Appunti di Esercitazione di Algebra I

Indice

Premesse

Questi appunti sono la riscrittura fatta da alunni di quanto detto dal prof. Callegaro durante le esercitazioni del corso di Algebra I, non vanno perciò intesi in nessun senso come dispense uffici del corso, sebbene alcune parti siano state riviste direttamente dal prof. Callegaro (cosa per cui lo ringraziamo).

Esercitazione 1

Il gruppo diedrale

Approfondimenti sul gruppo diedrale

Definizione 1 (Gruppo diedrale)**.** Sia $\mathcal{D}_n$ (con $n > 2$) l'insieme dei simboli $\sigma^i\rho^j$ (con $i \in \{0,1\}, j \in \{0,\dots,n-1\}$) dove:

$$\begin{aligned}\sigma^i\rho^j = \sigma^{i'}\rho^{j'} &\iff i = i',\ j = j'\\ \sigma^2 = \rho^n &= e\\ \sigma\rho &= \rho^{-1}\sigma\end{aligned}$$

(Come in ogni gruppo vale la proprietà associativa, inoltre pensando gli esponenti di ρ come interi modulo n e gli esponenti di σ come interi modulo 2 valgono per i prodotti la relazione $\rho^i\rho^j = \rho^{i+j}$ e l'analoga relazione per σ). Possiamo visualizzare in questo modo il gruppo diedrale: sia ρ una rotazione di $\mathbb{R}^2$ attorno all'origine di $\frac{2\pi}{n}$ gradi e σ la riflessione attorno all'asse verticale. $\mathcal{D}_n$ può essere visto come il gruppo delle isometrie del piano generate da σ e da ρ.

Osservazione 1. Possiamo visualizzare in questo modo il gruppo diedrale: sia ρ una rotazione di $\mathbb{R}^2$ attorno all'origine di $\frac{2\pi}{n}$ gradi e σ la riflessione attorno all'asse verticale. $\mathcal{D}_n$ può essere visto come il gruppo delle isometrie del piano generate da σ e da ρ.
Possiamo equivalentemente vedere il gruppo diedrale come il gruppo delle isometrie del piano che mandano un n-agono regolare in se stesso, con l'operazione di composizione. Anche in questo caso vi sono due generatori (che chiameremo comunque ρ e σ): la rotazione dell'n-agono attorno al suo centro che manda ciascun vertice nel vertice a lui adiacente (supponiamo in senso "orario") e la riflessione rispetto a un suo asse di simmetria.
Valgono chiaramente le regole che abbiamo dato nella definizione di gruppo diedrale.

Riflessione 1. Abbiamo definito in modo astratto il gruppo diedrale, e nella sua definizione è caratterizzante soprattutto la terza relazione che abbiamo dato:

$$\sigma\rho = \rho^{-1}\sigma \text{ o, equivalentemente, } \sigma\rho\sigma = \rho^{-1}$$

Abbiamo poi dato un modello geometrico del gruppo diedrale, dobbiamo quindi dimostrare che il modello in effetti corrisponde alla definizione data. Per ogni asse di riflessione che possiamo scegliere, la struttura del modello del gruppo

diedrale non cambia. Questo è vero perché, scelto un altro asse di simmetria, la riflessione σ' rispetto al nuovo asse può essere scritta come:

$$\sigma' = \sigma\rho^k$$

Per un opportuno k.
Vediamo che valgono comunque le tre proprietà della definizione (utilizzando il fatto, vero per il punto 2 della definizione, che non ci interessano tanto gli esponenti dei generatori quanto la loro classe di resto modulo, rispettivamente, 2 e n):

$$\sigma'^i\rho^j = \sigma'^{i'}\rho^{j'} \iff (\sigma\rho^k)^i\rho^j = (\sigma\rho^k)^{i'}\rho^{j'} \iff i = i',\ j = j'$$
$$(\sigma\rho^k)^2 = (\sigma\rho^k)(\sigma)(\rho^k) = (\sigma\rho\sigma\sigma\rho\sigma\ldots\sigma\rho)(\ \sigma\ )(\rho^k) = \rho^{-k}\rho^k = e$$
$$\sigma\rho^k\rho = \rho^{-1}\sigma\rho^k \iff \sigma\rho^{k+1} = \sigma\rho\sigma\sigma\rho^k$$

Osservazione 2. Chiamiamo:

- Rotazioni le potenze di ρ. Quindi sono rotazioni $e, \rho, \ldots, \rho^{n-1}$.
- Riflessioni, l'elemento σ e tutti i prodotti di σ per una rotazione (che possono essere visti come riflessioni rispetto a un diverso asse di simmetria). Questi possono essere tutti scritti nella forma $\sigma\rho^i$ per qualche $i = 0, \ldots, n-1$.

Abbiamo quindi trovato che nel gruppo diedrale vi sono $2n$ elementi, infatti tutti questi elementi sono diversi per il primo punto della definizione, inoltre questi sono chiaramente tutti gli elementi del gruppo, sempre per la definizione. Se vogliamo invece prendere il modello delle simmetrie del n-agono regolare, per dimostrare che questo gruppo contiene esattamente $2n$ elementi possiamo innanzitutto dimostrare che ce ne sono almeno $2n$ (le potenze della rotazione e le composizioni fatte dalla riflessione composta una qualsiasi rotazione, tutti elementi distinti), inoltre non possono essercene altri perché quelli contati contengono i generatori e inoltre formano un gruppo (andrebbe dimostrato: ogni elemento ha il suo inverso e la composizione vi appartiene sempre), non possono quindi che essere tutto il modello del gruppo diedrale.

Riflessione 2. Chi sono i sottogruppi di $\mathcal{D}_n$? Sicuramente ci sono $\{e\}$ e $\mathcal{D}_n$.
Si verifichi che i seguenti insiemi sono sottogruppi non banali:

- $< \rho >= \{\rho, \rho^2, \ldots, \rho^n\} \simeq \mathbb{Z}_n$.
- $\forall i$, $\{e, \sigma\rho^i\}$ è un altro sottogruppo.
- Poi possiamo considerare i sottogruppi di $\mathbb{Z}_n$ infatti abbiamo i vari $< \rho^{\frac{n}{m}} >$

Ma ci occorre un metodo per trovare tutti i sottogruppi.
Osserviamo intanto che $< \rho > \simeq \mathbb{Z}_n$ è un sottogruppo normale di $\mathcal{D}_n$ (chiamiamolo N). Dimostriamo che N è normale. Per dimostrare che è normale è sufficiente dimostrare che viene preservato dal coniugio per un generico elemento di $\mathcal{D}_n$. Ma per farlo ci è sufficiente mostrare che un suo generatore (ρ) viene sempre coniugato in un altro elemento di N, se infatti prendiamo un elemento di N che non è generatore lo possiamo vedere come potenza di ρ e riportarlo a

questo caso. Inoltre il diedrale è generato da due elementi, quindi ci basta verificare che un generatore di N viene mandato in N quando coniughiamo rispetto ai generatori del gruppo diedrale. Dobbiamo verificare quindi solo che:

$$\rho\rho\rho^{-1} \in N. \text{ Ovvio.}$$
$$\sigma\rho\sigma^{-1} \in N. \text{ Ma } \sigma\rho\sigma^{-1} = \sigma^{-1}\rho\sigma = \rho^{-1} \in N.$$

Quindi N in effetti è normale.
Sia ora $H < \mathcal{D}_n$ un generico sottogruppo di $\mathcal{D}_n$. Possiamo vedere cosa si ottiene con $H \cap N < \mathcal{D}_n$ (l'intersezione è un sottogruppo di N), questo ci è utile perché conosciamo già i sottogruppi di N (visto che è isomorfo a $\mathbb{Z}_n$).
Abbiamo chiaramente due possibilità: $H < N \implies H = H \cap N$. Oppure $H \not< N$, quindi H deve contenere almeno una riflessione. Ma se H non è contenuto in N vogliamo dimostrare che H è fatto di due sottoinsiemi con la stessa cardinalità:

$$H = (H \cap N) \cup (H \cap (\mathcal{D}_n - N))$$

Questi due sottoinsiemi di H sono chiaramente disgiunti. Vogliamo dimostrare che hanno la stessa cardinalità.
Vogliamo quindi trovare una bigezione tra $H \cap N$ e $H \cap (\mathcal{D}_n - N)$. Sia ξ una riflessione che stiamo supponendo appartenere ad H e consideriamo:

$$\begin{array}{rccc} f: & H \cap N & \longrightarrow & H \cap (\mathcal{D}_n - N) \\ & h & & h\xi \end{array}$$

Questa mappa è chiaramente iniettiva e surgettiva (semplici verifiche: L'inversa manda infatti la riflessione g' in $g'\xi$, che sarà una rotazione.
Abbiamo quindi che, se H non è sottogruppo di N, H è spezzato in due sottoinsiemi, che sono mandati l'uno nell'altro da un qualsiasi elemento di $H \cap (\mathcal{D}_n - N)$. Qualunque cosa succeda, dunque, $H \cap N$ sarà un sottogruppo (ciclico) di N, generato quindi da una rotazione. Nel caso interessante (H non è sottoinsieme di N) abbiamo che il completamento ad H di $H \cap N$ è l'immagine di un'applicazione che riflette ogni rotazione di $H \cap N$ di una riflessione fissata appartenente ad $H \cap (\mathcal{D}_n - N)$. Abbiamo quindi in questo caso

$$H \simeq \mathcal{D}_m = \langle \rho^{\frac{n}{m}}, \xi \mid (\rho^{\frac{n}{m}})^m = e,\ \xi^2 = e,\ \xi\rho^{\frac{n}{m}}\xi = \rho^{-\frac{n}{m}} \rangle$$

Si dimostra che infatti è isomorfo al gruppo diedrale con i generatori detti.
Si dimostra che infatti è isomorfo al gruppo diedrale con i generatori $\rho^{\frac{n}{m}}, \xi$.
Possiamo infatti definire opportunamente un omomorfismo da $\mathcal{D}_m$ ad H che manda gli usuali generatori di $\mathcal{D}_m$ nei generatori $\rho^{\frac{n}{m}}, \xi$ di H ed è ben definito perché i generatori di H soddisfano le stesse relazioni dei generatori del gruppo diedrale. I due gruppi hanno la stessa cardinalità e l'omomorfismo è chiaramente surgettivo, dunque è un isomorfismo.
Questo però non ci è sufficiente per concludere, sappiamo infatti che, fissato m *t.c.* $m \mid n$, esiste un unico sottogruppo isomorfo a $\mathbb{Z}_m$ in N, ma non sappiamo quanti sono i sottogruppi isomorfi a $\mathcal{D}_m$ in $\mathcal{D}_n$.
Per esempio nel caso banale in cui $H \cap N = \{e\}$ e H non è contenuto in N, abbiamo $H \simeq \mathcal{D}_1$, ma ci sono n gruppi isomorfi a $\mathcal{D}_1$ in $\mathcal{D}_n$, uno per ogni rotazione.
Sappiamo che un qualsiasi sottogruppo di $\mathcal{D}_n$ della forma $\mathcal{D}_m$ può essere scritto come:

$$< \rho^{\frac{n}{m}}, \sigma\rho^i > = < \rho^{\frac{n}{m}}, \sigma\rho^{i+\frac{n}{m}} >$$

Quindi in generale

$$< \rho^{\frac{n}{m}}, \sigma\rho^i >=< \rho^{\frac{n}{m}}, \sigma\rho^j > \iff i \equiv j \left(\frac{n}{m}\right)$$

La freccia $\Longleftarrow$ è ovvia. Per l'altra consideriamo che solo una ed una sola delle riflessioni in $< \rho^{\frac{n}{m}}, \sigma\rho^i >$ è nella forma $\sigma\rho^k$ con $0 \leq k < \frac{n}{m}$ (e se questa appartenesse a due sottogruppi, genererebbe entrambi e quindi sarebbero lo stesso).
Pertanto se due gruppi $< \rho^{\frac{n}{m}}, \sigma\rho^i >,< \rho^{\frac{n}{m}}, \sigma\rho^j >$ hanno la stessa intersezione con l'insieme delle riflessioni $\{\sigma\rho^h \mid 0 \leq h < \frac{n}{m}\}$ allora necessariamente le riflessioni $\sigma\rho^i$, $\sigma\rho^j$ devono differire per una rotazione $\rho^{\frac{n}{m}}$, ovvero i e j differiscono per un multiplo di $\frac{n}{m}$.
Quindi o $H < N =< \rho >$, ed in questo caso abbiamo un sottogruppo di questo tipo per ogni divisore di n, oppure H non è contenuto in N ed è isomorfo a $\mathcal{D}_m$, con $m \mid n$, ma in tal caso abbiamo diverse possibilità: per m fissato abbiamo esattamente $\frac{n}{m}$ gruppi distinti tutti isomorfi a $\mathcal{D}_m$.
Quali sono i sottogruppi normali? Un sottogruppo è normale se e solo se è unione di classi di coniugio dei suoi elementi. Possiamo dividere $\mathcal{D}_n$ per classi (di equivalenza) di coniugio e vedere quali unioni sono sottogruppi (ciascuna di queste classi deve appartenere del tutto o essere del tutto disgiunta rispetto a un sottogruppo normale).
Cerchiamo quindi le classi di coniugio in $\mathcal{D}_n$. Notiamo per prima cosa che una rotazione può essere coniugata solo ad altre rotazioni ed una riflessione può essere coniugata solo ad altre riflessioni.

