Università degli Studi di Cagliari

Dipartimento di Matematica e Informatica

Laurea Triennale in Matematica

Teoremi generali di classificazione per gruppi finiti e classificazione dei gruppi di ordine $n < 32$

Relatore: Prof. Andrea Loi **Candidato: Marco Damele**

Anno Accademico 2021/2022

Cagliari - 24/02/2023

Introduzione

Un problema affascinante nell'ambito della teoria dei gruppi è quello di classificare (a meno di isomorfismi) tutti i gruppi finiti. Ad oggi, una classificazione completa, non esiste. Sappiamo classificare solo pochi di essi. Notevole è,ad esempio, il teorema di Frobenius-Stickelberg circa la classificazione per i gruppi abeliani finiti oppure il teorema di classificazione per i gruppi semplici finiti (quest'ultimo non ha un vero e proprio nome, consiste di centinaia e centinaia di articoli che messi assieme permettono di classificare tutti i gruppi semplici finiti). Sfortunatamente esistono gruppi non abeliani e non semplici e una loro classificazione non è ancora stata prodotta. Ma che senso ha classificare i gruppi? In generale i teoremi di classificazione in matematica sono importanti perchè permettono di passare da qualcosa di astratto a qualcosa di più concreto. In che senso ? Per capirlo supponiamo che io non conosca un teorema di classificazione per i gruppi semplici non abeliani di ordine 60 e supponiamo che un giorno congetturi qualcosa su di essi. Senza un teorema di classificazione dovrei prendere un generico gruppo semplice di ordine 60 e non abeliano e vedere se la mia congettura è verificata. Se invece ci fosse un teorema di classificazione (esiste, come vedremo nel corso della tesi) questo mi direbbe quali gruppi studiare, su quali concentrare le mie attenzioni. Comunque essi, sono , a mia modestissima opinione , affascinanti di suo, a prescindere dal fatto che abbiano un'applicazione teorica rilevante. Uno degli strumenti più potenti per classificare i gruppi finiti (e non solo) sono i teoremi di Sylow. Questa tesi è suddivisa in 4 capitoli. Nel primo capitolo dimostreremo i teoremi di Sylow e la semplicità di A_n con n $\geq$ 5 (quest'ultimo fatto ci servirà in realtà solo nel caso particolare in cui n=5). Nel secondo capitolo introduciamo i prodotti semidiretti (perchè saranno importantissimi per i teoremi di classificazione) e introduremo il gruppo dei quaternioni generalizzato Q_{2^n}. Nel terzo capitolo dimostreremo alcuni teoremi di classificazione generali (ad esempio classificheremo i gruppi di ordine p^3 con p primo). Infine nell'ultimo capitolo classificheremo tutti i gruppi di ordine n con n < 32. Il lettore dovrà

avere giusto le conoscenze teoriche istituite in un corso introduttivo sulla teoria dei gruppi, ovvero le nozioni di gruppo,sottogruppo,omomorfismo,quoziente e prodotto diretto .

Indice

1 Preliminari **9**

1.1 Notazioni adottate 9

1.2 Teoremi principali sui gruppi 10

2 I teoremi di Sylow e la semplicità di An **13**

2.1 Sottogruppo derivato, cuore, chiusura normale e centralizzante 13

2.1.1 Sottogruppo derivato 13

2.1.2 Cuore e chiusura normale 14

2.1.3 Centralizzante 16

2.2 Equazione delle classi,lemma di Cauchy,p-gruppi e normalizzante 16

2.2.1 Equazione delle classi 16

2.2.2 Lemma di Cauchy 17

2.2.3 p-gruppi 18

2.2.4 Normalizzante 20

2.3 La semplicità di An 22

2.3.1 Alcune proposizioni preliminari 23

2.3.2 Sottogruppi normali di S_n con n $\geq$ 5 24

2.3.3 A_n è semplice e non abeliano $\forall$ n $\geq$ 5 26

2.4 Azioni di gruppo e teoremi di Sylow 28

2.4.1 Cenni alle azioni di gruppo 28

2.4.2 I teoremi di Sylow 31

3 Prodotti semidiretti e il gruppo Q_{2^n} **37**

3.1 Prodotti semidiretti 37

3.2 Il gruppo Q_{2^n} 41

4 Teoremi di classificazione per gruppi finiti **47**

4.1 Gruppi ciclici finiti 47

4.2 Gruppi di ordine p 48

4.3 Gruppi di ordine 2p 48

4.4 Gruppi di ordine p^2 50

4.5 Gruppi di ordine p^3 50

4.6 Gruppi di ordine pq,p^2q,p^2q^2 55

4.7 Gruppi abeliani finiti 57

4.8 Gruppi in cui l'equazione x^n=1 ha al più n soluzioni per ogni n $\in \mathbb{N}$ 57

4.9 Ogni gruppo finito è isomorfo a un sottogruppo di permutazioni 59

4.10 Ogni gruppo finito è isomorfo a un sottogruppo di matrici 59

4.11 Un teorema di classificazione per p-gruppi finiti 61

4.12 Gruppi semplici non abeliani di ordine 60 62

5 Classificazione dei gruppi di ordine n < 32 **67**

5.1 Gruppi di ordine 2,3,5,7,11,13,17,19,23,29,31 67

5.2 Gruppi di ordine 6,10,14,22,26 68

5.3 Gruppi di ordine 4,9,25 68

5.4 Gruppi di ordine 8 68

5.5 Gruppi di ordine 12 70

5.6 Gruppi di ordine 15 75

5.7 Gruppi di ordine 16 75

5.8 Gruppi di ordine 18 92

5.9 Gruppi di ordine 20 99

5.10 Gruppi di ordine 21 102

5.11 Gruppi di ordine 24 104

5.12 Gruppi di ordine 27 116

5.13 Gruppi di ordine 28 116

5.14 Gruppi di ordine 30 119

Ringraziamenti

Il compimento del mio percorso di laurea triennale e della realizzazione di questa tesi non sono stati solo merito mio, ho avuto al mio fianco persone speciali che ogni giorno mi hanno spronato ad andare avanti e a dare il meglio di me. In primis il mio migliore amico Nicola,una bellissima persona e un punto di riferimento per me. Non dimenticherò mai quanto mi è stato vicino nei momenti più bui. In secundis Nadia, la mia dolce metà, sempre al mio fianco, mi fa amare la vita ogni giorno sempre di più. Senza di lei non ce l'avrei mai fatta. Per non parlare della mia famiglia che non mi ha mai fatto mancare niente, papà che mi ha sempre spronato a fare di più e mi ha insegnato che nella vita bisogna prima di tutto amare se stessi e inseguire i propri sogni, qualunque essi siano, mamma che con la sua infinita dolcezza mi ha riscaldato nelle giornate più fredde e Giulio che, nei momenti in cui è stato a casa, è riuscito sempre, in un modo o nell'altro, a strapparmi un sorriso.Voglio ringraziare anche tutti i miei amici che sono stati al mio fianco nonostante non sia stato sempre presente.In particolare Stefano per il suo costante interessamento.Infine, come non ringraziare tutto il corpo docente, a partire dal mio relatore Professor Loi, per i suoi aiuti costanti e per i preziosi consigli dati. Non possono non citare anche la professoressa Onnis per avermi incitato ad andare avanti e per avermi regalato i suoi favolosi libri di geometria. Grazie anche a Benedetto che in dipartimento mi strappa sempre un sorriso.

Capitolo 1

Preliminari

In questo capitolo fissiamo le notazioni che adotteremo nel seguito e richiamiamo alcuni risultati fondamentali per la comprensione dei capitoli 2 ,3 e 4.

1.1 Notazioni adottate

Nel seguito se G è un gruppo e N è un sottogruppo normale di G (contenuto strettamente in esso) scriviamo N $\triangleleft$ G oppure N $\trianglelefteq$ G (se può capitare anche che G = N) Se invece H è un sottogruppo di G (non necessariamente normale) scriviamo H < G (se H è contenuto strettamente in G) o H $\leq$ G (nel caso possa capitare che H = G). Inoltre denoteremo con 1_G l'elemento neutro del gruppo oppure , se non ci sarà rischio di ambiguità , solamente con 1. Denotiamo con Aut(G) il gruppo degli automorfismi di G cioè il gruppo di tutti gli isomorfismi da G in G. Se H $\leq$ G e g $\in$ G, denotiamo con H^g il sottogruppo H^g = $\{g^{-1}hg : h \in H\}$.Se X è un sottoinsieme di G denotiamo con <X> il sottogruppo generato da X, cioè l'intersezione di tutti i sottogruppi di G che contengono X.Si ricordi che :

$$< X > = \left\{x_{i_1}^{k_1}...x_{i_m}^{k_m} : x_{i_j} \in X \forall i, j, k_t \in \mathbb{Z}, \forall t = 1, ..., m, m \in \mathbb{N}^+\right\}$$

Se x $\in$ G e H $\leq$ G denotiamo con xH e Hx le classi laterali sinistre e destre di x rispettivamente. Ovvero:

$$xH = \{xh : h \in H\}$$

$$Hx = \{hx : h \in H\}$$

Si ricordi inoltre che se N $\trianglelefteq$ G nel gruppo quoziente G / N (oppure lo indicheremo con $\frac{G}{N}$) l'operazione è :

(aN)(bN) = (ab)N

Ricordiamo che se H è un sottogruppo di G allora H $\trianglelefteq$ G $\iff$ $\forall$ x $\in$ G H = H^x Se H $\leq$ G allora H $\triangleleft$ G $\iff$ H = H^G. Inoltre denoteremo con Z(G) il centro di G. Nel seguito se X è un insieme denotiamo con | X | la sua cardinalità.Se a $\in$ G denotiamo l'ordine di a con o(a). Ricordiamo che se H è un sottogruppo di G allora [G:H] := | $\{xH : x \in G\}$ | viene detto indice di H in G. Se G è finito | G | = [G:H]| H |, tale relazione viene detto teorema di Lagrange.Ricordiamo che se H $\leq$ G e x,y $\in$ G allora: xH=yH $\iff$ $xy^{-1} \in$ H. Se X $\subseteq$ G e g $\in$ G, si denota con X^g = $\{g^{-1}xg : x \in X\}$

1.2 Teoremi principali sui gruppi

I teoremi che seguono verranno usati ripetutamente durante la tesi.

Teorema 1. *(Teorema fondamentale delle permutazioni) Sia X un insieme non vuoto e f* $\in$ S_X *: | suppf | < ∞ dove suppf = $\{x \in X : f(x) \neq x\}$. Allora esistono t* $\in \mathbb{N}^+$ *cicli* σ_1*,...,*σ_t *disgiunti (cioè supp*$\sigma_i \cap$ *supp*σ_j *= $\emptyset$ $\forall$ i $\neq$ j) tali che f =* $\sigma_1 \circ ... \circ \sigma_t$*. Tale decomposizione è unica a meno dell'ordine dei fattori.Inoltre o(f)=m.c.m(o(*σ_1*),...,o(*σ_t*))*

Teorema 2. *(Il segno è una funzione moltiplicativa) Sia X un insieme non vuoto e f,g* $\in$ S_X *: | suppf | < ∞ e | suppg | < ∞. Allora sgn(f $\circ$ g) = sgn(f)sgn(g) (dove sgn denota la funzione segno)*

Teorema 3. *Sia X un insieme non vuoto e f* $\in$ S_X *: | suppf | < ∞. Allora: sgn(f) = 1 $\iff$ f è il prodotto di un numero pari di trasposizioni*

Teorema 4. *Sia X un insieme non vuoto e f,g* $\in$ S_X *: suppf* $\cap$ *suppg =* $\emptyset$*. Allora f* $\circ$ *g = g* $\circ$ *f*

Teorema 5. *Se G è un gruppo finito e H,K* $\leq$ *G allora:*

1. $|HK| = \frac{|H||K|}{|H \cap K|}$
2. *se K* $\trianglelefteq$ *G* $\rightarrow$ *HK* $\leq$ *G*
3. *se H,K* $\trianglelefteq$ *G* $\rightarrow$ *HK* $\trianglelefteq$ *G*

Teorema 6. *(Teorema numerico) Sia G un gruppo : | G | = mn con (m,n)=1, H,K* $\trianglelefteq$ *G : | H | = m e | K | = n allora G* $\simeq$ *H* $\times$ *K.*

Teorema 7. *(Teorema prodotto) Sia G un gruppo e H,K* $\triangleleft$ *G : H* $\cap$ *K =* $\{1\}$ *e HK = G allora G* $\simeq H \times K$

Teorema 8. *Aut(*$\mathbb{Z}_m$*) è ciclico* $\iff$ *m* $\in \{1, 2, 4, p^k, 2p^k\}$ *con p primo dispari.*

Teorema 9. *Aut(*$\mathbb{Z}_m$*)* $\simeq$ *U(*$\mathbb{Z}_m$*) dove U(*$\mathbb{Z}_m$*) =* $\{[a]_m : (a, m) = 1\}$

Teorema 10. *Se H,K sono gruppi isomorfi allora Aut(H)* $\simeq$ *Aut(K)*

Teorema 11. *Se H,K sono gruppi finiti : (|H|,|K|)=1 allora Aut(H* $\times$ *K)* $\simeq$ *Aut(H)* $\times$ *Aut(K)*

Teorema 12. $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ $\iff$ *(m,n)=1*

Capitolo 2

I teoremi di Sylow e la semplicità di An

2.1 Sottogruppo derivato, cuore, chiusura normale e centralizzante

2.1.1 Sottogruppo derivato

Definizione 1. *Sia G un gruppo e a,b ∈ G.Viene detto commutatore di a e b l'elemento di G:*

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

Osservazione 1. *Sia G un gruppo e a,b ∈ G. Allora*

$$ab = ba \iff [a,b]=1$$

Infatti

$$ab=ba \iff ab(ba)^{-1}=1 \iff aba^{-1}b^{-1}=1$$

Osservazione 2. *Sia G un gruppo e N ⊴ G. Siano n ∈ N e g ∈ G. Allora*

$$[n,g] \in N$$

Infatti [n,g]=ngn^{-1}g^{-1} e siccome gn^{-1}g^{-1} ∈ N (esseno N normale in G) si ha [n,g] ∈ N.

Definizione 2. *Sia G un gruppo e H ≤ G. H è detto caratteristico in G se ∀ ϕ ∈ Aut(G) si ha che ϕ(H) ≤ H.*

Proposizione 1. *Sia G un gruppo e H ≤ G caratteristico.Allora H ⊴ G.*

Dimostrazione. Ricordiamo che H $\trianglelefteq$ G $\iff$ $\forall$ g $\in$ G $H^g \leq$ H .Sia quindi g $\in$ G, mostriamo che $H^g \leq$ H. Abbiamo che H^g= $\{g^{-1}hg : h \in H\}$ = $\{\phi_g(h) : h \in H\}$ = $\phi_g(H) \leq$ H dove ϕ_g denota l'automorfismo di G definito da $\phi_g(h)$:= g^{-1}hg $\forall$ h $\in$ H. Quindi si ha la tesi. □

Definizione 3. *Sia G un gruppo.Viene detto derivato di G il sottogruppo di G così definito:*

$$G' := < \{[a, b] : a, b \in G\} >$$

Proposizione 2. *Sia G un gruppo.Allora G' $\trianglelefteq$ G.*

Dimostrazione. Mostriamo che G' è caratteristico in G.Sia $\phi \in$ Aut(G),dimostriamo che ϕ(G') $\leq$ G'.Sia g $\in$ ϕ(G').Allora g=ϕ(x) per qualche x $\in$ G'. x avrà la forma:

$$x=[a_1, b_1]^{c_1} \dots [a_t, b_t]^{c_t}$$

per certi a_i e b_i i=1,...,t in G e per certi c_i i=1,...,t in $\mathbb{Z}$.Quindi:

$$g=\phi(x)=\phi([a_1, b_1]^{c_1} \dots [a_t, b_t]^{c_t})=\phi([a_1, b_1]^{c_1}) \dots \phi([a_t, b_t]^{c_t})$$

ora fissato i $\in \{1, \dots, t\}$ si ha che

$$\phi([a_i, b_i]^{c_i})=(\phi(a_i b_i a_i^{-1} b_i^{-1}))^{c_i}=[\phi(a_i),\phi(b_i)]^{c_i}$$

che è un elemento di G',quindi si ha la tesi. □

Proposizione 3. *Sia G un gruppo e N $\trianglelefteq$ G.Allora:*

$$G / N \text{ è abeliano} \iff G' \leq N$$

Dimostrazione. G / N è abeliano $\iff$ $\forall$ a,b $\in$ G aNbN = bNaN $\iff$ $\forall$ a,b $\in$ G (ab)N=(ba)N $\iff$ $\forall$ a,b $\in$ G (ab)(ba)$^{-1}$ $\in$ N $\iff$ $\forall$ a,b $\in$ G [a,b] $\in$ N $\iff$ G' $\leq$ N. □

2.1.2 Cuore e chiusura normale

Definizione 4. *Sia G un gruppo e H $\leq$ G. Definiamo:*

- *il cuore di H in G il sottogruppo:*

  H_G=$< \bigcup \{N : N \trianglelefteq G, N \leq H\} >$

- *la chiusura normale di H in G il sottogruppo*

  H^G= $\bigcap \{N : N \trianglelefteq G, H \leq N\}$

Osservazione 3. *Si osservi che*

1. H_G *è il più grande sottogruppo normale di G contenuto in H*

2. H^G *è il più piccolo sottogruppo normale di G contenente H*

Proposizione 4. *Sia G un gruppo e $H \leq G$, allora:*

- $H_G = \bigcap_{x \in G} H^x$
- $H^G = < \bigcup_{x \in G} H^x >$

Dimostrazione. Iniziamo a dimostrare che $H_G = \bigcap_{x \in G} H^x$.Sia $h_G \in H_G$, mostriamo che $h_G \in \bigcap_{x \in G} H^x$ cioè che $\forall$ x $\in$ G $h_G \in H^x$.Sia quindi x in G fissato.Siccome H_G è normale in G si ha che $H_G = (H_G)^x$ e quindi h_G=$x^{-1}yx$ per qualche y in H_G. Siccome $H_G \leq$ H si ha $h_G \in H^x$ e quindi $H_G \leq \bigcap_{x \in G} H^x$.Viceversa siccome H_G è il più grande sottogruppo normale di G contenuto in H e sufficiente mostrare che $\bigcap_{x \in G} H^x \trianglelefteq$ G e $\bigcap_{x \in G} H^x \leq$ H.Ovviamente $H^x \leq$ H $\forall$ x $\in$ G, mostriamo che $\bigcap_{x \in G} H^x \trianglelefteq$ G.Sia g $\in$ G e h $\in \bigcap_{x \in G} H^x$. Mostriamo che g^{-1}hg $\in \bigcap_{x \in G} H^x$. Sia x in G. Allora:

$$g^{-1}\text{hg} = x^{-1}((\text{gx}^{-1})^{-1}\text{h}(\text{gx}^{-1}))\text{x}$$

siccome h $\in H^{(gx^{-1})^{-1}}$ si ha

$$\text{h} = (\text{gx}^{-1})\tilde{h}(\text{gx}^{-1})^{-1}$$

con $\tilde{h}$ in H.Allora:

$$g^{-1}\text{hg}=x^{-1}\tilde{h}\text{x} \in H^x$$

Mostriamo ora che $H^G = < \bigcup_{x \in G} H^x >$.Mostriamo la doppia inclusione.Iniziamo a far vedere che $H^G \leq < \bigcup_{x \in G} H^x >$. Per farlo è sufficiente mostrare che $< \bigcup_{x \in G} H^x >$ è normale in G e contiene H. Sia quindi g in G e h in $< \bigcup_{x \in G} H^x >$. L'elemento h avrà la forma:

$$\text{h}=h_1 \ldots h_t$$

dove: $h_i \in H^{x_i}$ per un certo x_i in G per i=1,...,t e quindi h_i=$x_i^{-1}\tilde{h}_i x_i$ per un certo $\tilde{h}_i$ in H^{x_i} per i=1,...,t, da cui

$$g^{-1}\text{hg}=(x_1 g)^{-1}\tilde{h}_1(x_1 g)\ldots(x_t g)^{-1}\tilde{h}_t(x_t g) \in < \bigcup_{x \in G} H^x >.$$

Mostriamo ora che H $\leq <\bigcup_{x\in G} H^x>$. Ma questo è banale perchè se h $\in$ H allora h $\in \bigcup_{x\in G} H^x \leq <\bigcup_{x\in G} H^x>$. Dimostriamo ora l'altra inclusione ovvero che $<\bigcup_{x\in G} H^x> \leq H^G$. Sarà sufficiente mostrare che $\bigcup_{x\in G} H^x \leq H^G$. Sia y $\in \bigcup_{x\in G} H^x$ allora esiste x in G tale che y = $x^{-1}hx$ con h $\in$ H. Siccome H $\leq H^G$ si ha che y $\in$ (H^G)^x=H^G e quindi la tesi. □

2.1.3 Centralizzante

Definizione 5. *Sia G un gruppo e X $\subset$ G. Viene detto centralizzante di X in G l'insieme:*

$$C_G(X)=\{g \in G : gx = xg \forall x \in X\}$$

Proposizione 5. *Sia G un gruppo e X $\subset$ G.Allora :*

1. *C_G(X) $\leq$ G e Z(G) $\leq C_G$(X)*
2. *Se H allora $\leq$ G H $\cap C_G$(X) = Z(H)*

Dimostrazione. Dimostriamo i due punti:

1. Osserviamo che C_G(X) è non vuoto perchè 1 vi appartiene. Se a e b sono due elementi di C_G(X) allora per ogni x in G:

   (ab)x=axb=x(ab)

   quindi ab $\in C_G$(X).Inoltre per ogni x in G ax=xa e quindi per ogni x in G x=a^{-1}xa e quindi per ogni x in G a^{-1}x=xa^{-1} e quindi C_G(X) è un sottogruppo di G. Il fatto che Z(G) è contenuto in C_G(X) è banale perchè un generico elemento di Z(G) commuta con tutti gli elementi di G e quindi in particolare con tutti gli elementi di X.

2. H $\cap C_G$(X) = $\{h \in H : hx = xh \forall x \in H\}$=Z(H)

□

2.2 Equazione delle classi,lemma di Cauchy,p-gruppi e normalizzante

2.2.1 Equazione delle classi

Sia G un gruppo.Definiamo in G la seguente relazione binaria,ponendo per ogni x,y $\in$ G:

$$x \sim y \iff \exists\, g \in G : y = g^{-1}xg.$$

Si verifica facilmente che $\sim$ è una relazione di equivalenza in G.Quindi posto $\forall\, x \in G$:

$x^G := [x]_\sim$ (detta classe di coniugio di x)

si ha che:

$$G = \bigcup_{x \in G} x^G$$

Osserviamo che $| x^G | = 1 \iff x \in Z(G)$.Conseguentemente se G è un gruppo finito non abeliano, denotate con x_1^G,.., x_t^G $t \geq 1$ le classi di coniugio di G di ordine > 1, si ha che:

$$G = Z(G) \sqcup (x_1^G \sqcup .. \sqcup x_t^G)$$

da cui:

$$| G | = | Z(G) | + | x_1^G | + .. + | x_t^G |$$

quest'ultima identità viene detta equazione delle classi.

