LEZIONE 02-11-2025

Studio di D_n: determinare $\mathrm{Aut}(D_n)$ per $n \geq 3$

Ricordiamo che $\langle r \rangle =: R_n < D_n$ è caratteristico (perché è l'unico sottogr. di ordine n).

Quindi $\forall \varphi \in \mathrm{Aut}(D_n)$ si ha che $\varphi(r) \in R_n$ e $\mathrm{ord}\,\varphi(r) = n \Rightarrow \varphi(r) = r^k$ con $(k,n)=1$.

$$\begin{aligned} D_n &\xrightarrow{\sim} D_n \\ R_n &\longmapsto R_n \\ R_n \not\ni s &\longmapsto \varphi(s) \notin R_n \Rightarrow \varphi(s) = sr^h \quad \text{con } h \in [0, n-1] \cap \mathbb{Z}. \end{aligned}$$

Sia quindi $\varphi_{k,h}$ (se esiste) l'automorfismo $\begin{cases} r \mapsto r^k \\ s \mapsto sr^h \end{cases}$.

Verifichiamo che esiste, mostrando che le immagini scelte dei generatori diano ancora un gruppo con presentazione $\langle r^n = s^2 = 1,\ srs = r^{-1} \rangle$

- $\varphi(r)^n = 1$ sì perché $(r^k)^n = 1$
- $\varphi(s)^2 = 1$ sì perché $(sr^h)^2 = 1$
- $\varphi(s)\varphi(r)\varphi(s)\varphi(r) = 1$?

$$\underbrace{sr^h r^k s}_{r^{-h-k}} r^h r^k$$
$$r^{-h-k} r^{h+k} = 1$$

Quindi $\varphi_{k,h} \in \mathrm{End}(R_n)$.

È un isomorfismo?

Sì: $\mathrm{Imm}(\varphi) \ni r^k, sr^h$ che generano D_n

$$\Rightarrow \{\varphi_{k,h} : k \in (\mathbb{Z}/n\mathbb{Z})^\times, h \in \mathbb{Z}/n\mathbb{Z}\} = \mathrm{Aut}\, D_n.$$

Ma chi è $\mathrm{Aut}\, D_n =: G$ come gruppo astratto?

Osserviamo che
- $H_1 := \{\varphi_{1,h} : h \in \mathbb{Z}/n\mathbb{Z}\} < \mathrm{Aut}\, D_n$, $H_1 \cong \mathbb{Z}/n\mathbb{Z}$

(infatti $\varphi_{1,h}\varphi_{1,h'}(r) = r$, $\varphi_{1,h}\varphi_{1,h'}(s) = \varphi_{1,h}(sr^{h'}) = sr^{h+h'}$ $\Rightarrow \varphi_{1,h}\varphi_{1,h'} = \varphi_{1,h+h'}$)

- $H_2 := \{\varphi_{k,0} : k \in (\mathbb{Z}/n\mathbb{Z})^\times\} < \mathrm{Aut}\, D_n$, $H_2 \cong (\mathbb{Z}/n\mathbb{Z})^\times$

(infatti $\varphi_{k,0}\varphi_{k',0} = \begin{cases} r \mapsto r^{k'} \mapsto r^{kk'} \\ s \mapsto s \mapsto s \end{cases} = \varphi_{kk',0}$)

Inoltre $H_1 \cap H_2$ contiene gli autom. che fissano sia r che s $\Rightarrow H_1 \cap H_2 = \mathrm{id}$

Inoltre $H_1 \trianglelefteq \mathrm{Aut}(D_n)$:

$\varphi := \varphi_{k,h'} \varphi_{1,h} \varphi_{k,h'}^{-1} \overset{?}{\in} H_1 \iff \varphi$ fissa r

$$r \longmapsto r^{(k^{-1})} \longmapsto r^{(k^{-1})} \longmapsto r^{k(k^{-1})} = r \quad ✓$$

$$\Rightarrow G \simeq H_1 \rtimes H_2 \simeq \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times.$$

⌜OSS: $G \simeq \{ax+b : a \in \mathbb{Z}/n\mathbb{Z}^\times,\ b \in \mathbb{Z}/n\mathbb{Z}\}$. $H_1 \simeq$ Traslazioni $H_2 \simeq \{ax\}$. ⌟

Automorfismi di $D_m \times D_m$ con m dispari

Elenchiamone tanti!