- Consideriamo una generica rotazione ρ^i essa è coniugata solo a se stessa e alla sua inversa. Se n è dispari abbiamo quindi le seguenti classi di equivalenza: $\{e\}$, $\frac{n-1}{2}$ classi della forma $\{\rho^i, \rho^{-i}\}$; se invece n è pari abbiamo $\{e\}, \{\rho^{\frac{n}{2}}\}$ e $\frac{n-2}{2}$ classi della forma $\{\rho^i, \rho^{-i}\}$. Abbiamo quindi che:
  - Coniugando ρ^i rispetto a una rotazione si ottiene ρ^i (infatti le rotazioni commutano tra loro).
  - Coniugandola per una riflessione abbiamo due possibili casi:
    a) Se n è dispari abbiamo due tipi diversi di classi di coniugio: $\{e\}$ oppure abbiamo $\frac{n-1}{2}$ classi di coniugio della forma $\left\{\rho^i, \rho^{-i}\right\}$
    b) Se invece n è pari abbiamo sempre $\{e\}$ e $\frac{n}{2} - 1$ classi del tipo $\left\{\rho^i, \rho^{-i}\right\}$; ma in questo caso abbiamo anche una classe formata da $\left\{\rho^{\frac{n}{2}}\right\}$.
- Se invece consideriamo le classi rispetto a una riflessione $\sigma\rho^i$ abbiamo:
  - $\rho^j\sigma\rho^i\rho^{-j} = \sigma\rho^{i-2j}$
  - $\sigma\rho^j\sigma\rho^i\sigma\rho^j = \sigma\rho^{-i+2j}$

  Quindi $\sigma\rho^i \sim \sigma\rho^i \iff i \equiv j\,(2)$.
  Dunque se n è pari ci sono due classi di equivalenza per le riflessioni, se invece n è dispari esiste un unica classe di coniugio contenente le riflessioni (perché agli esponenti si può sempre aggiungere n che, essendo dispari, cambia la parità dell'esponente).
  Notiamo che le classi di coniugio delle rotazioni non danno informazioni

circa la normalità di un sottogruppo, perché un sottogruppo contiene sempre l'inverso di ogni suo elemento e dunque o un sottogruppo contiene totalmente la classe di coniugio di una rotazione o non la contiene per nulla.

È opportuno dunque riassumere quanto detto sino ad ora. Sia H sottogruppo di $\mathcal{D}_n$:

- Se H è formato solo da rotazioni è normale (abbiamo infatti visto che la classe di coniugio di una generica rotazione ρ^i è formata da $\left\{\rho^i, \rho^{-i}\right\}$, ma per definizione di sottogruppo se $\rho^i \in H$ abbiamo anche che $\rho^{-i} \in H$, quindi tutta la classe di coniugio di ρ^i appartiene ad H).
- Se H non è contenuto tutto nelle rotazioni si possono avere diversi casi:
  a) Se n è dispari H deve contenere tutte le riflessioni, quindi H può essere normale in $\mathcal{D}_n$ solo se $H = \mathcal{D}_n$ (infatti deve contenere tutta la classe di equivalenza di una generica riflessione, che è l'insieme di tutte loe riflessioni; inoltre abbiamo visto che se un sottogruppo non è tutto contenuto in N allora è spezzato in due sottoinsiemi equinumerosi: $H \cap N$ e $H \cap (\mathcal{D}_n - N)$, ma sappiamo che $|H \cap (\mathcal{D}_n - N)| = n$ per quanto detto fino ad ora, e quindi dobbiamo obbligatoriamente avere $H = \mathcal{D}_n$).
  b) Se invece n è pari un suo sottogruppo della forma $\mathcal{D}_m$ può essere normale solamente se $m = n$ oppure se $m = \frac{n}{2}$ (ma in quest'ultimo caso, come è stato già notato, abbiamo due distinti sottogruppi normali, entrambi isomorfi a $\mathcal{D}_m$).

Esercizio 1. Chi è il centro del diedrale?

Esercitazione 2

Esercitazione (2)

Altro sul gruppo diedrale

Riflessione 3. Cerchiamo adesso

$$|\mathcal{A}ut\left(\mathcal{D}_n\right)|$$

Per evitare casi particolari supponiamo $n > 2$. Il caso $n = 1$ è banale, il caso $n = 2$, ovvero $\mathcal{D}_2 = \mathbb{Z}_2^2$, può essere trattato facilmente a parte.
Ricordandoci che $\mathcal{D}_n = \left\{\sigma^i\rho^j \mid \rho^n = \sigma^2 = e,\ \sigma\rho\sigma = \rho^{-1}\right\}$. Ma come deve essere fatto un automomorfismo in questo gruppo?

$$\phi: \begin{array}{c}\mathcal{D}_n \\ \sigma \\ \rho\end{array} \longrightarrow \begin{array}{c}\mathcal{D}_n \\ a \\ b\end{array}$$

Ma abbiamo una condizione necessaria: $o(\phi(\rho))$ deve essere esattamente n (infatti vogliamo un omomorfismo bigettivo), abbiamo quindi $\phi(n)$ possibili immagini per ρ (le rotazioni devono infatti essere mandate in altre rotazioni, e sappiamo che vi sono $\phi(n)$ generatori delle rotazioni in $\mathcal{D}_n$, ρ deve andare in uno di essi).
Dobbiamo avere anche $o(\phi(\sigma)) = 2$. Ma quanti elementi di ordine 2 abbiamo? Abbiamo n simmetrie (che possiamo scrivere come $\sigma\rho^i$ con i qualsiasi) inoltre se abbiamo n pari avremmo anche $\rho^{\frac{m}{2}}$ ma possiamo escludere quest'ultima possibilità: infatti mandando σ in $\rho^{\frac{m}{2}}$ non avremmo una bigezione.
Ci siamo quindi ridotti a considerare al più $\phi(n)n$ possibili modi in cui mappare la coppia ρ, σ. Cerchiamo di capire se in tutti questi casi riusciamo a definire effettivamente un omomorfismo bigettivo. Supponiamo:

$$\phi(\rho) = \rho^i,\ con\ MCD(i, n) = 1$$
$$\phi(\sigma) = \sigma\rho^j,\ con\ j \in \{0, \ldots, n-1\}$$

Dobbiamo innanzitutto dare una buona definizione di una mappa su tutto il gruppo; per farlo abbiamo bisogno di scegliere un rappresentante per ogni elemento del gruppo. Infatti a priori la mappa che definiamo dipende dal rappresentante scelto.
Un qualsiasi elemento di $\mathcal{D}_n$ può essere scritto nella forma $\sigma^e\rho^h$, poniamo quindi:

$$\phi(\sigma^e\rho^h) = (\sigma\rho^j)^e\rho^{ih}$$

In questo modo abbiamo definito una mappa da $\mathcal{D}_2$ in sè. Dobbiamo capire se questa mappa (che è abbastanza ragionevole vista la condizione sui generatori) è un omomorfismo e se è bigettiva. Per dimostrare che la mappa è un omomorfismo verifichiamo:

- $\phi(e) = e$
- $\phi(\rho^{-h}) = \phi(\rho^{n-h}) = \rho^{i(n-h)} = \rho^{-ih} = \phi(\rho^h)^{-1}$
- $\phi((\sigma\rho^h)^{-1}) = \phi(\sigma\rho^h)^{-1}$
- $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$: (come esempio dimostriamo quest'ultima proprietà solo per le coppie di elementi della forma $g_1 = \sigma\rho^h,\ g_2 = \sigma\rho^k$ e lasciamo per esercizio gli altri casi).

$$g_1g_2 = \sigma\rho^h\sigma\rho^k = \rho^{-h+k},$$
$$\phi(g_1)\phi(g_2) = \rho^{-ih+ik} = \phi(g_1g_2)$$

Abbiamo dunque verificato che la mappa è un omomorfismo. Perché è bigettivo?

$$Im(\phi) \supseteq < \rho^i > \cup \left\{\sigma\rho^j\right\} \implies |Im(\phi)| \geq n+1 \implies Im(\phi) = \mathcal{D}_n$$

Alcuni risultati sui sottogruppi

Osservazione 3. È stato già visto che se dato $\mathcal{G} > N$ sottogruppo, allora $[\mathcal{G} : N] = 2 \implies N \triangleleft \mathcal{G}$. Sia ora $N \triangleleft \mathcal{G}$ con $[\mathcal{G} : N] = 2$, allora, dato $H < \mathcal{G}$ abbiamo due possibilità:

- $H < N$
- $[H : H \cap N] = 2$

Supponiamo che la prima possibilità non sia verificata e vediamo che vale la seconda. Abbiamo un omomorfismo da $\mathcal{G}$ a $\mathcal{G}/N$ la cui immagine è isomorfa a $\mathbb{Z}_2$. Restringendo questo omomorfismo ad H abbiamo due possibilità: $Im(\psi\mid_H) = \{0\}$ (ma in questo caso $H \subseteq Ker\psi = N$) oppure l'immagine è tutto $\mathbb{Z}_2$. Ma allora

$$[H : H \cap N] = [H : Ker(\psi\mid_H)] = 2$$

Osservazione 4. Sia $\mathcal{G}$ un gruppo (diverso dal gruppo banale $\{e\}$, p il più piccolo primo che divide l'ordine del gruppo. Allora, dato $H < \mathcal{G}$ tale che $[\mathcal{G} : H] = p$ abbiamo $H \triangleleft \mathcal{G}$.

Dimostrazione. Consideriamo infatti $X = \{g_0H, \ldots, g_{p-1}H\}$ l'insieme delle classi laterali di H in $\mathcal{G}$, questo questo insieme ha p elementi e su di esso $\mathcal{G}$ agisce per moltiplicazione a sinistra permutando le classi laterali. Consideriamo quindi l'omomorfismo indotto:

$$\begin{array}{rccc} \phi: & \mathcal{G} & \longrightarrow & Big(X) \\ & g & & \phi_g \text{ t.c. } \phi_g(aH) = gaH \end{array}$$

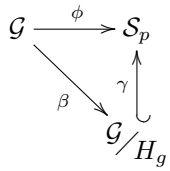
Il gruppo delle bigezioni di X è però isomorfo a $\mathcal{S}_p$. Ci chiediamo chi è il nucleo di ϕ; sappiamo intanto che:

- $Stab\,(eH) = H$
- Più in generale, per un qualsiasi $a \in \mathcal{G}$, vale $Stab\,(aH) = aHa^{-1}$

Abbiamo quindi:

$$\begin{aligned} Ker(\phi) &= \{g \in \mathcal{G} \ t.c. \ gaH = aH, \forall aH \in X\} \\ &= \bigcap_{i=1}^{p} Stab\,(g_i H) = \bigcap_{i=1}^{p} g_i H g_i^{-1} \triangleleft \mathcal{G} = H_g \end{aligned}$$

Abbiamo quindi diversi omomorfismi:



γ è l'omomorfismo indotto da $\phi : \mathcal{G} \to \mathcal{S}_p$ passando al quoziente rispetto al nucleo. Quindi

$$\left|\mathcal{G}/H_g\right| \mid |\mathcal{S}_p| = p! \implies \left|\mathcal{G}/H_g\right| \mid p$$

perché sappiamo che H aveva cardinalità del minimo primo che divide la cardinalità di $\mathcal{G}$. Abbiamo quindi che la cardinalità di $\mathcal{G}/H_g$ può essere 1 o p. Ma,poiché H è un sottogruppo proprio di $\mathcal{G}$, la cardinalità non può essere 1.
Quindi $H_g < H < \mathcal{G}$ e $[\mathcal{G} : H_g] = [\mathcal{G} : H] = p$, quindi $[H : H_g] = 1$, sono quindi lo stesso sottogruppo (e H_g, in quanto Ker di un omomorfismo, è normale). □

Studio dei centralizzatori

Osservazione 5 (Centralizzatori in $\mathcal{S}_n$). Sia $\sigma = (1,2)(3,4)$ in $\mathcal{S}_4$. Quanti coniugati ha? Abbiamo già detto il coniugio non varia la struttura della decomposizione in cicli, (abbiamo 3 possibili coniugati, quindi σ ha un orbita di 3 elementi). Possiamo inoltre dire:

$$|C\,(\sigma)| = \frac{|\mathcal{S}_4|}{|Orb\,(\sigma)|} = 8$$

Prendiamo invece ora $\sigma = (1,2,3)(4,5,6)$ in $\mathcal{S}_6$. L'orbita di σ ha 40 elementi, quindi il centralizzante è un gruppo di $\frac{6!}{40} = 18$ elementi. Per i teoremi di Sylow possiamo trovare un sottogruppo di 9 elementi, dato da $H =< (1,2,3)(4,5,6) >$ che è isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_3$. Notiamo che anche $(1,4)(2,5)(3,6)$ appartiene al centralizzatore e dunque tutti i prodotti $(1,4)(2,5)(3,6)H$, che costituiscono un insieme di 18 elementi che corrisponde dunque al centralizzatore di σ.
Questo nostro σ sta in $\mathcal{A}_6$, quindi ci possiamo chiedere chi sono centralizzatore e orbite di σ in $\mathcal{A}_6$. Le orbite in $\mathcal{A}_6$ e in $\mathcal{S}_6$ sono le stesse o no?
Vediamo che il centralizzatore in $\mathcal{S}_6$ non è contenuto in $\mathcal{A}_6$, quindi il centralizzatore in $\mathcal{A}_6$ di σ è composto dalla metà degli elementi del centralizzatore in $\mathcal{S}_6$. L'orbita ha cardinalità pari al rapporto tra la cardinalità del gruppo (rispettivamente $\mathcal{S}_6$ o $\mathcal{A}_6$) e la cardinalità del centralizzatore (rispettivamente 18 o 9); entrambe le cardinalità di dimezzano, dunque l'orbita mantiene la stessa quantità di elementi.