2.2.2 Lemma di Cauchy

Prima di dimostrare il lemma di Cauchy, dimostriamo il seguente fatto:

Proposizione 6. *Sia G un gruppo finito e x ∈ G. Allora:*

$$| x^G | = [G : C_G(\{x\})]$$

Dimostrazione. Abbiamo che:

$$[G : C_G(\{x\})] = | \{C_G(\{x\})g : g \in G\} |$$

Mostriamo quindi che x^G è in biezione con $\{C_G(\{x\})g : g \in G\}$ .Definiamo l'applicazione:

$$f : \{C_G(\{x\})g : g \in G\} \longrightarrow x^G$$

$$C_G(\{x\})g \longmapsto g^{-1}xg$$

Iniziamo a vedere che f è ben definita, cioè che non dipende dal rappresentante scelto. Effettivamente se $C_G(\{x\})a = C_G(\{x\})b$ con a e b in G allora $ab^{-1} \in C_G(\{x\})$ e quindi commuta con x, cioè:

$$ab^{-1}x = xab^{-1} \rightarrow b^{-1}xb = a^{-1}xa$$

quindi f è ben definita.Vediamo ora che f è biettiva.Ovviamente è suriettiva per com'è fatto x^G ed è iniettiva perchè se a,b sono due elementi di G tali che $b^{-1}xb=a^{-1}xa$ allora $ab^{-1}x=xab^{-1}$ e quindi $ab^{-1} \in C_G(\{x\})$ da cui $C_G(\{x\})a=C_G(\{x\})b$. □

Ricordiamo che vale il seguente:

Lemma 1. *(Lemma di Cauchy nel caso abeliano) Sia G un gruppo abeliano finito e p un primo : p | | G |. Allora esiste x ∈ G : o(x) = p.*

Siamo pronti per dimostrare il seguente:

Teorema 13. *(Lemma di Cauchy) Sia G un gruppo finito e p un primo : p | |G| allora ∃ x ∈ G : o(x)=p.*

Dimostrazione. Siccome p divide l'ordine di G esiste n ∈ N con n>0 tale che | G | =pn.Dimostriamo il lemma per induzione su n.Se n=1 allora | G | =p e quindi G è ciclico cioè esiste x in G tale che G = <x> e quindi esiste x in G tale che o(x)=p.Supponiamo ora vero il lemma per ogni α naturale positivo tale che α < n. Se esiste H < G tale che p divide | H | allora | H | =pα per qualche naturale positivo α minore di n e quindi per ipotesi induttiva esiste h ∈ H tale che o(h)=p e pertanto esiste h in G di ordine p.Supponiamo per assurdo che non esista H < G tale che p divide | H |. Allora G non può essere abeliano, infatti altrimenti per il lemma di Cauchy nel caso abeliano troverei x in G di ordine p e quindi <x> sarebbe un sottogruppo di G (contenuto strettamente in esso) tale che p divide | <x> |.Quindi Z(G) < G.Allora sia a ∈ G \ Z(G). Si ha che $C_G(\{a\})$ < G (altrimenti a ∈ Z(G)).Quindi p non divide | $C_G(\{a\})$ | ma siccome p divide | G | = [G:$C_G(\{a\})$] | $C_G(\{a\})$ | troviamo che p divide [G:$C_G(\{a\})$] = | a^G |.Allora, essendo a un generico elemento di G \ Z(G) dall'equazione delle classi deduciamo che p divide |G| - |Z(G)| quindi |G| - |Z(G)| = pk per quale naturale positivo k e quindi p(n-k) = pn-pk= |G| - pk = |Z(G)| che è assurdo essendo Z(G)< G. □

2.2.3 p-gruppi

Definizione 6. *Sia G un gruppo e p un primo. G è detto p-gruppo se ∀ x ∈ G o(x)=p^k per qualche k ∈ $\mathbb{N}$*

Definizione 7. *Sia G un gruppo e p un primo. Se H ≤ G : H è un p-gruppo allora H è detto p-sottogruppo di G.*

Proposizione 7. *Sia G un gruppo finito e p un primo.Allora G è un p-gruppo* $\iff$ $|G|=p^k$ *per qualche naturale positivo k*

Dimostrazione. Supponiamo che G sia un p-gruppo..Per il teorema fondamentale dell'aritmetica:

$$|\mathrm{G}|=p_1^{\alpha_1}...p_t^{\alpha_t}$$

dove p_1,..,p_t sono primi distinti e α_1,..,α_t sono naturali positivi.Supponiamo che esista $p_i \neq$ p per qualche i $\in \{1, ..., t\}$.Per il lemma di Cauchy esiste x in G di ordine p_i.Tuttavia esiste r in $\mathbb{N}$ tale che o(x)=p^r e quindi p_i=p^r che è assurdo, quindi per ogni i $\in \{1, ..., t\}$ si ha che p_i = p consegue che |G|=$p^{\alpha_1}...p^{\alpha_t}$=$p^k$ per qualche k naturale positivo.Il viceversa è immediato perchè preso x in G si ha che o(x) divide p^k e quindi,essendo p primo, si ha che o(x)=p^r per qualche naturale r e quindi G è un p-gruppo. □

Proposizione 8. *Sia G un p-gruppo finito con p primo. Allora Z(G)* $\neq \{1\}$ *(si dice che G ha centro non banale)*

Dimostrazione. Mostriamo che |Z(G)| > 1.Sappiamo che |G|=p^n per qualche naturale positivo n.Quindi se G è abeliano |Z(G)|=|G|>1.Supponiamo che G non sia abeliano, siano quindi x_1^G,..,x_t^G le classi di coniugio di G di ordine maggiore di 1 con t$\geq$1.Dall'equazione delle classi:

$$|\mathrm{Z(G)}|=p^n\text{-}(|\ x_1^G| + ... + |\ x_t^G|)$$

Ora, $\forall$ i $\in \{1, ..., t\}$ si ha che $|\ x_i^G|$ = [G:$C_G(\{x_i\})$] quindi $|\ x_i^G|$ divide p^n $\forall$ i $\in \{1, ..., t\}$ da cui $\forall$ i $\in \{1, ..., t\}$ $\exists$ r_i naturale positivo tale che $|x_i^G| = p^{r_i}$. Allora se r = min$\{r_1, ..., r_t\}$ si ha che:

$$|\mathrm{Z(G)}|=p^r(p^{n-r} - (p^{r_1-r} + ... + p^{r_t-r})) > 1$$

da cui la tesi. □

Proposizione 9. *Sia G un gruppo. Se G / Z(G) è ciclico allora G è abeliano.*

Dimostrazione. $\exists$ z $\in$ G : G / Z(G) = <zZ(G)>.Siano x,y $\in$ G, dimostriamo che xy=yx. Abbiamo che:

$$\mathrm{xZ(G)}=z^a\mathrm{Z(G)},\ a \in \mathbb{Z}$$

$$\mathrm{yZ(G)}=z^b\mathrm{Z(G)},\ b \in \mathbb{Z}$$

consegue:

$$x=z^a\tilde{x} \text{ con } \tilde{x} \in Z(G)$$

$$y=z^b\tilde{y} \text{ con } \tilde{y} \in Z(G)$$

da cui:

$$xy=z^a\tilde{x}z^b\tilde{y}=z^b\tilde{y}z^a\tilde{x}=yx$$

□

2.2.4 Normalizzante

Definizione 8. *Sia G un gruppo e X ⊆ G. Viene detto normalizzante di X in G l'insieme:*

$$N_G(X)=\{g \in G : X = X^g\}$$

Osservazione 4. *Si osservi che se G è un gruppo e H ≤ G allora:*

$$N_G(H)=\left\{g \in G : H = H^{g^{-1}}\right\}.$$

Proposizione 10. *Sia G un gruppo e H ≤ G. Allora:*

1. $N_G(H) \leq G$ *e* $[G: N_G(H)]=|\{H^g : g \in G\}|$
2. $H \trianglelefteq N_G(H)$
3. *Se* $K \leq G : H \trianglelefteq K$ *allora* $K \leq N_G(H)$

Dimostrazione. Dimostriamo i 3 punti

1. Osserviamo che $N_G(H)$ è non vuoto in quanto $1 \in N_G(H)$. Siano ora a e b in $N_G(H)$ mostriamo che $ab \in N_G(H)$ cioè che $H = H^{ab}$.Per dimostrarlo facciamo vedere la doppia inclusione. Sia h in H allora, essendo $H = H^b$

   $$h=b^{-1}\tilde{h}b$$

   con $\tilde{h} \in H$. Tuttavia $H = H^a$ quindi:

   $$\tilde{h}=a^{-1}\tilde{\tilde{h}}a$$

   con $\tilde{\tilde{h}}$ in H.Allora vediamo che:

h=$(ab)^{-1}$(abh$b^{-1}a^{-1}$)(ab)=$(ab)^{-1}$(a$\tilde{h}a^{-1}$)(ab)=$(ab)^{-1}\tilde{\tilde{h}}(ab)$

e quindi h $\in H^{ab}$.Viceversa se x $\in H^{ab}$ allora

x=$(ab)^{-1}$h(ab)

con h in H , cioè:

x=$b^{-1}(a^{-1}ha)b$

ma $a^{-1}ha \in H^a$ = H quindi $a^{-1}ha$=$\tilde{h}$ con $\tilde{h}$ in H e quindi:

x=$b^{-1}\tilde{h}b \in H^b$ = H

consegue che ab $\in N_G(H)$. Mostriamo ora che $a^{-1} \in N_G(H)$ cioè che H=$H^{a^{-1}}$.Sia h $\in$ H allora:

h=a(a^{-1}ha)a^{-1}

ma a^{-1}ha $\in H^a$ = H quindi h $\in H^{a^{-1}}$. Viceversa se x $\in H^{a^{-1}}$ allora:

x=aha^{-1}

con h $\in$ H. Ma H=H^a quindi h=$a^{-1}\tilde{h}$a con $\tilde{h}$ in H consegue x=$\tilde{h}$ e pertanto x $\in$ H.Quindi $N_G(H) \leq$ G. Ora:

[G:$N_G(H)$]=| $\{N_G(H)g : g \in G\}$ |

Mostriamo quindi che $\{N_G(H)g : g \in G\}$ è in biezione con $\{H^g : g \in G\}$.Definiamo l'applicazione:

$$f : \{N_G(H)g : g \in G\} \longrightarrow \{H^g : g \in G\}$$

$$N_G(H)g \longmapsto H^g$$

mostriamo che f è bigettiva.Iniziamo a far vedere che f è ben definita.Siano a e b in G tali che $N_G(H)a$=$N_G(H)b$, dimostriamo che H^a=H^b.Se x $\in H^a$ allora:

$$x=b^{-1}((ab^{-1})^{-1})h(ab^{-1})b$$

per un certo h in H. Ma $(ab^{-1})^{-1}h(ab^{-1}) \in H^{ab^{-1}}$ = H quindi x $\in H^b$.Similmente se x $\in H^b$ allora x $\in H^a$. Quindi f è ben definita. Mostriamo ora che è bigettiva. Ovviamente f è suriettiva, per mostrare che è iniettiva si prendano a e b in G tali che $H^a = H^b$, mostriamo che $H^{ab^{-1}}$=H. Se h $\in$ H si ha che:

$$h=(ab^{-1})^{-1}(ab^{-1}hba^{-1})(ab^{-1})$$

siccome $b^{-1}hb \in H^b$=H^a si ha che $b^{-1}hb = a^{-1}\tilde{h}a$ con $\tilde{h} \in$ H e quindi:

$$h = (ab^{-1})^{-1}\tilde{h}(ab^{-1}) \in H^{ab^{-1}}.$$

Similmente se x $\in H^{ab^{-1}}$ allora:

$$x=b(a^{-1}ha)b^{-1} \in H$$

e quindi il primo punto è dimostrato.

2. Osserviamo che se h $\in$ H allora H = H^h e quindi H $\leq N_G(H)$.Inoltre preso g $\in N_G(H)$ e h $\in$ H si ha che $g^{-1}hg \in H^g$=H e quindi H $\trianglelefteq N_G(H)$.

3. Sia k $\in$ K, mostriamo che H = H^k. Se h $\in$ H allora essendo H normale in K

$$h=k^{-1}(khk^{-1})k \in H^k$$

Viceversa se y $\in H^k$ troviamo che y=k^{-1}hk con h $\in$ H e quindi, per la normalita di H in K, si ha che y $\in$ H.

□

2.3 La semplicità di An

In questa sezione dimostreremo che $\forall$ n $\geq$ 5 il gruppo alterno A_5 è semplice e non abeliano.

2.3.1 Alcune proposizioni preliminari

Teorema 14. *Sia $\sigma \in A_n$ con n $\geq$ 3 allora σ è prodotto di 3-cicli.*

Dimostrazione. Se σ = Id allora σ = (123)(123)(123).Supponiamo quindi $\sigma \neq$ Id. Siccome σ ha segno 1 è il prodotto di un numero pari di trasposizioni.Se mostriamo dunque che ogni coppia di trasposizioni è un triciclo o il prodotto di tricicli avremmo concluso.Siano (ab) e (cd) due trasposizioni.Abbiamo tre possibilità:

1. $|\{a,b\} \cap \{c,d\}|$ = 0

   allora (ab) e (cd) sono trasposizioni disgiunte e dunque:

   (ab)(cd)=(ab)(bc)(bc)(cd)=(abc)(bcd)

2. $|\{a,b\} \cap \{c,d\}|$ = 1

   allora (ab)(cd) è un triciclo

3. $|\{a,b\} \cap \{c,d\}|$ = 2

   allora (ab)(cd)=Id=(123)(123)(123)

□

Proposizione 11. *Siano $(a_1...a_d)$, $\sigma \in S_n$.Allora:*

$$\sigma(a_1...a_d)\sigma^{-1}=(\sigma(a_1)...\sigma(a_d))$$

Dimostrazione. Sia f = $(a_1...a_d)$, dimostriamo che $\sigma f\sigma^{-1}=(\sigma(a_1)...\sigma(a_d))$.Abbiamo che $\forall$ i =1,...,d-1:

$$\sigma f\sigma^{-1}(\sigma(a_i))=\sigma(a_{i+1})=(\sigma(a_1)...\sigma(a_d))(\sigma(a_i)$$

inoltre:

$$\sigma f\sigma^{-1}(\sigma(a_d))=\sigma(a_1)=(\sigma(a_1)...\sigma(a_d))(\sigma(a_d))$$

infine se x $\in \{1,...,n\} \setminus \{\sigma(a_1),...,\sigma(a_d)\}$ si ha che:

$$\sigma f\sigma^{-1}(x)=x=(\sigma(a_1)...\sigma(a_d))(x)$$

□

Proposizione 12. *Siano* $(a_1...a_d),(b_1...b_d) \in S_n$*.Allora* $\exists\ \gamma \in S_n$ *:* $(b_1...b_d)=\gamma^{-1}(a_1...a_d)\gamma$

Dimostrazione. Osserviamo che $\forall\ \gamma \in S_n\ \gamma(a_1...a_d)\gamma^{-1}=(\gamma(a_1)...\gamma(a_d))$ quindi definiamo:

$$\gamma : \{1, ..., n\} \longrightarrow \{1, ..., n\}$$

$$\mathrm{x} \longmapsto \gamma(\mathrm{x})$$

dove γ(x)=b_i se x=a_i e γ(x)=x altrimenti.Si vede subito che $\gamma \in S_n$ ed inoltre:

$$\gamma(a_1...a_d)\gamma^{-1} =(\gamma(a_1)...\gamma(a_d))= (b_1...b_d)$$

quindi $\beta=\gamma^{-1} \in S_n$ è tale che

$$\beta^{-1}(a_1...a_d)\beta=(b_1...b_d)$$

segue la tesi. □

Proposizione 13. *Siano* σ,ρ *tricili di* A_n *con* $n \geq 5$*. Allora* $\exists\ \alpha \in A_n$ *:* $\alpha^{-1}\sigma\alpha=\rho$*.*

Dimostrazione. Per la proposizione anteriore esiste $\alpha \in S_n$: $\alpha^{-1}\sigma\alpha=\rho$. Ora se $\alpha \in A_n$ avremmo finito.Supponiamo che α non sia un elemento di A_n. σ avrà la forma:σ=(abc). Siano d,e $\in \{1, ..., n\} \setminus \{a, b, c\}$ distinti allora β=(de)$\sigma \in A_n$ e si ha che:

$$\beta^{-1}\sigma\beta=\alpha^{-1}\sigma\alpha=\rho.$$

e quindi la tesi. □

2.3.2 Sottogruppi normali di S_n con n $\geq$ 5

Teorema 15. *Sia* $N \triangleleft S_n$ *,* $n \geq 5$*, allora* $N = \{Id\} \vee N = A_n$*.*

Dimostrazione. Abbiamo due possibilità: N $\cap$ A_n = $\{Id\}$ oppure N $\cap$ $A_n \neq \{Id\}$. Analizziamo i due casi separatamente:

- N $\cap$ A_n = $\{Id\}$

  Dimostriamo che N = $\{Id\}$. Per farlo dimostreremo che |N| = 1.Poichè A_n e N sono sottogruppi di S_n si ha che:

$$|NA_n|=\frac{|\ N\ ||\ A_n\ |}{N \cap A_n} = |\ \mathrm{N}\ ||\ A_n\ |$$

quindi:

$$|\mathrm{N}| = \frac{|\ NA_n\ |}{|\ A_n\ |}$$

tuttavia $A_n \triangleleft \mathrm{N}A_n$ e quindi:

$$|\ \mathrm{N}A_n\ | = |\ \frac{NA_n}{A_n}\ |\ |\ A_n\ |$$

da cui:

$$|\ \mathrm{N}\ | = |\ \frac{NA_n}{A_n}\ |$$

Ora $\frac{NA_n}{A_n} \leq \frac{S_n}{A_n}$ quindi:

$$|\ \frac{NA_n}{A_n}\ | \leq |\ \frac{S_n}{A_n}\ | = 2$$

da cui:

$$|\ \mathrm{N}\ | \leq 2.$$

Se per assurdo | N | = 2 scriviamo N = $\{Id, a\}$ con a $\in S_n$: a $\neq$ Id.Sia b $\in S_n$ allora essendo N normale in S_n troviamo che b^{-1}ab $\in$ N e quindi b^{-1}ab=a oppure b^{-1}ab=Id ma se per assurdo b^{-1}ab=Id allora a=Id, assurdo, quindi b^{-1}ab=a e quindi ab=ba cioè N $\leq$ Z(S_n).Tuttavia Z(S_n)=$\{Id\}$ quindi abbiamo trovato un assurdo. Pertanto N=$\{Id\}$.

- N $\cap$ $A_n \neq \{Id\}$

  Dimostriamo che N = A_n. Osserviamo che se $A_n \leq \mathrm{N} \cap A_n$ allora $A_n \leq$ N quindi | A_n | divide | N | da cui | N | =k$\frac{n!}{2}$ con k naturale positivo e quindi essendo N contenuto strettamente in S_n si deduce che N=A_n Mostriamo allora che $A_n \leq \mathrm{N} \cap A_n$.Sia $\rho \in A_n$. Siccome n $\geq$ 5 > 3 si ha che ρ è prodotto di tricicli:

  $$\rho = \beta_1 ... \beta_t$$

  dove β_i è un triciclo per ogni i=1,...,t con t naturale positivo.Ora prendiamo un attimo per buono che N $\cap$ A_n contenga un triciclo (lo dimostriamo alla fine) e chiamiamolo γ. Siccome n $\geq$ 5 $\forall$ i=1,...,t $\exists$ $\alpha_i \in A_n$: β_i=$\alpha_i^{-1}\gamma\alpha_i$ e quindi:

$$\rho=\alpha_1^{-1}\gamma\alpha_1...\alpha_t^{-1}\gamma\alpha_t$$

ma N $\cap$ $A_n \trianglelefteq A_n$ quindi $\forall$ i=1,..,t $\alpha_i^{-1}\gamma\alpha_i \in$ N $\cap$ A_n segue che $\rho \in$ N $\cap$ A_n e quindi la tesi. Manca da dimostrare che N $\cap$ A_n contiene un triciclo. Poichè N $\cap$ $A_n \neq \{Id\}$ possiamo prendere σ in N $\cap$ A_n diverso da Id.Quindi esiste b $\in \{1, ..., n\}$ tale che σ(b):=c$\neq$b.Sia ora a $\in \{1, ..., n\}$ tale che a è diverso da b e c. Allora [σ,(ac)](a)=(σ(ac)σ^{-1}(ac))(a)=c quindi esiste una trasposizione τ tale che [σ,τ] $\neq$Id.Osserviamo che [σ,τ] $\in$ N $\cap$ A_n essendo N $\cap$ A_n normale in S_n.Inoltre [σ,τ] = $\sigma\tau\sigma^{-1}\tau^{-1}$ quindi [σ,τ] è il prodotto di due trasposizioni e dunque, non potendo essere l'identità, o è un triciclo oppure è il prodotto di due trasposizioni disgiunte.Ora se [σ,τ] è un triciclo abbiamo finito. Supponiamo allora che [σ,τ]=(ab)(cd) con ab,c e d tutti distinti, mostriamo che comunque N $\cap$ A_n contiene un triciclo.Sia e $\in \{1, ..., n\} \setminus \{a, b, c, d\}$.Si ha che:

$$(eba)^{-1}\text{(ab)(cd)(eba)} \in \text{N} \cap A_n$$

ma:

$$(eba)^{-1}\text{(ab)(cd)(eba)=(be)(cd)}$$

quindi (be)(cd) $\in$ N $\cap$ A_n.Consegue:

$$\text{(be)(cd)(ab)(cd)} \in \text{N} \cap A_n$$

ma:

$$\text{(be)(cd)(ab)(cd) =(eba)}$$

e quindi l'asserto.