OSS: $\mathrm{Aut}(G_1 \times G_2) \supseteq \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2)$

Quindi $\mathrm{Aut}(D_n^2) \supseteq \mathrm{Aut}(D_n)^2$. Ce n'è un altro evidente:

$$\tau : D_n \times D_n \xrightarrow{\sim} D_n \times D_n$$
$$(a,b) \longmapsto (b,a)$$

Sono tutti? Cerchiamo di capire $\varphi \in \mathrm{Aut}(D_n^2)$ dove può mandare i 4 generatori

$$(r,e) \qquad (s,e) \qquad (e,r) \qquad (e,s)$$

Vorremmo dire che $(r,e) \mapsto (r^k, e)$ oppure (e, r^k)

Vogliamo dire che (r^k,e), (e,r^k) sono gli unici el. che soddisfano una certa proprietà.

⌜OSS: dato che m è dispari $\Rightarrow Z(D_m \times D_m) \simeq Z(D_m) \times Z(D_m) = \{e\}$. ⌟

Osserviamo che $Z_G((r^i,e)) = \underbrace{R_m}_{\text{è indice 2 in } D_m} \times D_m$

$\Rightarrow Z_G((r^i,e))$ ha indice 2 in $D_m \times D_m$

Sia $(a,b) \in D_m^2$ t.c. $Z_G((a,b))$ ha indice 2.

$$Z_G((a,b)) = Z_{D_m}(a) \times Z_{D_m}(b) < D_m^2$$

Ma $[D_m^2 : Z_{D_m}(a) \times Z_{D_m}(b)] = [D_m : Z_{D_m}(a)] \cdot [D_m : Z_{D_m}(b)] \overset{!}{=} 2$

$\Leftrightarrow$ $\begin{cases} Z_{D_m}(a) = D_m \text{ e } Z_{D_m}(b) = R_m \Leftrightarrow a \in Z(D_m) = \{e\} \text{ e } b \in R_m \\ Z_{D_m}(b) = D_m \text{ e } Z_{D_m}(a) = R_m \Leftrightarrow b \in Z(D_m) = \{e\} \text{ e } a \in R_m. \end{cases}$

Siccome $|Z_G((r,e))| = \frac{1}{2}|G|$ segue che $|Z_G(\varphi(r,e))| = \frac{1}{2}|G|$

$\Rightarrow \varphi((r,e)) = (r^i, e)$ oppure (e, r^i)

Simmetricamente $\varphi((e,r)) = (r^i, e)$ oppure (e, r^i)

Per quanto ne sappiamo però potrebbe essere $\varphi((r,e)) = (r^i, e)$ ma $\varphi((e,r)) = (e, r^j)$.

Vorrei dire che ciò è impossibile ⌜o le coord. si scambiano oppure no⌟

Se $\varphi(r,e) = (e, r^j)$ e $\varphi(e,r) = (e, r^i)$, allora

$$\langle \varphi(r,e) \rangle = \langle \varphi(e,r) \rangle = \{id\} \times R_m \quad , \text{ma}$$

$\langle (r,e)\rangle \neq \langle (e,r)\rangle \implies \varphi\langle (r,e)\rangle \quad \varphi\langle (e,r)\rangle$

$\langle \varphi(r,e)\rangle \neq \langle \varphi(e,r)\rangle$

Dato $\varphi \in \mathrm{Aut}(D_m^2)$ qualsiasi, si ha che φ o $\tau\varphi$ non scambia le coordinate.

Componendo con un opportuno $\varphi_{a,0} \times \varphi_{b,0}$ posso supporre $\varphi((r,e)) = (r,e)$
$\varphi((e,r)) = (e,r)$

Sia φ un tale autom. Qual è l'imm. di (s,e)?

