# I prodotti semidiretti e i gruppi complementari

Francesca Erdas Relatore: Andrea Loi

Università degli studi di Cagliari-Corso di studi Matematica

24 Febbraio 2023

## Obiettivi

- Classificare i gruppi di ordine $pq$, con $p,q$ primi e $q \equiv 1 \mod p$, utilizzando i prodotti semidiretti di gruppi.
- Dare delle condizioni equivalenti all'esistenza di sottogruppi complementari ad un sottogruppo normale di un gruppo dato.

## Indice

# Prodotti semidiretti

## Definizione

Dati due gruppi $H$ e $K$ e un omomorfismo $\varphi : K \to Aut(H)$, il corrispondente **prodotto semidiretto** $H \times_{\varphi} K$ è l'insieme:

$$H \times K = \{(h, k) : h \in H, k \in K\},$$

con il prodotto:

$$(h, k)(h', k') = (h\varphi_k(h'), kk').$$

## Osservazione

Si verifica, usando la definizione di prodotto semidiretto, che $H \times_{\varphi} K$ è un gruppo.

# Alcuni teoremi sui prodotti semidiretti

**Teorema 1**

Sia $G$ un gruppo, $H, K < G$ tali che:

(1) $G = HK$

(2) $H \cap K = \{1\}$

(3) $H \lhd G$

e sia $\varphi : K \to Aut(H)$ definita come segue: $\varphi_k(h) = khk^{-1}$, $k \in K$, $h \in H$.
Allora $\varphi$ è un omomorfismo e l'applicazione $f : H \times_\varphi K \to G$ definita come $f(h, k) = hk$ è un isomorfismo.

# Alcuni teoremi sui prodotti semidiretti

**Teorema 2**

Siano $f : H_1 \to H_2$ e $f' : K_1 \to K_2$ isomorfismi di gruppi. Per ogni omomorfismo $\varphi : K_1 \to Aut(H_1)$ esiste un omomorfismo $\varphi' : K_2 \to Aut(H_2)$ tale che:

$$H_1 \times_\varphi K_1 \cong H_2 \times_{\varphi'} K_2.$$

# Alcuni teoremi sui prodotti semidiretti

**Lemma**

Siano $H$ e $K$ due gruppi e $\varphi : K \to Aut(H)$ un omomorfismo. Allora per ogni automorfismo $f : K \to K$ vale:

$$H \times_{\varphi \circ f} K \cong H \times_{\varphi} K.$$

## Gruppi di ordine $pq$ con $p, q$ primi e $q \equiv 1 \mod p$

**Teorema 3**

Se i primi $p < q$ soddisfano $q \equiv 1 \mod p$ allora, a meno di isomorfismi, ci sono due gruppi di cardinalità $pq$: uno è ciclico e uno è non abeliano.

# Gruppi di ordine $pq$ con $p, q$ primi e $q \equiv 1 \mod p$

**Dimostrazione**

Per ipotesi $|G| = pq$ e $p, q$ sono primi, perciò, per il teorema di Cauchy, esistono $P$ e $Q$ sottogruppi di $G$ rispettivamente con cardinalità $p$,$q$. Siano $n_p$ e $n_q$ il numero di $p-$sottogruppi di Sylow e $q-$sottogruppi di Sylow di $G$. Dall'ipotesi che $p$,$q$ sono primi segue che:

- $n_q = 1$, quindi $Q \lhd G$ (secondo e terzo teorema di Sylow);
- $n_p = 1$ oppure $n_p = q$ (secondo e terzo teorema di Sylow);
- $P \cap Q = \{1\}$.

Caso $n_p = 1$
Si dimostra che se $x \in P$ e $y \in Q$ con $x, y \neq 1$ allora $xy = yx$, da cui segue che: $o(xy) = pq$, quindi $G = \langle xy \rangle$. Perciò $G$ è ciclico.

# Gruppi di ordine $pq$ con $p, q$ primi e $q \equiv 1 \mod p$

**Dimostrazione**

CASO $n_p = q$

Si dimostra che vale la seguente implicazione: $Q \triangleleft G \Rightarrow G = PQ$. Perciò dal teorema 1 segue che: $G \cong Q \times_{\varphi} P$, dove $\varphi : P \to Aut(Q)$ è definita come $\varphi_k(h) = khk^{-1}$, $k \in P, h \in Q$.

Dal teorema 2 segue che: esiste $\varphi' : \mathbb{Z}_p \to Aut(\mathbb{Z}_q)$ omomorfismo tale che $Q \times_{\varphi} P \cong \mathbb{Z}_q \times_{\varphi'} \mathbb{Z}_p$. Quindi $G \cong \mathbb{Z}_q \times_{\varphi'} \mathbb{Z}_p$.