□

2.3.3 A_n è semplice e non abeliano $\forall$ n $\geq$ 5

Il teorema che segue è, a mio avviso, un vero e proprio gioiellino:

Teorema 16. *A_n è semplice e non abeliano $\forall$ n $\geq$ 5.*

Dimostrazione. Sia n $\geq$ 5. Iniziamo a dimostrare che A_n è semplice.Sia N $\trianglelefteq$ A_n : N $\neq$ $\{Id\}$,mostriamo che N = A_n.Siccome N $\trianglelefteq$ A_n allora $A_n \leq N_{S_n}(N)$ quindi A_n=$N_{S_n}(N)$ $\vee$ S_n=$N_{S_n}(N)$.Se S_n=$N_{S_n}(N)$ allora siccome N $\triangleleft$ $N_{S_n}(N)$ risulta che N $\triangleleft$ S_n (strettamente perchè N è contenuto in A_n) e quindi, essendo N $\neq$ $\{Id\}$ si ha che N=A_n.Mostriamo che questo è proprio il caso che si verifica cioè che non può accadere che A_n=$N_{S_n}(N)$.Supponiamo per assurdo che A_n=$N_{S_n}(N)$ allora:

$$\mid \{N^\rho : \rho \in S_n\} \mid = [S_n,N_{S_n}(N)]=[S_n,A_n]=2$$

quindi se $\tau \in S_n$ è una trasposizione, essendo $\tau \notin A_n$. si avrebbe $\tau \notin N_{S_n}(N)$ e cioè N $\neq$ N^τ e quindi:

$$N_{S_n} = \mathrm{N} \cap N^\tau \text{ e } N^{S_n}=<\mathrm{N} \cup N^\tau>=\mathrm{N}N^\tau$$

Osserviamo che N,N^τ sono sottogruppi normali di A_n.Infatti N è normale per ipotesi, per vedere che N^τ è normale in A_n consideriamo un tipico elemento in N^τ, τnτ , con n $\in$ N e sia poi $\alpha \in A_n$ allora:

$$\alpha^{-1}(\tau \mathrm{n} \tau)\alpha=\tau((\tau\alpha\tau)^{-1}\mathrm{n}(\tau\alpha\tau))\tau$$

siccome N è normale in A_n allora $(\tau\alpha\tau)^{-1}$n$(\tau\alpha\tau)$ $\in$ N e quindi $\alpha^{-1}(\tau \mathrm{n} \tau)\alpha \in N^\tau$.Mostriamo ora che N $\cap$ N^τ = $\{Id\}$ e NN^τ=A_n.Di fatto N $\cap$ N^τ = N_{S_n} $\triangleleft$ S_n, quindi N $\cap$ N^τ = $\{Id\}$ oppure N $\cap$ N^τ = A_n.Tuttavia N $\cap$ N^τ è contenuto strettamente in N dato che altrimenti N=N^τ, ma N è contenuto in A_n quindi non può che essere N $\cap$ N^τ = $\{Id\}$.Similmente NN^τ = N^{S_n} $\triangleleft$ S_n quindi NN^τ = $\{Id\}$ oppure NN^τ = A_n. Tuttavia N $\leq$ NN^τ e N $\neq$ $\{Id\}$ quindi non può che essere NN^τ=A_n.Pertanto per il teorema prodotto si ha che:

$$A_n \simeq \mathrm{N} \times N^\tau$$

Quindi $\mid A_n \mid$ = $\mid$ N $\mid^2$ ma essendo n $\geq$ 5 , 2 divide $\mid A_n \mid$ e quindi, essendo 2 primo, 2 divide $\mid$ N $\mid$. Allora per il lemma di Cauchy esiste x $\in$ N : o(x)=2.Per il teorema fondamentale delle permutazioni:

$$\mathrm{x}=\rho_1 \circ ... \circ \rho_t$$

dove i ρ_i sono cicli disgiunti.Allora:

$$2=\mathrm{m.c.m}(\mathrm{o}(\rho_1),...,\mathrm{o}(\rho_t))$$

e quindi $\forall$ i=1,...,t 2=o(ρ_i)k_i per qualche k_i nei naturali positivi.Siccome $\rho_i \neq$ Id $\forall$ i=1,...,t si ha che o(ρ_i) = 2 $\forall$ i=1,...,t.Allora x è prodotto di trasposizioni disgiunte, da cui:

$$x=\rho_1 \circ ... \circ \rho_t=\rho_1 \circ \rho_1 \circ ... \circ \rho_t \circ \rho_1 = \rho_1 \; x \; \rho_1$$

quindi x ∈ N cap N^{ρ_1} = $\{Id\}$ e quindi x = Id, assurdo. Quindi A_n è semplice. Per mostrare che non è abeliano basta osservare che (123) e (214) sono elementi di A_n tali che (123)(214)=(143)≠(234)=(214)(123) □

Corollario 1. *Sia p un primo ≥ 5. L'equazione n! = 2p^2 non ha soluzioni in* $\mathbb{N}$

Dimostrazione. Se esistesse un n ∈ $\mathbb{N}$ soddisfacente l'equazione allora n sarebbe tale che $\frac{n!}{2}$ = p^2 (si osservi che n ≥ 5) Allora il gruppo A_n avrebbe ordine p^2 e quindi sarebbe abeliano.Infatti sarebbe un p-gruppo e allora il suo centro sarebbe non banale quindi o avrebbe ordine p e in tal caso $\frac{A_n}{Z(A_n)}$ ha ordine p e quindi è ciclico e quindi A_n è abeliano oppure avrebbe ordine p^2 e in tal caso A_n=Z(A_n). Quindi A_n sarebbe abeliano con n>5, assurdo. □

2.4 Azioni di gruppo e teoremi di Sylow

2.4.1 Cenni alle azioni di gruppo

Definizione 9. *Sia G un gruppo e Ω un insieme non vuoto.Se esiste un omomorfismo di gruppi f : G ⟶ S_Ω diciamo che G agisce su Ω tramite f ed f è detta l'azione di G su Ω*

Esempio 1. *Sia G un gruppo.Allora:*

$$\Psi_1 : G \longrightarrow S_G$$

$$g \longmapsto \Psi_1(g)$$

dove $\Psi_1(g)(x)=x \; \forall \; x \in G$ *è un azione*

Esempio 2. *Sia G un gruppo.Allora:*

$$\Psi_2 : G \longrightarrow S_G$$

$$g \longmapsto \Psi_2(g)$$

dove $\Psi_2(g)(x)=gxg^{-1} \; \forall \; x \in G$ *è un azione*

Esempio 3. *Sia G un gruppo e H ≤ G. Allora detti:*

$$\Omega = \{xH : x \in G\}$$

$$\tilde{\Omega}=\{Hx : x \in G\}$$

le applicazioni:

$$\beta_1 : G \longrightarrow S_\Omega$$

$$g \longmapsto \beta_1(g)$$

$$\beta_2 : G \longrightarrow S_{\tilde{\Omega}}$$

$$g \longmapsto \beta_2(g)$$

dove $\beta_1(g)(xH)=gxH \; \forall \; xH \in \Omega$ *e* $\beta_2(g)(Hx)=Hxg^{-1} \; \forall \; Hx \in \tilde{\Omega}$ *sono azioni.*

Esempio 4. *Sia G un gruppo e* Ω *un insieme non vuoto.Supponiamo che G agisca su* Ω *tramite* $f : G \longrightarrow S_\Omega$*, allora G agisce su P(*Ω*) tramite:*

$$\Psi : G \longrightarrow S_{P(\Omega)}$$

$$g \longmapsto \Psi(g)$$

dove $\Psi(g)(X)=\{f(g)(x) : x \in X\} \; \forall \; X \in P(\Omega)$*. Tale azione può essere ristretta ai sottoinsiemi di* Ω *di ordine n,* $n \in N^+$ *, cioè , posto:*

$$[\Omega]^n = \{X \in P(\Omega) :| \; X \; |= n\}$$

l'applicazione:

$$\Phi : G \longrightarrow S_{[\Omega]^n}$$

$$g \longmapsto \Phi(g)$$

dove $\Phi(g)(X)=\{f(g)(x) : x \in X\} \; \forall \; X \in [\Omega]^n$ *è un azione*

Definizione 10. *Sia G un gruppo e* Ω *un insieme non vuoto e sia* $f : G \longrightarrow S_\Omega$ *un omomorfismo di gruppi. Allora* $\forall \; x \in \Omega$ *definiamo:*

- $\Theta_x := \{f(g)(x) : g \in G\}$ *l'orbita di x*
- $G_x = \{g \in G : f(g)(x) = x\}$ *lo stabilizzatore di x*

inoltre definiamo i punti fissi di Ω *come :*

- $\Omega_G = \{x \in \Omega : f(g)(x) = x \forall g \in G\}$

Sia ora G un gruppo e Ω un insieme non vuoto e sia f : G $\longrightarrow S_\Omega$ un omomorfismo di gruppi.Osserviamo che le orbite indotte dall'azione f possono essere viste come classi di equivalenza.Infatti definiamo su Ω la seguente relazione binaria, ponendo $\forall$ x,y $\in \Omega$:

$$x \sim y \iff \exists\, g \in G : f(g)(x)=y$$

è immediato verificare che $\sim$ è una relazione di equivalenza su Ω.Inoltre, osserviamo che, fissato x $\in \Omega$:

$$[x]_\sim = \{f(g)(x) : g \in G\} = \Theta_x$$

e quindi:

$$\Omega = \sqcup_{x\in\Omega}\Theta_x$$

Osserviamo inoltre che:

$$| \Theta_x | = 1 \iff x \in \Omega_G$$

infatti se $| \Theta_x |$ = 1 allora $\Theta_x = \{x\}$ e quindi $\forall$ g $\in$ G : f(g)(x)=x cioe x $\in \Omega_G$, viceversa se x $\in \Omega_G$ allora $\forall$ g $\in$ G : f(g)(x)=x e quindi $\Theta_x = \{x\}$ cioè $| \Theta_x |$ = 1. Mettiamo ora in relazione orbite e stabilizzatori:

Proposizione 14. *Sia G un gruppo che agisce su insieme non vuoto* Ω *tramite f :* $G \longrightarrow S_\Omega$*.Allora:*

- $G_x \leq G \,\forall\, x \in \Omega$.
- $| \Theta_x |$ = $[G:G_x] \,\forall\, x \in \Omega$.

Dimostrazione. Dimostriamo i due punti.Sia x $\in \Omega$.

- Osserviamo che G_x è non vuoto in quanto 1 vi appartiene (poichè f(1)(x)=Id(x)=x).Siano ora a e b in G_x.Allora

$$f(ab)(x)=f(a)(f(b)(x))=f(a)(x)=x$$

quindi ab $\in G_x$. Inoltre essendo f(a)(x)=x si ha che x = f(a^{-1})(x) e quindi G_x è un sottogruppo di G.

- Osserviamo che [G:G_x]=| $\{gG_x : g \in G\}$ | . Mostriamo quindi che $\{gG_x : g \in G\}$ è in biezione con Θ_x.Definiamo l'applicazione:

$$\Phi : \{gG_x : g \in G\} \longrightarrow \Theta_x$$

$$gG_x \longmapsto \text{f(g)(x)}$$

mostriamo che Φ è bigettiva.Iniziamo a vedere che Φ è ben definita.Se a e b sono due elementi di G tali che aG_x=bG_x allora f($a^{-1}b$)(x)=x e sfruttando il fatto che f è un omomorfismo si ottiene che f(a)(x)=f(b)(x).Quindi Φ è ben definita.Ora Φ è banalmente suriettiva ed è iniettiva perchè se f(a)(x)=f(b)(x) allora f($a^{-1}b$)(x)=x e quindi $a^{-1}b \in G_x$ da cui aG_x=bG_x.Segue l'asserto.

□

2.4.2 I teoremi di Sylow

Definizione 11. *Sia G un gruppo :* | G | = $p^a m$ *con p un primo , a* $\in \mathbb{N}$, *m* $\in \mathbb{N}^+$ *, (p,m)=1. H* $\leq$ *G :* | H | = p^a *è detto p - sottogruppo di Sylow di G (o semplicemente p-sylow di G). L'insieme dei p-sylow di G è denotato con Sylp(G)*

Teorema 17. *(Primo teorema di Sylow) Sia G un gruppo :* | G | = $p^a m$ *con p un primo , a* $\in$ $\mathbb{N}$, *m* $\in \mathbb{N}^+$ *, (p,m)=1. Allora* $\exists$ *H* $\leq$ *G :* | H | = p^a.

Dimostrazione. Consideriamo l'insieme:

$$\Omega = \{X \subseteq G :| X |= p^a\}$$

L'applicazione:

$$\text{f : G} \longrightarrow S_\Omega$$

$$\text{X} \longmapsto \{gx : x \in X\}$$

è un azione di G su Ω. Denotiamo con $\triangle_1$,...,$\triangle_t$ le orbite indotte dall'azione, allora:

$$| \Omega | = | \triangle_1 | + ... + | \triangle_t |$$

ora siccome:

$$| \Omega | = \binom{p^a}{p^a m}$$

si verifica (lo facciamo alla fine della dimostrazione) che p non divide $| \Omega |$ e quindi esiste i $\in \{1, ..., t\}$ tale che p non divide $| \triangle_i |$ allora p^a non divide $| \triangle_i |$. Adesso $\triangle_i$ avrà la forma:

$$\triangle_i = \Theta_X$$

per qualche X $\in \Omega$. Quindi siccome p^a divide | G | = [G:G_X]$| G_X |$ = $| \Theta_X | | G_X |$ si ottiene che p^a divide $| G_X |$ quindi $| G_X |$ = p^ak per qualche naturale positivo k.Se mostriamo che k=1 abbiamo finito.Sia x $\in$ X, consideriamo G_Xx.Abbiamo che G_Xx $\subseteq$ X infatti se y $\in G_X$x allora y=gx con g $\in G_X$. Ma se g $\in G_X$ si ha f(g)(X)=X e allora $\{gx : x \in X\}$ = X da cui y=gx $\in$ X.Allora:

$$| G_X | = | G_X \text{x} | \leq | \text{X} | = p^a$$

consegue che k = 1. Per concludere rimane da dimostrare che p non divide $\binom{p^a}{p^a m}$. Supponiamo per assurdo che p divida $\binom{p^a}{p^a m}$ allora:

$$\text{p} \mid \frac{(p^a m)!}{(p^a)!(p^a m - p^a)!}$$

cioè:

$$\text{p} \mid \text{m} \cdot \frac{(p^a m - 1)...(p^a m - i)...(p^a m - p^a + 1)}{(p^a - 1)...(p^a - i)...(p^a - p^a + 1)}$$

ma (p,m)=1, quindi:

$$\text{p} \mid \frac{(p^a m - 1)...(p^a m - i)...(p^a m - (p^a - 1))}{(p^a - 1)...(p^a - i)...(p^a - (p^a - 1))}$$

ora $\forall$ s $\in \mathbb{N}^+$ se i $\in \{1, ..., p^a - 1\}$ si ha che:

$$p^s \mid p^a m\text{-i} \iff p^s \mid p^a\text{-i}$$

infatti se s $\in \mathbb{N}^+$: $p^s \mid p^a m$-i allora esiste un naturale positivo k tale che i = p^am-p^sk da cui p^a - i = p^s(k-$p^{a-s}(1 - m)$) e siccome a $\geq$ s deduciamo che $p^s \mid p^a$-i.Similmente se s $\in \mathbb{N}^+$: $p^s \mid p^a$-i allora esiste un naturale positivo k tale che i = p^a-p^sk da cui: p^am - i = p^s(k+p^{a-s}(m-1)) e siccome a $\geq$ s deduciamo che $p^s \mid p^a$m - i. Allora $\forall$ i =1,...,p^a-1 denotiamo con p^{s_i} la massima potenza di p che divide p^am -i e p^a - i cioè :

$$p^a\text{m -i} = p^{s_i} k_i \text{ , } k_i \in \mathbb{N}^+ \text{ e (p,}k_i\text{)=1}$$

$$p^a \text{ -i} = p^{s_i} q_i \text{ , } q_i \in \mathbb{N}^+ \text{ e (p,}q_i\text{)=1}$$

allora:

$$\mathrm{p} \mid \frac{k_1 \ldots k_{p^a-1}}{q_1 \ldots q_{p^a-1}}$$

e quindi:

$$\mathrm{p} \mid k_1 \ldots k_{p^a-1}$$

ma allora essendo p primo divide un k_i e questo è assurdo. □

Lemma 2. *Sia G un p-gruppo finito che agisce su insieme finito e non vuoto* Ω *tramite f : G* $\longrightarrow S_\Omega$*.Allora:*

$$\mid \Omega \mid \equiv_p \mid \Omega_G \mid$$

Dimostrazione. Se $\mid \Omega \mid = \mid \Omega_G \mid$ allora il teorema è banalmente vero. Supponiamo quindi che $\mid \Omega \mid > \mid \Omega_G \mid$ e denotiamo con $\triangle_1$,...,$\triangle_t$ le orbite di ordine maggiore di 1 indotte dall'azione f, allora essendo:

$$\Omega = \Omega_G \sqcup (\triangle_1 \sqcup \ldots \sqcup \triangle_t)$$

si ha che:

$$\mid \Omega \mid - \mid \Omega_G \mid = \mid \triangle_1 \mid + \ldots + \mid \triangle_t \mid$$

Sia ora $i \in \{1, \ldots, t\}$. Supponiamo che $\triangle_i = \Theta_x$ con $x \in \Omega$ allora:

$$\mid \triangle_i \mid = \mid \Theta_x \mid = [G:G_x]$$

quindi $\mid \triangle_i \mid$ divide p^n per qualche naturale $n \in \mathbb{N}^+$ da cui $\mid \triangle_i \mid = p^{r_i}$ per qualche $r_i \in \mathbb{N}^+$ deduciamo che p divide $\mid \Omega \mid - \mid \Omega_G \mid$ e quindi si ha la tesi. □

Lemma 3. *Sia G un gruppo :* $\mid G \mid = p^a m$ *con p un primo , a* $\in \mathbb{N}$*, m* $\in \mathbb{N}^+$ *, (p,m)=1. Siano S* $\leq G : \mid S \mid = p^a$ *e P* $\leq G$ *un p-sottogruppo di G. Allora* $\exists\ x \in G : P \leq S^x$

Dimostrazione. Sia $\Omega = \{Sx : x \in G\}$. Definiamo l'applicazione:

$$\mathrm{f} : \mathrm{P} \longrightarrow S_\Omega$$

$$\mathrm{g} \longmapsto \mathrm{f(g)}$$

dove f(g)(Sx)=Sxg^{-1} $\forall$ Sx $\in \Omega$. □

f è un'azione di P su Ω. Osserviamo che $\mid \Omega_P \mid \neq 0$. Infatti se $\mid \Omega_P \mid = 0$ siccome P è un p-gruppo finito:

$$| \Omega | \equiv_p | \Omega_P | = 0$$

quindi p divide | Ω | = [G:S] e cioè esiste un naturale positivo k, tale che: [G:S]=pk quindi:

$$p^a \text{m} = | \text{G} | = \text{pk}p^a$$

e quindi

$$\text{m} = \text{pk da cui (m,p)} \neq 1.$$

assurdo. Quindi esiste Sx ∈ Ω tale che ∀ g ∈ P Sx=Sxg^{-1}. Sia allora g ∈ P, allora:

$$\text{x}g^{-1}=\text{sx, s} \in \text{S}$$

da cui:

$$\text{g} \in S^x$$

allora P $\leq S^x$

Teorema 18. *(Secondo teorema di Sylow) Sia G un gruppo :* | *G* | = $p^a m$ *con p un primo , a* ∈ ℕ, *m* ∈ $\mathbb{N}^+$ *, (p,m)=1. Siano S,P* ∈ *Sylp(G). Allora* ∃ *x* ∈ *G : P = S^x (si dice tutti i p-sylow di G sono coniugati). Conseguentemente* | *Sylp(G)* | = [G:$N_G(S)$] *e* | *Sylp(G)* | *divide [G:S]*

Dimostrazione. Poichè P è un p-sottogruppo di G esiste x in G tale che P $\leq S^x$. Ma | P | = | S | = | S^x | quindi P = S^x. Allora deduciamo che:

$$\text{Sylp(G)}=\{S^x : x \in G\}$$

consegue:

$$| \text{Sylp(G)} | = [\text{G}:N_G(S)]$$

Inoltre applicando 3 volte il teorema di Lagrange si ha che:

$$| \text{G} | = [\text{G}:N_G(S)]| N_G(S)$$

$$| N_G(S) | = [N_G(S):\text{S}] | \text{S} |$$

$$| \text{G} | = [\text{G:S}] | \text{S} |$$

da cui deduciamo che

$$[\text{G:S}]=| \text{Sylp(G)} | [N_G(S):\text{S}]$$

e quindi la tesi. □

Teorema 19. *(Terzo teorema di Sylow) Sia G un gruppo :* $|\ G\ | = p^a m$ *con p un primo ,* $a \in \mathbb{N}$, $m \in \mathbb{N}^+$ *, (p,m)=1. Allora:*

$$|\ Sylp(G)\ | \equiv_p 1$$

Dimostrazione. Sia S ∈ Sylp(G).Per il secondo teorema di Sylow [G:S]=| Sylp(G) | $[N_G(S)$:S] . Definiamo l'insieme:

$$\Omega = \{xS : x \in G\}$$

allora:

$$|\ \Omega\ | = [G:S]$$

e dunque:

$$|\ \Omega\ | = |\ Sylp(G)\ |\ [N_G(S):S]$$

Definiamo l'applicazione:

$$f : S \longrightarrow S_\Omega$$

$$g \longmapsto f(g)$$

dove f(g)(xS)=gxS ∀ xS ∈ Ω. f è un'azione di S su Ω e si ha che $|\ \Omega_S\ |$ = $[N_G(S)$:S] . Per mostrare questo fatto, essendo :

$$[N_G(S):S] =|\ \{xS : x \in N_G(S)\}\ |$$

è sufficiente dimostrare che:

$$\Omega_S = \{xS : x \in N_G(S)\}$$

Sia xS ∈ Ω_S, mostriamo che x ∈ $N_G(S)$ e cioè che S=S^x.Poichè xS ∈ Ω_S si ha che ∀ g ∈ S xS=gxS. Sia quindi g ∈ S allora gx=xs per qualche s ∈ S da cui g ∈ $S^{x^{-1}}$ e quindi S ≤ $S^{x^{-1}}$ e quindi S = $S^{x^{-1}}$.Allora sia g ∈ S. Abbiamo g = x^{-1}(xgx^{-1})x ∈ S^x consegue che S = S^x.Viceversa consideriamo un elemento della forma xS con x ∈ $N_G(S)$ e sia g ∈ S, vogliamo mostrare che xS=gxS. Di fatto:

$$S=S^x \rightarrow xS=Sx \rightarrow gxS=gSx=Sx=xS$$

e quindi $|\ \Omega_S\ |$ = $[N_G(S)$:S].Allora:

$$| \Omega | = | \text{Sylp(G)} | | \Omega_S |$$

tuttavia S è un p-gruppo e quindi:

$$| \Omega | \equiv_p | \Omega_S |$$

allora:

$$| \text{Sylp(G)} | | \Omega_S | \equiv_p | \Omega_S |$$

ma p non divide Ω_S (altrimenti p divide m e questo è assurdo essendo (p,m)=1).Quindi:

$$| \text{Sylp(G)} | \equiv_p 1$$

□

Osservazione 5. *Sia G un gruppo :* $| G | = p^a m$ *con p un primo ,* $a \in \mathbb{N}$, $m \in \mathbb{N}^+$ *, (p,m)=1. Sia* $S \in$ *Sylp(G) allora:*

$$S \triangleleft G \iff | \textit{Sylp(G)} | = 1$$

inoltre nel seguito porremo $| \textit{Sylp(G)} | = n_p(G)$ *o se non ci sarà rischio di ambiguità semplicemente* $| \textit{Sylp(G)} | = n_p$ *.*

Capitolo 3

Prodotti semidiretti e il gruppo Q_{2^n}

3.1 Prodotti semidiretti

Teorema 20. . *Siano H e K due gruppi , Φ : K $\longrightarrow$ Aut(H) un omomorfismo di gruppi e $\cdot$ l'applicazione:*

$$\cdot : (H \times K) \times (H \times K) \longrightarrow H \times K$$

$$(h,k)(h',k') \longrightarrow \cdot ((h,k)(h',k')) = (h\, \Phi(k)(h'), kk')$$

allora la coppia $(H \times K, \cdot)$ è un gruppo detto prodotto semidiretto tra H e K relativo all'omomorfismo Φ e viene denotato con $H \rtimes_{\Phi} K$.