Siccome (e,r) e (s,e) commutano, $\varphi(e,r) = (e,r)$ e $\varphi(s,e)$ commutano.

$\implies \varphi(s,e)$ è un el. di ordine 2 in $Z_G((e,r)) = D_m \times R_m$.

m è dispari ⇓ non ha el. di ordine 2!

gli unici el. di ordine 2 sono le simm.

$\implies \varphi(s,e) = (sr^h, e)$

Simmetricamente $\varphi(e,s) = (e, sr^l)$

Componendo con $\varphi_{1,-h} \circ \varphi_{1,-l}$ ottengo che

$$\left.\begin{array}{ll} \varphi(r,e) = (r,e) & \varphi(e,r) = (e,r) \\ \varphi(s,e) = (s,e) & \varphi(e,s) = (e,s) \end{array}\right\} \implies \varphi = \mathrm{id}.$$

$\implies$ Dato un qualsiasi $\varphi \in \mathrm{Aut}(D_m^2)$ ho dim che posso trovare $\varepsilon \in \{0,1\}$, $a,b \in (\mathbb{Z}/n\mathbb{Z})^*$, $h,l \in \mathbb{Z}/n\mathbb{Z}$

tali che

$$\underbrace{(\varphi_{1,-h} \times \varphi_{1,-l})}_{\substack{(s,e)\mapsto(s,e)\\(e,s)\mapsto(e,s)}} \circ \underbrace{(\varphi_{a,0} \times \varphi_{b,0})}_{\substack{(r,e)\mapsto(r,e)\\(e,r)\mapsto(e,r)}} \circ \underbrace{\tau^{\varepsilon}}_{\text{le coord non si scambiano}} \circ \varphi = \mathrm{id}$$

$$\iff \varphi = \tau^{\varepsilon} \circ \underbrace{(\varphi_{a,0} \times \varphi_{b,0})^{-1} \circ (\varphi_{1,h} \circ \varphi_{1,l})}_{\in \mathrm{Aut}(D_m) \times \mathrm{Aut}(D_m)}$$

Dunque $\mathrm{Aut}(D_m^2) \underset{\text{Sets}}{=} (\mathrm{Aut}\, D_m)^2 \amalg \tau(\mathrm{Aut}\, D_m)^2$

Come gruppo? $\mathrm{Aut}(D_m^2) \overset{2}{\triangleright} (\mathrm{Aut}\, D_m)^2$ e $\mathrm{Aut}(D_m^2) > \langle \tau \rangle$.

La loro int. è banale $\implies \mathrm{Aut}(D_m \times D_m) \simeq (\mathrm{Aut}\, D_m \times \mathrm{Aut}\, D_m) \rtimes_{\psi} \mathbb{Z}/2\mathbb{Z}$

Ora $\psi : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathrm{Aut}\, D_m \times \mathrm{Aut}\, D_m)$

$1 \longmapsto (\varphi_1 \times \varphi_2 \longmapsto \varphi_2 \times \varphi_1)$

$$\big(\underset{\mathrm{Aut}(D_m^2)}{\tau(\varphi_1 \times \varphi_2)\tau}\big)(\underset{D_m^2}{a,b}) = \tau(\varphi_1 \times \varphi_2)(b,a) = \tau(\varphi_1(b), \varphi_2(a)) = (\varphi_2(a), \varphi_1(b))$$
$$= (\varphi_2 \times \varphi_1)(a,b) \quad ✓$$

$Aut(\mathbb{Z} \times \mathbb{Z}/_{13}\mathbb{Z})$

OSS: gli el. di $\mathbb{Z}$ hanno ord ∞, mentre quelli di $\mathbb{Z}/_{13}\mathbb{Z}$ sono tutti di ordine finito

$\Rightarrow \mathbb{Z}/_{13}\mathbb{Z}$ ha tutti e soli gli el di ordine finito $\Rightarrow \mathbb{Z}/_{13}\mathbb{Z}$ è caratteristico!