Esempio 1. Vediamo in $\mathcal{S}_8$ cosa possiamo dire di $\sigma = (1,2,3)(4,5,6,7,8)$. L'orbita di σ ha $8 \cdot 7 \cdot 6 \cdot 2 \cdot 4$ elementi, il centralizzatore avrà quindi 15 elementi. Si riescono a trovare facilmente un elemento di ordine 5 e uno di ordine 3 che centralizzano e commutano tra di loro, quindi $C(\sigma) =< (1,2,3), (4,5,6,7,8) >$. Il centralizzatore in $\mathcal{A}_8$ è uguale a quello in $\mathcal{S}_8$ (sia la prima che la seconda permutazione sono pari). Quindi l'orbita in $\mathcal{A}_8$ viene divisa in 2.
Se il centralizzatore è generato solo da permutazioni pari, abbiamo sempre che il centralizzatore è contenuto in $\mathcal{A}_n$ e quindi la cardinalità dell'orbita in $\mathcal{A}_n$ di σ è la metà della cardinalità dell'orbita in $\mathcal{S}_n$.
Possiamo quindi chiederci cosa succede per una permutazione $\sigma \in A_n$ fissata se la consideriamo come elemento di $\mathcal{S}_n$ o se la consideriamo come permutazione in $\mathcal{S}_{n+k}$. Come cambia, al variare di k, la relazione tra la classe di coniugio di σ rispetto all'azione del gruppo simmetrico o e la classe di coniugio rispetto all'azione del gruppo alternante? Per capirlo dobbiamo studiare l'intersezione del centralizzatore di σ con il gruppo alternante e dobbiamo quindi chiederci quando $C_{\mathcal{S}_n}(\sigma) \subset \mathcal{A}_n$.
Se non voglio elementi dispari in $C_{\mathcal{S}_n}(\sigma)$, allora σ non vede contenere cicli di lunghezza pari (altrimenti un ciclo pari starebbe nel centralizzatore di σ, ma non in A_n), non deve avere due cicli della stessa lunghezza (altrimenti la permutazione che coniuga l'uno nell'altro, prodotto di un numero dispari di trasposizioni, starebbe nel centralizzatore), inoltre non ci devono essere due elementi fissati (altrimenti la trasposizione che li scambia starebbe nel centralizzatore). Queste condizioni sono chiaramente necessarie affinché $C_{\mathcal{S}_n}(\sigma) \subset A_n$. Dimostriamo che sono sufficienti.
Sia $\sigma = \gamma_1\gamma_2 \dots \gamma_h$, con γ_i un ciclo di lunghezza l_i. Siano l_i tutti distinti, possiamo supporre $l_1 > \dots > l_h$. Solo ai fini di questa dimostrazione possiamo supporre che la decomposizione in cicli di σ contenga anche dei cicli di lunghezza 1, corrispondenti agli elementi fissati da σ. Abbiamo quindi che $\sum l_i = n$, infatti tra i γ_i contiamo anche gli 1-cicli. Che cardinalità avrà allora la classe di coniugio in $\mathcal{S}_n$ di σ?

$$\binom{n}{l_1}(l_1-1)!\binom{n-l_1}{l_2}(l_2-1)! \cdot \dots \cdot \binom{n-l_1-\dots-l_k}{l_{k+1}}(l_{k+1}-1)! \cdot \\ \cdot \dots \cdot \binom{l_n}{l_n}(l_n-1)! = \frac{n!}{l_1 \cdot \dots \cdot l_h}$$

Allora la cardinalità del centralizzatore in $\mathcal{S}_n$ sarà $l_1 \cdot \dots \cdot l_h$. Adesso abbiamo finito: vogliamo trovare un gruppo di quella cardinalità che è il centralizzatore, ma $g_1, g_2, \dots, g_h$ sono cicli disgiunti di lunghezza $l_1, l_2, \dots, l_h$, che quindi commutano tra di loro, sono contenuti tutti nel centralizzatore in $\mathcal{S}_n$ di σ e generano un gruppo isomorfo a $\mathbb{Z}_{l_1} \times \dots \times \mathbb{Z}_{l_h}$ ma questo ha cardinalità del centralizzatore ed è contenuto nel centralizzatore, sarà quindi il centralizzatore, inoltre tutti i cicli hanno lunghezza pari, quindi è contenuto in $\mathcal{A}_n$.
Abbiamo trovato delle condizioni necessarie e sufficienti per avere l'uguaglianza tra il centralizzatore di σ in A_n e quello in $\mathcal{S}_n$.

Esempio 2. Per esempio $\sigma = (1,2,3,4,5)$ in S_5 ha orbita di 4! elementi, e la sua orbita si spezza in $\mathcal{A}_5$. Invece la sua orbita in $\mathcal{S}_6$ ha $6 \cdot 4!$ elementi e continua a spezzarsi in $\mathcal{A}_6$. Mentre invece da $\mathcal{S}_n$ con $n \geq 7$ l'orbita di σ rimane costante.

Osservazione 6. Sia $\mathcal{G}$ un gruppo finito che agisce su un insieme X finito. Consideriamo il prodotto cartesiano $\mathcal{G}\times X$, e in esso l'insieme $A = \{(g, x) \mid g \cdot x = x\}$. Come facciamo a contare gli elementi di A? Vi sono due modi per farlo: possiamo contare, per ogni $x \in X$, tutti i g che lo fissano, oppure fare il contrario, preso un elemento $g \in \mathcal{G}$, contare quanti sono gli elementi che fissa. Quindi, detto per ogni $g \in \mathcal{G}$, $X^g = \{x \in X \ t.c. \ (g \cdot x) = x\}$ abbiamo:

$$|A| = \sum_{x \in X} |Stab\,(x)| = \sum_{g \in \mathcal{G}} |X^g|$$

Raggruppo gli elementi di X per $\mathcal{G}$-orbite. Abbiamo quindi che la somma precedente è uguale a:

$$|A| = \sum_{x \in \{\text{rappr. orbite}\}} |Stab\,(x)|\,|Orb\,(x)|$$

Sappiamo infatti che gli stabilizzatori degli elementi di una stessa orbita sono tra loro coniugati e quindi hanno la stessa cardinalità, quindi è possibile raggruppare gli elementi di X in orbite e moltiplicare la cardinalità degli stabilizzatori di un'orbita per la cardinalità dell'orbita stessa. Ma $|Stab\,(x)|\,|Orb\,(x)| = |\mathcal{G}|$. Quindi quello che otteniamo è:

$$|A| = \sum_{x \in \{\text{rappr. orbite}\}} |\mathcal{G}| = |\mathcal{G}|\,|\{orbite\}|$$

Quindi abbiamo scoperto che:

$$|\{\mathcal{G} - orbite\}| = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} |X^g|$$

Questa formula è detta formula di Burnside.

Esercizio 2. Supponiamo di avere una scacchiera 3×3 e di poter colorare ognuna delle sue caselle di bianco o nero. Possiamo trasformare la scacchiera girandola o ribaltandola come vogliamo (sopra e sotto e ruotarla). Quante scacchiere diverse si riescono a fare a meno di queste trasformazioni?

Esercizio 3. Classificare tutti i gruppi di cardinalità al più 8.

Esercitazione 3

Esercitazione (3)

Esercizio 4. Quante sono le possibili colorazioni differenti (diverse a meno di rotazioni dello spazio) di una scacchiera 3×3 con i soli colori bianco e nero? Quello che ci stiamo chiedendo in realtà è quante orbite ha $\mathcal{D}_4$ nello spazio di tutte le scacchiere (che è isomorfo a $S = \mathbb{Z}_2^9$). Abbiamo, come sappiamo:

$$|\{orbite\}| = \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} |S^g|$$

In $\mathcal{D}_4$ abbiamo:

- e
- 4 riflessioni r
- 2 rotazioni s di ordine 4
- 1 rotazione d di ordine 2

Vediamo quante colorazioni diverse sono invarianti rispetto ai vari elementi di $\mathcal{D}_4$ (cioè quante colorazioni sono mandate in se stesse da un dato elemento di $\mathcal{D}_4$):

- $|S^e| = 2^9$ (l'identità manda tutte le scacchiere in se stesse).
- $|S^r| = 2^6$, possono infatti essere scelte liberamente tutte le caselle lungo l'asse di riflessione, metà delle altre caselle.
- $|S^s| = 2^3$, queste rotazioni permettono di distinguere solamente il centro, gli angoli e gli spigoli.
- $\left|S^d\right| = 2^5$. Vi sono meno colorazioni invarianti di quante ve ne fossero con le riflessioni perché la rotazione impone che gli spigoli dell'asse di rotazione non varino.

Quindi il numero di orbite è:

$$|\{orbite\}| = \frac{1}{8}(2^9 + 4 \cdot 2^6 + 2 \cdot 2^3 + 1 \cdot 2^5) = 2^6 + 2^5 + 2^1 + 2^2$$

Esercizio 5. Quante sono le diverse (differenti a meno di operazioni di D_8) colorazioni possibili di un ottagono con n colori diversi?

Definizione 2 (Prodotto diretto)**.** Se G_1 e G_2 sono gruppi, allora $G_1 \times G_2$ ha struttura di gruppo:

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$$

Riflessione 4. Prima di introdurre il prossimo esercizio vediamo una proprietà dei gruppi di ordine p^2. Abbiamo già dimostrato che ogni gruppo $\mathcal{G}$ di ordine p^2 è abeliano, dividiamoli adesso in due casi:

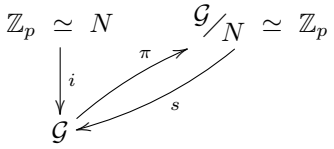
- in $\mathcal{G}$ vi è un elemento di ordine p^2; in questo caso certamente $\mathcal{G} \simeq \mathbb{Z}_{p^2}$.
- tutti gli elementi diversi dall'identità hanno ordine p. In questo caso prendiamo $g \in \mathcal{G}$ un qualsiasi elemento di ordine p e consideriamo $N =< g >$, (che sappiamo essere normale, essendo un sottogruppo di un gruppo abeliano), abbiamo allora (ricordandoci che $\mathcal{G}/_N \simeq \mathbb{Z}_p$):

$$\mathcal{G} \xrightarrow{\pi} \mathcal{G}/_N$$

Ci chiediamo se esiste un omomorfismo s che sia inverso destro rispetto alla proiezione al quoziente π, (in generale questo s non esiste, ma qui sappiamo che ogni elemento ha ordine p), cioè tale che $\pi \circ s = Id_{\mathcal{G}/N}$, ovvero che $\pi(s(g)) = g, \forall g \in \mathcal{G}$. Mostriamo questo omomorfismo, scegliamo $g_1 \in \mathcal{G}$ tale che $g_1 \notin N$ e imponiamo:

$$\begin{array}{rccc} s: & \mathcal{G}/_N & \longrightarrow & \mathcal{G} \\ & g_1^i N & & g_1^n \end{array}$$

(questa funzione non è la funzione che manda hN in h per ogni $h \in \mathcal{G}$, che in generale non è nemmeno una funzione, ma è una funzione che abbiamo creato dopo aver scelto un g_1). Quello che facciamo è mandare ogni laterale in una delle sue possibili controimmagini rispetto a π. Si verifica facilmente che s è in effetti un omomorfismo.
Riassumendo la situazione delle applicazioni abbiamo:



Visto che $\mathcal{G}$ è abeliano possiamo definire:

$$\begin{array}{rccc} (i,s): & N \times \mathcal{G}/_N & \longrightarrow & \mathcal{G} \\ & (h, g_1^n N) & & h \cdot g_1^n \end{array}$$

Questa applicazione è un isomorfismo di gruppi, infatti l'immagine è un sottogruppo di $\mathcal{G}$ che contiene strettamente N (visto che contiene anche g_1) e quindi, per Lagrange, $Im(s,i) = \mathcal{G}$. Per questioni di cardinalità, quindi, (s,i) è anche iniettiva. Abbiamo trovato allora un isomorfismo tra due gruppi isomorfi a $\mathbb{Z}_p$ e $\mathcal{G}$

Esercizio 6. Classificazione dei gruppi $\mathcal{G}$ con cardinalità non superiore a 8.

- $|\mathcal{G}| = 1$. C'è solo il gruppo banale.
- $|\mathcal{G}| = 2$. C'è solamente $\mathbb{Z}_2$.
- $|\mathcal{G}| = 3$. C'è solamente $\mathbb{Z}_3$.
- $|\mathcal{G}| = 4$. Vi sono due possibilità: $\mathcal{G} \simeq \mathbb{Z}_4$ oppure $\mathcal{G} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. (Per quanto detto nell'ultima Riflessione).
- $|\mathcal{G}| = 5$. C'è solamente $\mathbb{Z}_5$.
- $|\mathcal{G}| = 6$. Abbiamo certamente $\mathbb{Z}_6$ e $\mathcal{S}_3$.
  Cosa sappiamo di questo $\mathcal{G}$? Sappiamo che esiste $N \triangleleft \mathcal{G}$ con $|N| = 3$. Inoltre $\mathcal{G}$ contiene anche H isomorfo a $\mathbb{Z}_2$.
  Diciamo $N =< n >$ e $H =< h >$, abbiamo un sottogruppo normale facciamo allora agire H su N per coniugio. Questo ci fornisce un omomorfismo tra H e $\mathcal{A}ut\,(N)$:

$$\begin{array}{rccc} \phi: & H & \longrightarrow & \mathcal{A}ut\,(N) \\ & h^i & & \phi_{h^i}: \begin{array}{ccc} N & \longrightarrow & N \\ g & & g^i g h^{-i} \end{array} \end{array}$$

  Ma $\mathcal{A}ut\,(N) \simeq \mathbb{Z}_3^*$, ha quindi due elementi. Quanti omomorfismi possiamo avere da H a $\mathcal{A}ut\,(N)$? Esattamente due, quindi H può agire in $\mathcal{A}ut\,(N)$ in due modi descritti dai due omomorfismi visti:

  - omomorfismo banale: h commuta con n. In questo caso abbiamo la mappa:

$$\begin{array}{ccc} \mathbb{Z}_2 \times \mathbb{Z}_3 & \longrightarrow & \mathcal{G} \\ H \times N & \longrightarrow & \mathcal{G} \end{array}$$

  - h coniuga n con n^{-1}. La situazione in questo caso è più complicata, abbiamo infatti:

$$\begin{array}{ccc} \mathcal{D}_3 \simeq \mathcal{S}_3 & \longrightarrow & \mathcal{G} \\ H \times N & \longrightarrow & \mathcal{G} \\ \sigma^e, \rho^i & & h^e n^i \end{array}$$

    Nell'ultimo diagramma il prodotto in basso a sinistra è solo un prodotto di insiemi, non è da intendersi come prodotto di gruppi. Infatti la struttura di gruppo del prodotto è quella di $\mathcal{D}_3 \simeq \mathcal{S}_3$. È quindi possibile verificare che la mappa $\mathcal{D}_3 \to \mathcal{G}$ è un omomorfismo di gruppi e dunque i due gruppi sono isomorfi.

- $|\mathcal{G}| = 7$. C'è solamente $\mathbb{Z}_7$.
- $|\mathcal{G}| = 8$. Conosciamo certamente $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2^3$ oppure $\mathcal{D}_4$. Ci chiediamo:
  - Ci sono elementi di ordine 8? Se si tutto a posto (è isomorfo a $\mathbb{Z}_8$).
  - Ci sono elementi di ordine 4? Se non ce ne sono tutti gli elementi hanno ordine 2, vorremmo dire che ci troviamo per forza in $\mathbb{Z}_2^3$, (sotto-esercizio, se $\mathcal{G}$ è un gruppo e ogni elemento ha ordine 2, questo gruppo è abeliano? (banale dimostrare che è vero). Altro sotto-esercizio: sia $\mathcal{G}$ un gruppo di ordine 2^n abeliano, supponiamo che tutti gli elementi di $\mathcal{G}$ abbiano ordine 2, allora $\mathcal{G} \simeq \mathbb{Z}_2^n$. (da dimostrare usando induzione, quoziente e sollevamenti)).

