |H| \Rightarrow n/|H| = \eta$, e allora

$$(\psi \circ \phi)(H) = \psi(|H|) = \langle g^{n/|H|} \rangle = \langle g^{\eta} \rangle = H$$

PERCIÒ $\psi = \phi^{-1}$ e ϕ è una bijezione $\Rightarrow$ (b) è (ok). $\square$

Proposizione 3: **Hp:** $G = \langle g \rangle$ ciclico di ordine finito $n \in \mathbb{N}_+$

$$\mathcal{G}_G := \{\text{generatori di } G\} = \{\gamma \in G \mid \langle \gamma \rangle = G\}$$

Th: L'isomorfismo standard $f: \mathbb{Z}_n \xrightarrow{\cong} G = \langle g \rangle$, $\bar{z} \longmapsto f(\bar{z}) := g^z$

si restringe a una biiezione

$$f': U(\mathbb{Z}_n) \longrightarrow \mathcal{G}_G, \quad \bar{z} \longmapsto f'(\bar{z}) = g^z \quad (\forall\, \bar{z} \in U(\mathbb{Z}_n)).$$

Dim.: $\forall\, \gamma \in G = \langle g \rangle = \{g^{\bar{z}} \mid \bar{z} \in \mathbb{Z}_n\}$, sia $a \in \mathbb{Z}$: $\gamma = g^a$

allora $\gamma = g^a \in \mathcal{G}_G \iff \langle \gamma = g^a \rangle = \langle g \rangle \iff$

$\iff g \in \langle g^a \rangle \iff \exists\, x \in \mathbb{Z} : g^1 = g = (g^a)^x = g^{ax} \iff$

$\iff \exists\, x \in \mathbb{Z} : f(\bar{1}) = g^1 = g^{ax} = f(\bar{a} \cdot \bar{x}) \iff$

$\iff \exists\, \bar{x} \in \mathbb{Z}_n : \bar{1} = \bar{a} \cdot \bar{x} \iff \exists\, \bar{a}^{-1} \in \mathbb{Z}_n \overset{a}{\iff} \bar{a} \in U(\mathbb{Z}_n)$

così $\bar{a} \in U(\mathbb{Z}_n) \iff f(\bar{a}) := g^a \in \mathcal{G}_G$ q.e.d. □

((Hp: G è gruppo))

SOTTOGRUPPI

Def. 1: $\forall\, H \leq G$, definiamo in G le relazioni ("destra, risp. sinistra, associate a H in G") ρ_d^H e ρ_s^H date da

$$\forall\, a, b \in G, \quad a \,\rho_d^H\, b \overset{\Delta}{\iff} ab^{-1} \in H, \quad a \,\rho_s^H\, b \overset{\Delta}{\iff} b^{-1}a \in H$$

Def. 3.: $\forall\, H \leq G$, $\forall\, g \in G$, poniamo

$gH :=$ classe laterale sinistra di g modulo H

$Hg :=$ classe laterale destra di g modulo H

$$G/H := \left\{ \begin{array}{c} \text{classi laterali sinistre} \\ \text{in } G \text{ modulo } H \end{array} \right\} = \{ gH \mid g \in G \}$$

$$H\backslash G := \left\{ \begin{array}{c} \text{classi laterali destre} \\ \text{in } G \text{ modulo } H \end{array} \right\} = \{ Hg \mid g \in G \}$$

Lemma 2: **Hp:** $H \leq G$

Th: (1) ρ_d^H e ρ_s^H sono equivalenze in G.