Si può ora dimostrare che, se $n_p = q$, a meno di isomorfismi, esiste un unico gruppo $G$ non abeliano, con $|G| = pq$ e $q \equiv 1 \mod p$. La prova si basa sui seguenti punti:

- Se $\varphi' : \mathbb{Z}_p \to Aut(\mathbb{Z}_q)$ omomorfismo non banale, allora $\varphi'_1(1)$ soddisfa le condizioni: $z^p \equiv 1 \mod q$, $z \neq 1$;
- $\{z \in (\mathbb{Z}_q)^x : z^p \equiv 1 \mod q\}$ è un sottogruppo di $(\mathbb{Z}_q)^x$ di ordine $p$;

# Gruppi di ordine $pq$ con $p, q$ primi e $q \equiv 1 \mod p$

**Dimostrazione**

- Dati due omomorfismi non banali $\varphi', \psi' : \mathbb{Z}_p \to Aut(\mathbb{Z}_q)$, esiste $f : \mathbb{Z}_p \to \mathbb{Z}_p$ automorfismo tale che $\psi' = \varphi' \circ f$. Perciò dal lemma segue che: $\mathbb{Z}_q \times_{\varphi'} \mathbb{Z}_p \cong \mathbb{Z}_q \times_{\psi'} \mathbb{Z}_p$;
- Se $\varphi' : \mathbb{Z}_p \to Aut(\mathbb{Z}_q)$ omomorfismo non banale, allora $\mathbb{Z}_q \times_{\varphi'} \mathbb{Z}_p$ è non abeliano $\square$

# Gruppi complementari

**Definizione**

Sia $G$ un gruppo e $H, K$ due suoi sottogruppi tali che:

- $G = HK$
- $H \cap K = \{1\}$

allora $H$ e $K$ sono chiamati sottogruppi complementari.

# Gruppi complementari

## Osservazioni

1) Dato un sottogruppo $H \lhd G$ non è detto esista un sottogruppo complementare:
   Sia $G$ un gruppo ciclico con $|G| = p^\alpha$, $p$ primo, $\alpha \geq 2$, $\alpha \in \mathbb{N}$ e $H \lhd G$, $1 < |H| < |G|$. Supponiamo che $G = HK$, con $K < G$. Per il teorema di Cauchy $H$ e $K$ hanno sottogruppi di ordine $p$. Poichè $G$ è ciclico, ha un solo sottogruppo di ordine $p$, perciò $H$ e $K$ hanno lo stesso sottogruppo di ordine $p$. Quindi $H \cap K \neq \{1\}$, di conseguenza $H$ non ha sottogruppi complementari.

2) Dal teorema 1 sappiamo che: se $H \lhd G$ e $\exists\, K$ t.c. $H, K$ siano sottogruppi complementari $\Rightarrow \exists\, \varphi$ omomorfismo t.c. $G \cong H \times_\varphi K$.

Quindi è utile studiare l'esitenza di sottogruppi complementari ad un sottogruppo dato $H \lhd G$.

# Gruppi complementari

**Teorema 4**

Sia $H \lhd G$, allora le seguenti condizioni sono equivalenti:

(1) esiste un sottogruppo $K$ complememtare ad $H$ in $G$;

(2) per ogni classe laterale di $G/H$ si può scegliere un rappresentante in modo che l'insieme dei rappresentanti scelti formi un sottogruppo di $G$;

(3) esiste una sezione della proiezione canonica $\pi : G \to G/H$.

**Definizione**

Siano $G_1$ e $G_2$ due gruppi e $\varphi : G_1 \to G_2$ un omomorfismo suriettivo, una sezione di $\varphi$ è un omomorfismo $\psi : G_2 \to G_1$ tale che $\varphi(\psi(y)) = y, \forall y \in G_2$.

# Gruppi complementari

Dimostrazione

**(1) ⇒ (2)**

Per ipotesi $G = HK$, perciò, dato $g \in G$ $\exists h \in H, k \in K$ tali che $g = hk$ e poichè $hk \equiv k \bmod H$, allora $\forall g \in G$ esiste $k \in K$ che è rappresentante della classe di $g$ in $G/H$.
Dall'ipotesi $H \cap K = \{1\}$ segue che $\forall k_1, k_2 \in K$ tali che $k_1 \equiv k_2 \bmod H$ si ha $k_1 = k_2$. Quindi per ogni classe esiste un unico rappresentante $k \in K$.
Perciò l'insieme $K$ è un sottogruppo che rispetta la condizione (2).

**(2) ⇒ (1)**

Sia $K$ un sottogruppo che rispetta la condizione (2). Segue che $G = HK$ e $H \cap K = \{1\}$. Perciò $H$ e $K$ sono sottogruppi complementari.

**Dimostrazione**

**(1) $\Rightarrow$ (3)**

Per ipotesi $G = HK \Rightarrow \forall g \in G, \exists h \in H,\ k \in K$ tali che $g = hk \Rightarrow \bar{g} = \bar{k}$.

Definiamo $s : G/H \to G$ come: $s(\bar{g}) = k$. Segue che:

- $s$ è ben definita;
- $\pi(s(\bar{g})) = \bar{g},\ \forall g \in G$;
- $s$ è un omomorfismo di gruppi.

Perciò $s$ è una sezione.

# Gruppi complementari

Dimostrazione

**(3) $\Rightarrow$ (1)**

Per ipotesi esiste $s : G/H \to G$ omomorfismo tale che $\pi(s(\bar{g})) = \bar{g}$, $\forall \bar{g} \in G/H$ e definiamo $K = s(G/H)$. Segue che:

- $K$ è sottogruppo di $G$;
- $G = HK$;
- $H \cap K = \{1\}$.

Pertanto $H, K$ sono sottogruppi complementari in $G$ $\square$