Dimostrazione. Prima di tutto osserviamo che $\cdot$ è ben definita, nel senso che se (h,k) e (h',k') sono elementi di H $\times$ K allora $\cdot$((h,k)(h',k')) è di fatto un elemento di H $\times$ K. Ora dobbiamo dimostrare che (H $\times$ K, $\cdot$) è un gruppo cioè un monoide in cui tutti gli elementi sono invertibili.Iniziamo a verificare che $\cdot$ è associativa. A tal proposito si prendano (h,k),(h',k') e (h",k") in H $\times$ K allora abbiamo:

$\cdot$(((h,k)(h',k'))(h",k"))=$\cdot$(hΦ(k)(h'),kk')(h",k"))

=(((hΦ(k)(h'))(Φ(k)$\circ\Phi$(k'))(h")),kk'k")

=(((hΦ(k)(h'Φ(k')(h")))),kk'k")=(h,k)(h'Φ(k')(h"),k'k")=(h,k)((h',k')(h",k"))

pertanto $\cdot$ è di fatto associativa. Osserviamo ora che detto 1_H l'elemento neutro di H e 1_K l'elemento neutro di K si ha che comunque scelto (h,k) in H $\times$ K : (h,k)(1_H,1_K)=(1_H,1_K)(h,k)=(h,k)

infatti: (h,k)(1_H,1_K)=(hΦ(k)(1_H),k)=(h,k) dove l'ultima uguaglianza segue dal fatto che essendo Φ(k) un isomorfismo da H in H esso manda 1_H in 1_H.Similmente (1_H,1_K)(h,k)=(Φ(1_K)(h),k)=(h,k) dove l'ultima uguaglianza segue dal fatto che essendo Φ un omomorfismo esso manda 1_K nell'elemento neutro di Aut(H) cioe l'identita di H e pertanto Φ(1_K)(h)=h. Quindi (H × K, ·) è un monoide con elemento neutro (1_H,1_K).Per finire mostriamo che ogni elemento in (H × K, ·) è invertibile.Sia quindi (h,k) ∈ H × K definiamo:

$$(h,k)^{-1} := ((\Phi(k^{-1})(h))^{-1},k^{-1}) \in \mathrm{H} \times \mathrm{K}$$

Osserviamo che

$$(h,k)^{-1}\text{(h,k)=(h,k)}(h,k)^{-1}=(1_H,1_K)$$

Infatti

$$(h,k)^{-1}\text{(h,k)=}((\Phi(k^{-1})(h))^{-1},k^{-1})\text{(h,k)=}((\Phi(k^{-1})(h))^{-1}(\Phi(k^{-1})\text{(h)},k^{-1}\text{k)=}(1_H,1_K)$$

Similmente:

$$\begin{aligned}\text{(h,k)}(h,k)^{-1}&=\text{(h,k)}((\Phi(k^{-1})(h))^{-1},k^{-1})=(\text{h}\Phi\text{(k)}((\Phi(k^{-1})\text{(h)})^{-1}),1_K)\\&=(\text{h}\Phi\text{(k)}(\Phi(k^{-1})(h^{-1})),1_K)=(\text{h}\Phi(1_K)(h^{-1}),1_K)=(1_H,1_K)\end{aligned}$$

Pertanto (h,k) è invertibile con inverso $(h,k)^{-1}$. Consegue che (H × K, ·) è un gruppo. □

Osservazione 6. *Si osservi che se H e K sono due gruppi e Φ: K ⟶ Aut(H) è l'omomorfismo banale, cioè Φ è tale che ∀ k ∈ K Φ(k)=$1_{Aut(H)}$=Id_H allora il prodotto semidiretto H ⋊$_\Phi$ K non è altro che il prodotto diretto tra H e K. Un prodotto semidiretto sarà detto non banale se è determinato da un omomorfismo non banale, verrà invece detto banale se è determinato dall'omomorfismo banale .*

Osservazione 7. *Siano H e K due gruppi e Φ: K ⟶ Aut(H) un omomorfismo non banale cioè ∃ k ∈ K tale che Φ(k) ≠ Id_K, mostriamo che H ⋊$_\Phi$ K non è abeliano.Sia k ∈ K tale che Φ(k) ≠ Id_K.Allora ∃ h ∈ H tale che Φ(k)(h) ≠ h, pertanto: (1_H,k)(h,1_K)=(Φ(k)(h),k) ≠ (h,k)=(h,1_K)(1_H,k).*

Teorema 21. *Sia G un gruppo e H,K ≤ G tali che:*

1. *G=HK*
2. *H ∩ K =$\{1_G\}$*
3. *H ⊴ G*

allora $G \simeq H \rtimes_\Phi K$ *dove* Φ*:* $K \longrightarrow$ *Aut(H),* $k \mapsto \Phi(k)=\Phi_k$ *con* Φ_k $H \longrightarrow H$, $h \mapsto khk^{-1}$.

Dimostrazione. Definiamo l'applicazione:

$$\psi\text{: H} \rtimes_\Phi \text{K} \longrightarrow \text{G}$$

$$\text{(h,k)} \mapsto \text{hk}$$

Chiaramente ψ è suriettiva dato che se g ∈ G, essendo G=HK, si ha che esistono h ∈ H e k ∈ K tali che g=hk pertanto g = ψ (h,k).Mostriamo ora che ψ è iniettiva.Consideriamo (h,k) ∈ Kerψ,allora hk=1_G da cui h=k^{-1} e quindi h ∈ H ∩ K. Per 2. deduciamo che h=1_G. Similmente k=1_G.Pertanto (h,k)=(1_G,1_G) che è l'elemento neutro di H $\rtimes_\Phi$ K,pertanto ψ è iniettiva. Mostriamo adesso che ψ è un omomorfismo. Siano (h,k) e (h',k') due elementi di H $\rtimes_\Phi$ K allora: ψ((h,k)(h',k'))=ψ(hΦ_k(h'),kk')= hΦ_k(h')kk'=hkh'k^{-1}kk '=hkh'k'=ψ(h,k)ψ(h',k'). Pertanto ψ è un isomorfismo e quindi il teorema è dimostrato. □

Teorema 22. *Siano* H_1,H_2,K_1,K_2 *dei gruppi tali che* $H_1 \simeq H_2$ *e* $K_1 \simeq K_2$. *Per ogni omomorfismo* $\gamma : K_1 \longrightarrow$ *Aut(*H_1*) esiste un omomorfismo* $\psi : K_2 \longrightarrow$ *Aut(*H_2*) tale che* $H_1 \rtimes_\gamma K_1 \simeq H_2 \rtimes_\psi K_2$.

Dimostrazione. Sia $\gamma : K_1 \longrightarrow$ Aut(H_1) un omomorfismo e siano f : $H_1 \longrightarrow H_2$ e g : $K_1 \longrightarrow K_2$ degli isomorfismi.Definiamo l'applicazione:

$$\Phi : \text{Aut}(H_1) \longrightarrow \text{Aut}(H_2)$$

$$\chi \longmapsto \text{f} \circ \chi \circ f^{-1}$$

Osserviamo che Φ è ben definita, nel senso che per ogni $\chi \in$ Aut(H_1) la funzione f ∘ χ ∘ f^{-1} è di fatto un isomorfismo da H_2 in H_2 essendo composizione di isomorfismi.Verifichiamo ora che Φ è un isomorfismo. Di fatto Φ è invertibile con inversa:

$$\omega : \text{Aut}(H_2) \longrightarrow \text{Aut}(H_1)$$

$$\text{g} \longmapsto f^{-1} \circ \text{g} \circ \text{f}$$

ed inoltre prese χ_1,$\chi_2 \in$ Aut(H_1) si ha che:

$$\Phi(\chi_1 \circ \chi_2)=\text{f} \circ \chi_1 \circ \chi_2 \circ f^{-1}=(\text{f} \circ \chi_1 \circ f^{-1})(\text{f} \circ \chi_2 \circ f^{-1})= \Phi(\chi_1) \circ \Phi(\chi_2).$$

Quindi Φ è un isomorfismo.Adesso definiamo l'applicazione:

$$\psi : K_2 \longrightarrow \text{Aut}(H_2)$$

$$k \longmapsto (\Phi \circ \gamma \circ g^{-1})(k)$$

ψ è un omomorfismo essendo composizione di omomorfismi, quindi ha senso considerare il prodotto semidiretto $H_2 \rtimes_\psi K_2$. Mostriamo che $H_1 \rtimes_\gamma K_1 \simeq H_2 \rtimes_\psi K_2$. Definiamo l'applicazione:

$$F: H_1 \rtimes_\gamma K_1 \longrightarrow H_2 \rtimes_\psi K_2$$

$$(h,k) \longmapsto (f(h),g(k))$$

Essendo f e g biettive l'applicazione F è biettiva.Mostriamo ora che F è un omomorfismo. Siano (h,k) e (h',k') in $H_1 \rtimes_\gamma K_1$ allora:

F((h,k)(h',k'))=(f(hγ(k)(h')),g(kk'))=(f(h)f(γ(k)(h')),g(k)g(k'))

mentre

F(h,k)F(h',k')=(f(h),g(k))(f(h'),g(k'))=(f(h)ψ(g(k))(f(h')),g(k)g(k'))

quindi se mostro che:

f(γ(k)(h'))=ψ(g(k))(f(h'))

avremmo concluso.

Effettivamente abbiamo che:

ψ(g(k))(f(h'))=($\Phi \circ \gamma \circ g^{-1}$)(g(k))(f(h'))=($\Phi \circ \gamma$)(k)(f(h'))=(f $\circ$ γ(k) $\circ$ f^{-1})(f(h'))=f(γ(k)(h')).

□

Capire se due prodotti semidiretti sono isomorfi non è banale, per questo ci serviremo spesso della seguente:

Proposizione 1. *Siano H e K due gruppi e $\Phi,\Psi : K \longrightarrow$ Aut(H) due omomorfismi. Se esistono $\alpha \in$ Aut(H) e $\beta \in$ Aut(K) tali che $\forall$ $k \in K$*

$$\alpha \circ \Phi(k) \circ \alpha^{-1} = \Psi(\beta(k))$$

allora $H \rtimes_\Phi K \simeq H \rtimes_\Psi K$

Dimostrazione. Consideriamo la mappa:

$$\Gamma : H \rtimes_\Phi K \longrightarrow H \rtimes_\Psi K$$

$$(h,k) \longmapsto (\alpha(h),\beta(k))$$

Γ è biettiva essendo α e β biettive.Mostriamo che Γ è un omomorfismo.Presi (h,k),(h',k') in $H \rtimes_\Phi K$ abbiamo che:

$\Gamma((h,k)(h',k'))=(\alpha(h)((\alpha \circ \Phi(k))(h')),\beta(k)\beta(k'))=(\alpha(h)((\Psi(\beta(k)) \circ \alpha)(h')),\beta(k)\beta(k'))=(\alpha(h),\beta(k))(\alpha(h'),\beta(k'))$

consegue l'asserto. □

3.2 Il gruppo Q_{2^n}

Un gruppo costruito tramite prodotto semidiretto è il gruppo Q_{2^n} che comparirà spesso nei teoremi di classificazione del capitolo 4.

Sia n un naturale maggiore o uguale a 3.Consideriamo il prodotto semidiretto:

$$\mathbb{Z}_{2^{n-1}} \rtimes_\Psi \mathbb{Z}_4$$

dove

$$\Psi : \mathbb{Z}_4 \longrightarrow \mathrm{Aut}(\mathbb{Z}_{2^{n-1}})$$

$$[1]_4 \longmapsto \Psi([1]_4)(x)=-x$$

Per costruire il gruppo dei quaternioni generalizzato dobbiamo verificare che il sottogruppo $<([2^{n-2}]_{2^{n-1}},[2]_4)>$ è normale in $\mathbb{Z}_{2^{n-1}} \rtimes_\Psi \mathbb{Z}_4$.Per mostrarlo è sufficiente far vedere che $([2^{n-2}]_{2^{n-1}},[2]_4) \in Z(\mathbb{Z}_{2^{n-1}} \rtimes_\Psi \mathbb{Z}_4)$.Effettivamente preso $([a^{n-2}]_{2^{n-1}},[b]_4) \in \mathbb{Z}_{2^{n-1}} \rtimes_\Psi \mathbb{Z}_4$ si ha che:

$([a]_{2^{n-1}},[b]_4)([2^{n-2}]_{2^{n-1}},[2]_4)= ([a]_{2^{n-1}}+\Psi([b]_4)([2^{n-2}]_{2^{n-1}}),[b+2]_4)=$
$(([a]_{2^{n-1}}+[2^{n-2}]_{2^{n-1}},[b+2]_4)=(([a+2^{n-2}]_{2^{n-1}},[b+2]_4)$

mentre

$([2^{n-2}]_{2^{n-1}},[2]_4)([a]_{2^{n-1}},[b]_4)=([2^{n-2}]_{2^{n-1}}+ \Psi([2]_4)([a]_{2^{n-1}}),[b+2]_4)=(([a+2^{n-2}]_{2^{n-1}},[b+2]_4)$

quindi:

$$<([2^{n-2}]_{2^{n-1}},[2]_4)> \trianglelefteq \mathbb{Z}_{2^{n-1}} \rtimes_\Psi \mathbb{Z}_4$$

Possiamo allora dare la seguente:

Definizione 1. *Sia $n \in \mathbb{N}$ con $n \geq 3$.Viene detto gruppo dei quaternioni generalizzato il gruppo quoziente:*

$$Q_{2^n} := \mathbb{Z}_{2^{n-1}} \rtimes_\Psi \mathbb{Z}_4 / \langle([2^{n-2}]_{2^{n-1}},[2]_4)\rangle$$

dove

$$\Psi : \mathbb{Z}_4 \longrightarrow Aut(\mathbb{Z}_{2^{n-1}})$$

$$[1]_4 \longmapsto \Psi([1]_4)(x)=-x$$

Osservazione 8. *Consideriamo il gruppo dei quaternioni generalizzato Q_{2^n}. Osserviamo che $|Q_{2^n}| = 2^n$. Infatti: $|Q_{2^n}| = (2^{n-1}2^2)/2 = 2^n$ dove abbiamo utilizzato il fatto che l'ordine di $([2^{n-2}]_{2^{n-1}},[2]_4)$ è due dato che*

$([2^{n-2}]_{2^{n-1}},[2]_4)([2^{n-2}]_{2^{n-1}},[2]_4)=([2^{n-2}+2^{n-2}]_{2^{n-1}},[2+2]_4)=([2^{n-2}-2^{n-2}]_{2^{n-1}},[2+2]_4)=1_{\mathbb{Z}_{2^{n-1}}\rtimes_\Psi\mathbb{Z}_4}$

Proposizione 2. *Sia $n \in \mathbb{N}$ con $n \geq 3$.Detto $N=\langle([2^{n-2}]_{2^{n-1}},[2]_4)\rangle$, $x=([1]_{2^{n-1}},[0]_4)N$ e $y=([0]_{2^{n-1}},[1]_4)N$ si ha che:*

1. $Q_{2^n} = \langle x,y\rangle$
2. $o(x)=2^{n-1}$, $o(y)=4$
3. $x^{2^{n-2}} = y^2$
4. *Se $g \in Q_{2^n}$ allora $g=x^a$ o $g=x^a y$ per qualche $a \in \mathbb{Z}$*
5. $\forall\, g \in Q_{2^n}$ $\langle x\rangle$ *si ha che* $gxg^{-1}=x^{-1}$

Dimostrazione. 1. Dobbiamo dimostrare che:

$$\mathbb{Z}_{2^{n-1}} \rtimes_\Psi \mathbb{Z}_4 / \langle([2^{n-2}]_{2^{n-1}},[2]_4)\rangle = \langle([1]_{2^{n-1}},[0]_4)N,([0]_{2^{n-1}},[1]_4)N\rangle.$$

Chiaramente $\langle([1]_{2^{n-1}},[0]_4)N,([0]_{2^{n-1}},[1]_4)N\rangle$ è contenuto in $\mathbb{Z}_{2^{n-1}} \rtimes_\Psi \mathbb{Z}_4 / \langle([2^{n-2}]_{2^{n-1}},[2]_4)\rangle$, mostriamo l'altra inclusione.Preso $([a]_{2^{n-1}},[b]_4)N$ in $\mathbb{Z}_{2^{n-1}} \rtimes_\Psi \mathbb{Z}_4 / \langle([2^{n-2}]_{2^{n-1}},[2]_4)\rangle$ si ha che: $([a]_{2^{n-1}},[b]_4)N = (([1]_{2^{n-1}},[0]_4)N))^a(([0]_{2^{n-1}},[1]_4)N)^b \in \langle([1]_{2^{n-1}},[0]_4)N,([0]_{2^{n-1}},[1]_4)N\rangle$ quindi si ottiene la 1.

2. Basta osservare che la prima potenza di $([1]_{2^{n-1}},[0]_4)$ che sta in N è la 2^{n-1} - esima e quindi o(x)=2^{n-1}, similmente la prima potenza di $([0]_{2^{n-1}},[1]_4)$ che sta in N è la quarta e quindi o(y)=4

3. Abbiamo che $1_{Q_{2^n}}$ = $([2^{n-2}]_{2^{n-1}},[2]_4)$N = $(([1]_{2^{n-1}},[0]_4)\text{N}))^{2^{n-2}}(([0]_{2^{n-1}},[1]_4)\text{N})^2$=$x^{2^{n-2}}y^2$ e quindi $x^{2^{n-2}}$=y^2.

4. Per il procedimento fatto al punto 1 abbiamo che se g $\in Q_{2^n}$ allora esistono a e b in $\mathbb{Z}$ tali che g = $x^a y^b$.Si hanno due casi:

   - se b è pari allora essendo $x^{2^{n-2}}$ = y^2 troviamo che g=$x^a y^{2k}$=$x^a(y^2)^k$=$x^{a'}$ per un certo a' in $\mathbb{Z}$
   - se b è dispari g=$x^a y^{2k}$y=$x^{a''}$y per qualche a" in $\mathbb{Z}$.

5. Prima di tutto osserviamo che $yxy^{-1}=x^{-1}$ (sono semplici conti) quindi preso g $\in Q_{2^n}$ <x>, e quindi g ha la forma g=x^ay, si ha che $gxg^{-1}=x^a yxy^{-1}x^{-a}=x^a x^{-1-1}x^{-a}=x^{-1}$.

□

Osservazione 9. *Osserviamo che per ogni n $\in \mathbb{N}$ con n $\geq$ 3 il gruppo dei quaternioni generalizzato Q_{2^n} è non abeliano.Infatti se per assurdo lo fosse yx=xy e quindi yxy^{-1}=x da cui x^{-1}=x,che è assurdo dato che x ha ordine maggiore di 2.*

Siamo pronti per il seguente:

Teorema 23. *Sia n $\in \mathbb{N}$ con n $\geq$ 3 e G un gruppo tale che:*

1. $|G| = 2^n$
2. *G=<x,y> con x,y $\in$ G tali che o(x)=2^{n-1}, o(y)=4, $yxy^{-1}=x^{-1}$*

allora $G \simeq Q_{2^n}$.

Dimostrazione. Abbiamo che Q_{2^n} = <$\bar{x}$,$\bar{y}$> con o($\bar{x}$)=2^{n-1},o($\bar{y}$)=4, $\bar{y}\bar{x}\bar{y}^{-1}=\bar{x}^{-1}$ e $\bar{y}^2=\bar{x}^{2^{n-2}}$.Per induzione si mostra facilmente che per ogni i in $\mathbb{N}$ si ha che $\bar{y}\bar{x}^i\bar{y}^{-1}=\bar{x}^{-i}$ e yx^iy^{-1}= x^{-i}.Inoltre osserviamo che:

G=<x><y>

infatti | <x><y> | = $(2^{n-1}4)/2=2^n$.Definiamo ora la mappa:

$$f: Q_{2^n} \longrightarrow G$$

$$\bar{x}^a\bar{y}^b \longmapsto x^a y^b$$

con a $\in \{0, ..., 2^{n-1}\}$ e b $\in \{0, 1\}$.Osserviamo che f è suriettiva perchè se g $\in$ G allora g=$x^a y^b$ con a $\in \{0, ..., 2^{n-1}\}$ e b $\in \{0, 1, 2, 3\}$. Quindi si hanno quattro casi:

- b=0 quindi g=x^a=f($\bar{x}^a$)
- b=1 quindi g=x^ay=f($\bar{x}^a\bar{y}$)
- b=2 quindi g=$x^a y^2$=$x^a x^{2^{n-2}}$=f($\bar{x}^a$) con a' in $\mathbb{N}$ (abbiamo utilizzato il fatto che y^2=$x^{2^{n-2}}$ infatti $y^2 \in$ <x> $\cap$ <y> quindi y^2 = x^k per qualche k in $\mathbb{N}$ ma siccome y^2 ha ordine 2 l'unica possibilità è che k=2^{n-2})
- g=$x^a y^3$=$x^{a'}$y=f($\bar{x}^{a'}\bar{y}$) per qualche a' in $\mathbb{N}$

consegue che f è suriettiva e siccome dominio e codominio sono insiemi finiti con la stessa cardinalità tale applicazione è anche iniettiva. mostriamo che f è un omomorfismo. Consideriamo due tipici elementi in Q_{2^n}:

$$\bar{x}^a\bar{y}^b \text{ e } \bar{x}^c\bar{y}^d$$

con a,c $\in \{0, ..., 2^{n-1}\}$ e b,d $\in \{0, 1\}$.Proviamo che:

$$f(\bar{x}^a\bar{y}^b\bar{x}^c\bar{y}^d) = f(\bar{x}^a\bar{y}^b)f(\bar{x}^c\bar{y}^d)$$

A tal proposito distinguiamo quattro possibili casi:

- b=d=0. In tal caso:

  $f(\bar{x}^a\bar{y}^b\bar{x}^c\bar{y}^d) = f(\bar{x}^a\bar{x}^c) = x^a x^c = f(\bar{x}^a)f(\bar{x}^c) = f(\bar{x}^a\bar{y}^b)f(\bar{x}^c\bar{y}^d)$

- b=0,d=1. In tal caso:

  $f(\bar{x}^a\bar{y}^b\bar{x}^c\bar{y}^d) = f(\bar{x}^a\bar{x}^c\bar{y}) = x^a x^c y = f(\bar{x}^a)f(\bar{x}^c\bar{y}) = f(\bar{x}^a\bar{y}^b)f(\bar{x}^c\bar{y}^d)$

- b=1,d=0. In tal caso:

  $f(\bar{x}^a\bar{y}^b\bar{x}^c\bar{y}^d) = f(\bar{x}^a\bar{x}^{-c}\bar{y}) = x^a x^{-c} y = x^a y x^c = f(\bar{x}^a\bar{y})f(\bar{x}^c) = f(\bar{x}^a\bar{y}^b)f(\bar{x}^c\bar{y}^d)$

- b=d=1. In tal caso:

f($\bar{x}^a\bar{y}^b\bar{x}^c\bar{y}^d$)=f($\bar{x}^a\bar{y}\bar{x}^c\bar{y}$)=f($\bar{x}^{a-c}\bar{y}^2$)=x^{a}x^{-c}yy=x^{a}yx^{c}y=f($\bar{x}^a\bar{y}$)f($\bar{x}^c\bar{y}$)=f($\bar{x}^a\bar{y}^b$)f($\bar{x}^c\bar{y}^d$).