- Supponendo che ci siano elementi di ordine 4, prendiamo $N =< n > \simeq \mathbb{Z}_4$ sottogruppo di $\mathcal{G}$ (chiaramente $N \triangleleft \mathcal{G}$). La domanda che ci dobbiamo porre è: fuori da N ci sono altri elementi di ordine 2?
  a) Se la risposta è sì, allora prendiamo $h \notin N$ di ordine 2 e facciamo agire h su N per coniugio. Questo ci fornisce una mappa da $H =< h >$ agli automorfismi di N:

$$\begin{array}{ccccc} \phi: & H & \longrightarrow & \mathcal{A}ut\,(N) & \\ & x & & \phi_x:\ \underset{g}{N} & \longrightarrow \underset{xgx^{-1}}{N} \end{array}$$

  Abbiamo che H è isomorfo a $\mathbb{Z}_2$, ma anche $\mathcal{A}ut\,(N)$ è isomorfo a $\mathbb{Z}_2$, quindi la mappa ci dà due omomorfismi: quello per cui H commuta con N (l'omomorfismo banale). Oppure l'automorfismo non banale, ma abbiamo detto che l'automorfismo non banale è quello che manda ogni elemento nell'inverso. Quindi in questo caso h coniuga x in x^{-1}.
  Vediamo entrabi i casi:
  1) Se consideriamo l'isomorfismo banale vogliamo dimostrare che $\mathcal{G} = \mathbb{Z}_2 \times \mathbb{Z}_4$.
     Sappiamo che $\mathcal{G}$ contiene un sottogurppo N normale, il cui quoziente $\mathcal{G}/N$ è isomorfo a $\mathbb{Z}_2$. Abbiamo inoltre trovato un omomorfismo da $H \times N$ a $\mathcal{G}$ (si dimostra facilmente che questo in realtà è un automorfismo, quindi abbiamo che $\mathcal{G} \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$).
  2) Consideriamo l'isomorfismo non banale, vorremmo che $\mathcal{G} \simeq \mathcal{D}_4$. H e N si comportano come sottogruppi di $\mathcal{D}_4$. Possiamo infatti definire una mappa da $\mathcal{D}_4$ a G (consideriamo $\mathcal{D}_4 =< \rho, \sigma >$):

$$\begin{array}{ccccc} f: & \mathcal{D}_4 & \longrightarrow & \mathcal{G} \\ & \rho^i\sigma^j & & n^i h^j \end{array}$$

     Si verifica che questo è un omomorfismo, inoltre è anche un isomorfismo.
  b) Ci resta il caso in cui fuori da N ci sono elementi di ordine 4 ma non ci sono elementi di orine 2. Avremo allora $h \notin N$ di ordine 4. Sappiamo che $h^2 \in N$ (altrimenti avremmo elementi di ordine 2 fuori da N e in particolare abbiamo che $n^2 = h^2$) e in particolare possiamo dire $< h > \triangleleft G$. Facciamo agire H su N per coniugio e troviamo un omomorfismo da H agli automorfismi di N.
     Questa volta partiamo da un gruppo isomorfo a $\mathbb{Z}_4$ per arrivare a $\mathcal{A}ut\,(\mathbb{Z}_4)$, che è un gruppo isomorfo a $\mathbb{Z}_2$. Abbiamo solo 2 omomorfismi da $\mathbb{Z}_4$ a $\mathbb{Z}_2$:
     1) Caso dell'omomorfismo banale. Se h e n commutano tra di loro, abbiamo che hn ha ordine 2 (infatti $h^2 = n^2$ è l'unico elemento di ordine 2 di $\mathcal{G}$ e quindi $(hn)^2 = h^2n^2 = e$), ma hn non può appartenere a N ed abbiamo dunque una contraddizione perché N contiene l'unico elemento di ordine 2.
     2) Abbiamo ancora l'omomorfismo non banale. Deve essere allora che hn ha ordine 4 (come anche h e n), chiamando questi

elementi i, j, k e vediamo che siamo in un gruppo di 8 elementi con delle relazioni particolari:

$$Q_8 = \left\{\pm 1, \pm i, \pm j, \pm k \text{ } t.c. \text{ } i^2 = j^2 = k^2 = ijk = -1\right\}$$

Chiamato gruppo dei quaternioni.

Esercizio 7. Sia $|\mathcal{G}| = 2n$ e supponiamo che esattamente la metà degli elementi abbia ordine 2. Inoltre l'altra metà degli elementi forma un sottogruppo $H \triangleleft \mathcal{G}$. Vogliamo dimostrare che $|H| = n$ è dispari e che H è abeliano.

Svolgimento. Che n sia dispari segue dal teorema di Cauchy: se n fosse pari allora in H ci sarebbe un elemento di ordine 2, questo va contro le ipotesi.
Consideriamo ora $H \times H$; quante sono, qui dentro, le coppie della forma (a, a^{-1})? Sia $b \in \mathcal{G}$ di ordine 2 ($b \notin H$), visto che H è normale in $\mathcal{G}$ e ha indice 2 posso fare agire b su H per coniugio. Ho quindi una mappa

$$\begin{array}{rccc} T_b: & H & \longrightarrow & H \\ & h & & bhb^{-1} \end{array}$$

Abbiamo quindi che T_b ha ordine ≤ 2. Ma allora, preso $h \in H$,

$$hb \notin H \implies hbhb = e \implies h(bhb) = h(bhb^{-1}) = e$$

e quindi il coniugio di h è proprio h^{-1}, quindi T_b manda h in h^{-1}.
Abbiamo un sottogruppo normale con un automorfismo di ordine 2 che manda ogni elemento nel suo inverso. In generale, se K è un gruppo e ϕ è un automorfismo di K e $\phi(x) = x^{-1}$, allora K è abeliano. Cioè mandare nell'inverso è un automorfismo se e solo se il gruppo è abeliano. Infatti:

$$x^{-1}y^{-1} = \phi(x)\phi(y) = \phi(xy) = y^{-1}x^{-1}$$

Esercitazione 4

Esercitazione (4)

Siano H e N sottogruppi, N normale e $H \cap N = \{e\}$; se $HN = \mathcal{G}$ allora abbiamo che $\mathcal{G} = N \rtimes H$.

Esempio 3. Un esempio di un gruppo che non può essere scritto come un prodotto semidiretto non banale è Q_8. Gli elementi di ordine 4 in Q_8 sono 6, quindi ogni sottogruppo di ordine 4 in Q_8 è isomorfo a $\mathbb{Z}_4$, possiamo quindi chiederci se c'è un modo per scrivere $Q_8 = \mathbb{Z}_4 \rtimes \mathbb{Z}_2$ (non possiamo infatti scrivere $Q_8 = \mathbb{Z}_2 \rtimes \mathbb{Z}_4$, in quanto se in Q_8 $\mathbb{Z}_2$ fosse normale lo sarebbe anche $\mathbb{Z}_4$ e quindi il prodotto semidiretto sarebbe un prodotto diretto, quindi il coniugio che definisce il prodotto semidiretto sarebbe l'automorfismo banale, ma allora in questo caso $Q_8 = \mathbb{Z}_4 \times \mathbb{Z}_2$ ma Q_8 non è abeliano, assurdo). Ma se fosse $Q_8 = \mathbb{Z}_2 \rtimes \mathbb{Z}_4$ avremmo un'unica possibilità, infatti $\mathcal{A}ut(\mathbb{Z}_4) \simeq \mathbb{Z}_2$, (e quindi gli unici omomorfismi sono l'identità (che non va bene, visto che ci darebbe un gruppo commutativo) e l'isomomorfismo inverso che manda ogni elemento nel suo inverso). Ma allora dovremmo avere:

$$Q_8 = < a, b \ t.c. \ a^4 = b^2 = e, \ bab = a^1 > \ \simeq \ \mathcal{D}_4$$

Ma questo non va bene: $\mathcal{D}_4$ ha 5 elementi di ordine 2, questo è assurdo.
Avremmo pituto dire che, dato un sottogruppo H di ordine 4 in Q_8, non esistono elementi di ordine 2 fuori da H, non è quindi possibile trovare due sottogruppi disgiunti di ordine 2 e 4.

Esercizio 8. Abbiamo classificato tutti i gruppi fino a 8. Andiamo avanti:

- $|\mathcal{G}| = 9$. Ci sono solo $\mathbb{Z}_9$ e $\mathbb{Z}_3 \times \mathbb{Z}_3$.
- $|\mathcal{G}| = 10$. Abbiamo solo $\mathbb{Z}_{10}$ e D_5.
- $|\mathcal{G}| = 11$. C'è solo $\mathbb{Z}_{11}$.
- $|\mathcal{G}| = 12$. Cerchiamo di esaminare i possibili 2 e 3-Sylow in $\mathcal{G}$; quanti 3-Sylow possiamo avere? Uno oppure quattro, infatti $n_3 \equiv 1\,(3)$, inoltre deve dividere 12.
  - $n_3 = 1$, il 3-Sylow è normale.

- $n_3 = 4$, in questo caso abbiamo 4 sottogruppi di ordine 3 in un gruppo di cardinalità 12 (che si intersecano tutti solamente in $\{e\}$, infatti ogni elemento non banale è generatore del proprio 3-Sylow). Abbiamo quindi che in questo caso l'unione dei 3-Sylow è formata da $1 + 4 \cdot 2 = 9$ elementi differenti. Vi sono quindi solo tre elementi che non appartengono a 3-Sylow. Questi devono però appartenere tutti ad un unico 2-Sylow (che sappiamo avere ordine 4 in $\mathcal{G}$).

Possiamo dire che in questo caso un gruppo di ordine 12 è sempre esprimibile come prodotto semidiretto: infatti o il 3-Sylow è normale oppure lo è il 2-Sylow. Possiamo quindi trovarci nei seguenti casi:

a) $\mathcal{G} = \mathbb{Z}_3 \rtimes_\phi \mathbb{Z}_4$. Abbiamo solo due possibilità per $\mathbb{Z}_4 \xrightarrow{\phi} Aut(\mathbb{Z}_3)$:
   1) ϕ è l'omomorfismo banale. In questo caso abbiamo che $\mathcal{G} \simeq \mathbb{Z}_3 \times \mathbb{Z}_4$
   2) Se ϕ è l'unico omomorfismo non banale da $\mathbb{Z}_4$ a $\mathcal{A}ut(\mathbb{Z}_3) \simeq \mathbb{Z}_2$ abbiamo un gruppo a parte (studiarlo meglio).

b) $\mathcal{G} = \mathbb{Z}_3 \rtimes_\phi \mathbb{Z}_2 \times \mathbb{Z}_2$. Dobbiamo in questo caso studiare gli omomorfismi $\mathbb{Z}_2 \times \mathbb{Z}_2 \xrightarrow{\phi} \mathcal{A}ut(\mathbb{Z}_3)$. Vediamo che ϕ può essere banale oppure surgettivo. Possiamo allora studiarne il Ker e vediamo che abbiamo $|Ker(\phi)| = 2$; vi sono quindi tre possibilità per il Ker di ϕ. Ma quello che ci dobbiamo chiedere è: il fatto che il nucleo sia diverso induce un prodotto semidiretto differente? O potrebe essere che vi sono omomorfismi differenti che inducono lo stesso prodotto semidiretto? Sappiamo che abbiamo solo tre possibilità: per il generatore del nucleo: $(0,1)$, $(1,0)$ oppure $(1,1)$; queste tre possibilità danno tre omomorfismi diversi, ma riflettiamo che tutti questi possono essere scritti come:

$$\phi: \quad \underset{\substack{a \\ b}}{\mathbb{Z}_2 \times \mathbb{Z}_2} \quad \longrightarrow \quad \underset{\substack{0 \\ 1}}{\mathcal{A}ut(\mathbb{Z}_3)}$$

   Con a e b di ordine 2. Quello che vogliamo dire è che in realtà è indifferente chi si nasconde dietro a e b, l'importante è la struttura che ha l'omomorfismo, ovvero, a meno di automorfismi di $\mathbb{Z}_2 \times \mathbb{Z}_2$ le tre situazioni sono isomorfe. Possiamo quindi ridurre questo caso a due situazioni (a meno di isomorfismi tra i prodotti semidiretti ottenuti):
   1) ϕ è l'omomorfismo banale che come al solito ci dà il prodotto cartesiano $\mathbb{Z}_2^2 \times \mathbb{Z}_3$.
   2) Consideriamo il caso di ϕ che manda $(1,0)$ in 1 e $(0,1)$ in 0 (abbiamo detto che gli altri casi sono isomorfi a questo). Ma 1 come elemento di $\mathcal{A}ut(\mathbb{Z}_3)$ è l'isomorfismo inverso, mentre 0 è l'automorfismo banale. Quindi il primo elemento $(1,0)$ coniuga $\mathbb{Z}_3$ mandando ogni elemento nell'inverso, invece $(0,1)$ commuta con $Z3$. Abbiamo quindi:

$$\mathbb{Z}_2 \times (\mathbb{Z}_3 \rtimes \mathbb{Z}_2) \simeq \mathbb{Z}_2 \times \mathcal{D}_3$$

c) $\mathcal{G} = \mathbb{Z}_4 \rtimes \mathbb{Z}_3$. Abbiamo un solo omomorfismo da $\mathbb{Z}_3$ agli automorfismi di $\mathbb{Z}_4$: l'omomorfismo banale (che dà, come sappiamo, $\mathbb{Z}_4 \times \mathbb{Z}_3$)

d) $\mathcal{G} = \mathbb{Z}_2^2 \rtimes_\phi \mathbb{Z}_3$. Abbiamo che $\mathcal{A}ut\left(\mathbb{Z}_2^2\right) \simeq \mathcal{S}_3$, in $\mathcal{S}_3$ vi è un unico sottogruppo di ordine 3, quindi abbiamo che gli omomorfismi possibili non banali da $\mathbb{Z}_3$ a $\mathcal{A}ut\left(\mathbb{Z}_2^2\right)$ sono solo due: l'identità e l'inverso (nel sottogruppo di ordine 3 di $\mathcal{S}_3$). Ma ancora una volta, come nel caso di prima, questi due omomorfismi sono equivalenti a meno di automorfismi di $\mathbb{Z}_3$ e dunque inducono prodotti semidiretti entrambi isomorfi allo stesso gruppo $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_3$, dove in questo caso $\mathbb{Z}_3$ coniuga $\mathbb{Z}_2^2$ permutando ciclicamente gli elementi di ordine 2

Riflessione 5. Abbiamo utilizzato nell'ultimo esercizio un fatto che formalizzeremo solo poi: se $H \xrightarrow{\phi} \mathcal{A}ut(N)$ e $H \xrightarrow{\psi} \mathcal{A}ut(N)$ sono tali che $\phi = \psi \circ \pi$ con π automorfismo di H, allora abbiamo che

$$H \rtimes_\phi N \simeq H \rtimes_\psi N$$

Osservazione 7. Proviamo a generalizzare quanto visto fino ad ora. Vediamo cosa succede con i gruppi di ordine p^2q con p, q primi e distinti tra di loro.