(2) $\forall\, a, b \in G$ si ha $a \rho_d^H b \iff Ha = Hb$, $a \rho_s^H b \iff aH = bH$

(3) $\forall\, g \in G$ si ha $[g]_{\rho_d^H} = Hg$, $[g]_{\rho_s^H} = gH$

(4) $\rho_d^H = \rho_s^H \iff Hg = gH$, $\forall\, g \in G$

Dim: (1) << ESERCIZIO! IDEA (R) $\longleftrightarrow 1 \in H$, (T) $\longleftrightarrow H \cdot H \subseteq H$, (S) $\longleftrightarrow H^{-1} \subseteq H$ >>

OPPURE Sia $G/H := \{gH \mid g \in G\}$, $H\backslash G := \{Hg \mid g \in G\}$

$$\pi_s^H : G \twoheadrightarrow G/H \qquad g \longmapsto gH$$

&

$$\pi_d^H : G \twoheadrightarrow H\backslash G \qquad g \longmapsto Hg$$

La (2) ci dà $\rho_d^H = \rho_{\pi_d^H}$:= equivalenza associata a π_d^H

$\rho_s^H = \rho_{\pi_s^H}$:= equivalenza associata a π_s^H $\Longrightarrow$ (OK)

(2) $a \rho_d^H b \overset{\Delta}{\iff} ab^{-1} \in H \iff a \in Hb \iff Ha \subseteq Hb$

$\Updownarrow$ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\Updownarrow$ $\quad Ha = Hb$

$ba^{-1} \in H \iff b \in Ha \iff Hb \subseteq Ha$

OK

Analogamente, si ha

$a \rho_s^H b \overset{\Delta}{\iff} b^{-1}a \in H \iff a \in bH \iff aH \subseteq bH$

$\Updownarrow$ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\Updownarrow$ $\quad aH = bH$

$a^{-1}b \in H \iff b \in aH \iff bH \subseteq aH$

q.e.d.

(3) $\forall\, g \in G$, $\forall\, a \in G$ si ha

$a \in [g]_{\rho_d^H} \iff a \,\rho_d^H\, g \overset{(2)}{\iff} Ha = Hg \iff a \in Hg$

vd. oss. succ. (2)

per cui $[g]_{\rho_d^H} = Hg$ q.e.d.

Analogamente

$a \in [g]_{\rho_s^H} \iff a \,\rho_s^H\, g \overset{(2)}{\iff} aH = gH \iff a \in gH$

vd. oss. succ. (2)

per cui $[g]_{\rho_s^H} = gH$ q.e.d.

(4) $\rho_d^H = \rho_s^H \iff [g]_{\rho_d^H} = [g]_{\rho_s^H}$ $\forall g \in G$ $\overset{(3)}{\iff}$ $Hg = gH$ $\forall g \in G$

q.e.d. □

Proposizione 4: **Hp:** $H \leq G$

Th: (1) Tutte le classi laterali (destre e sinistre) modulo H sono equipotenti ad H stesso

(2) G/H e $H\backslash G$ sono equipotenti.

Dim: (1) Segue dall'$\exists$ delle due funzioni

$$H \longrightarrow Hg, \quad h \longmapsto hg \qquad \& \qquad H \longrightarrow gH, \quad h \longmapsto gh \qquad (\forall g \in G)$$

che sono ovviamente biiettive.

(2) Segue dall'$\exists$ delle due funzioni

$$G/H \xrightarrow{\sigma} H\backslash G \quad \& \quad H\backslash G \xrightarrow{\delta} G/H$$

$$gH \longmapsto Hg^{-1} \qquad Hg \longmapsto g^{-1}H$$

che sono inverse l'una dell'altra (ovvio),

MA bisogna provare che siano ben definite!

ORA $g_1H = g_2H \Rightarrow (g_1H)^{-1} = (g_2H)^{-1} \Rightarrow$

$\Rightarrow H^{-1}g_1^{-1} = H^{-1}g_2^{-1} \Rightarrow Hg_1^{-1} = Hg_2^{-1} \Rightarrow$

$\Rightarrow \sigma$ è ben definita, q.e.d. (ed è iniettiva, perché tutte le frecce si invertono...)

IDEM per δ... $\square$

Def. 5: $\forall\ H \leq G$, si definisce

INDICE di H (in G) $\triangleq (G:H) := \begin{cases} |G/H| \\ |H\backslash G| \end{cases}$

TEOREMA di LAGRANGE:

Hp: G gruppo finito, $H \leq G$

Th: $|G| = (G:H)\cdot|H|$, o $\quad \omega(G) = (G:H)\cdot\omega(H)$

In particolare, $|H| = \omega(H)$ e $(G:H)$ dividono $|G| = \omega(G)$.