Pertanto f è un isomorfismo e quindi G $\simeq$ Q_{2^n} □

Capitolo 4

Teoremi di classificazione per gruppi finiti

4.1 Gruppi ciclici finiti

Teorema 24. *Sia G un gruppo ciclico :* $|\ G\ | = n$. *Allora:*

$$G \simeq \mathbb{Z}_n$$

Dimostrazione. Sia x ∈ G : G = <x>. Definiamo l'applicazione:

$$\Psi : \mathrm{G} \longrightarrow \mathbb{Z}_n$$

$$\mathrm{x}^h \longmapsto [h]_n$$

mostriamo che Ψ è un isomorfismo. Effettivamente Ψ è suriettiva ed essendo | G | = | $\mathbb{Z}_n$ | si ha che Ψ è iniettiva e quindi bigettiva.Per mostrare che è un omomorfismo si prendano g e g' in G.Allora esistono h e h' in $\{0, 1, ..., n-1\}$ tali che:

$$\mathrm{g}=\mathrm{x}^h$$

e

$$\mathrm{g'}=\mathrm{x}^{h'}$$

consegue: Ψ(gg')=Ψ($\mathrm{x}^{h+h'}$)=$[h+h']_n$=$[h]_n$+$[h']_n$=Ψ(g)+Ψ(g'). □

4.2 Gruppi di ordine p

Teorema 25. *Sia G un gruppo tale che | G | = p con p primo, allora* $G \simeq \mathbb{Z}_p$

Dimostrazione. Basta osservare che G è ciclico e quindi avendo ordine p si ha, per il teorema anteriore, G $\simeq \mathbb{Z}_p$ □

4.3 Gruppi di ordine 2p

Ricordiamo la definizione del gruppo diedrale. Si prenda $X_n \subset \mathbb{R}^2$, n $\in \mathbb{N}$ con n $\geq$ 3, un n-agono regolare. Viene detto gruppo diedrale D_n il gruppo delle isometrie di X_n. Si mostra che X_n=<x><y> dove o(x)=n,o(y)=2 e yxy=x^{-1}.

Teorema 26. *Sia p un primo maggiore di 2 e G un gruppo : | G | = 2p.Allora:*

$$G \simeq \mathbb{Z}_{2p} \vee G \simeq D_p$$

Dimostrazione. Poichè n_p = 1+pk con k $\in \mathbb{N}$ e p>2 necessariamente n_p = 1. Sia P il p-sylow di G (che è normale in G).Inoltre n_2 divide p,che è primo, quindi ci sono due possibilità: n_2 = 1 oppure n_2 = p. Analizziamo i due casi separatamente.Se n_2 = 1 detto Q il 2-sylow di G (che è normale in G) essendo (2,p)=1 per il teorema numerico si ha immediatamente che:

$$\mathrm{G} \simeq \mathrm{P} \times \mathrm{Q} \simeq \mathbb{Z}_p \times \mathbb{Z}_2 \simeq \mathbb{Z}_{2p} \, .$$

Supponiamo ora che n_2 = p allora ci sono p elementi di ordine 2 in G,prendiamone uno,diciamolo y.Ora P=<x> per qualche x in G : o(x)=p.Osserviamo che G=<x><y>.Infatti <x> e <y> si intersecano banalmente (ovvero solo in 1_G) dato che (2,p)=1 quindi | <x><y> | = 2p/1=2p=| G | quindi non può che essere G = <x><y>. Vogliamo mostrare che G $\simeq$ D_p= <r><s> dove o(r)=p, o(s)=2, srs=r^{-1}.Iniziamo ad osservare che yxy=x^{-1}.Effettivamente essendo <x> normale in G si ha che yxy=x^i per qualche i in $\{0, 1, ..., p-1\}$.Ora $(yx)^2$ = yxyx= x^{i+1} e o(yx) divide 2p quindi o(yx) $\in \{2, p, 2p\}$.Tuttavia se o(yx)=2p allora G sarebbe ciclico e quindi abeliano e pertanto n_2=1, assurdo.Inoltre o(yx) non può essere p infatti se o(yx)=p allora yx $\in$ <x> da cui y $\in$ <x> che è assurdo.Quindi o(yx)=2 e quindi x^{i+1} = 1 da cui p$\leq$ i+1 e quindi i $\geq$ p-1 allora i=p-1.Pertanto: yxy=x^{-1}.Per induzione si mostra facilmente che $\forall$ i $\in$ $\mathbb{N}$ si ha che $yx^iy=x^{-i}$ e che $sr^is=r^{-i}$.Definiamo l'applicazione:

$$\Phi : \mathrm{G} \longrightarrow \mathrm{D}_p$$

$$x^i y^j \longmapsto r^i s^j$$

con i $\in \{0, 1, ..., p-1\}$ e j $\in \{0, 1\}$ Dimostriamo che Φ è un isomorfismo di gruppi.Chiaramente Φ è suriettiva e siccome $\mid G \mid = \mid D_p \mid$ abbiamo che Φ è iniettiva e quindi bigettiva.Rimane da mostrare che Φ è un omomorfismo di gruppi.Siano g_1 e g_2 due elementi di G. Allora

$$g_1 = x^i y^j \text{ per certi i} \in \{0, 1, ..., p-1\} \text{ e j} \in \{0, 1\}$$

e

$$g_2 = x^{i'} y^{j'} \text{ per certi i'} \in \{0, 1, ..., p-1\} \text{ e j'} \in \{0, 1\}$$

dimostriamo che: $\Phi(x^i y^j x^{i'} y^{j'}) = \Phi(x^i y^j)\Phi(x^{i'} y^{j'})$.Distinguiamo 4 possibili casi:

1. j=j'=0.

   allora $\Phi(x^i y^j x^{i'} y^{j'}) = \Phi(x^i y^0 x^{i'} y^0) = \Phi(x^i x^{i'}) = r^{i+i'} = r^i s^0 r^{i'} s^0 = \Phi(x^i y^0)\Phi(x^{i'} y^0) = \Phi(x^i y^j)\Phi(x^{i'} y^{j'})$.

2. j=0,j'=1

   allora $\Phi(x^i y^j x^{i'} y^{j'}) = \Phi(x^i y^0 x^{i'} y) = \Phi(x^i x^{i'} y) = r^{i+i'} s = r^i s^0 r^{i'} s = \Phi(x^i y^0)\Phi(x^{i'} y) = \Phi(x^i y^j)\Phi(x^{i'} y^{j'})$.

3. j=1,j'=0

   allora $\Phi(x^i y^j x^{i'} y^{j'}) =$
   $\Phi(x^i y x^{i'} y^0) = \Phi(x^i y x^{i'}) = \Phi(x^i x^{-i'} y) = r^{i-i'} s = r^i s r^{i'} = \Phi(x^i y)\Phi(x^{i'} y^0) = \Phi(x^i y^j)\Phi(x^{i'} y^{j'})$.

4. j=j'=1

   $\Phi(x^i y^j x^{i'} y^{j'}) = \Phi(x^i y x^{i'} y) = \Phi(x^i x^{-i'}) = r^{i-i'} = r^i s r^{i'} s = \Phi(x^i y)\Phi(x^{i'} y) = \Phi(x^i y^j)\Phi(x^{i'} y^{j'})$.

   quindi Φ è un isomorfismo e pertanto $G \simeq D_p$ tramite Φ.

□

Osservazione 10. *Sia p un primo dispari. Osserviamo che $\mathbb{Z}_{2p}$ e D_p non sono isomorfi essendo il primo abeliano e il secondo non abeliano.*

4.4 Gruppi di ordine p^2

Per classificare i gruppi di ordine 4 e 9 ci serviamo del seguente fatto più generale:

Teorema 27. *Sia G un gruppo :* $|G| = p^2$ *con p primo.Allora:*

$$G \simeq \mathbb{Z}_{p^2} \vee G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$$

Dimostrazione. Se $\exists$ x $\in$ G : o(x)=p^2 allora G = <x> $\simeq \mathbb{Z}_{p^2}$.Supponiamo che non esista x in G di ordine p^2. Siccome | G | = p^2 >1 esiste x in G di ordine p.Definiamo H :=<x> .Iniziamo a mostrare che H è normale in G. Supponiamo per assurdo che H non sia normale in G, allora esiste g in G tale che $H \neq H^g$. Ora $H \cap H^g$ è un sottogruppo di H che è contenuto strettamente in esso perchè se per assurdo $H \cap H^g = H$ allora $H \leq H^g$ ma | H | = $|H^g|$ e quindi $H = H^g$,assurdo. Allora,essendo l'ordine di H p,che è primo, si deduce che $H \cap H^g$ è il sottogruppo banale e quindi $|HH^g| = p^2$ da cui $G = HH^g$. Allora esistono h e h' in H tali che $g^{-1}=g^{-1}hgh'$e quindi $g=h^{-1}h'^{-1}$ da cui g $\in$ H e pertanto $H = H^g$,assurdo.Quindi H è normale in G.Sia ora y $\in$ G $\setminus$ H tale che o(y)= p. Similmente a come fatto prima,se K := <y>, abbiamo che K è normale in G.Quindi abbiamo trovato H e K sottogruppi normali di G tali che | H | = | K | = p, $H \cap K = \{1_G\}$ (infatti se H e K non si intersecano banalmente allora H $\cap$ K = K e quindi K è un sottogruppo di H e quindi y sta in H assurdo) da cui HK=G,per il teorema prodotto deduciamo che G $\simeq$ H $\times$ K $\simeq \mathbb{Z}_p \times \mathbb{Z}_p$. □

Osservazione 11. *Sia p un primo. Osserviamo che* $\mathbb{Z}_{p^2}$ *e* $\mathbb{Z}_p \times \mathbb{Z}_p$ *non sono isomorfi dato che il primo ha un elemento di ordine* p^2 *mentre il secondo no.*

4.5 Gruppi di ordine p^3

Sia p un primo maggiore (stretto) di 2. Si consideri il gruppo (detto gruppo di Heisenberg) :

$$\text{Heis}(\mathbb{Z}_p) := \left\{ M_{abc} := \begin{pmatrix} [1]_p & [a]_p & [b]_p \\ 0 & 1 & [c]_p \\ 0 & 0 & [1]_p \end{pmatrix} : [a]_p, [b]_p, [c]_p \in \mathbb{Z}_p \right\}$$

e il gruppo:

$$G_p := \left\{ N_{mb} := \begin{pmatrix} [1+pm]_{p^2} & [b]_{p^2} \\ 0 & [1]_{p^2} \end{pmatrix} : m, b \in \mathbb{Z} \right\}$$

Osserviamo che Heis($\mathbb{Z}_p$) e G_p sono gruppi di ordine p^3. Iniziamo a mostrare che non sono isomorfi.Contiamo gli elementi di ordine p in entrambi i gruppi.Osserviamo che, in generale, se n $\in \mathbb{N}$

$$(M_{abc})^n = \begin{pmatrix} [1]_p & [na]_p & [nb + \frac{(n-1)n}{2}ac]_p \\ 0 & 1 & [nc]_p \\ 0 & 0 & [1]_p \end{pmatrix} \forall\ [a]_p, [b]_p, [c]_p \in \mathbb{Z}_p$$

e quindi

$$(M_{abc})^p = \text{Id}\ \forall\ [a]_p, [b]_p, [c]_p \in \mathbb{Z}_p$$

quindi tutti gli elementi di Heis($\mathbb{Z}_p$) che non sono l'elemento neutro del gruppo hanno ordine p mentre in G_p l'elemento N_{01} ha ordine p^2 infatti, preso un naturale n:

$$(N_{01})^n = \begin{pmatrix} [1]_{p^2} & [n]_{p^2} \\ 0 & [1]_{p^2} \end{pmatrix}$$

che è diverso da Id se n = p. Quindi G_p e Heis($\mathbb{Z}_p$) non sono isomorfi. Si osservi che:

- $M_{abc}M_{a'b'c'} = M_{(a+a')(b+b'+ac')(c+c')}$
- $N_{mb}N_{m'b'} = N_{(m+m')(b+b'+pmb')}$

allora osserviamo che i due gruppi non sono abeliani. Effettivamente $M_{abc}M_{a'b'c'} = M_{a'b'c'}M_{abc}$ $\iff$ ac'=a'c che in generale è falsa (basta prendere c=0,a' qualunque, a=c'=1) ed inoltre $N_{mb}N_{m'b'} = N_{m'b'}N_{mb}$ $\iff$ pmb'=pm'b che, anche in questo caso, è falsa in generale.

Lemma 4. *Sia G un gruppo non abeliano di ordine p^3 con p un primo $\geq$ 3.Allora:*

- $|\ Z(G)\ | = p$
- $G\ /\ Z(G) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$
- *G'=Z(G)*

Dimostrazione. Dimostriamo i tre punti:

- Essendo G un p-gruppo il centro è non banale ed essendo G non abeliano non può capitare che il suo ordine sia p^3. Quindi le uniche possibilità sono che l'ordine di Z(G) sia p o p^2. Ma quest'ultimo caso è assurdo in quanto implicherebbe che G/Z(G) ha ordine p e quindi ciclico e quindi G sarebbe abeliano.Pertnato Z(G) ha ordine p^2.

- Siccome Z(G) ha ordine p il quoziente G / Z(G) ha ordine p^2, siccome non può essere ciclico l'unica possibilità è che sia isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$.
- Siccome G / Z(G) è abeliano si ha che G' $\leq$ Z(G) e siccome G non è abeliano G' non è banale quindi G'=Z(G)

□

Si osservi che vale il seguente fatto generale (non necessariamente per gruppi finiti)

Lemma 5. *Sia G un gruppo e g,h due elementi di G che commutano con [g,h] allora:*

- $\forall$ *n,m* $\in \mathbb{Z}$ $[g,h]^{mn}$=*[*g^m, h^n*]*
- $\forall$ *n* $\in \mathbb{Z}$ $(gh)^n$=$g^n h^n [g,h]^{\binom{n}{2}}$

Teorema 28. *Sia p un primo* $\geq$ *3 e G un gruppo :* $|G|$ = p^3*.Allora* $G \simeq \mathbb{Z}_{p^3} \vee G \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_p \vee G \simeq \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \vee G \simeq$ *Heis(*$\mathbb{Z}_p$*)* $\vee G \simeq G_p$.

Dimostrazione. Per il lemma anteriore:

$$\frac{G}{Z(G)} \simeq \mathbb{Z}_p \times \mathbb{Z}_p = < ([1]_p,[0]_p), ([0]_p,[1]_p) >$$

quindi esistono x e y in G con x $\notin$ <y> tali che:

$$\frac{G}{Z(G)} = <xZ(G),yZ(G)>$$

Ora Z(G)=<z> per qualche z in G di ordine p. Osserviamo che [x,y] $\neq$ 1 altrimenti G è abeliano (infatti se $\tilde{g} \in$ G allora esistono interi a_i e b_i per i=1,...,t tali che:

$$\tilde{g}Z(G)=(x^{a_1}Z(G))(y^{b_1}Z(G))...(x^{a_t}Z(G))(y^{b_t}Z(G))$$

e quindi $\tilde{g} = x^{a_1}y^{b_1}...x^{a_t}y^{b_t}z^k$ per un certo intero k. Tuttavia presi comunque i e j interi si ha per il lemma anteriore che $x^i y^j = y^j x^i [x,y]^{ij}$ quindi $\tilde{g}$ alla fine avrà la forma $\tilde{g}$=$y^{\tilde{a}}x^{\tilde{b}}\tilde{z}^{k'}$ dove $\tilde{a}$,$\tilde{b}$ e k' sono interi e $\tilde{z}$ è un elemento del centro di G allora presi g e g' in G si ha che g = $x^i y^j \tilde{z}^k$ per certi interi i,j e k e g'=$x^{i'}y^{j'}\tilde{\tilde{z}}^{k'}$ per certi interi i',j' e k' e con $\tilde{z}$ e $\tilde{\tilde{z}}$ in Z(G) quindi siccome x e y commutano allora x^a commuta con y^b comunque scelti due interi a e b e quindi x^i,y^j,$\tilde{z}^k$, $x^{i'}$,$y^{j'}$ e $\tilde{\tilde{z}}^{k'}$ commutano tutti tra loro e quindi gg'=g'g). Pertanto possiamo scegliere come generatore per Z(G) l'elemento [x,y] ovvero:

$$\frac{G}{Z(G)} = < [x,y] >$$

e quindi si ha anche che G = < x,y> (Infatti chiaramente <x,y> $\leq$ G e inoltre preso un elemento g in G si ha che g ha la forma $x^i y^j [x,y]^k$ con i,j e k interi e quindi g $\in$ <x,y>).Distinguiamo due casi:

1. o(x)=o(y)=p

   Definiamo l'applicazione:

   $$\Phi : \text{Heis}(\mathbb{Z}_p) \longrightarrow \text{G}$$

   $$M_{abc} \longmapsto y^c x^a [x,y]^b$$

   mostriamo che Φ è un isomorfismo. L'applicazione Φ è ben definita, nel senso che di fatto $\Phi(Ma_{abc})$ è un elemento di G.Iniziamo a vedere che Φ è un omomorfismo.In effetti se M_{abc} e $M_{a'b'c'}$ sono due tipici elementi di Heis($\mathbb{Z}_p$) si ha che:

   $\Phi(M_{abc}M_{a'b'c'})$=$\Phi(M_{(a+a')(b+b'+ac')(c+c')})$=
   $y^{c+c'}x^{a+a'}[x,y]^{b+b'+ac'}$=$y^{c+c'}x^{a+a'}[x,y]^{b+b'}[x,y]^{ac'}$ = $y^c(y^{c'}x^a[x,y]^{ac'})x^{a'}[x,y]^{b+b'}$ =
   $y^c(x^a y^{c'})x^{a'}[x,y]^{b+b'}$=$(y^c x^a [x,y]^b)(y^{c'}x^{a'}[x,y]^{b'})$ = $\Phi(M_{abc})\Phi(M_{a'b'c'})$

   quindi Φ è un omomorfismo.Per mostrare che è biettiva è sufficiente verificare che è suriettiva (essendo G e Heis($\mathbb{Z}_p$) dello stesso ordine). Sia g un elemento in G. Allora esistono i,j e k interi tali che: g=$y^i x^j [x,y]^k$.Ora per il teorema della divisone euclidea:

   i = m_ip + q_i con m_i e q_i in $\mathbb{Z}$ e $0 \leq q_i <$ p

   j = m_jp + q_j con m_j e q_j in $\mathbb{Z}$ e $0 \leq q_j <$ p

   k = m_kp + q_k con m_k e q_k in $\mathbb{Z}$ e $0 \leq q_k <$ p

   da cui, avendo x,y e [x,y] ordine p

   g=$y^{q_i}x^{q_j}[x,y]^{q_k}$ = $\Phi(M_{q_i q_j q_k})$

   e quindi G $\simeq$ Heis($\mathbb{Z}_p$).

2. Uno tra x e y ha ordine p^2. Senza perdita di generalità supponiamo che y abbia ordine p^2. Vogliamo dimostrare che esiste $\tilde{\tilde{x}} \in$ G di ordine p : G = <$\tilde{\tilde{x}}$,y> e [$\tilde{\tilde{x}}$,y]=y^p. Iniziamo ad osservare che esiste r $\in \mathbb{Z}$ tale che G = <xy^{-r},y>. Infatti $\forall$ g $\in$ G si ha che g^pZ(G) = $(gZ(G))^p$ = Z(G) e quindi $g^p \in$ Z(G) e inoltre presi g e h in G :

$$(gh)^p = g^p h^p [g,h]^{\frac{p(p-1)}{2}} = g^p h^p$$

ora: o(y^p)=p e $y^p \in$ Z(G) quindi Z(G)=<y^p> allora $x^p=(y^p)^r$ per qualche intero r consegue:

$$(xy^{-r})^p = x^p y^{-rp} = 1$$

e siccome x $\notin$ <y> si ha che $xy^{-r} \neq 1$ e quindi xy^{-r} ha ordine p e allora:

$$G = \langle xy^{-r}, y \rangle$$

poniamo $\tilde{x} = xy^{-r}$. Quindi

$$G = \langle \tilde{x}, y \rangle \text{ con } o(\tilde{x})=p \text{ e } o(y)=p^2$$

Adesso:

$$[\tilde{x}, y] = (y^p)^k \text{ per qualche k intero : k} \neq_p 0$$

Sia l in intero tale che kl $\equiv_p$ 1 (l $\neq_p$ 0) allora:

$$y^p = (y^{lk})^p = [\tilde{x}, y]^l = [\tilde{x}^l, y]$$

quindi definendo l'elemento $\tilde{\tilde{x}} := \tilde{x}^l$ notiamo che $\tilde{\tilde{x}} \neq 1$ (perchè l $\neq_p$ 0) e quindi G = < $\tilde{\tilde{x}}$,y> con o($\tilde{\tilde{x}}$)=p,o(y)=p^2 e [$\tilde{\tilde{x}}, y$]=y^p. Definiamo l'applicazione :

$$\tilde{\Phi} : G_p \longrightarrow G$$

$$N_{mb} \longmapsto y^b \tilde{\tilde{x}}^m$$

$\tilde{\Phi}$ è ben definita nel senso che $\tilde{\Phi}(N_{mb})$ è di fatto un elemento di G. Mostriamo che è un omomorfismo.Effettivamente se N_{mb} e $N_{m'b'}$ sono due tipici elementi di G_p si ha che:

$\tilde{\Phi}(N_{mb}N_{m'b'})$=$\tilde{\Phi}(N_{(m+m')(b+b'+pmb')})$=$y^{b+b'+pmb'}\tilde{\tilde{x}}^{m+m'}$=
$y^{b+b'}\tilde{\tilde{x}}^{m}(y^p)^{mb'}\tilde{\tilde{x}}^{m'}$=$y^b(y^{b'}\tilde{\tilde{x}}^{m}[\tilde{\tilde{x}},y]^{mb'})\tilde{\tilde{x}}^{m'}$=$y^b\tilde{\tilde{x}}^{m}y^{b'}\tilde{\tilde{x}}^{m'}$= $\tilde{\Phi}(N_{mb})\tilde{\Phi}(N_{m'b'})$

quindi $\tilde{\Phi}$ è un omomorfismo.Per mostrare che è biettiva è sufficiente verificare che è suriettiva.Effettivamente sia g $\in$ G. Allora esistono interi i,j e k tali che:

$$\text{g=}y^j\tilde{\tilde{x}}^i[\tilde{\tilde{x}},y]^k\text{=}[\tilde{\tilde{x}},y]^k y^j\tilde{\tilde{x}}^i = y^{pk+j}\tilde{\tilde{x}}^i$$

quindi:

$$\text{g = } y^b\tilde{\tilde{x}}^a \text{ per certi interi a e b}$$

per il teorema della divisione euclidea:

$$\text{a=}a_1p^2 \text{ + r con } a_1,\text{r} \in \mathbb{Z} \text{ e } 0 \leq \text{r < p}$$

$$\text{b=}b_1p^2 \text{ + q con } b_1,\text{q} \in \mathbb{Z} \text{ e } 0 \leq \text{q < } p^2$$

da cui:

$$\text{g=}y^q\tilde{\tilde{x}}^r \text{ = } \tilde{\Phi}(N_{rq})$$

e quindi G $\simeq G_p$

□

Osservazione 12. *Si osservi che i gruppi $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ e $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ sono gruppi abeliani non isomorfi e siccome i gruppi Heis($\mathbb{Z}_p$) e G_p sono non abeliani non isomorfi si deduce che i gruppi che compaiono nel teorema anteriore sono tutti non isomorfi.*