- Sia $p < q$ e consideriamo i q-Sylow, se vi è un solo q-Sylow questo è normale, se ve ne sono diversi tutti questi sono coniugati tra di loro, ma se ha coniugati ne può averne solo p o p^2 (il numero dei q-Sylow deve dividere la cardinalità del gruppo ed essere congruo ad 1 modulo q), ma $p < q$, quindi p non è congruo ad 1 modulo q. Quindi devono essere p^2. Quanti possono essere allora gli elementi di ordine q? Ogni q-Sylow ne contiene $q-1$, inoltre due q-Sylow distinti si possono intersecare solo nell'elemento neutro. Abbiamo quindi $(q-1)p^2$ elementi di ordine q. Un p-Sylow in $\mathcal{G}$ ha p^2 elementi, può quindi esserci al massimo un p-Sylow (per questioni di cardinalità, infatti $(q-1)p^2 + p^2 = qp^2 = |\mathcal{G}|$), e uno almeno ci deve essere, quindi l'unico che c'è è normale. Quindi in questo caso almeno uno dei due Sylow è normale. Abbiamo allora dimostrato che possiamo scrivere $\mathcal{G}$ come prodotto semidiretto.

- $p > q$, allora il p-Sylow ha indice q. E q è il più piccolo primo che divide l'ordine di $\mathcal{G}$, quindi il p-Sylow è normale.

Quindi tutti i gruppi di ordine p^2q sono un prodotto semidiretto di p-Sylow e q-Sylow, visto che uno dei due deve essere normale.

Esercizio 9. Cerchiamo tutti i gruppi $\mathcal{G}$ tali che $|\mathcal{G}| = 30$.
Sappiamo che esiste $x \in \mathcal{G}$ di ordine 5, sia $H =< x >$ di 5 elementi; vorremmo cercare il normalizzatore di H. Quanti elementi può avere?
Potrebbe essere $|N(H)| = 30, 15, 10, 5$, deve infatti essere multiplo di 5 e deve dividere $|H|$.

1) Se il normalizzatore di H avesse ordine 15 allora $N(H)$ sarebbe un sottogruppo normale di $\mathcal{G}$; ma dobbiamo escludere questo caso, infatti non possono esserci solo due 5-Sylow.

2) Se invece $N(H)$ avesse ordine 10 avremo che ci sarebbero tre 5-Sylow, ma questo non è possibile, in questo caso infatti non sarebbe vero che $n_5 \equiv 1\,(5)$.

3) Non presenta invece complicazioni di questo genere il caso $|N(H)| = 5$: avemmo sei 5-Sylow, e $6 \equiv 1\,(5)$. Ogni 5-Sylow contiene quattro elementi di ordine 5, avremmo quindi in totale 24 elementi di ordine 5.
Quanti sottogruppi di ordine 3 possiamo avere in questo caso? Abbiamo solo 6 elementi liberi (di cui non sappiamo l'ordine) e i 3-Sylow possono essere solo 1 o 4, ma non abbiamo abbastanza elementi liberi per potere avere quattro 3-Sylow (che richiederebbero almeno otto elementi di ordine 3). Quindi abbiamo un unico sottogruppo normale di ordine 3. Possiamo quindi dire che esiste un sottogruppo di ordine 6: infatti il 3-Sylow è normale ed abbiamo un unico 2-Sylow, è un sottogruppo di ordine 6 (il prodotto è un sottogruppo perché uno dei due è normale).
Possiamo concludere dicendo che il sottogruppo N di ordine 6 è normale in $\mathcal{G}$ (il suo coniugato non può che essere lui stesso), quindi possiamo scrivere:

$$\mathcal{G} = N \rtimes \mathbb{Z}_5$$

ed esaminare esplicitamente i casi possibili (quello che faremo per il punto d).

d) Se invece $|N(H)| = 30$ allora il 5-Sylow è normale, quindi esiste un sottogruppo di ordine 15 (dato dal prodotto diretto del 5-Sylow con un sottogruppo di ordine 3). Ma questo gruppo K ha indice 2 in $\mathcal{G}$, quindi $K \triangleleft \mathcal{G}$, allora abbiamo che $\mathcal{G} = K \rtimes \mathbb{Z}_2$.
Analizziamo nel dettaglio questa situazione. Se $|K| = 15$ vuol dire che $\mathbb{Z}_5$ è normale in K (per questioni di indice), quanti sono gli omomorfismi possibili da $\mathbb{Z}_3$ ad $\mathcal{A}ut(\mathbb{Z}_5)$? Solo l'omomorfismo banale. Quindi abbiamo

$$\mathcal{G} = (\mathbb{Z}_3 \times \mathbb{Z}_5) \rtimes \mathbb{Z}_2$$

Abbiamo inoltre che $\mathcal{A}ut(\mathbb{Z}_3 \times \mathbb{Z}_5)$ è isomorfo a $\mathcal{A}ut(\mathbb{Z}_3) \times \mathcal{A}ut(\mathbb{Z}_5) \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$ (questo in generale è falso per un prodotto qualsiasi di due gruppi: provare per esercizio a trovare delle condizioni sufficienti per cui vale questo isomorfismo). Quanti omomorfismi possiamo avere da $\mathbb{Z}_2$ a $\mathbb{Z}_2 \times \mathbb{Z}_4$?

- Se mandiamo 1 in $(0,0)$ il $\mathcal{G}$ è isomorfo a

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

- Se 1 va in $(1,0)$ allora corrisponde all'inverso in $\mathbb{Z}_3$ e all'identità in $\mathbb{Z}_5$. Allora abbiamo

$$\mathcal{G} \simeq \mathbb{Z}_5 \times D_3$$

- Se 1 va in $(0,2)$ abbiamo l'inverso su $\mathbb{Z}_5$ e l'identità in $\mathbb{Z}_3$ quindi

$$\mathcal{G} \simeq \mathbb{Z}_3 \times D_5$$

- Possiamo altrimenti mandare 1 in $(1,2)$, quindi abbiamo l'inverso sia in $\mathbb{Z}_3$ che in $\mathbb{Z}_5$. Ma questo è l'inverso in $\mathbb{Z}_{15}$. Quindi in questo caso

$$\mathcal{G} = D_{15}$$

Esercitazione 5

Esercitazione (5)

Definizione 3 (Sottogruppo caratteristico)**.** Sia H un gruppo e $K < H$ tale che

$$\forall \phi \in \mathcal{A}ut\,(H)\,,\ \phi(K) = K$$

Allora K si dice sottogrupo caratteristico.

Osservazione 8. Ogni sottogruppo caratteristico H di un gruppo $\mathcal{G}$ è normale. Dato infatti $g \in \mathcal{G}$, c_g è un automorfismo, quindi in particolare lascia H invariato.

Osservazione 9. Sia $\mathcal{G}$ gruppo, $H \triangleleft \mathcal{G}$ e $K \triangleleft H$. Allora in generale non possiamo dire che $K \triangleleft H$. Ma se K è l'unico gruppo di cardinalità $|K|$ in H (e il sapere questo ci indica anche la normalità di K in H) allora possiamo dirlo, infatti il coniugio rispetto a un qualsiasi elemento $g \in \mathcal{G}$ deve mandare H in H (in quanto H è normale), ma deve anche mandare (in quanto automorfismo) un sottogruppo di ordine $|K|$ in un altro sottogruppo di cardinalità $|K|$; visto che K è l'unico con la sua cardinalità in H, allora sarà mandato in se stesso dal coniugio.
Più in generale possiamo arrivare alla stessa conclusione se sappiamo che K è sottogruppo caratteristico di H. Infatti quello che facciamo è, per ogni $g \in \mathcal{G}$, esaminare $c_g\ |_H$, la restrizione ad H del coniugio rispetto a g, questo è un automorfismo e dunque manda K in K. Quindi questo è normale.

Esercizio 10. Abbiamo cercato, durante la scorsa Esercitazione, di capire come può essere fatto un gruppo $\mathcal{G}$ di ordine 30. Abbiamo detto che se abbiamo un 5-Sylow normale allora esiste $H < \mathcal{G}$ con $|H| = 15$ (e quindi abbiamo $H \triangleleft \mathcal{G}$, inoltre $H \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$). Ci siamo quindi ricondotti ad esaminare come $\mathbb{Z}_2$ può agire su $\mathbb{Z}_{15}$, questo può avvenire in 4 modi diversi, infatti, l'omomorfismo $\mathbb{Z}_2 \xrightarrow{\phi} \mathcal{A}ut\,(\mathbb{Z}_3 \times \mathbb{Z}_5)$ può per ciascun fattore di $\mathbb{Z}_3 \times \mathbb{Z}_5$ mandare 1_2 solamente nell'identità o nell'automorfismo inverso(le due scelte sono indipendenti, visto che abbiamo la somma diretta dei due sottogruppi).
Questi 4 modi diversi coincidono con i gruppi:

- $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.
- $\mathbb{Z}_5 \times \mathcal{D}_3$. Se ϕ agisce banalmente in $\mathbb{Z}_5$.
- $\mathbb{Z}_3 \times \mathcal{D}_5$. Se ϕ agisce banalmente in $\mathbb{Z}_3$.

- $\mathcal{D}_{15}$. Se ϕ agisce non banalmente in nessuno dei due fattori.

Ma se il 5-Sylow non fosse normale allora esisterebbe un unico sottogruppo di ordine 3, dunque normale, e quindi esiste comunque un sottogruppo di ordine 15, ci siano quindi comunque ricondotti alla situazione precedente in cui vi era un sottogruppo di ordine 15.

Esercizio 11. Sia $\mathcal{G}$ un gruppo di ordine $255 = 3 \cdot 5 \cdot 17$. Supponiamo che esista $H < \mathcal{G}$ di cardinalità 85. Vogliamo dimostrare che H è ciclico e normale e che $\mathcal{G}$ deve essere un gruppo ciclico (quindi abeliano).

Svolgimento. H è ciclico, possiamo dirlo perché abbiamo già esaminato le possibili strutture di gruppi di ordine pq con $q \nmid p-1$. Sappiamo inoltre che H è normale. Infatti ha indice 3 in $\mathcal{G}$ e 3 è il più piccolo primo che divide l'ordine del gruppo $\mathcal{G}$.
Andiamo ora ad esaminare $\mathcal{G}$, consideriamo L un generico 3-Sylow di $\mathcal{G}$, come agisce questo su H? Abbiamo che:

$$L \cap H = \{e\}\,,\ |L|\,|H| = |\mathcal{G}| \implies \mathcal{G} = H \rtimes L$$

Ma come può agire L su H? A cosa è isomorfo $\mathcal{A}ut\,(H)$? Visto che $H \simeq \mathbb{Z}_{85}$ possiamo di certo dire:

$$\mathcal{A}ut\,(H) \simeq \mathcal{A}ut\,(\mathbb{Z}_{85}) \overset{*}{\simeq} \mathcal{A}ut\,(\mathbb{Z}_5) \times \mathcal{A}ut\,(\mathbb{Z}_{17}) \simeq \mathbb{Z}_4 \times \mathbb{Z}_{16}$$

Dove $\overset{*}{\simeq}$ sarà più chiaro avanti (anche se vediamo già che un qualsiasi automorfismo di $\mathbb{Z}_5 \times \mathbb{Z}_{17}$ agisce indipendentemente su i due fattori perché questo sono sottogruppi caratteristici, quindi possiamo idealmente spezzare un generico automorfismo in due restrizioni tra di loro indipendenti che individuano univocamente l'automorfismo su tutto $\mathbb{Z}_5 \times \mathbb{Z}_{17}$).
Quindi quello che possiamo dire è che non esistono omomorfismi non banali da $L \simeq \mathbb{Z}_3$ agli automorfismi di $\mathbb{Z}_{85}$, perchè $\mathcal{A}ut\,(\mathbb{Z}_{85})$ ha ordine non divisibile per 3, quindi $\mathcal{G}$ sarà prodotto diretto tra i due sottogruppi e quindi isomorfo a $\mathbb{Z}_{255}$.

Riflessione 6. Sia $n \in \mathbb{N}$, a cosa è isomorfo $\mathcal{A}ut\,(\mathbb{Z}_n)$?
Sappiamo intanto che ogni automorfismo $\psi \in \mathcal{A}ut\,(\mathbb{Z}_n)$ è completamente determinato da $\psi(1)$, inoltre un automorfismo deve mandare un elemento di ordine n (come 1) in un altro elemento di ordine n, abbiamo quindi $\phi(n)$ (qui ϕ è la funzione di Eulero) elementi possibili in cui mandare 1, a ciascuno di questi si può associare infatti un automorfismo. Inoltre in questo modo la composizione di due automorfismi corrisponde al prodotto tra gli elementi che li individuano, abbiamo quindi che $\mathcal{A}ut\,(\mathbb{Z}_n) \simeq \mathbb{Z}_n^*$.

- $\mathbb{Z}_n^*$ è ciclico? Non è detto! Abbiamo visto il caso $n = 85$, in cui $\mathbb{Z}_{85}^* \simeq \mathbb{Z}_4 \times \mathbb{Z}_{16}$.

