Automorfismi del gruppo diedrale

Deborah Scampuddu Relatore: Andrea Loi

Università di Cagliari - Corso di studi di Matematica

24 novembre 2022

Obiettivo

- Per $n \geq 3$ $|Aut(D_n)| = n\varphi(n)$, dove $\varphi(n)$ è la funzione di Eulero.
- Se p è un primo della forma $p = 1 + 2^k$ $(k \geq 2)$, allora $Aut(D_p)$ è un gruppo *POS* non abeliano il cui ordine non è divisibile per 3.

Indice

1 Gruppo diedrale
2 Automorfismi del gruppo diedrale
3 Classi d'ordine e gruppi POS

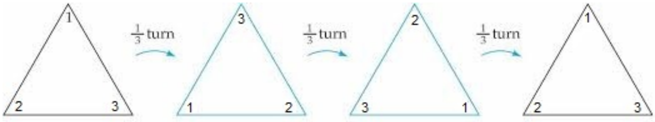
Gruppo diedrale

Rotazioni e riflessioni di un poligono regolare

Consideriamo un poligono regolare di n lati. Per ogni vertice individuiamo n rotazioni ed n riflessioni distinte.
Il gruppo costituito da tali isometrie è detto **gruppo diedrale**.

Rotazioni

Per $n \geq 3$ avremo n rotazioni determinate ruotando in senso antiorario i vertici del poligono di un angolo pari a $\frac{2\pi}{n}$.

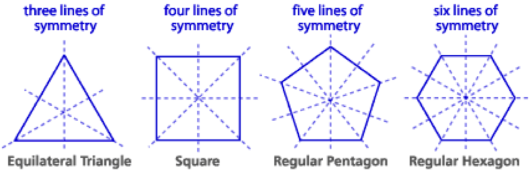


Gruppo diedrale

Riflessioni

Distinguiamo i casi in cui n sia pari o dispari.

- **n dispari**: avremo n riflessioni rispetto all'asse che passa per un vertice fissato e il punto medio del lato opposto.
- **n pari**: distinguiamo $\frac{n}{2}$ riflessioni rispetto all'asse che congiunge un vertice fissato e il punto medio del lato opposto e $\frac{n}{2}$ riflessioni rispetto all'asse che congiunge i punti medi di lati opposti.



Gruppo diedrale

Definizione 1.1

Un **gruppo diedrale** D_n è un gruppo generato da due elementi r_1 ed s_0 rispettivamente di ordine n e 2 tali che $s_0 r_1 s_0^{-1} = r_1^{-1}$.
Ovvero $D_n = \langle r, s \mid r^n = s^2 = (r^k s)^2 = id,\ k = 1, 2, , , n \rangle$.

Osservazione 1.1

Introduciamo un'operazione binaria su D_n tramite le seguenti relazioni:

$$r_i r_j = r_{i+j \bmod n} \qquad r_i s_j = s_{i+j \bmod n}$$
$$s_i s_j = r_{i-j \bmod n} \qquad s_i s_j = s_{i-j \bmod n}$$

$\forall\ 0 \leq i, j \leq n - 1$

Automorfismi del gruppo diedrale

Definizione 2.1

Sia G un gruppo. Un **automorfismo** di G è un isomorfismo da G in se stesso.

Osservazione 2.1

L'insieme $Aut(G)$=$\{\phi : G \to G \mid \phi$ è un automorfismo$\}$
è un gruppo rispetto all'operazione di composizione di funzioni.

Automorfismi del gruppo diedrale

Teorema 2.1

Per $n \geq 3$ $|Aut(D_n)| = n\varphi(n)$.

Dimostrazione

Sia $\phi : D_n \to D_n$ un automorfismo. Per le proprietà degli omomorfismi $o(\phi(r_1)) = n$ e $o(\phi(s_0)) = 2$ e dalla definizione di gruppo diedrale segue che $D_n = \langle \phi(r_1), \phi(s_0) \rangle$. Per $n \geq 3$ $\phi(r_1) = r_k$ per qualche $0 \leq k \leq n-1$ e $(k, n) = 1$ e $\phi(s_0) = s_j$ per qualche $0 \leq j \leq n-1$.
Allora $|Aut(D_n)| \leq n\varphi(n)$.
Al contrario, per ogni $0 \leq k, j \leq n-1$ con $(k, n) = 1$, sia $\phi_{k,j} : D_n \to D_n$ una funzione tale che $\forall$ $0 \leq i \leq n-1$

$$\phi_{k,j}(r_i) = r_{ik \bmod n} \qquad \phi_{k,j}(s_i) = s_{ik+j \bmod n}$$

Automorfismi del gruppo diedrale

Dimostrazione

Presi $0 \leq i, t \leq n-1$, allora:

- $\phi_{k,j}(r_i r_t) = \phi_{k,j}(r_{i+t}) = r_{(i+t)k \bmod n} = r_{ik \bmod n} r_{tk \bmod n} = \phi_{k,j}(r_i)\phi_{k,j}(r_t)$
- $\phi_{k,j}(s_i s_t) = \phi_{k,j}(r_{i-t}) = r_{(i-t)k \bmod n} = s_{ik+j \bmod n} s_{tk+j \bmod n} = \phi_{k,j}(s_i)\phi_{k,j}(s_t)$
- $\phi_{k,j}(r_i s_t) = \phi_{k,j}(s_{i+t}) = s_{(i+t)k+j \bmod n} = r_{ik \bmod n} s_{tk+j \bmod n} = \phi_{k,j}(r_i)\phi_{k,j}(s_t)$
- $\phi_{k,j}(s_t r_i) = \phi_{k,j}(s_{t-i}) = s_{(t-i)k+j \bmod n} = s_{tk+j \bmod n} r_{ik \bmod n} = \phi_{k,j}(s_t)\phi_{k,j}(r_i)$

$\implies \phi_{k,j} : D_n \to D_n$ è un omomorfismo.