4.6 Gruppi di ordine pq,p^2q,p^2q^2

Teorema 29. *Siano p,q primi e G un gruppo finito.Se*

1. $|G| = pq$ *con* $p>q$, $q \nmid p-1$ *allora*

$$G \simeq \mathbb{Z}_{pq}$$

2. $|G| = p^2q$ *con* $p>q$, $q \nmid p-1$ *e* $q \nmid p+1$ *allora*

$$G \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_q \vee G \simeq \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$$

3. $|G| = p^2q$ *con* $q>p$, $p \nmid q-1$ *e* $q \nmid p^2-1$ *allora*

$$G \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_q \vee G \simeq \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$$

4. $|G| = p^2q^2$ *con* $p \nmid q^2-1$, $q \nmid p^2-1$ *allora:*

$$G \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_{q^2} \vee G \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_q \times \mathbb{Z}_q \vee G \simeq \mathbb{Z}_{q^2} \times \mathbb{Z}_p \times \mathbb{Z}_p \vee G \simeq \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_p \times \mathbb{Z}_p$$

Dimostrazione. 1. Mostriamo che n_p=n_q=1.Effettivamente n_p=1+pk per qualche naturale k e n_p divide q.Se per assurdo k>0 allora n_p > p > q assurdo,quindi k=0 e n_p=1.Similmente n_q divide p, quindi n_q=1 o n_q=p.Tuttavia n_q=1+qk per qualche naturale k,quindi se n_q=p allora q divide p-1 che è assurdo per l'ipotesi fatta e quindi n_q=1.Allora se P è il sottogruppo normale di G di ordine p e Q il sottogruppo normale di G di ordine q siccome P e Q si intersecano banalmente:

$$\mathrm{G} \simeq \mathrm{P} \times \mathrm{Q} \simeq \mathbb{Z}_p \times \mathbb{Z}_q \simeq \mathbb{Z}_{pq}$$

2. Mostriamo che n_p=n_q=1.Effettivamente n_p=1+pk per qualche naturale k e n_p divide q.Se per assurdo k>0 allora n_p > p > q assurdo,quindi k=0 e n_p=1.Similmente n_q divide p^2 quindi n_q=1 o n_q=p o n_q=p^2.Tuttavia n_q=1+qk per un naturale k.Quindi se n_q=p allora q divide p-1 ed è assurdo per l'ipotesi fatta,se n_q=p^2 allora q divide p^2 -1 e quindi q divide p+1,assurdo.Pertanto se P è il sottogruppo normale di G di ordine p^2 e Q il sottogruppo normale di G di ordine q siccome P e Q si intersecano banalmente:

$$\mathrm{G} \simeq \mathrm{P} \times \mathrm{Q}$$

tenendo conto che P è un sottogruppo di G di ordine p^2 si ha immediatamente che:

$$\mathrm{G} \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_q \vee \mathrm{G} \simeq \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$$

3. Mostriamo che n_p=n_q=1.Abbiamo che n_p divide q.Se n_p=q allora p divide q-1,assurdo per ipotesi.Similmente n_q divide p^2.Se n_q=p allora q divide p-1 e quindi q divide p^2 -1 assurdo per ipotesi.Se n_q=p^2 allora q divide p^2 -1,assurdo per ipotesi,quindi n_q=1.Pertanto se P è il sottogruppo normale di G di ordine p^2 e Q il sottogruppo normale di G di ordine q siccome P e Q si intersecano banalmente:

$$G \simeq P \times Q$$

tenendo conto che P è un sottogruppo di G di ordine p^2 si ha immediatamente che:

$$G \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_q \vee G \simeq \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$$

4. Ragionando come nei punti precedenti si trova che n_p=n_q=1.Allora se P è il sottogruppo normale di G di ordine p^2 e Q il sottogruppo normale di G di ordine q^2 siccome P e Q si intersecano banalmente:

$$G \simeq P \times Q$$

allora

$$G \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_{q^2} \vee G \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_q \times \mathbb{Z}_q \vee G \simeq \mathbb{Z}_{q^2} \times \mathbb{Z}_p \times \mathbb{Z}_p \vee G \simeq \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_p \times \mathbb{Z}_p$$

□

4.7 Gruppi abeliani finiti

Enunciamo, senza dimostrazione,il teorema di classificazione per i gruppi abeliani finiti.

Teorema 30. *(Teorema di Frobenius-Stickelberg) Sia G un gruppo abeliano finito. Allora G è isomorfo a un prodotto diretto di gruppi ciclici.*

4.8 Gruppi in cui l'equazione x^n=1 ha al più n soluzioni per ogni n $\in \mathbb{N}$

Teorema 31. *Sia G un gruppo :* $|G| = m$. *Se* $\forall\ n \in \mathbb{N}$ *l'equazione*

$$x^n = 1$$

ha al più n soluzioni in G allora $G \simeq \mathbb{Z}_m$

Dimostrazione. Sia p un primo che divide l'ordine di G e sia P un p-sylow di G.Mostriamo che P è normale in G ed è ciclico. Supponiamo che | P | = p^a con a $\in \mathbb{N}$.Per il teorema di Lagrange si ha che:

$$x^{p^a} = 1$$

$\forall$ x $\in$ P.Se per assurdo $n_p \neq 1$ allora troverei un elemento y $\in$ G $\setminus$ P tale che:

$$y^{p^a} = 1$$

contraddicendo l'ipotesi quindi n_p=1 e perciò P è normale.Osserviamo inoltre che P è ciclico.Infatti se P non fosse ciclico preso y $\in$ P, o(y)=p^k per qualche k $\in \mathbb{N}$ con k<a.Allora siccome $p^k \mid p^{a-1}$ troviamo $y^{p^{a-1}} = 1$.Quindi si avrebbe che per ogni x $\in$ P:

$$x^{p^{a-1}} = 1$$

assurdo per l'ipotesi fatta.Quindi P è ciclico.Ora per il teorema fondamentale dell'aritmetica:

$$m = p_1^{a_1} ... p_t^{a_t}$$

con p_1,...,p_t primi distinti (osserviamo che possiamo assumere t>1 perche se t=1 allora G è ciclico e quindi isomorfo a $\mathbb{Z}_m$ e pertanto avremmo concluso) e a_1,...,a_t naturali positivi. Allora siano P_1,...,P_t i sottogruppi di Sylow di G con | P_i | =$p_i^{a_i}$ $\forall$ i=1,...,t. Essi sono sottogruppi normali di G (per il discorso fatto sopra) quindi l'applicazione:

$$f : P_1 \times ... \times P_t \longrightarrow G$$

$$(n_1,...,n_t) \longmapsto n_1 ... n_t$$

è un omomorfismo.Inoltre tale applicazzione è suriettiva dato che:

$$G = P_1 ... P_t$$

in quanto $P_1 ... P_t \leq$ G e | $P_1 ... P_t$ | = $p_1^{a_1} ... p_t^{a_t}$ = m ma allora essendo | G | = | $P_1 \times ... \times P_t$ | tale applicazzione è anche suriettiva e quindi:

$$G \simeq P_1 \times ... \times P_t$$

ma $\forall$ i=1,...,t P_i è ciclico di ordine $p_i^{a_i}$ e dunque:

$$G \simeq \mathbb{Z}_{p_1^{a_1}} \times ... \times \mathbb{Z}_{p_t^{a_t}} \simeq \mathbb{Z}_{p_1^{a_1}...p_t^{a_t}} = \mathbb{Z}_m.$$

e quindi la tesi □

4.9 Ogni gruppo finito è isomorfo a un sottogruppo di permutazioni

Teorema 32. *Sia G un gruppo :* $|\ G\ |$ *= n. Allora* $G \simeq H$ *con* $H \leq S_n$.

Dimostrazione. $\forall$ g $\in$ G è definita l'applicazione L_g : G $\longrightarrow$ G x $\longmapsto$ gx. Si vede immediatamente che $\forall$ g $\in$ G L_g è biettiva (se g $\in$ G l'inversa di L_g è $L_{g^{-1}}$). Allora è ben definita l'applicazione:

$$\text{L} : \text{G} \longrightarrow S_G$$

$$\text{g} \longmapsto L_g$$

Osserviamo che L è un omomorfismo. Infatti se x, y $\in$ G allora preso a $\in$ G $L_{xy}(a)$=xy(a)=x(ya)=x($L_y(a)$)=L $\circ$ L_y)(a). Allora per il primo teorema di isomorfismo:

$$\frac{G}{KerL} \simeq \text{L(G)} \leq S_G$$

tuttavia KerL=$\{g \in G : ga = a \forall a \in G\}$=$\{1\}$ quindi:

$$\text{G} \simeq \frac{G}{\{1\}} = \frac{G}{KerL} \simeq \text{L(G)}$$

Sia ora $\Psi : S_G \longrightarrow S_n$ un isomorfismo. Allora:

$$\text{G} \simeq \text{L(G)} \simeq \Psi\text{(L(G))} \leq S_n$$

e quindi la tesi □

4.10 Ogni gruppo finito è isomorfo a un sottogruppo di matrici

Ricordiamo due fatti di algebra lineare:

Lemma 6. *Siano V e W due spazi vettoriali a dimensione finita e f: V* $\longrightarrow$ *W un'applicazione lineare. Allora:*

1. *dim(Imf)=dim(W)* $\iff$ *f è suriettiva*

2. *se dim(V) = dim(W) allora f è biettiva* $\iff$ *f è iniettiva* $\iff$ *f è suriettiva*

Lemma 7. *Sia V uno spazio vettoriale a dimensione finita, B una sua base e f,g : V* $\longrightarrow$ *V applicazioni lineari.Allora:*

$$M_{BB}(f \circ g)=M_{BB}(f)M_{BB}(g)$$

dove $M_{BB}(f)$ *denota la matrice associata ad f rispetto alla base B*

Teorema 33. *Sia G un gruppo :* $\mid G \mid$ *= n e K un campo. Allora G* $\simeq$ *H per qualche H* $\leq$ $GL_n(K)$

Dimostrazione. L'idea è costruire un omomorfismo iniettivo Ψ : G $\longrightarrow$ $GL_n(K)$ di modo che

$$\text{G} \simeq \frac{G}{\{1\}} = \frac{G}{Ker_\Psi} \simeq \Psi(\text{G}) \leq GL_n(K)$$

Per il teorema anteriore possiamo considerare un isomorfismo :

$$\text{L} : \text{G} \longrightarrow S_n$$

Denotiamo con Iso(K^n) lo spazio vettoriale delle applicazioni lineari e invertribili da K^n in se. Definiamo ora l'applicazione:

$$\Phi : S_n \longrightarrow \text{Iso}(K^n)$$

$$\sigma \longmapsto f_\sigma$$

dove, per $\sigma \in S_n$, f_σ è costruita nel seguente modo: Sia B = $\{e_1, ..., e_n\}$ la base canonica di K^n e sia F : B $\longrightarrow$ K^n definita da F(e_i)=$e_{\sigma(i)}$. Per il teorema fondamentale delle applicazioni lineari esiste un unica applicazione lineare f : $K^n \longrightarrow K^n$ tale che la restrizione di f a B coincide con F. Poniamo f = f_σ.Ora per mostarre che Φ è ben definita occore verificare che f_σ sia bigettiva. Effettivamente Imm(f_σ) è un sottospazio vettoriale di K^n che contiene i vettori e_1,...,e_n e quindi dim(f_σ)=n=dim(K^n) quindi f_σ è suriettiva e quindi per il lemma anteriore biettiva. Mostriamo ora che Φ è un omomorfismo iniettivo di gruppi. Infatti se σ e $\tau \in S_n$ si ha che $\forall$ i=1,...,n

$$\Phi(\sigma \circ \tau)(e_i)=e_{(\sigma\circ\tau)(i)}=f_\sigma(e_{\tau(i)})=(f_\sigma \circ f_\tau)(e_i)=(\Phi(\sigma) \circ \Phi(\tau))(e_i)$$

e quindi Φ è un omomorfismo.Osserviamo che Φ è iniettivo dato che se $\sigma \in \text{Ker}\Phi$ allora $e_{\sigma(i)}$=e_i $\forall$ i=1,...,n e quindi $\sigma(i)$=i $\forall$ i=1,...,n da cui $\sigma = 1_{S_n}$. Infine definiamo l'applicazione:

$$\gamma : \text{Iso}(K^n) \longrightarrow GL_n(K)$$

$$\text{f} \longmapsto M_{BB}(\text{f})$$

dove M_{BB}(f) denota la matrice associata a f rispetto alla base canonica B. γ è un omomorfismo iniettivo di gruppi. Infatti prese f,g $\in M_{BB}$(f) si ha che γ(f $\circ$ g) = M_{BB}(f $\circ$ g)=M_{BB}(f)M_{BB}(g)=γ(f)γ(g) ed è iniettiva perchè se γ(f)=γ(g) allora $\forall$ i=1,...,n si ha che f(e_i)=g(e_i) e quindi f=g.Quindi la composizione:

$$\Psi=\gamma \circ \Phi \circ \text{L} : \text{G} \longrightarrow S_n \longrightarrow \text{Iso}(K^n) \longrightarrow GL_n(K)$$

è un omomorfismo iniettivo di gruppi. □

4.11 Un teorema di classificazione per p-gruppi finiti

Teorema 34. *Sia G un gruppo :* $\mid G \mid = p^m$*=n con m,n* $\in \mathbb{N}$ *e p primo.Allora:*

$$G \simeq H$$

per qualche $H \leq U_n^+(\mathbb{Z}_p)$ *dove:*

$$U_n^+(\mathbb{Z}_p) = \{A = (a_{ij}) \in T_n^+(\mathbb{Z}_p) : a_{ii} = [1]_p \forall i = 1, ..., n\}$$

essendo $T_n^+(\mathbb{Z}_p)$ *l'insieme delle matrici n*$\times$*n triangolari superiori a entrate in* $\mathbb{Z}_p$*.*

Dimostrazione. Iniziamo ad osservare che $U_n^+(\mathbb{Z}_p)$ è un sottogruppo di $GL_n(\mathbb{Z}_p)$ in quanto prese A=(a_{ij}) e B=(bij) in $U_n^+(\mathbb{Z}_p)$ si ha che la matrice C=AB è triangolare superiore e dette c_{ij} le sue entrate per ogni i=1,...,n si ha che: c_{ii}=$a_{ii}b_{ii} = [1]_p$.Ora è noto che:

$$\mid GL_n(\mathbb{Z}_p) \mid = p^{\frac{n(n-1)}{2}} \prod_{k=0}^{n-1}(p^{n-k} - 1)$$

con (p,$\prod_{k=0}^{n-1}(p^{n-k} - 1)$)=1.Allora essendo

$$\mid U_n^+(\mathbb{Z}_p) \mid = p^{\frac{n(n-1)}{2}}$$

si ha che $U_n^+(\mathbb{Z}_p)$ è un p-sylow di G.Ora siccome G è finito di ordine n :

$$\text{G} \simeq \text{K}$$

per qualche K $\leq GL_n(\mathbb{Z}_p)$.Osserviamo che K è un p-sottogruppo di $GL_n(\mathbb{Z}_p)$ e quindi $\exists$ S p-sylow di $GL_n(\mathbb{Z}_p)$ tale che:

$$\mathrm{K} \leq \mathrm{S}$$

Ora sia x $\in GL_n(\mathbb{Z}_p)$ tale che:

$$U_n^+(\mathbb{Z}_p) = S^x$$

allora vediamo che

$$U_n^+(\mathbb{Z}_p) \simeq \mathrm{S}$$

Quindi:

$$\mathrm{G} \simeq \mathrm{K} \leq \mathrm{S} \simeq U_n^+(\mathbb{Z}_p)$$

Consideriamo allora due isomorfismi:

$$\mathrm{f} : \mathrm{G} \longrightarrow \mathrm{K}$$

$$\mathrm{g} : \mathrm{S} \longrightarrow U_n^+(\mathbb{Z}_p)$$

L'applicazione:

$$\mathrm{h} : \mathrm{K} \longrightarrow \mathrm{g(K)}$$

$$\mathrm{k} \longmapsto \mathrm{g(k)}$$

è ancora un isomorfismo con g(K) sottogruppo di $U_n^+(\mathbb{Z}_p)$ .Allora la composizione Φ = h $\circ$ f è un isomorfismo tra G è g(K) e quindi si ha la tesi. □

4.12 Gruppi semplici non abeliani di ordine 60

Lemma 8. *Sia G un gruppo finito,semplice e non abeliano e H < G.Allora*

$$|\ G\ |\ |\ [G:H]\ !$$

Dimostrazione. Consideriamo l'insieme così definito :

$$\tfrac{G}{H} := \{gH : g \in G\}$$

G agisce su $\frac{G}{H}$ tramite:

$$\phi : \mathrm{G} \longrightarrow S_{\frac{G}{H}}$$

$$g \longmapsto \phi(g)$$

dove ϕ(g)($\tilde{g}$H)=(g$\tilde{g}$)H.Ora Kerϕ è un sottogruppo normale di G quindi essendo G semplice:

$$\text{Ker}\phi=\{1\} \vee \text{Ker}\phi=G$$

Tuttavia se Kerϕ = G allora preso g ∈ G con g $\neq$ 1 si ottiene che $\forall\ \tilde{g} \in$ G :

$$\phi(g)(\tilde{g}H)=\tilde{g}H$$

e quindi

$$gH=\phi(g)(1H) = 1H = H$$

da cui g ∈ H, e pertanto G=H,assurdo.Allora ϕ è iniettiva e quindi

$$| G | = | \phi(G) | | | S_{\frac{G}{H}} | = [G:H] !$$

□

Corollario 2. *Sia G un gruppo finito,semplice e non abeliano e p un primo tale che p | | G |.Allora:*

$$| G | | n_p !$$

Dimostrazione. Sia P un p-sylow di G.Allora n_p=[G:$N_G(P)$].Quindi se mostro che $N_G(P)$ per il lemma anteriore avremmo finito.Se per assurdo $N_G(P)$ = G allora P è normale in G e quindi P=G, ma allora G è un p-gruppo e quindi non è semplice,assurdo. □

Corollario 3. *I gruppi di ordine 24,36 e 48 non sono semplici e non abeliani.*

Dimostrazione. basta osservare che non soddisfano la proprietà enunciata nel corollario anteriore. □

Teorema 35. *Sia G un gruppo semplice e non abeliano : | G | = 60.Allora:*

$$G \simeq A_5$$

Dimostrazione. Iniziamo a mostrare che esiste H $\leq$ G : [G:H]=5.Abbiamo che | G | = 2^2·15.Ora $n_2 \in \{1, 3, 5, 15\}$ tuttavia per la semplicità non può capitare che n_2=1 inoltre se n_2=3 allora 60 divide 3! che è assurdo.Supponiamo per assurdo che n_2=15.Abbiamo che n_3=10 e n_5=6.Quindi ci sono 20 elementi di ordine 3 e 24 elementi di ordine 5.Siano H_1,...,H_{15} i 2-sylow di G.Osserviamo che $\forall$ i $\neq$ j si ha che | $H_i \cap H_j$ | $\geq$ 2.Allora ci sono almeno 30 elementi di ordine 2.Quindi:

$$| \text{G} | \geq 1+20+24+30=75$$

assurdo.Quindi n_2=5 da cui [G:$N_G(S)$]=5 per qualche 2-sylow S.Quindi sia H < G tale che [G:H]=5. Ora G / H (come insieme) avrà la forma :

$$\text{G / H} = \{g_1H, ..., g_5H\}$$

G agisce su G / H tramite:

$$\phi : \text{G} \longrightarrow S_{G/H}$$

$$\text{g} \longmapsto \phi(g)$$

dove $\phi(g)(g_iH)$=(gg_i)H i=1,...,5.Ragionando come nel corollario anteriore si ottiene che ϕ è iniettiva.Allora:

$$\tilde{\phi} : \text{G} \longrightarrow \phi(G)$$

$$\text{g} \longmapsto \phi(g)$$

è un isomorfismo.Sia ora:

$$\psi : S_{G/H} \longrightarrow S_5$$

un isomorfismo.Allora:

$$\tilde{\psi} : \phi(G) \longrightarrow \psi(\phi(G))$$

$$\text{a} \longmapsto \psi(a)$$

è un isomorfismo.Pertanto G $\simeq \psi(\phi(G))$ tramite $\tilde{\psi} \circ \tilde{\phi}$.Ora $\psi(\phi(G))$ è un sottogruppo di S_5 di ordine 60.Se mostro che $\psi(\phi(G))$ è contenuto in A_5 abbiamo finito.Consideriamo l'omomorfismo:

$$\text{sgn} : \psi(\phi(G)) \longrightarrow \{1, -1\}$$

$$\rho \longmapsto \text{sgn}(\rho)$$

Siccome $\psi(\phi(G))$ è semplice Ker(sgn)=$\psi(\phi(G))$ oppure Ker(sgn)=$\{1\}$:Tuttavia la funzione sgn non è iniettiva quindi Ker(sgn)=$\psi(\phi(G))$, consegue che $\forall$ x $\in \psi(\phi(G))$ sgn(x)=1 e quindi $\psi(\phi(G))$ è contenuto in A_5, segue la tesi. □

Lemma 9. *Sia p un primo tale che 2^p-1 è primo . Se G è un gruppo : | G | = 2^p(2^p-1) allora G non è semplice.*

Dimostrazione. Sia q=2^p-1.Abbiamo che n_q divide 2^p e n_q=1+(2^p-1)k per qualche naturale k.Quindi n_q=1 o n_q=2^p.Supponiamo per assurdo che n_q=2^p.Siano H_1,...,H_{2^p} i q-sylow di G. Essi hanno ordine q che è primo quindi hanno intersezione banale.Quindi se n è il numero di elementi di G di ordine q:

$$n=(q-1)2^p=|G| - 2^p$$

quindi | G | = n + 2^p. Pertanto n_2 = 1 e quindi G non è semplice. □

Teorema 36. *A_5 è (a meno di isomorfismo) il più piccolo gruppo semplice e non abeliano.*

Dimostrazione. Sappiamo che A_5 è semplice e non abeliano e ha ordine 60 (e , a meno di isomorfismo,è l'unico ad avere queste proprietà).Sia G un gruppo finito semplice e non abeliano dobbiamo mostrare che il suo ordine è maggiore o uguale a 60.

- Vediamo immediatamente che | G | non stà nell'insieme

  $$\{1, 2, 3, 4, 5, 7, 9, 11, 13, 15, 17, 19, 23, 29, 31, 33, 35, 37, 41, 43, 45, 47, 51, 53, 59\}$$

  perchè in tal caso sarebbe abeliano.