- Vediamo allora se $\mathbb{Z}_n$ ha sottogruppi caratteristici (che vengono mandati in loro stessi dagli automorfismi), questo ci ha infatti aiutato nell'analisi di $\mathcal{A}ut\,(\mathbb{Z}_{85})$.
  È facile verificare che i p-Sylow sono caratteristici, abbiamo infatti che vi è un unico p-Sylow per ogni p primo che divide la cardinalità di $\mathcal{G}$ (questo vale per ogni gruppo abeliano in quanto in un gruppo tutti i p-Sylow sono tra loro coniugati, ma in un gruppo abeliano il coniugio è

banale), questo sottogruppo deve dunque essere mandato in se stesso da un generico automorfismo. Possiamo quindi spezzare $\mathbb{Z}_n$ nella prodotto dei suoi Sylow, infatti se $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ possiamo scrivere:

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}}$$

Questo è vero infatti, dato un generico gruppo $\mathcal{G}$ abeliano con $N_1, \ldots, N_k$ i suoi p-Sylow, allora abbiamo che $N_1 \times N_2$ è un sottogruppo di $\mathcal{G}$, e in particolare è caratteristico o dunque normale. Possiamo allora iterare il ragionamente fino ad arrivare a dire che $\mathcal{G} = N_1 \times \ldots \times N_k$. Quindi un gruppo abeliano è prodotto diretto dei suoi p-Sylow.
Ma allora la fattorizzazione $\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}}$ è una fattorizzazione di $\mathbb{Z}_n$ in sottogruppi caratteristici. Quello che vorremmo dire è che se $\mathcal{G} = H \times K$ è un prodotto di sottogruppi caratteristici di $\mathcal{G}$, allora

$$\mathcal{A}ut(\mathcal{G}) \simeq \mathcal{A}ut(H) \times \mathcal{A}ut(K)$$

Ma questo è vero, infatti gli automorfismi devono agire internamente rispetto ad H e a K, inoltre i due sottogruppi commutano tra di loro, quindi la restrizione di un automorfismo a K è indipendente dalla restrizione rispetto ad H. Abbiamo quindi che una qualsiasi coppia (ϕ, ψ) di automorfismi con $\phi \in \mathcal{A}ut(H)$ e $\psi \in \mathcal{A}ut(K)$ determina univocamente un automorfismo in $\mathcal{G}$. Possiamo quindi dire:

$$\mathcal{A}ut(\mathbb{Z}_n) \simeq \mathcal{A}ut\left(\mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}}\right) \simeq \mathcal{A}ut\left(\mathbb{Z}_{p_1^{a_1}}\right) \times \ldots \times \mathcal{A}ut\left(\mathbb{Z}_{p_k^{a_k}}\right)$$

Siamo dunque riusciti a ricondurre il problema all'analisi dei vari $\mathcal{A}ut(\mathbb{Z}_{p^m}) \simeq \mathbb{Z}_{p^m}^*$

Riflessione 7. Esaminiamo ora a cosa può essere isomorfo $\mathbb{Z}_{p^m}^*$. Possiamo innanzitutto dire che non è detto che un sottogruppo di questo genere sia ciclico, infatti $\mathbb{Z}_8^* \simeq \mathbb{Z}_2^2$. Distinguiamo dunque due casi:

'$p = 2$' Quello che vogliamo dimostrare è:

$$\mathbb{Z}_{2^m}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}$$

Per farlo dobbiamo trovare:

- $a \in \mathbb{Z}_{2^m}^*$ *t.c.* $o(a) = 2^{m-2}$.
- $b \in \mathbb{Z}_{2^m}^*,\ b \notin < a >$ *t.c.* $o(b) = 2$.

La condizione $b \notin < a >$ corrisponde a chiedere $b \neq a^{2^{m-3}}$.
Prendiamo $a = 5$ e $b = -1$. Quello che vogliamo dimostrare (e che ci è sufficiente per concludere) è che:

$$(1+4)^{2^{m-2}} \equiv 1\,(2^m)$$
$$(1+4)^{2^{m-3}} \not\equiv \pm 1\,(2^m)$$

'$p \neq 2$' In questi casi abbiamo che $\mathcal{A}ut(\mathbb{Z}_{p^n})$ è ciclico. Quello che vogliamo dimostrare è:

$$\mathbb{Z}_{p^n}^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_{p^{n-1}}$$

Per farlo troviamo:

- $a \in \mathbb{Z}_{p^n}^*$ *t.c.* $o(a) = p^{n-1}$.
- $b \in \mathbb{Z}_{p^n}^*$ *t.c.* $o(b) = p-1$.

Non ci serve richiedere che $b \notin < a >$ visto che gli ordini dei due elementi sono coprimi. Dobbiamo quindi solo trovare due elementi di questo tipo.

Per trovare un elemento di ordine $p-1$ consideriamo la seguente mappa:

$$F: \underset{[x]_{p^n}}{\mathbb{Z}_{p^n}^* \simeq \mathcal{A}ut(\mathbb{Z}_{p^n})} \longrightarrow \underset{[x]_p}{\mathbb{Z}_p^* \simeq \mathcal{A}ut(\mathbb{Z}_p)}$$

Questa mappa è evidentemente un omomorfismo ben definito e surgettivo, inoltre sappiamo che per ogni classe di resto modulo p abbiamo diversi rappresentanti della stessa classe modulo $\mathbb{Z}_{p^n}$, inoltre tutti questi elementi (che potremmo scrivere come $F^{-1}([x]_p)$) appartengono a $\mathbb{Z}_{p^n}^*$.
Prendiamo a questo punto $y \in \mathbb{Z}_p^*$ generatore del gruppo (abbiamo cioè $o(y) = p-1$) e scegliamo $\widetilde{y} \in F^{-1}(y)$ possiamo allora dire che $p-1 \mid o(\widetilde{y})$ e quindi $< \widetilde{y} >$ contiene certamente un sottogruppo isomorfo a $\mathbb{Z}_{p-1}$. Abbiamo trovato in via del tutto non costruttiva il nostro elemento di ordine $p-1$.
Consideriamo invece $a = (1+p)$ per concludere ci è sufficiente dimostrare che:

$$(1+p)^{p^{n-1}} \equiv 1\,(p^n)$$
$$(1+p)^{p^{n-2}} \not\equiv 1\,(p^n)$$

Ci siamo quindi ricondotti a dover verificare quattro congruenze; ricordiamole:

- $(1+p)^{p^{n-1}} \equiv 1\,(p^n)$
- $(1+p)^{p^{n-2}} \not\equiv 1\,(p^n)$
- $(1+4)^{2^{m-2}} \equiv 1\,(2^m)$
- $(1+4)^{2^{m-3}} \not\equiv \pm 1\,(2^m)$

Per farlo dimostreremo due congruenze più generali (che implicano tutte le congruenze che ci servono):

$$(1+p^m)^{p^n} \equiv 1\left(p^{n+m}\right)$$
$$(1+p^m)^{p^{n-1}} \equiv 1 + p^{m+n-1}\left(p^{n+m}\right)$$

Partiamo dall'osservare:

$$A \equiv B\left(p^h\right) \implies A^p \equiv B^p\left(p^{h+1}\right)$$

Infatti

$$A \equiv B\left(p^h\right) \implies A \equiv B + p^h C\left(p^{h+1}\right)$$
$$\implies A^p \equiv B^p + \sum_{i=1}^{p} B^{p-i}\binom{p}{i}(p^h C)^i \equiv B^p\left(p^{h+1}\right)$$

Dimostriamo allora le due congruenze per induzione:

- $(1+p^m)^{p^n} \equiv 1\,(p^{n+m})$.

  ι) Vediamo il passo base:

  $$(1+p^m) \equiv 1\,(p^m) \implies (1+p^m)^p \equiv 1\left(p^{m+1}\right)$$

  $\iota\iota$) Per il passo induttivo vediamo che:

  $$\left((1+p^m)^{p^n}\right)^p \equiv (1+p^m)^{p^{n+1}} \equiv 1\left(p^{m+n+1}\right)$$

- Sapendo che $(1+p^m)^{p^{n-1}} \equiv 1 + p^{m+n-1}\,(p^{m+n})$ dimostriamo il passo induttivo della seconda congruenza; elevando alla p entrambi i termini otteniamo:

  $$\begin{aligned}(1+p^m)^{p^n} &\equiv (1+p^{m+n-1})^p \equiv 1 + p\cdot p^{m+n-1} + \sum_{i=2}^{p}\binom{p}{i}p^{m+n-1+i}\\ &\equiv 1 + p^{m+n}\left(p^{m+n+1}\right)\end{aligned}$$

Ricapitoliamo dunque quanto detto nel seguente Teorema.

Teorema 1. *Sia $n \in \ltimes$ e p un primo. Allora abbiamo:*

'$p = 2$' In questo caso:

$$\mathcal{A}ut\,(\mathbb{Z}_{2^n}) \simeq \mathbb{Z}_{2^n}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$$

'$p \neq 2$' Abbiamo qui:

$$\mathcal{A}ut\,(\mathbb{Z}_{p^n}) \simeq \mathbb{Z}_{p^n}^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_{p^{n-1}}$$

Esercizio 12. Trovare i sottogruppi caratteristici (e a cosa sono isomorfi i gruppi degli automorfismi) dei seguenti gruppi:

- $\mathbb{Z}_2 \times \mathbb{Z}_4$ - $\mathbb{Z}_6^2$ - $\mathbb{Z}_9^2$

Esercitazione 6

Esercitazione (6)

Esercizio 13. Cerchiamo di analizzare la struttura di $\mathcal{A}ut(\mathcal{D}_n)$.
Abbiamo già detto che $\mathcal{A}ut(\mathcal{D}_n)$ è costituito da $n \cdot \phi(n)$ elementi e che, come insieme (non come gruppo), è uguale a $\mathbb{Z}_n \times \mathbb{Z}_n^*$. Possiamo però anche dire che $\mathbb{Z}_n$ è normale in $\mathcal{A}ut(\mathcal{D}_n)$, consideriamo infatti:

$$\begin{array}{ccccc} F: & \mathcal{A}ut(\mathcal{D}_n) & \longrightarrow & \mathcal{A}ut(\mathbb{Z}_n) \\ & \begin{array}{c} f\colon \mathcal{D}_n \longrightarrow \mathcal{D}_n \\ \sigma \quad\quad \sigma\rho^i \\ \rho \quad\quad \rho^j \end{array} & & \begin{array}{c} g\colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \\ 1 \quad\quad j \end{array} \end{array}$$

Questa applicazione, ottenuta restringendo un automorfismo di $\mathcal{D}_n$ ad un automorfismo del sottogruppo caratteristico delle rotazioni $\mathbb{Z}_n$, è un omomorfismo surgettivo, il cui nucleo è formato dagli automorfismi di $\mathcal{D}_n$ che fissano ρ, appartenenti a $\mathbb{Z}_n$. Inoltre la sua immagine è isomorfa al sottogruppo degli automorfismi di $\mathcal{D}_n$ che fissano σ, isomorfo a $\mathbb{Z}_n^*$, del quale è immagine isomorfa. Quindi possiamo dire:

$$\mathcal{A}ut(\mathcal{D}_n) \simeq \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$$

Proviamo a vedere questo prodotto semidiretto, sia P un poligono regolare di n lati, come può essere fatto un automorfismo di $\mathcal{A}ut(\mathcal{D}_n)$? Gli elementi di $\mathbb{Z}_n < \mathcal{A}ut(\mathcal{D}_n)$ sono gli automorfismi della forma:

$$\begin{array}{ccccc} \phi_j: & \mathcal{D}_n & \longrightarrow & \mathcal{D}_n \\ & \begin{array}{c} \rho \\ \sigma \end{array} & & \begin{array}{c} \rho \\ \sigma\rho^j \end{array} \end{array}$$

Mentre invece se abbiamo i un numero primo con p allora possiamo anche scrivere:

$$\begin{array}{ccccc} \psi_i: & \mathcal{D}_n & \longrightarrow & \mathcal{D}_n \\ & \begin{array}{c} \rho \\ \sigma \end{array} & & \begin{array}{c} \rho^i \\ \sigma \end{array} \end{array}$$

Possiamo quindi esaminare:

$$\begin{array}{ccccccc} \psi_i \circ \phi_j: & \mathcal{D}_n & \longrightarrow & \mathcal{D}_n & \longrightarrow & \mathcal{D}_n \\ & \begin{array}{c} \rho \\ \sigma \end{array} & & \begin{array}{c} \rho \\ \sigma\rho^j \end{array} & & \begin{array}{c} \rho^i \\ \sigma\rho^{ji} \end{array} \\ \phi_j \circ \psi_i: & \mathcal{D}_n & \longrightarrow & \mathcal{D}_n & \longrightarrow & \mathcal{D}_n \\ & \begin{array}{c} \rho \\ \sigma \end{array} & & \begin{array}{c} \rho^i \\ \sigma \end{array} & & \begin{array}{c} \rho^i \\ \sigma\rho^j \end{array} \end{array}$$

Proviamo ora a rinominare i vertici del poligono: sostituiamo al numero i dell'i-esimo vertice l'elemento $\sigma\rho^i$. Ma allora abbiamo:

$$\psi_i \circ \phi_j(\sigma\rho^a) = \sigma\rho^{ij}\rho^{ia} = \sigma\rho^{ij+ia}$$
$$\phi_j \circ \psi_i(\sigma\rho^a) = \sigma\rho^{j}\rho^{ai} = \sigma\rho^{ai+j}$$

Tutti gli elementi del gruppo possono essere espressi in questa forma, visto che abbiamo un prodotto semidiretto. Possiamo cioè dire:

$$\mathcal{A}ut\left(\mathcal{D}_n\right) = \{\phi_j \circ \psi_i \ t.c. \ i \in \mathbb{Z}_n^*, j \in \mathbb{Z}_n\}$$

La riflessione $\sigma\rho^a$, che possiamo vedere come l'intero a modulo n, viene mandato in $j + ia$, anch'esso un intero modulo n. Ma questa trasformazione descrive un'affinità su $\mathbb{Z}_n$. Abbiamo quindi un omomorfismo da $\mathcal{D}_n$ ad $\mathrm{Aff}(\mathbb{Z}_n)$:

$$\begin{array}{rccc} \vartheta: & \mathcal{A}ut\left(\mathcal{D}_n\right) & \longrightarrow & \mathrm{Aff}(\mathbb{Z}_n) \\ & \phi_j \circ \psi_i & & \begin{array}{ccc} \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ a & & j+ia \end{array} \end{array}$$