Automorfismi del gruppo diedrale

Dimostrazione

Essendo $\phi_{k,j}(r_1) = r_k$ e $\phi_{k,j}(s_0) = s_j$ con $(k,n) = 1$, segue che

$$D_n = \langle r_k, s_j \rangle \subseteq \phi_{k,j}(D_n) \subseteq D_n$$

da cui $\phi_{k,j}(D_n) = D_n$, ovvero $\phi_{k,j}$ è <u>suriettiva</u>.
Ma D_n è un gruppo finito, quindi $\phi_{k,j}$ è anche <u>iniettiva</u>.
Quindi $\phi_{k,j}$ è un automorfismo $\forall\ 0 \leq k, j \leq n-1$ e $(k,n) = 1$.
Pertanto $|Aut(D_n)| \geq n\varphi(n)$.
$\Longrightarrow |\mathrm{Aut}(\mathrm{D}_n)| = n\varphi(n)$ ∎

Automorfismi del gruppo diedrale

Definizione 2.2

Per un numero naturale n definiamo l'insieme delle matrici:

$$\tilde{G}_n = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| \, a \in \mathbb{Z}_n^* \text{ e } b \in \mathbb{Z}_n \right\}$$

Allora $\tilde{G}_n$ è un gruppo di ordine $n\varphi(n)$ rispetto al prodotto tra matrici.

Osservazione 2.2

Si dimostra che $Aut(D_n) \simeq \tilde{G}_n$ per ogni n tramite l'isomorfismo:

$$\psi(\phi_{i,j}) = \begin{pmatrix} i & j \\ 0 & 1 \end{pmatrix}$$

$\forall\ 0 \leq i, j \leq n-1,\ (i,n)=1.$

Classi d'ordine e gruppi POS

Definizione 3.1

Sia G un gruppo finito e sia $S(G) = \{o(x) \mid x \in G\}$ l'insieme di tutti gli ordini possibili in G.
Per ogni $k \in S(G)$ denotiamo con $S_k = \{x \in G \mid o(x) = k\}$ l'insieme degli elementi di G che hanno ordine k.
La **classe d'ordine** di G è definita come l'insieme delle coppie $\{(k, |S_k|) : k \in S(G)\}$.

Definizione 3.2

Diciamo che un gruppo G ha sottoinsiemi di ordine perfetto **(Perfect Order Subset o POS group)** se la cardinalità di S_k divide l'ordine di G per ogni k.

Classi d'ordine e gruppi POS

Teorema 3.1

Sia p un numero primo. Allora la classe d'ordine di $Aut(D_p)$ è:
$\{(1,1),(p,p-1),(k,p\varphi(k)) : k \in d(p-1), k \neq 1\}$

Osservazione 3.1

Per $n > 1$ $\varphi(k)$ divide n $\forall k \in d(n) \Longleftrightarrow$ n=$2^k 3^l$, $k \geq 1$, $l \geq 0$.

Classi d'ordine e gruppi POS

Corollario 3.1

$Aut(Dp)$ è un gruppo *POS* $\iff$ $p = 1 + 2^k 3^l$ per qualche k $\geq$ 1, l $\geq$ 0.

Dimostrazione

Dal Teorema 2.1 sappiamo che $|Aut(D_p)| = p(p-1)$.
Per il Teorema 3.1 allora $Aut(D_p)$ è un gruppo *POS* $\iff$ $\varphi(k)$ divide $p - 1$ $\forall$ k $\in d(p-1)$.
Dall'osservazione 3.1 segue dunque che $Aut(Dp)$ è un gruppo *POS* $\iff$ $p = 1 + 2^k 3^l$. ∎

Classi d'ordine e gruppi POS

Teorema 3.2

Sia p un primo della forma $p = 1 + 2^k$ $(k \geq 2)$.
Allora $Aut(D_p)$ è un gruppo *POS* non abeliano il cui ordine non è divisibile per 3.

Dimostrazione

Sia p della forma $1 + 2^k$. Applicando il Corollario 3.1 per $l = 0$ segue che $Aut(D_p)$ è un gruppo *POS*.
Sappiamo che $|Aut(D_p)| = p(p-1) = (1+2^k)2^k$, ma essendo per ipotesi $k \geq 2$, $p \geq 5$ quindi $|Aut(D_p)|$ non è divisibile per 3.
Ricordando che $Aut(D_p)$ è isomorfo al gruppo non abeliano delle matrici $\tilde{G}_n$ concludiamo che $Aut(D_p)$ è un gruppo *POS* non abeliano il cui ordine non è divisibile per 3. ∎

Grazie per l'attenzione!