- Inoltre | G | $\notin \{8, 16, 25, 32, 49, 27\}$ perchè in tal caso G sarebbe un p-gruppo non abeliano e quindi non sarebbe semplice

- Inoltre G | $\notin \{6, 10, 14, 18, 20, 21, 22, 26, 28, 34, 38, 39, 42, 44, 46, 50, 52, 54, 55, 57, 58\}$ dato che in tal caso l'ordine di G sarebbe della forma $p^k m$ con p primo e m un naturale tali che 0<m<p e quindi non sarebbe semplice.

Rimane da dimostrare che | G | $\notin \{12, 24, 30, 36, 40, 48, 56\}$.

- Dal lemma 9 | G | $\notin \{12, 56\}$

- Inoltre G non può avere ordine 40 perchè i gruppi di ordine 40 ammettono un sotto-gruppo normale di ordine 5

- Per il corollario 3 G non può avere ordine 24,36 e 48

Rimane da mostrare che G non può avere ordine 30. Supponiamo per assurdo che | G | = 30=2·3·5.Siccome G è semplice avremmo che n_3=10 e n_5=6.Siccome 3 e 5 sono primi il numero di elementi di ordine 3 sarebbe 20 mentre quello di ordine 5 sarebbe 24, quindi | G | $\geq$ 44, assurdo.Quindi | G | $\geq$ 60. □

Capitolo 5

Classificazione dei gruppi di ordine n < 32

5.1 Gruppi di ordine 2,3,5,7,11,13,17,19,23,29,31

Siccome 2,3,5,7,11,13,17,19 sono numeri primi se G è un gruppo:

- $|G| = 2$ allora $G \simeq \mathbb{Z}_2$
- $|G| = 3$ allora $G \simeq \mathbb{Z}_3$
- $|G| = 5$ allora $G \simeq \mathbb{Z}_5$
- $|G| = 7$ allora $G \simeq \mathbb{Z}_7$
- $|G| = 11$ allora $G \simeq \mathbb{Z}_{11}$
- $|G| = 13$ allora $G \simeq \mathbb{Z}_{13}$
- $|G| = 17$ allora $G \simeq \mathbb{Z}_{17}$
- $|G| = 19$ allora $G \simeq \mathbb{Z}_{19}$
- $|G| = 23$ allora $G \simeq \mathbb{Z}_{23}$
- $|G| = 29$ allora $G \simeq \mathbb{Z}_{29}$
- $|G| = 31$ allora $G \simeq \mathbb{Z}_{31}$

5.2 Gruppi di ordine 6,10,14,22,26

Per il teorema sui gruppi di ordine 2p con primo risulta che se G è un gruppo tale che:

- $|\,G\,| = 6$ allora $G \simeq \mathbb{Z}_6 \vee G \simeq D_3 \simeq S_3$
- $|\,G\,| = 10$ allora $G \simeq \mathbb{Z}_{10} \vee G \simeq D_5$
- $|\,G\,| = 14$ allora $G \simeq \mathbb{Z}_{14} \vee G \simeq D_7$
- $|\,G\,| = 22$ allora $G \simeq \mathbb{Z}_{22} \vee G \simeq D_{11}$
- $|\,G\,| = 26$ allora $G \simeq \mathbb{Z}_{26} \vee G \simeq D_{13}$

5.3 Gruppi di ordine 4,9,25

Per la classificazione dei gruppi di ordine p^2 con p primo risulta che se G è un gruppo tale che:

- $|\,G\,| = 4$ allora $G \simeq \mathbb{Z}_4 \vee G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$
- $|\,G\,| = 9$ allora $G \simeq \mathbb{Z}_9 \vee G \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$
- $|\,G\,| = 25$ allora $G \simeq \mathbb{Z}_{25} \vee G \simeq \mathbb{Z}_5 \times \mathbb{Z}_5$

5.4 Gruppi di ordine 8

Prima di vedere il teorema di classificazione per i gruppi di ordine 8 osserviamo il seguente fatto:

Osservazione 13. *Quanti prodotti semidiretti ci sono tra $\mathbb{Z}_4$ e $\mathbb{Z}_2$? Per rispondere alla domanda dobbiamo capire chi sono gli omomorfismi tra $\mathbb{Z}_2$ e Aut($\mathbb{Z}_4$). Siccome Aut($\mathbb{Z}_4$) ha solamente due elementi (perchè è isomorfo a $\mathbb{Z}_2$) abbiamo solamente due omomorfismi possibili.Uno sarà quello banale che indurrà il prodotto diretto tra $\mathbb{Z}_4$ e $\mathbb{Z}_2$ e quindi sarà abeliano, mentre l'altro non sarà banale,chiamiamolo ϕ_1 e quindi il prodotto semidiretto da esso indotto $\mathbb{Z}_4 \rtimes_{\phi_1} \mathbb{Z}_2$ non sarà abeliano.Quindi ci sono solo due prodotti semidiretti tra $\mathbb{Z}_4$ e $\mathbb{Z}_2$ ed essi sono non isomorfi.*

Teorema 37. *Sia G un gruppo tale che $|\,G\,| = 8$ allora:*

$G \simeq \mathbb{Z}_8 \vee G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2 \vee G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \vee G \simeq D_4 \vee G \simeq Q_8$.

Dimostrazione. Se $\exists$ x $\in$ G : o(x)=8 allora G = <x> $\simeq \mathbb{Z}_8$, supponiamo quindi che non esista x in G di ordine 8.Allora ci sono due possibilità:

1. $\forall$ x $\in$ G o(x)=2.

   Se tutti gli elementi di G hanno ordine 2 significa che G è abeliano.Siano quindi a,b $\in$ G $\setminus \{1_G\}$ con a $\neq$ b.Allora <a,b> $\triangleleft$ G (perchè G è abeliano) e <a,b> $\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ (perchè ha ordine 4 con almeno due elementi di ordine 2).Sia ora c $\in$ G $\setminus$ <a,b> (esiste perchè G ha ordine 8 e <a,b> ordine 4).Allora <c> $\triangleleft$ G e <c> $\simeq \mathbb{Z}_2$.Ora <a,b> $\cap$ <c> si intersecano banalmente (perchè c non appartiene a <a,b>) quindi deduciamo anche che G = <a,b><c> ma allora per il teorema prodotto si ha immediatamente che: G $\simeq$ <a,b> $\times$ <c> $\simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

2. $\exists$ x $\in$ G : o(x)=4

   Sia quindi a $\in$ G . o(a)=4.Distinguiamo due sottocasi:

   - $\exists$ y $\in$ G $\setminus$ <a> : o(y)=2. Sia allora b $\in$ G $\setminus$ <a> di ordine 2. Allora essendo <a> normale in G, <a> $\cap$ <b> = $\{1_G\}$ deduciamo che:

     $$G \simeq \langle a \rangle \rtimes_\phi \langle b \rangle$$

     per un certo omomorfismo ϕ da <b> in Aut(<a>).Quindi:

     $$G \simeq \mathbb{Z}_4 \rtimes_\Psi \mathbb{Z}_2$$

     Se Ψ è l'omomorfismo banale allora G $\simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ se Ψ non è l'omomorfismo banale allora G $\simeq \mathbb{Z}_4 \rtimes_{\phi_1} \mathbb{Z}_2$.

   - $\forall$ x $\in$ G $\setminus$ <a> o(x)=4. Sia b $\in$ G $\setminus$ <a> di ordine 4. Chiaramente G=<a,b>.Vediamo che $bab^{-1}=a^{-1}$.Effettivamente ba $\in \{ab, a^2b, a^3b\}$ (poichè ba $\in$ G=<a,b>=<a><b>e quindi $ba=a^ib^j$ e se per assurdo j= 0 allora ba $\in$ <a> e quindi b $\in$ <a>,che è assurdo).Tuttavia ba $\neq$ ab e ba $\neq a^2b$ infatti se ba=ab allora G è abeliano e quindi $(a^3b)^2=a^6b^2=a^8=1_G$ (dove abbiamo utilizzato il fatto che essendo a^2 l'unico elemento di ordine 2 di G e $o(b^2)=2$ allora $a^2=b^2$) che è assurdo perchè a^3b ha ordine 4.Infine se per assurdo $ba=a^2b$ allora $ba=b^3$ da cui a = b^2,assurdo perche a ha ordine 4 e b^2 ha ordine 2.Allora si deduce che G $\simeq Q_8$.

Pertanto se G è un gruppo di ordine 8 è,isomorfo ad uno dei seguenti gruppi:

$G \simeq \mathbb{Z}_8 \vee G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2 \vee G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \vee G \simeq \mathbb{Z}_4 \rtimes_{\phi_1} \mathbb{Z}_2 \vee G \simeq Q_8$. Ora D_4 è un gruppo di ordine 8 non abeliano che non può essere isomorfo a Q_8 (perchè D_4 ha solo due elementi di ordine 4 mentre Q_8 ne ha almeno 3) quindi $D_4 \simeq \mathbb{Z}_4 \rtimes_{\phi_1} \mathbb{Z}_2$, segue l'asserto.

□

5.5 Gruppi di ordine 12

Lemma 10. *Sia $\Phi \in$ Hom($\mathbb{Z}_3$,Aut($\mathbb{Z}_4$)) allora $\mathbb{Z}_4 \rtimes_\Phi \mathbb{Z}_3 = \mathbb{Z}_4 \times \mathbb{Z}_3$.*

Dimostrazione. Essendo Φ un omomorfismo o(Φ (1)) deve dividere o(1)=3 e siccome in Aut($\mathbb{Z}_4$) non ci sono elementi di ordine 3 l'unica possibilità è che o(Φ(1))=1 e cioè che $\Phi(1)=Id_{\mathbb{Z}_4}$ quindi deduciamo che Φ è l'omomorfismo banale. □

Lemma 11. *Aut($\mathbb{Z}_2 \times \mathbb{Z}_2$) $\simeq S_3$*

Dimostrazione. Basta osservare che Aut($\mathbb{Z}_2 \times \mathbb{Z}_2$) ha ordine 6 ed è non abeliano, quindi possiamo applicare il teorema di classificazione per gruppi di ordine 6. □

Lemma 12. *$\forall \Psi \in$ Hom($\mathbb{Z}_3$,Aut($\mathbb{Z}_2 \times \mathbb{Z}_2$)) non banale, si ha che ($\mathbb{Z}_2 \times \mathbb{Z}_2$) $\rtimes_\Psi \mathbb{Z}_3 \simeq A_4$.*

Dimostrazione. Sia $\Psi \in$ Hom($\mathbb{Z}_3$,Aut($\mathbb{Z}_2 \times \mathbb{Z}_2$)) non banale ,mostriamo che ($\mathbb{Z}_2 \times \mathbb{Z}_2$) $\rtimes_\Psi$ $\mathbb{Z}_3 \simeq A_4$.Osserviamo che

$$A_4 \simeq K \rtimes_\beta \langle(123)\rangle$$

dove K=$\{Id, (12)(34), (13)(24), (14)(23)\}$ e β è un qualche omomorfismo da <(123)> a Aut(K). Ora essendo K $\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ e <(123)> $\simeq \mathbb{Z}_3$, $A_4 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\alpha \mathbb{Z}_3$ per qualche α $\in$ Hom($\mathbb{Z}_3$,Aut($\mathbb{Z}_2 \times \mathbb{Z}_2$)) non banale (perchè A_4 è non abeliano). Quindi per mostrare il lemma è sufficiente dimostrare che se $\Phi,\Gamma \in$ Hom($\mathbb{Z}_3$,Aut($\mathbb{Z}_2 \times \mathbb{Z}_2$)) non banali allora ($\mathbb{Z}_2$ $\times \mathbb{Z}_2$) $\rtimes_\Phi \mathbb{Z}_3 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\Gamma \mathbb{Z}_3$.Consideriamo un isomorfismo

$$\Omega : S_3 \longrightarrow \text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$$

Allora l'applicazione:

$$F: \text{Hom}(\mathbb{Z}_3,S_3) \longrightarrow \text{Hom}(\mathbb{Z}_3,\text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2))$$

$$\phi \longmapsto \Omega \circ \phi$$

è una bigezione.Quindi | Hom($\mathbb{Z}_3$,S_3) | = | Hom($\mathbb{Z}_3$,Aut($\mathbb{Z}_2 \times \mathbb{Z}_2$)) |.Contiamo gli omomorfismi non banali da $\mathbb{Z}_3$ a S_3. Un generico omomorfismo non banale da $\mathbb{Z}_3$ a S_3 è univocamente determinato da dove mappa $[1]_3$. L'ordine dell'immagine di $[1]_3$ deve dividere 3,siccome in S_3 gli elementi hanno ordine 1,2 e 3 deduciamo che l'ordine dell'immagine di $[1]_3$ è 3 quindi gli omomorfismi non banali da $\mathbb{Z}_3$ a S_3 sono:

$$\phi_1 \colon \mathbb{Z}_3 \longrightarrow S_3$$

$$[1]_3 \longmapsto (123)$$

e

$$\phi_2 \colon \mathbb{Z}_3 \longrightarrow S_3$$

$$[1]_3 \longmapsto (132)$$

Quindi gli omomorfismi non banali da $\mathbb{Z}_3$ a Aut($\mathbb{Z}_2 \times \mathbb{Z}_2$) sono F ($\phi_1$) e F($\phi_2$).Vogliamo mostrare che $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{F(\phi_1)} \mathbb{Z}_3 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{F(\phi_2)} \mathbb{Z}_3$. Definiamo l'applicazione:

$$f \colon \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$$

$$[1]_3 \longmapsto [2]_3$$

f è un isomorfismo e $\phi_2 = \phi_1 \circ f$. Allora:

$$F(\phi_2) = \Omega \circ \phi_2 = \Omega \circ \phi_1 \circ f = F(\phi_1) \circ f.$$

Consegue:

$$(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{F(\phi_1)} \mathbb{Z}_3 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{F(\phi_2)} \mathbb{Z}_3$$

e quindi si ha la tesi. □

Esempio 5. *Studiamo adesso i prodotti semidiretti tra $\mathbb{Z}_3$ e $\mathbb{Z}_4$. Iniziamo a capire quanti sono gli omomorfismi tra $\mathbb{Z}_4$ e Aut($\mathbb{Z}_3$). Siccome Aut($\mathbb{Z}_3$) è isomorfo a $\mathbb{Z}_2$ abbiamo solamente due omomorfismi possibili: quello banale, che determina il prodotto diretto $\mathbb{Z}_3 \times \mathbb{Z}_4$ e quello che manda 1 nell'unico elemento di ordine 2 in Aut($\mathbb{Z}_3$) e cioè l'omomorfismo:*

$$\Psi \colon \mathbb{Z}_4 \longrightarrow Aut(\mathbb{Z}_3)$$

dove

$$\Psi([1]_4) \colon \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$$

$$[1]_3 \longmapsto [2]_3$$

Lemma 13. *$\forall\ \Psi \in Hom(\mathbb{Z}_2 \times \mathbb{Z}_2, Aut(\mathbb{Z}_3))$ non banale, si ha che $\mathbb{Z}_3 \rtimes_\Psi (\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq D_6$.*

Dimostrazione. Sia $\Psi \in$ Hom($\mathbb{Z}_2 \times \mathbb{Z}_2$,Aut($\mathbb{Z}_3$)) non banale.Osserviamo che:

$$\mathrm{D}_6 \simeq \{Id, r^2, r^4\} \rtimes_\gamma \{Id, s, r^3, r^3 s\}$$

per qualche omomorfismo $\gamma : \{Id, s, r^3, r^3 s\} \longrightarrow$ Aut($\{Id, r^2, r^4\}$). Infatti

$$\{Id, s, r^3, r^3 s\} \leq \mathrm{D}_6, \{Id, r^2, r^4\} \lhd \mathrm{D}_6,\ \{Id, s, r^3, r^3 s\} \cap \{Id, r^2, r^4\} = \{Id\}$$

Tuttavia:

$$\{Id, s, r^3, r^3 s\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \text{ e } \{Id, r^2, r^4\} \simeq \mathbb{Z}_3$$

consegue che esiste un omomorfismo non banale Φ: $\mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow$ Aut($\mathbb{Z}_3$) tale che:

$$\mathrm{D}_6 \simeq \mathbb{Z}_3 \rtimes_\Phi (\mathbb{Z}_2 \times \mathbb{Z}_2)$$

Pertanto per provare il lemma è sufficiente dimostrare che comunque scelti f,g $\in$ Hom($\mathbb{Z}_2$ $\times$ $\mathbb{Z}_2$,Aut($\mathbb{Z}_3$)) non banali si ha che:

$$\mathbb{Z}_3 \rtimes_f (\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_3 \rtimes_g (\mathbb{Z}_2 \times \mathbb{Z}_2)$$

Sia

$$\Omega\text{: } \mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

un isomorfismo. L'applicazione:

$$\text{F: Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2\ ) \longrightarrow \text{Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2, \text{Aut}(\mathbb{Z}_3))$$

$$\phi \longmapsto \Omega \circ \phi$$

è una bigezione.Quindi:

$$|\ \text{Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2\ )\ | = |\ \text{Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2, \text{Aut}(\mathbb{Z}_3))\ |$$

Adesso, gli omomorfismi non banali tra $\mathbb{Z}_2 \times \mathbb{Z}_2$ e $\mathbb{Z}_2$ sono ϕ_1,ϕ_2 e ϕ_3 completamente determinati da:

- $\phi_1([1]_2,[0]_2)=[0]_2$ e $\phi_1([0]_2,[1]_2)=[1]_2$
- $\phi_2([1]_2,[0]_2)=[1]_2$ e $\phi_2([0]_2,[1]_2)=[0]_2$
- $\phi_3([1]_2,[0]_2)=[1]_2$ e $\phi_3([0]_2,[1]_2)=[1]_2$

Consideriamo ora le applicazioni h_1,$h_2 : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ definite da:

- $h_1([1]_2,[0]_2)=([0]_2,[1]_2)$ e $h_1([0]_2,[1]_2)=([1]_2,[0]_2)$
- $h_2([1]_2,[0]_2)=([1]_2,[1]_2)$ e $h_2([0]_2,[1]_2)=([1]_2,[0]_2)$

h_1 e h_2 sono isomorfismi tali che:

$$\phi_2=\phi_1 \circ h_1 \text{ e } \phi_3=\phi_2 \circ h_2$$

Ora tutti e soli gli omomorfismi non banali da $\mathbb{Z}_2 \times \mathbb{Z}_2$ a Aut($\mathbb{Z}_3$) sono F(ϕ_1),F(ϕ_2) e F(ϕ_3) e sono tali che:

$$F(\phi_2)=\Omega \circ \phi_2 = \Omega \circ \phi_1 \circ h_1=F(\phi_1) \circ h_1$$

$$F(\phi_3)=\Omega \circ \phi_3 = \Omega \circ \phi_2 \circ h_2=F(\phi_2) \circ h_2$$

Consegue:

$$\mathbb{Z}_3 \rtimes_{F(\phi_1)} (\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_3 \rtimes_{F(\phi_2)} (\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_3 \rtimes_{F(\phi_3)} (\mathbb{Z}_2 \times \mathbb{Z}_2)$$

e quindi la tesi. □

Siamo pronti per il seguente:

Teorema 38. *Sia G un gruppo :* $|G| = 12$. *Allora:*

$G \simeq \mathbb{Z}_{12} \vee G \simeq \mathbb{Z}_2 \times \mathbb{Z}_6 \vee G \simeq A_4 \vee G \simeq D_6 \vee G \simeq \mathbb{Z}_3 \rtimes_\Psi \mathbb{Z}_4$

dove

$$\Psi: \mathbb{Z}_4 \longrightarrow Aut(\mathbb{Z}_3)$$

con $\Psi([1]_4): \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$, $[1]_3 \longmapsto [2]_3$.

Dimostrazione. Abbiamo $|G| = 12 = 2^2 3$. Allora $n_2 \mid 3$ e quindi n_2=1 o n_2=3.Similmente n_3=1 o n_3=4.Osserviamo che uno tra n_2 e n_3 vale 1.Effettivamente se $n_3 \neq 1$ allora $n_3 = 4$ e quindi,siccome tutti i 3-sylow si intersecano banalmente, ci sono 8 elementi di ordine 3.I restanti elementi possono formare un solo 2-sylow e quindi n_2=1.Distinguiamo i vari casi.

- n_2=1 e n_3=1.

  Siano P_2 il 2-sylow di G e P_3 il tre sylow di G .Entrambi sono normali, $|P_2| = 4$ e $|P_3| = 3$.Per il teorema numerico si ha immediatamente che:

$$G \simeq P_2 \times P_3$$

quindi:

$$G \simeq \mathbb{Z}_4 \times \mathbb{Z}_3 \simeq \mathbb{Z}_{12} \text{ o } G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_2 \simeq \mathbb{Z}_6.$$

- n_2=1 e n_3=4.

  Siano P_2 il 2-sylow di G (normale)e P_3 un tre sylow di G. Siccome P_2 e P_3 si intersecano banalmente si ha che:

  $$G \simeq P_2 \rtimes_\phi P_3$$

  per un qualche $\phi : P_3 \longrightarrow \text{Aut}(P_2)$ omomorfismo.Siccome $|P_2|$ = 4 abbiamo due sottocasi:

  1. $P_2 \simeq \mathbb{Z}_4$ e quindi G sarebbe isomorfo un prodotto semidiretto tra $\mathbb{Z}_4$ e $\mathbb{Z}_3$ e quindi abeliano,ma questo è assurdo perchè implicherebbe n_3=1.
  2. $P_2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ allora G sarebbe isomorfo a un prodotto semidiretto (determinato da un omomorfismo non banale non essendo G abeliano) tra $\mathbb{Z}_2 \times \mathbb{Z}_2$ e $\mathbb{Z}_3$ e quindi isomorfo ad A_4

- n_2=3 e n_3=1

  Sia allora P_3 il 3-sylow di G (normale) e P_2 un 2-sylow di G.Siccome P_2 e P_3 si intersecano banalmente si ha che:

  $$G \simeq P_3 \rtimes_\gamma P_2$$

  per un qualche $\gamma : P_2 \longrightarrow \text{Aut}(P_3)$ omomorfismo.Siccome $|P_2|$ = 4 abbiamo due sottocasi:

  1. $P_2 \simeq \mathbb{Z}_4$ e quindi G sarebbe un prodotto semidiretto tra $\mathbb{Z}_3$ e $\mathbb{Z}_4$.Siccome G non è abeliano l'unica possibilità è che $G \simeq \mathbb{Z}_3 \rtimes_\Psi \mathbb{Z}_4$ dove

     $$\Psi\colon \mathbb{Z}_4 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

     con

con $\Psi([1]_4)$: $\mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$, $[1]_3 \longmapsto [2]_3$.