Ma i due gruppi hanno la stessa cardinalità, inoltre questa mappa è iniettiva, infatti l'immagine determina univocamente i e j, che a loro volta determinano univocamente l'automorfismo di $\mathcal{D}_n$. Possiamo quindi costruire anche un'altro omomorfismo:

$$\begin{array}{rccc} \chi: & \mathrm{Aff}(\mathbb{Z}_n) & \longrightarrow & \mathbb{Z}_n^* \\ & \begin{array}{ccc} \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ a & & j+ia \end{array} & & i \end{array}$$

Il nucleo di χ è per l'appunto $\mathbb{Z}_n$, che dunque è normale in $\mathrm{Aff}(\mathbb{Z}_n)$. Quindi anche qui (ovviamente visto che $\mathrm{Aff}(\mathbb{Z}_n) \simeq \mathcal{A}ut\left(\mathcal{D}_n\right)$) possiamo dire che $\mathrm{Aff}(\mathbb{Z}_n) = \mathbb{Z}_n \rtimes_\mu \mathbb{Z}_n^*$, ma in questo caso è evidente chi è l'automorfismo dato dal coniugio, se infatti conveniamo di indicare con (i, j) l'affinità che manda a in $ia+j$ possiamo scrivere:

$$\big(\mu(i,0)\big)(i,j) = (i,0)(i,j)(i^{-1},0) = (1,ij)$$

Quindi quello che abbiamo scoperto è che $\mathbb{Z}_n^*$ agisce su $\mathbb{Z}_n^* \simeq \mathcal{A}ut\left(\mathbb{Z}_n\right)$ semplicemente per moltiplicazione, cioè la mappa da $\mathbb{Z}_n^*$ a $\mathcal{A}ut\left(\mathbb{Z}_n\right)$ è semplicemente l'identità, se consideriamo $\mathcal{A}ut\left(\mathbb{Z}_n\right)$ come $\mathbb{Z}_n^*$.

Osservazione 10. Quanto fatto alla fine dell'ultimo esercizio vale in generale per ogni gruppo: sia $\mathcal{G}$ un gruppo, $N \triangleleft \mathcal{G}$, $H < \mathcal{G}$ tali che $\mathcal{G} = N \rtimes_\alpha H$. Allora:

$$\forall h \in H, \ n \in N, \ hnh^{-1} = \alpha(h)(n)$$

Questo vale per definizione di α, inoltre è il nostro unico modo di trovare α se abbiamo un gruppo di cui sappiamo l'operazione interna.

Esercizio 14. Chi sono gli automorfismi di $\mathbb{Z}_6^2$? Per trovarli dividiamo $\mathbb{Z}_6^2$ nei suoi Sylow, scriviamo quindi $\mathbb{Z}_6^2 \simeq \mathbb{Z}_2^2 \times \mathbb{Z}_3^2$. Ma questi sottogruppi sono caratteristici, dunque:

$$\mathcal{A}ut\left(\mathbb{Z}_6^2\right) \simeq \mathcal{A}ut\left(\mathbb{Z}_6^2\right) \times \mathcal{A}ut\left(\mathbb{Z}_6^2\right) \simeq GL_2(\mathbb{Z}_3) \times GL_2(\mathbb{Z}_2)$$

(dove indichiamo con $GL_i(\mathbb{K})$ le matrici invertibili di ordine i a coefficienti in $\mathbb{K}$). Inoltre non vi sono altri sottogruppi caratteristici di $\mathbb{Z}_6^2$, infatti l'intersezione

di sottogruppi caratteristici è un sottogruppo caratteristico, ma non vi sono sottogruppi caratteristici propridi $\mathbb{Z}_2^2$ o di $\mathbb{Z}_3^2$, infatti dati due qualsiasi vettori non nulli, esiste una matrice invertibile che manda uno nell'altro (questo è vero in generale e per questo $\mathbb{Z}_p^n$ non può avere sorrogruppi caratteristici non banali).

Esercizio 15. Trovare gli automorfismi e i sottogruppi caratteristici di $\mathbb{Z}_9^2$.
Un sottogruppo caratteristico di $\mathbb{Z}_9$ è $3\mathbb{Z}_3 = \{3 \cdot i \ t.c. \ i \in \mathbb{Z}_9\}$. Possiamo inoltre vedere che $3 \cdot \mathbb{Z}_9^2$ è un sottogruppo caratteristico di $\mathbb{Z}_9^2$, infatti, dato un automorfismo ϕ su $\mathbb{Z}_9^2$ abbiamo che $\phi(3x) = 3\phi(x)$, che è quindi a sua volta un elemento di $3\mathbb{Z}_9^2$ (possiamo osservare che questo vale per ogni gruppo abeliano $\mathcal{G}$ e per ogni intero m: $m\mathcal{G}$ è un sottogruppo caratteristico).

> *Osservazione* 11. Se $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_2$ e $\mathcal{G}_1, \mathcal{G}_2, H$ sono sottogruppi caratteristici, allora anche $H \cap \mathcal{G}_1$ e $H \cap \mathcal{G}_2$ sono sottogruppi caratteristici. Quindi se $\mathcal{G}_1$ e $\mathcal{G}_2$ non hanno sottogruppi caratteristici propri, dobbiamo avere che, se H è caratteristico, intersechi banalmente $\mathcal{G}_1$ e $\mathcal{G}_2$.
> Questo nel nostro caso particolare ci permette di dire che se $\mathcal{G} \simeq \mathbb{Z}_{p_1}^{a_1} \times \ldots \times \mathbb{Z}_{p_k}^{a_k}$ con i vari p_i primi distinti, abbiamo che non esistono sottogruppi caratteristici non banali, infatti i vari p_i-Sylow di un qualsiasi sottogruppo H devono essere contentuti nei p_i-Sylow di $\mathcal{G}$, che però non ammettono sottogruppi caratteristici non banali.

Sia $x_1 \in \mathbb{Z}_9^2$ di ordine 9. Ogni $\phi \in \mathcal{A}ut\left(\mathbb{Z}_9^2\right)$ manda x_1 in y_1 con $o(y_1) = 9$. Consideriamo ora $x_2 \notin < x_1 >$, certamente condizione necessaria affinché ϕ sia un automorfismo è che $\phi(x_2) = y_2 \notin < y_1 >$. Ma questa condizione non è sufficiente, infatti l'applicazione:

$$f: \begin{array}{ccc} \mathbb{Z}_9^2 & \longrightarrow & \mathbb{Z}_9^2 \\ \begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix} & & \begin{smallmatrix} x_1 \\ x_1+3x_2 \end{smallmatrix} \end{array}$$

rispetta le richieste ma non è un automorfismo. Non è un automorfismo anche perchè la sua restrizione a $3\mathbb{Z}_9^2$ non è iniettiva (manda sia $3x_1$ che $3x_2$ nell'elemento $3x_1$). Per avere un automorfismo è quindi sufficiente e necessario chiedere:

- $\phi(x_1) = y_1$, con $o(y_1) = 9$.
- $\phi(x_2) = y_2$, con $o(y_2) = 9$, $y_2 \notin < y_1 >$ e tale che $< y_2 > \cap < y_2 > = \{e\}$ (per questo è sufficiente che $3y_2 \notin < 3y_1 >$

Date queste condizioni abbiamo $81 - 9 = 72$ scelte possibili per y_1 e $81 - 27 = 54$ scelte possibili per y_2.

Esercizio 16. Cerchiamo di esaminare gli automorfismi di $H = \mathbb{Z}_2 \times \mathbb{Z}_4$. Sappiamo che H è generato da $x_1 \in \mathbb{Z}_2$ e da $x_2 \in \mathbb{Z}_4$, ma allora x_2 deve essere mandato da un automorfismo in un elemento di ordine 4, mentre invece x_1 deve essere mandato in un elemento di ordine 2. In H vi sono quattro elementi di ordine 4 e tre elementi di ordine 2. Possiamo innanzitutto dire che Abbiamo 4 scelte possibili per $y_2 = \phi(x_2)$ mentre abbiamo al più 2 scelte per $y_1 = \phi(x_1)$.
Ma per vedere se tutte queste scelte sono possibili dobbiamo considerare anche che un automorfismo deve mandare in se stessi tutti i sottogruppi caratteristici. In particolare abbiamo che un sottogruppo caratteristico di H è $2H$, ma vediamo che l'unico elemento non banale di $2H$ è $2y_2$, cioè l'unico elemento di

ordine 2 in $\mathbb{Z}_4$. L'imposizione che questo sottogruppo caratteristico vada in se stesso corrisponde alla richiesta: $y_1 \notin < y_2 >$, necessaria comunque a rendere l'applicazione bigettiva.
Per trovare dunque tutti gli automorfismi di $\mathbb{Z}_2 \times \mathbb{Z}_4$ abbiamo bisogno di imporre che il generatore x_1 di $\mathbb{Z}_4$ venga mandato in un elemento di ordine 4 (chiamiamolo y_1, questo lo possiamo fare in 4 modi). A questo punto, per avere un endomorfismo surgettivo dobbiamo mandare un generatore x_2 del fattore $\mathbb{Z}_2$ in un elemento di ordine 2 non contenuto nel gruppo generato da y_1 (possiamo dunque farlo in $3 - 1 = 2$ modi). Queste condizioni sono ora sufficienti per determinare un endomorfismo surgettivo di $\mathbb{Z}_2 \times \mathbb{Z}_4$ e dunque un automorfismo. Quindi in totale abbiamo $4 \cdot 2 = 8$ possibili endomorfismi.
Un altro sottogruppo caratteristico è formato dagli elementi che moltiplicati per 2 danno $0 \in H$; in generale, dato un gruppo commutativo $\mathcal{G}$ considerando

$$\begin{array}{rccc} *_m : & \mathcal{G} & \longrightarrow & \mathcal{G} \\ & g & & m \cdot g \end{array}$$

abbiamo che sia l'immagine ($m\mathcal{G}$), sia il Ker di questa funzione sono sottogruppi caratteristici.

Proposizione 1.

$$\forall n \geq 5,\ \mathcal{A}_n \text{ è semplice}$$

Dimostrazione. Dimostriamolo per induzione. Abbiamo già visto il caso $n = 5$, dimostriamo dunque il passo induttivo. Sia $n \in \mathbb{N}$, diciamo:

$$\mathcal{A}_n \supseteq G_i = \{\sigma \in \mathcal{A}_n \text{ t.c. } \sigma(i) = i\} \ \simeq \ \mathcal{A}_{n-1}$$

Utilizzando quindi l'ipotesi induttiva possiamo dire che G_i è semplice $\forall i$. Inoltre i vari G_i sono tra di loro coniugati, dato indatti σ tale che $\sigma j = i$, è immediato verificare che:

$$\sigma G_i \sigma^{-1} = G_j$$

Sia ora $N \triangleleft A_n$, per quanto detto fino ad ora (i G_i sono semplici) abbiamo solo due possibilità:

- $\forall i_1^n,\ N \cap G_i = \{e\}$.
- $\exists i$ *t.c.* $G_i \cap N = G_i$, ma abbiamo detto che tutti i G_i sono tra di loro coniugati, inoltre N è normale per ipotesi. In questo caso dunque $\forall k_1^n,\ N \cap G_k = G_k$. Ma in questo caso è facile concludere che $N = \mathcal{A}_n$ (l'unione dei G_i contiene un insieme di generatori di $\mathcal{A}_n$).

Consideriamo dunque il caso in cui $N \triangleleft \mathcal{A}_n$ non abbia punti fissi (e non sia il sottogruppo banale). Possiamo allora dire che, dati $\sigma, \tau \in N$, $\exists i_1^n$ *t.c.* $\sigma(i) = \tau(i) \implies \sigma =$, infatti altrimenti avremmo che $\tau^{-1}\sigma(i) = i$.
Dunque due permutazioni di N non mandano mai elementi uguali nello stesso posto. Sia dato allora $\sigma \in N$, una permutazione il cui spezzamento in cicli disgiunti è dato da k cicli $c_1, \ldots, c_k$ di lunghezza rispettivamente $r_1, \ldots, r_k$.
Se $r_1 \geq 3$ allora sia $c_1 = (i_1, \ldots, i_{r_1})$, prendiamo a questo punto $\rho = (i_3, j, k)$ con $j, k \notin \{i_1, i_2, i_3\}$ allora $\sigma \neq \rho\sigma\rho^{-1} = \tau \in N$ (visto che N è normale), ma allora $\sigma(i_1) = \tau(i_1)$ e le due permutazioni sono diverse. Assurdo.
Deve essere allora che $r_1 = 2$ ma allora $c_1 c_2 = (i, j)(k, h)$. Consideriamo quindi $\rho = (h, p, q)$ con $p, q \notin \{i, j, k, h\}$; abbiamo ancora che $\sigma \neq \tau = \rho\sigma\rho^{-1} \in N$ ma $\sigma(i) = \rho(i)$. Quindi un altro assurdo. □

Esercizio 17. Sia $\mathcal{G}$ un gruppo di cardinalità pqr con p, q, r dei primi distinti ($p < q < r$). Allora valgono:

a) L'r-Sylow è normale in $\mathcal{G}$.

b) $\exists H \triangleleft \mathcal{G}$ di ordine qr.

c) Se $q \nmid r - 1$ allora anche il q-Sylow è normale in $\mathcal{G}$.