Dim: Sia $k := (G:H)$, così $G/H = \{g_1H, \dots, g_kH\} \Rightarrow$

$\Rightarrow \exists$ partizione di G come $G = \coprod_{i=1}^{k} g_iH \Rightarrow$

$$\Rightarrow \boxed{|G|} = \left|\coprod_{i=1}^{k} g_iH\right| = \sum_{i=1}^{k} |g_iH| = \sum_{i=1}^{k} |H| = k\cdot|H| = \boxed{(G:H)\cdot|H|} \quad \square$$

(per la Proposizione 4)

COROLLARIO 6: **Hp:** G è gruppo finito.

Th: (1) $\forall g \in G$ si ha $\omega(g) \mid \omega(G) = |G|$

(2) Se $|G|$ è primo, allora
G ha soltanto i sottogruppi banali

(3) Se $|G| = p$ è primo, allora
G è ciclico, isomorfo a $(\mathbb{Z}_p ; +)$

Dim: (1) $\forall g \in G$, $\exists \langle g \rangle \leq G$, $\Rightarrow$ $\omega(g) = \omega(\langle g \rangle) \mid \omega(G) = |G|$ (ok)
(T. d. Lagrange)

(2) $\forall H \leq G \Rightarrow |H| \mid |G|$ primo $\Rightarrow |H| = \begin{cases} 1 \Rightarrow H = \{1_G\} \\ |G| \Rightarrow H = G \end{cases}$ (ok)
(T. d. Lagrange)

(3) $\forall g \in G \setminus \{1_G\} \Rightarrow \{1_G\} \neq \langle g \rangle \leq G \overset{(2)}{\Rightarrow} \langle g \rangle = G$

& $\omega(g) = \omega(\langle g \rangle) = \omega(G) = p \Rightarrow G = \langle g \rangle \cong (\mathbb{Z}_p ; +)$ □

Corollario 7 (PICCOLO TEOREMA DI FERMAT):

Hp: p primo, $a \in \mathbb{Z}$

Th: $a^p \equiv a \pmod p$ cioè $\bar{a}^p = \bar{a}$ in $\mathbb{Z}_p$

Dim.: La Th è ovvia per $a \equiv 0 \pmod p$ cioè $\bar{a} = \bar{0} \in \mathbb{Z}_p$

$\forall\, \bar{a} \in \mathbb{Z}_p \setminus \{\bar{0}\} \Rightarrow \bar{a} \in U(\mathbb{Z}_p) \Rightarrow \omega_\cdot(\bar{a}) \mid \omega(U(\mathbb{Z}_p)) = p-1 \Rightarrow$

$\Rightarrow \bar{a}^{p-1} = \bar{1}$ in $U(\mathbb{Z}_p) \Rightarrow \bar{a}^p = \bar{a}$ in $\mathbb{Z}_p$, q.e.d. □

Corollario 8 (TEOREMA DI EULERO - FERMAT):

Hp: $n \in \mathbb{N}_+$, $a \in \mathbb{Z}$: $MCD(a,n) = 1$

Th: $a^{\varphi(n)} \equiv 1 \pmod n$ cioè $\bar{a}^{\varphi(n)} = \bar{1}$ in $\mathbb{Z}_n$

Dim.: $MCD(a,n) = 1 \Rightarrow \bar{a} \in U(\mathbb{Z}_n) \Rightarrow \omega_\cdot(\bar{a}) \mid \omega_\cdot(U(\mathbb{Z}_n)) = \varphi(n) \Rightarrow$

$\Rightarrow \bar{a}^{\varphi(n)} = \bar{1}$ in $U(\mathbb{Z}_n) \Rightarrow \bar{a}^{\varphi(n)} = \bar{1}$ in $\mathbb{Z}_n$, q.e.d. □