Altro modo: $\underset{(a,b)}{\varphi(1,0)} \overset{}{}$ deve avere ord ∞, $\underset{(c,d)}{\varphi(0,1)}$ deve avere ordine 13 $\Rightarrow$ l'ordine in $\mathbb{Z}\times\mathbb{Z}/_{13}\mathbb{Z}$ è il mcm degli ordini

$\varphi(1,0) = (a,b)$ Ma φ deve essere surg $\qquad \varphi(0,1) = (c,d)$

$\Rightarrow \varphi(0,1) = (0, d)$ con $d \in \mathbb{Z}/_{13}\mathbb{Z}^\times$

$\Rightarrow \operatorname{Im}\varphi = \langle \varphi(1,0), \varphi(0,1)\rangle$

$\mathbb{Z}\times\mathbb{Z}/_{13}\mathbb{Z} = \langle (a,b), (0,d)\rangle$ $\qquad \Rightarrow \varphi(\mathbb{Z}/_{13}\mathbb{Z}) = \mathbb{Z}/_{13}\mathbb{Z}$

$\Rightarrow (a,b) = (\pm 1, b)$.

Affermo ora che ogni scelta di $a \in \{\pm 1\}$, $b \in \mathbb{Z}/_{13}\mathbb{Z}$, $d \in (\mathbb{Z}/_{13}\mathbb{Z})^\times$ dà un automorfismo.

(*) È omom: banale

(*) Iniettività:

$$(0,0) = \varphi((x,y)) = x\varphi(1,0) + y\varphi(0,1) = x(a,b) + y(0,d) = (xa, bx+dy)$$

$\Rightarrow$. $xa = 0$ ma $a = \pm 1 \Rightarrow x = 0$ ✓

. $bx + dy \equiv 0 \ (13) \iff dy \equiv 0 \ (13) \iff y = 0$

(*) Surg: ✓

Dentro $Aut(\mathbb{Z}\times\mathbb{Z}/_{13}\mathbb{Z})$ ci sono $\to$ card: $2\cdot 13\cdot 12$

- $\tau = (x,y) \mapsto (-x, y)$ di ord 2 $\qquad H_1$
- $\psi_d = (x,y) \mapsto (x, dy)$ $\quad d \in (\mathbb{Z}/_{13}\mathbb{Z})^\times \Rightarrow$ sgrp $\simeq (\mathbb{Z}/_{13}\mathbb{Z})^\times$ $\qquad H_2$
- $\psi_b = (x,y) \mapsto (x, bx+y)$ $\quad b \in \mathbb{Z}/_{13}\mathbb{Z} \Rightarrow$ sgrp $\simeq \mathbb{Z}/_{13}\mathbb{Z}$ $\qquad H_3$

Allora: $\langle H_2, H_3\rangle \simeq \mathbb{Z}/_{13}\mathbb{Z} \rtimes (\mathbb{Z}/_{13}\mathbb{Z})^\times \overset{2}{\triangleleft} Aut(\mathbb{Z}\times\mathbb{Z}/_{13}\mathbb{Z})$

$$\Rightarrow Aut(\mathbb{Z}\times\mathbb{Z}/_{13}\mathbb{Z}) \simeq \left(\mathbb{Z}/_{13}\mathbb{Z} \rtimes (\mathbb{Z}/_{13}\mathbb{Z})^\times\right) \rtimes \mathbb{Z}/_2\mathbb{Z}.$$

∎

Classificare i gruppi di ordine dato

- $|G| = 16 \cdot 9$. Allora $G \simeq G(2) \times G(3)$

inoltre $G(2) \simeq \{ \mathbb{Z}/_{16\mathbb{Z}}, \mathbb{Z}/_{8\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}, \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{4\mathbb{Z}}, \mathbb{Z}/_{4\mathbb{Z}} \times (\mathbb{Z}/_{2\mathbb{Z}})^2, (\mathbb{Z}/_{2\mathbb{Z}})^4 \}$

$G(3) \simeq \{ \mathbb{Z}/_{9\mathbb{Z}}, (\mathbb{Z}/_{3\mathbb{Z}})^2 \}$

$\rightsquigarrow$ in tot. ho 10 possibilità

- $|G| = 105$. Vogliamo dim. che esistono 2 possibilità a meno di isom.