Dimostrazione. a) Se l'r-Sylow non fosse normale abbiamo le seguenti possibilità per n_r:

- $n_r = q$. Non è congruo ad 1 modulo r.
- $n_r = p$. Non è congruo ad 1 modulo r.
- $n_r = pq$. Unico altro caso possibile (a parte $n_r = 1$). Ma in questo caso avremmo $(r-1)pq$ elementi di ordine r, rimangono dunque nel gruppo solo pq elementi che hanno ordine diverso; per questo deve essere che o il p-Sylow o il q-Sylow sono normali; in entrambi i casi abbiamo un prodotto $N = N_p N_q$ di ordine pq che è normale in $\mathcal{G}$ (è normale perchè non c'è spazio in $\mathcal{G}$ per averne altri). Detto dunque H un r-Sylow avremmo:

$$\mathcal{G} = N \rtimes_\phi H$$

Cerchiamo dunque un possibile $H \xrightarrow{\phi} \mathcal{A}ut(N)$ omomorfismo. Abbiamo però che $r \nmid |\mathcal{A}ut(N)|$ (visto che $r > q, p$) dunque ϕ deve essere banale, ma allora in questo caso l'r-Sylow sarebbe normale. Assurdo.

b) Sia H l'r-Sylow. Allora, detto L un qualunque q-Sylow, abbiamo che

$$K = H \rtimes L$$

è un sottogruppo di $\mathcal{G}$ di indice p, dunque normale.

c) Se $q \nmid r-1$ allora $K = H \times L$ e quindi L è l'unico sottogruppo di ordine q in K (visto che un gruppo di ordine primo è ciclico), dunque è un sottogruppo normale di $\mathcal{G}$.

□

Definizione 4 (Commutatori e derivato)**.** Sia $\mathcal{G}$ un gruppo e $a, b \in \mathcal{G}$; si dice allora commutatore di ab l'elemento:

$$[a, b] = aba^{-1}b^{-1}$$

Viene invece detto derivato o sottogruppo dei commutatori il sottogruppo:

$$\mathcal{G}' = < [a, b] \text{ } t.c. \text{ } a, b \in \mathcal{G} >$$

Osservazione 12. A proposito di commutatori vi sono da fare alcune annotazioni:

- In generale non si può dire che due elementi di un gruppo commutano, ma certamente commutano a meno di un commutatore, dato infatti un gruppo $\mathcal{G}$ e due suoi elementi a e b abiamo che

$$ab = [a, b]ba$$

- $\mathcal{G}'$ è caratteristico in $\mathcal{G}$, perché gli automorfismi conservano la sua struttura di sottogruppo che fa commutare tutti gli elementi del gruppo.
- Il gruppo $\mathcal{G}/\mathcal{G}'$ è abeliano (è un gruppo visto che, in particolare $\mathcal{G}'$ è normale), abbiamo infatti:

$$ab = ba[a^{-1}, b^{-1}]$$

- $\mathcal{G}/\mathcal{G}'$ è il più grande quoziente abeliano su $\mathcal{G}$, cioè se $N \triangleleft \mathcal{G}$ e $\mathcal{G}/N$ è abeliano, allora $\mathcal{G}' \subseteq N$. Dati infatti $a, b \in \mathcal{G}$ e $\overline{a}, \overline{b} \in \mathcal{G}/N$ abbiamo:

$$\overline{a}\ \overline{b} = \overline{b}\ \overline{a} \implies \overline{a}\ \overline{b}\ \overline{a^{-1}}\ \overline{b^{-1}} = \overline{e}$$

  quindi $[a, b] \in N$.

Definizione 5 (Risolubile)**.** Sia $\mathcal{G}$ un gruppo finito. $\mathcal{G}$ si dice risolubile se esiste una successione di sottogruppi

$$\mathcal{G} = H_0 \triangleright H_1 \triangleright \ldots \triangleright H_n = \{e\}$$

tali che $\forall i_0^{n-1} H_i/H_{i+1}$ è abeliano

Osservazione 13. Se $\mathcal{G}$ è un gruppo risolubile allora è risolubile con quozienti ciclici. Cioè se $H_i/H_i + 1$ è abeliano finito, allora esiste una successione:

$$H_i = K_{i,0} \triangleright \ldots \triangleright K_{i,h} = H_{i+1}$$

tale che $K_{i,j}/K_{i,j+1}$ è ciclico.

Dimostrazione. Siano infatti:

$$H_i/H_{i+1} \simeq \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$$
$$L_{i,j} = \mathbb{Z}_{n_j} \oplus \ldots \oplus \mathbb{Z}_{n_k}$$

Abbiamo quindi che $L_{i,j}/L_{i,j+1} \simeq \mathbb{Z}_{n_j}$. Consideriamo ora l'omomorfismo $H_i \xrightarrow{\pi} H_i/H_{i+1}$ e indichiamo con $K_{i,j} = \pi^{-1} L_{i,j}$.
Prendiamo ora la successione:

$$\mathcal{G}^{(0)} = \mathcal{G}$$
$$\mathcal{G}^{(i+1)} = \mathcal{G}^{(i)}$$
$$\mathcal{G}^{(0)} \triangleright \ldots \triangleright (\mathcal{G}^{(n)})'$$

Se non esiste n per il quale $\mathcal{G}^{(n)} = \{e\}$ allora il gruppo non è risolubile, se invece questo n esiste il gruppo è risolubile per definizione di risolubilità. E in questo caso possiamo applicare quanto detto per avere una successione ciclica. □

Esempio 4. Sia $\sigma = (1, 2)(3, 4)$, cerchiamo il centralizzante e il normalizzatore di σ in $\mathcal{S}_6$.

Dimostrazione. Sappiamo che il centralizzante di una permutazione è dato innanzitutto dalle potenze dei vari cicli disgiunti che compongono la permutazione, ai quali vanno aggiunte le permutazioni che variano gli elementi non toccati dalla permutazione. Inoltre anche gli elementi che scambiano tra di loro gli n-cicli della permutazione sono elementi del centralizzante. Abbiamo dunque (dato che per motivi di cardinalità abbiamo l'uguaglianza):

$$C_{\mathcal{S}_6}(\sigma) =< (1,2), (3,4), (5,6), (1,3)(2,4) >$$

Vediamo invece cosa avviene se consideriamo σ in $\mathcal{S}_7$:

$$C_{\mathcal{S}_7}(\sigma) =< (1,2), (3,4), (1,3)(2,4) > \times \mathcal{S}_{\{5,6,7\}}$$

Il normalizzatore in $\mathcal{S}_6$ è uguale al centralizzante, infatti un sottogruppo di due elementi ha solo l'automorfismo banale. □

Lezione del 4/11

Riflessione 8. Sia $\sigma \in \mathcal{S}_n$ consideriamo allora l'omomorfismo:

$$\begin{array}{ccccc} \Phi: & N(\sigma) & \longrightarrow & \mathcal{A}ut(<\sigma>) \\ & \tau & & \tau:\ {\scriptstyle <\sigma>} \longrightarrow {\scriptstyle <\sigma>} \\ & & & \quad {\scriptstyle \sigma^i} \quad\ {\scriptstyle \tau\sigma^i\tau^{-1}} \end{array}$$

Il Ker di Φ è il centralizzante di σ. Abbiamo quindi la successione:

$$C(\sigma) \longrightarrow N(\sigma) \overset{\Phi}{\twoheadrightarrow} \mathcal{A}ut(\sigma)$$

Ci chiediamo se esiste una $\mathcal{A}ut(<\sigma>) \overset{\Psi}{\longrightarrow} N(\sigma)$ tale che $\Phi \circ \Psi = Id$, facendo questo avremmo che $N(\sigma)$ è prodotto semidiretto di $C(\sigma)$ e degli automorfismi di $<\sigma>$ (sappiamo infatti che la successione è sicuramente esatta in $N(\sigma)$, inoltre detto $K = Im\Psi$ allora abbiamo che $C(\sigma) \cap K = \{e\}$ e inoltre vale anche $C(\sigma)\,K = N(\sigma)$).
Il prodotto semidiretto è quello che vi è in $\mathcal{S}_n$, infatti entrambi i sottogruppi vivono in $\mathcal{S}_n$, quindi le relazioni che vi sono tra di loro sono conosciute

Esempio 5. Sia $\sigma = (1,2,3,4,5)(6,7,8)$, questa permutazione ha ordine 15, abbiamo dunque che $\mathcal{A}ut(\sigma) \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$, vogliamo dunque che uno $\mathbb{Z}_2 \times \mathbb{Z}_4$ agisca per coniugio su σ.

Esercizio 18. Un gruppo di ordine 144 non è semplice.

Dimostrazione. Se fosse semplice allora il 3-Sylow non potrebbe essere normale, possiamo quindi averne 4 o 16. Vediamo i casi:

- Se avessimo quattro 3-Sylow potremmo considerare l'omomorfismo $\mathcal{G} \overset{\phi}{\longrightarrow} \mathcal{S}_4$ data dall'azione coniugio di $\mathcal{G}$ sull'insieme dei 3-Sylow. Questo omomorfismo non può essere banale (tutti i 3-Sylow sono coniugati), dunque il Ker sarebbe non banale (per motivi di ordine: $\mathcal{S}_4$ è troppo piccolo), ma questo è assurdo.
- Allora supponiamo di avere 16 diversi 3-Sylow. Come possono intersecarsi tra di loro?
  - Intersezione banale. Avremmo allora che $8 \cdot 16$ elementi in $\mathcal{G}$ hanno un ordine diviso da 3, ma in questo caso ci sarebbe posto per un unico 3-Sylow.
  - Allora vi sono due 3-Sylow che si intersecano in modo non banale. Chiamiamoli P_1 e P_2 e consideriamo: $r = |N(P_1 \cap P_2)|$, sappiamo che $9 \mid r$ e inoltre deve essere $r > 9$, visto che $N(P_1 \cap P_2)$ contiene sia P_1 che P_2. Ma allora possiamo avere:

a) $r = 144$. In questo caso abbiamo finito: l'intersezione è normale e non banale.

b) $r = 36, 72$. In questi casi avremmo che ha indice 2 oppure 4, avremmo quindi un omomorfismo non banale di $\mathcal{G}$ su $\mathcal{S}_2$ o su $\mathcal{S}_4$, abbiamo quindi un sottogruppo normale che ci viene dato dal Ker.

c) $r = 18$ Ma allora $[N(P_1 \cap P_2) : P_1] = 2$, dunque $P_1 \triangleleft N(P_1 \cap P_2)$. Ma $N(P_1) = P_1$, dunque P_1 non può essere normale in un sottogruppo più grande. Assurdo.

□

Esercizio 19. Sia $\mathcal{G}$ un gruppo di cardinalità $168 = 2^3 \cdot 3 \cdot 7$ e semplice.

a) Quanti sono i sottogruppi di ordine 7?

b) $\exists H < \mathcal{G}$ *t.c.* $|H| = 21$.

c) $\nexists H < \mathcal{G}$ *t.c.* $|H| = 14$.

Dimostrazione. a) Equivale a chiedersi quanti sono i 7-Sylow. Per motivi di ordine e per il teorema di Sylow questi possono essere solo 1 (non può accadere, altrimenti sarebbe normale), 15 (non può essere: $15 \nmid 168$) oppure 8, che sarà la nostra risposta.

b) Cerchiamo un normalizzatore di N_7 (un $7 - Sylow$) che abbia in lui un elemento di ordine 3, infatti in un sottogruppo di ordine 21 il 7-Sylow è normale. Dunque sia $g \in \mathcal{G}$ di ordine 3, consideriamo allora $< g >$ e lo facciamo agire per coniugio sull'insieme dei 7-Sylow; ma gli elementi di ordine 3 in $\mathcal{S}_8$ lasciano comunque almeno due punti fissi. Quindi ci sono almeno 2 diversi 7-Sylow normalizzati da g. Quindi abbiamo che $\mathbb{Z}_3 < \mathcal{G}$ e $\mathbb{Z}_7 < \mathcal{G}$ con $\mathbb{Z}_3 < N(\mathbb{Z}_7)$. Possiamo allora certamente considerare $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ di ordine 21.

c) Se esistesse allora avremmo $H \simeq \mathcal{D}_7$, ma allora $N_7 \triangleleft H$. Allora esiste un g di ordine 2 nel normalizzante del 7-Sylow. Ma abbiamo già visto che il normalizzante di un 7-Sylow ha ordine 21, non ci possono dunque essere elementi di ordine 2.

□

Esercizio 20. Chi è un 2-Sylow di $\mathcal{S}_4$?

- Sappiamo che ha 8 elementi, potrebbe quindi essere isomorfo a $\mathcal{D}_4$, ne abbiamo un esempio pensando a:

$$< (1,2,3,4), (2,4) > \simeq \mathcal{D}_4$$

E in $\mathcal{S}_5$? Lo stesso! Infatti non vengono aggiunti fattori 2 nella cardinalità del gruppo.
In $\mathcal{S}_6$ qual'è il 2-Sylow? Vediamo esplicitamente che sono tutti i coniugati di:

$$< (1,2,3,4)(2,4)(5,6) >$$

Cosa possiamo dire di $\mathcal{S}_8$? Il 2-Sylow questa volta ha ordine 2^7, sappiamo trovare facilmente un sottogruppo di ordine 2^6: consideriamo infatti:

$$< (1,2,3,4),(2,4) > \times < (5,6,7,8),(6,8) >$$

Possiamo però espanderlo al suo normalizzatore con $\tau = (1,5)(2,6)(3,7)(4,8)$. Abbiamo quindi un 2-Sylow isomorfo a $(\mathcal{D}_4 \times \mathcal{D}_4) \rtimes \mathcal{S}_2$.

Esercizio 21. Come sono fatti i p-Sylow in $\mathcal{S}_n$?
Per farlo può essere utile ripetere il ragionamento fatto per i 2-Sylow in $\mathcal{S}_n$ che abbiamo appena fatto.

Esercizio 22. Qual'è il più piccolo n tale che si può immergere $\mathcal{Q}_8$ in $\mathcal{S}_n$?

Osservazione 14. Un gruppo è risolubile se e solo se è risolubile per commutatori.

Dimostrazione. Chiaramente se un gruppo è risolubile per commutatori allora è risolubile. È evidente che $\mathcal{G}$ è risolubile per commutatori se e solo se lo è anche $\mathcal{G}'$. Ma allora se $\mathcal{G}$ è finito e risolubile abbiamo:

$$\mathcal{G} > H_1 > \ldots > H_n = \{e\}$$

con quozienti abeliani. Ma se $\mathcal{G}/H_1$ è abeliano allora $\mathcal{G}' \triangleleft H_1$. Consideriamo allora la successione

$$\mathcal{G}' \cap H_1 > \ldots > \mathcal{G}' \cap H_n$$

Questi sono tutti quozienti abeliani, dunque $\mathcal{G}'$ è risolubile. Si ha la tesi per induzione sull'ordine di $\mathcal{G}$. □