$\begin{array}{r|l} 105 & 5 \\ 5 & 21 \end{array}$

$105 = 3 \cdot 5 \cdot 7$

- $n_7 \mid 15$ e $n_7 \equiv 1 \ (7) \Rightarrow n_7 \in \{1, 15\}$
- $n_5 \mid 21$ e $n_5 \equiv 1 \ (5) \Rightarrow n_5 \in \{1; 21\}$
- $n_3 \mid 35$ e $n_3 \equiv 1 \ (3) \Rightarrow n_3 \in \{1; 7\}$

⊙ Se $n_7 = 15$ allora si hanno in G $15 \cdot 6 = 90$ el. di ordine 7

$\left[P_7 \simeq \mathbb{Z}/7 \Rightarrow P_7 \cap P_7' = \{e\} \right]$

Rimangono quindi 15 elementi di ordine $\neq 7$ $\Rightarrow$ non possono esserci 21 P_5 o 7 P_3 $\Rightarrow P_3, P_5 \triangleleft G$.

Siccome sono normali, $P_3 P_5 < G$ di ordine 15 $\Rightarrow P_3 P_5 \simeq \mathbb{Z}/_{15}\mathbb{Z} \triangleleft G$

Inoltre $P_3 P_5 \cap P_7 = \{e\}$ e $P_3 P_5 P_7 = G$

$\Rightarrow G \simeq P_3 P_5 \rtimes_\varphi P_7$

con $\varphi : P_7 \to \mathrm{Aut}(P_3 P_5) \simeq \mathbb{Z}/_2\mathbb{Z} \times \mathbb{Z}/_4\mathbb{Z}$ } deve essere banale!

$1 \longmapsto 1$

$\Rightarrow G \simeq \mathbb{Z}/_{105}\mathbb{Z}$. ASSURDO! $P_7 \triangleleft G$ ma avevamo supposto $n_7 = 15$.

⊙ Se $n_7 = 1$ allora $P_7 \triangleleft G \Rightarrow G \twoheadrightarrow G/_{P_7} \simeq \mathbb{Z}/_{15}\mathbb{Z}$

$\Rightarrow \exists\, gP_7 \in G/_{P_7}$ di ord 15 $\Rightarrow \mathrm{ord}\, g^{\in \pi^{-1}(gP_7)} \in \{15 ; 105\}$.

Se è 105 allora siamo nel caso $G \simeq \mathbb{Z}/_{105}\mathbb{Z}$

Altrimenti $\exists H \overset{\langle g \rangle}{<} G$ di ord 15 $\Rightarrow P_7 \cap H = \{e\}$

$\Rightarrow G \simeq P_7 \rtimes H \simeq \mathbb{Z}/_{7\mathbb{Z}} \rtimes_\varphi \mathbb{Z}/_{15}\mathbb{Z}$

$\varphi : \mathbb{Z}/_{15}\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/_7\mathbb{Z}) \simeq \mathbb{Z}/_6\mathbb{Z}$

$1 \longmapsto \cancel{1}, 2, 4$

↳ va in un el. di ord che divide 15 $\Rightarrow$ che divide 3

$\mathbb{Z}/_{105}\mathbb{Z}$

Vorremo dimostrare che ψ_2 e ψ_4 danno lo stesso prod. semidiretto.

Lo sappiamo se esistono $f \in Aut(\mathbb{Z}/_{15}\mathbb{Z})$ t.c. $\psi_4 = \psi_2 f$

Ma $4 = -2$ in $\mathbb{Z}/_6\mathbb{Z}$ $\Rightarrow$ $\psi_4 = \psi_2 \circ (-id)$

$\Rightarrow$ il semidiretto dato è lo stesso. $\boxtimes$