2. $P_2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Allora G è isomorfo a un prodotto semidiretto (determinato da un omomorfismo non banale non essendo G abeliano) tra $\mathbb{Z}_3$ e $(\mathbb{Z}_2 \times \mathbb{Z}_2)$ e quindi $G \simeq D_6$.

quindi il teorema è dimostrato. □

Osservazione 14. *Si osservi che i gruppi $\mathbb{Z}_{12}$ e $\mathbb{Z}_2 \times \mathbb{Z}_6$ sono abeliani non isomorfi (il primo ha un elemento di ordine 12, il secondo no) mentre i gruppi A_4, D_6 e $\mathbb{Z}_3 \rtimes_\Psi \mathbb{Z}_4$ sono non abeliani e non isomorfi tra loro. In effetti A_4 ha 3 elementi di ordine 2, D_6 invece ha 7 elementi di ordine 2 mentre $\mathbb{Z}_3 \rtimes_\Psi \mathbb{Z}_4$ ha 2 elementi di ordine 2. Quindi tutti i gruppi del teorema anteriore sono non isomorfi.*

5.6 Gruppi di ordine 15

Se G è un gruppo di ordine 15 allora $G \simeq \mathbb{Z}_{15}$. Infatti $15 = 5 \cdot 3$ con 3 e 5 primi tali che 3 non divide (5-1) e quindi $G \simeq \mathbb{Z}_{15}$.

5.7 Gruppi di ordine 16

Lemma 14. *Siano Φ e $\Psi \in Hom(\mathbb{Z}_4, Aut(\mathbb{Z}_2 \times \mathbb{Z}_2))$ non banali, allora:*

$$(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\Phi \mathbb{Z}_4 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\Psi \mathbb{Z}_4.$$

Dimostrazione. Osserviamo che: $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) = \{Id, \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5\}$ dove le γ_i,i=1,...,5 sono definite da:

- $\gamma_1([1]_2, [0]_2) = ([1]_2, [0]_2)$ e $\gamma_1([0]_2, [1]_2) = ([1]_2, [1]_2)$
- $\gamma_2([1]_2, [0]_2) = ([0]_2, [1]_2)$ e $\gamma_2([0]_2, [1]_2) = ([1]_2, [0]_2)$
- $\gamma_3([1]_2, [0]_2) = ([1]_2, [1]_2)$ e $\gamma_3([0]_2, [1]_2) = ([0]_2, [1]_2)$
- $\gamma_4([1]_2, [0]_2) = ([0]_2, [1]_2)$ e $\gamma_4([0]_2, [1]_2) = ([1]_2, [1]_2)$
- $\gamma_5([1]_2, [0]_2) = ([1]_2, [1]_2)$ e $\gamma_5([0]_2, [1]_2) = ([1]_2, [0]_2)$

Gli elementi di ordine 2 di Aut($\mathbb{Z}_2 \times \mathbb{Z}_2$) sono γ_1,γ_2 e γ_3,Deduciamo che gli omomorfismi non banali da $\mathbb{Z}_4$ a Aut($\mathbb{Z}_2 \times \mathbb{Z}_2$) sono:

$$\Phi_i\colon \mathbb{Z}_4 \longrightarrow \text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$$

$$[1]_4 \longmapsto \gamma_i$$

con i=1,2,3.Vogliamo dunque dimostrare che:

$$(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Phi_1} \mathbb{Z}_4 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Phi_2} \mathbb{Z}_4 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Phi_3} \mathbb{Z}_4$$

Osserviamo che per ogni x in $\mathbb{Z}_4$ si ha che:

$$\Phi_2(x)=\gamma_3 \circ \Phi_1(x) \circ {\gamma_3}^{-1}$$

Consegue:

$$(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Phi_1} \mathbb{Z}_4 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Phi_2} \mathbb{Z}_4$$

Similmente per ogni x in $\mathbb{Z}_4$ si ha che:

$$\Phi_3(x)=\gamma_1 \circ \Phi_2(x) \circ {\gamma_1}^{-1}$$

e quindi

$$(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Phi_3} \mathbb{Z}_4 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Phi_2} \mathbb{Z}_4$$

segue l'asserto. □

Lemma 15. *C'è un solo prodotto semidiretto non banale tra $\mathbb{Z}_4$ e $\mathbb{Z}_4$*

Dimostrazione. Basta osservare che Aut($\mathbb{Z}_4$) $\simeq \mathbb{Z}_2$. □

Osservazione 15. *Osserviamo che il prodotto semidiretto non banale tra $\mathbb{Z}_4$ e $\mathbb{Z}_4$ è $\mathbb{Z}_4 \rtimes_f \mathbb{Z}_4$ dove*

$$f\colon \mathbb{Z}_4 \longrightarrow Aut(\mathbb{Z}_4)$$

con

$$dove\ f([1]_4)([1]_4)=[3]_4$$

Lemma 16. *Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) $\simeq D_4$*

Dimostrazione. Iniziamo ad osservare che Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) ha 8 elementi. In effetti il generatore $([0]_4, [1]_2)$ può essere mappato, da un isomorfismo $\phi \in$ Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$), solamente in $([0]_4, [1]_2)$ e $([2]_4, [1]_2)$ mentre il generatore $([1]_4, [0]_2)$ in $([1]_4, [0]_2)$, $([1]_4, [1]_2)$,$([3]_4, [0]_2)$ e $([3]_4, [1]_2)$. Inoltre Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) non è abeliano, ad esempio:

$$\phi_1 : \mathbb{Z}_4 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \times \mathbb{Z}_2$$

$$([0]_4, [1]_2) \longmapsto ([0]_4, [1]_2)$$

$$([1]_4, [0]_2) \longmapsto ([1]_4, [1]_2)$$

e

$$\phi_2 : \mathbb{Z}_4 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \times \mathbb{Z}_2$$

$$([0]_4, [1]_2) \longmapsto ([2]_4, [1]_2)$$

$$([1]_4, [0]_2) \longmapsto ([3]_4, [0]_2)$$

sono tali che :

$$(\phi_1 \circ \phi_2)([1]_4, [0]_2)=([3]_4, [1]_2)$$

e

$$(\phi_2 \circ \phi_1)([1]_4, [0]_2)=([2]_4, [1]_2)$$

quindi Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) non è abeliano. Quindi Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) $\simeq Q_8 \vee$ Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) $\simeq D_4$.Tuttavia Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) non può essre isomorfo a Q_8. Infatti in Q_8 c'è un solo elemento di ordine 2 mentre in Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) gli elementi:

$$\psi_1 : \mathbb{Z}_4 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \times \mathbb{Z}_2$$

$$([0]_4, [1]_2) \longmapsto ([0]_4, [1]_2)$$

$$([1]_4, [0]_2) \longmapsto ([3]_4, [1]_2)$$

e

$$\psi_2 : \mathbb{Z}_4 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \times \mathbb{Z}_2$$

$$([0]_4, [1]_2) \longmapsto ([2]_4, [1]_2)$$

$$([1]_4, [0]_2) \longmapsto ([3]_4, [0]_2)$$

hanno ordine 2. Quindi Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) $\simeq D_4$.

□

Lemma 17. *A meno di isomorfismo ci sono due soli prodotti semidiretti non banali tra* $\mathbb{Z}_4 \times \mathbb{Z}_2$ *e* $\mathbb{Z}_2$.

Dimostrazione. Sia

$$\Gamma : D_4 \longrightarrow \text{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_2)$$

un isomorfismo. L'applicazione

$$\Phi : \text{Hom}(\mathbb{Z}_2, D_4) \longrightarrow \text{Hom}(\mathbb{Z}_2, \text{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_2))$$

$$\phi \longmapsto \Gamma \circ \phi$$

è bigettiva.Quindi il numero di omomorfismi non banali tra $\mathbb{Z}_2$ e Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) coincide con il numero di omomorfismi non banali tra $\mathbb{Z}_2$ e D_4.Gli elementi di ordine 2 in D_4 sono s,r^2,sr,sr^2 e sr^3.Deduciamo che gli omomorfismi non banali tra $\mathbb{Z}_2$ e D_4 sono ψ_1,ψ_2,ψ_3,ψ_4,ψ_5 definiti da:

- $\psi_1([1]_2)$=s
- $\psi_2([1]_2)$=r^2
- $\psi_3([1]_2)$=sr
- $\psi_4([1]_2)$=sr^2
- $\psi_5([1]_2)$=sr^3

e quindi gli omomorfismi non banali tra $\mathbb{Z}_2$ e Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) sono ϕ_i=$\Phi(\psi_i)$ per i=1,...,5.Osserviamo che fissati i,j in $\{1, ..., 5\}$ se trovo k in D_4 tale che:

$$\text{k}\psi_i([1]_2)\text{k}^{-1} = \psi_j([1]_2)$$

allora applicando ambo i membri Γ si ottiene che esiste $\alpha \in$ Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) tale che $\forall$ x $\in$ $\mathbb{Z}_2$:

$$\alpha \circ \phi_i(\text{x}) \circ \alpha^{-1} = \phi_j(\text{x})$$

e quindi:

$$(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\phi_i} \mathbb{Z}_2 \simeq (\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\phi_j} \mathbb{Z}_2$$

Allora essendo:

- $rsr^{-1} = sr^2$ si ha: $(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\phi_1} \mathbb{Z}_2 \simeq (\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\phi_4} \mathbb{Z}_2$
- $(r^2s)(sr^3)(r^2s)^{-1}$ si ha $(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\phi_5} \mathbb{Z}_2 \simeq (\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\phi_3} \mathbb{Z}_2$
- $(rs)(sr^2)(rs)^{-1}=sr$ si ha $(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\phi_4} \mathbb{Z}_2 \simeq (\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\phi_3} \mathbb{Z}_2$

quindi:

$$(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\phi_1} \mathbb{Z}_2 \simeq (\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\phi_4} \mathbb{Z}_2$$

$$\simeq (\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\phi_3} \mathbb{Z}_2 \simeq (\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\phi_5} \mathbb{Z}_2$$

deduciamo che a meno di isomorfismo ci sono $n \leq 2$ prodotti semidiretti non banali tra $\mathbb{Z}_4 \times \mathbb{Z}_2$ e $\mathbb{Z}_2$. Ora siano Γ_1 e Γ_2 in Hom($\mathbb{Z}_2$,Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$)) così definiti:

$$\Gamma_1([1]_2)=\alpha \text{ e } \Gamma_2([1]_2)=\beta$$

dove

$$\alpha(([1]_4, [0]_2)) = ([1]_4, [0]_2) \text{ e } \alpha(([0]_4, [1]_2)) = ([2]_4, [1]_2)$$

e

$$\beta(([1]_4, [0]_2)) = ([3]_4, [0]_2) \text{ e } \beta(([0]_4, [1]_2)) = ([2]_4, [1]_2)$$

è immediato verificare che $(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\Gamma_1} \mathbb{Z}_2$ ha 7 elementi di ordine 2 mentre $(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\Gamma_2} \mathbb{Z}_2$ ha 11 elementi di ordine 2,quindi si ha la tesi.

□

Lemma 18. *Ci sono 3 prodotti semidiretti non banali tra $\mathbb{Z}_8$ e $\mathbb{Z}_2$ e questi sono non isomorfi.*

Dimostrazione. Osserviamo che: Aut($\mathbb{Z}_8$)=$\{Id, \phi_1, \phi_2, \phi_3\}$ dove:

$$\phi_1([1]_8) = [3]_8$$

$$\phi_2([1]_8) = [5]_8$$

$$\phi_3([1]_8) = [7]_8$$

le ϕ_i, i=1,2,3 hanno ordine 2. Deduciamo che gli omomorfismi non banali da $\mathbb{Z}_2$ a Aut($\mathbb{Z}_8$) sono Ψ_1,Ψ_2,Ψ_3 dove:

$$\Psi_1([1]_2) = \phi_1$$

$$\Psi_2([1]_2) = \phi_2$$

$$\Psi_3([1]_2) = \phi_3$$

Abbiamo quindi i prodotti semidiretti non banali:

$$\mathbb{Z}_8 \rtimes_{\Psi_1} \mathbb{Z}_2, \mathbb{Z}_8 \rtimes_{\Psi_2} \mathbb{Z}_2 \text{ e } \mathbb{Z}_8 \rtimes_{\Psi_3} \mathbb{Z}_2$$

si mostra facilmente che:

$$\mathbb{Z}_8 \rtimes_{\Psi_1} \mathbb{Z}_2 \text{ ha 5 elementi di ordine 2}$$

$$\mathbb{Z}_8 \rtimes_{\Psi_2} \mathbb{Z}_2 \text{ ha 3 elementi di ordine 2}$$

$$\mathbb{Z}_8 \rtimes_{\Psi_3} \mathbb{Z}_2 \text{ ha 9 elementi di ordine 2}$$

pertanto non possono essere isomorfi. □

Lemma 19. *Sia G un gruppo non abeliano : | G | = 16 e che contiene almeno due sottogruppi di ordine 8 abeliani allora | Z(G) | $\geq$ 4*

Dimostrazione. Siano G_1 e G_2 due sottogruppi di G di ordine 8 abeliani.Abbiamo che:

$$| G_1G_2 | = 64 / | G_1 \cap G_2 |$$

deduciamo che:

$$G = G_1G_2 \text{ e } | G_1 \cap G_2 | = 4$$

Sia ora g $\in G_1 \cap G_2$ e g' $\in$ G. Mostriamo che gg' = g'g.Abbiamo che esistono $g_1 \in G_1$ e $g_2 \in G_2$ tali che g'=g_1 g_2.Quindi:

$$gg' = g g_1\ g_2 = g_1 g g_2 = g_1 g_2 g = g'g$$

pertanto $G_1 \cap G_2 \leq$ Z(G) e quindi si ha la tesi. □

Teorema 39. *Sia G un gruppo : | G | = 16. Allora G è isomorfo ad uno dei gruppi sotto elencati:*

- $\mathbb{Z}_{16}$
- $\mathbb{Z}_8 \times \mathbb{Z}_2$
- $\mathbb{Z}_4 \times \mathbb{Z}_4$
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- $D_4 \times \mathbb{Z}_2$
- $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Phi_2} \mathbb{Z}_4$
- $\mathbb{Z}_4 \rtimes_f \mathbb{Z}_4$
- $Q_8 \times \mathbb{Z}_2$
- $(\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\Gamma_1} \mathbb{Z}_2$
- $\mathbb{Z}_8 \rtimes_{\Psi_1} \mathbb{Z}_2$
- $\mathbb{Z}_8 \rtimes_{\Psi_2} \mathbb{Z}_2$
- $\mathbb{Z}_8 \rtimes_{\Psi_3} \mathbb{Z}_2$
- Q_{16}

dove Φ_2,f,Γ_1,Ψ_1,Ψ_2 *e* Ψ_3 *sono definiti nei lemmi precedenti.*

Dimostrazione. Se G è abeliano per il teorema di Frobenius-Stickelberg si ha immediatamente che:

$G \simeq \mathbb{Z}_{16} \vee G \simeq \mathbb{Z}_8 \times \mathbb{Z}_2 \vee G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \vee G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \vee G \simeq \mathbb{Z}_4 \times \mathbb{Z}_4$

Supponiamo quindi che G non sia abeliano, allora il gruppo quoziente:

$$G \,/\, Z(G)$$

non può essere ciclico. Per il teorema di Lagrange:

$$|\, Z(G) \,| \in \{1, 2, 4, 8, 16\}$$

ma essendo G non abeliano non può essere $|\, Z(G) \,| = 16$ e similmente se $|\, Z(G) \,| = 8$ il gruppo $G \,/\, Z(G)$ sarebbe ciclico.Inoltre,essendo G un p-gruppo, non può capitare che $|\, Z(G) \,| = 1$.Per tanto

$$|\, Z(G) \,| = 4 \vee |\, Z(G) \,| = 2$$

Studiamo quindi i due casi separatamente.

1. $|\, Z(G) \,| = 4$

Siccome G / Z(G) non può essere ciclico si ha che G / Z(G) $\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.Siccome $\mathbb{Z}_2 \times \mathbb{Z}_2$ ha esattamente 3 sottogruppi di ordine 2 allora G / Z(G) ha esattamente 3 sottogruppi di ordine 2 e quindi esistono esattamente 3 sottogruppi di G,diciamoli G_1,G_2 e G_3, di ordine 8 contenenti il centro Z(G).

G_1,G_2 e G_3 soddisfano i seguenti fatti:

i) Se $g_i \in G_i \setminus$ Z(G) e $g_j \in G_j \setminus$ Z(G) allora $g_i g_j \in G_k \setminus$ Z(G) con i,j,k $\in \{1,2,3\}$ distinti

ii) Se $g_i \in G_i \setminus$ Z(G) e $g_j \in G_j \setminus$ Z(G) allora $g_i g_j \neq g_j g_i$ con i,j $\in \{1,2,3\}$ distinti

iii) $\forall$ i,j $\in \{1,2,3\}$ distinti $G_i \cap G_j$ = Z(G)

iv) G_1,G_2 e G_3 sono abeliani.

Dobbiamo distinguere due sottocasi:

(a) Z(G) $\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$

Allora Z(G) avrà la forma:

$$\text{Z(G)}=\{1, \alpha, \beta, \gamma\}$$

con α,β e γ elementi di G di ordine 2.

Osserviamo che G_1,G_2 e G_3 non possono essere isomorfi a $\mathbb{Z}_8$ dato che quest'ultimo non contiene 3 elementi di ordine 2.Quindi si possono presentare solamente le seguenti possibilità:

a_1) $G_i \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ per ogni i=1,2,3

a_2) $G_1 \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ e G_2,$G_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

a_3) G_1,$G_2 \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ e $G_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

a_4) $G_i \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ per ogni i=1,2,3

Analizziamole separatamente:

a_1) Mostriamo che si giunge ad un assurdo. Effettivamente esistono a,b e c in G $\setminus$ Z(G) di ordine 2 e distinti tali che:

G_1=$\{1, \alpha, \beta, \gamma, a, a\alpha, a\beta, a\gamma\}$

G_2=$\{1, \alpha, \beta, \gamma, b, b\alpha, b\beta, b\gamma\}$

G_3=$\{1, \alpha, \beta, \gamma, c, c\alpha, c\beta, c\gamma\}$

e abbiamo che baab=bb=1=baba e quindi ba=ab che è assurdo.

a_2) Mostriamo che G $\simeq$ $D_4 \times \mathbb{Z}_2$.Effettivamente esistono a $\in$ G $\setminus$ Z(G) di ordine 4 e b,c $\in$ G $\setminus$ Z(G) di ordine 2 tutti distinti tra loro tali che

G_1=$\{1, \alpha = a^2, \beta, \gamma, a, a^3, a\beta, a\gamma = a^3\beta\}$

G_2=$\{1, \alpha, \beta, \gamma, b, b\alpha, b\beta, b\gamma\}$

G_3=$\{1, \alpha, \beta, \gamma, c, c\alpha, c\beta, c\gamma\}$

Osserviamo che:

$$G \simeq \langle a\rangle\langle b\rangle \times \langle\beta\rangle$$

Effettivamente <a><b> ha ordine 8 (e quindi è normali in G) e ha intersezione banale con <β> (che è normale in G) e quindi si ha quanto scritto sopra.Ora poichè ba $\in G_3$ esso ha ordine 2 e quindi baba=1 da cui bab=a^3 e quindi <a><b> $\simeq$ D_4 e quindi si ha:

$$G \simeq D_4 \times \mathbb{Z}_2$$

a_3)Mostriamo che G $\simeq$ $(\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Phi_2} \mathbb{Z}_4$.Osserviamo che non può capitare che esistono a,b in G $\setminus$ Z(G) distinti di ordine 4 e c in G $\setminus$ Z(G) di ordine 2 tali che:

G_1=$\{1, \alpha = a^2, \beta, \gamma, a, a^3, a\beta, a\gamma = a^3\beta\}$

G_2=$\{1, \alpha = b^2, \beta, \gamma, b, b^3, b\beta, b\gamma = b^3\beta\}$

G_3=$\{1, \alpha, \beta, \gamma, c, c\alpha, c\beta, c\gamma\}$

Infatti in tal caso si ha che essendo ba $\in G_3$, ba ha ordine 2 e pertanto baba=1 da cui ba=a^3b^3=a^2abb^2=ab che è assurdo. Quindi esistono a,b in G $\setminus$ Z(G) distinti di ordine 4 e c in G $\setminus$ Z(G) di ordine 2 tali che:

G_1=$\{1, \alpha = a^2, \beta, \gamma, a, a^3, a\beta, a\gamma = a^3\beta\}$

G_2=$\{1, \alpha, \beta = b^2, \gamma, b, b^3, b\alpha, b\gamma = b^3\alpha\}$

G_3=$\{1, \alpha, \beta, \gamma, c, c\alpha, c\beta, c\gamma\}$

Osserviamo che:

$$G \simeq \langle\gamma\rangle\langle c\rangle \rtimes_h \langle b\rangle$$

per qualche h : <b> $\longrightarrow$ Aut(<γ><c>) omomorfismo. Di fatto <γ><c> è normale in G e ha intersezione banale con <b> (che ha ordine 4) e quindi G $\simeq$ <γ><c> $\rtimes_h$ <b>. Siccome <γ><c> $\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ e <b> $\simeq \mathbb{Z}_4$ si ha che G è isomorfo a un prodotto semidiretto tra $\mathbb{Z}_2 \times \mathbb{Z}_2$ e $\mathbb{Z}_4$ ma essi sono tutti isomorfi e quindi possiamo scrivere:

$$G \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Phi_2} \mathbb{Z}_4$$

a_4) Mostriamo che G $\simeq \mathbb{Z}_4 \rtimes_f \mathbb{Z}_4 \vee$ G $\simeq Q_8 \times \mathbb{Z}_2$.Si possono presentare due casi:

i) Esistono a,b e c in G $\setminus$ Z(G) di ordine 4 distinti tali che:

G_1=$\{1, \alpha = a^2, \beta, \gamma, a, a^3, a\beta, a\gamma = a^3\beta\}$

G_2=$\{1, \alpha, \beta = b^2, \gamma, b, b^3, b\alpha, b\gamma\}$

G_3=$\{1, \alpha, \beta, \gamma, c...\}$

per capire come sono fatti i restanti elementi di G_3 dobbiamo capire chi è c^2.Abbiamo che ba $\in G_3 \setminus$ Z(G) quindi ba ha ordine 4 e siccome in $\mathbb{Z}_4 \times \mathbb{Z}_2$ se x,y hanno ordine 4 allora x^2 = y^2 otteniamo che:

$$(ba)^2 = c^2$$

allora poichè:

$$(ba)^2ba=(ba)^3=a^2abb^2=\gamma ab$$

otteniamo

$$c^2 \neq \gamma$$

allora possiamo assumere senza ledere generalità che $c^2 = \beta$.Pertanto:

$G_3=\{1, \alpha, \beta = c^2, \gamma, c, c^3, c\alpha, c\gamma\}$

Osserviamo che:

$$G \simeq \langle a \rangle \rtimes_q \langle b \rangle$$

per qualche omomorfismo q : <b> $\longrightarrow$ Aut(<a>).Effettivamente <a> è normale in G e ha intersezione banale con <b> e siccome entrambi sono isomorfi a $\mathbb{Z}_4$ si ha che G è isomorfo a un prodotto semidiretto tra $\mathbb{Z}_4$ e $\mathbb{Z}_4$ non banale. Ma di prodotto semidiretto tra $\mathbb{Z}_4$ e $\mathbb{Z}_4$ non banale vi è solo $\mathbb{Z}_4 \rtimes_f \mathbb{Z}_4$ e quindi:

$$G \simeq \mathbb{Z}_4 \rtimes_f \mathbb{Z}_4$$

ii) Esistono a,b e c in G $\setminus$ Z(G) di ordine 4 distinti tali che:

$$G_1=\{1, \alpha = a^2, \beta, \gamma, a, a^3, a\beta, a\gamma = a^3\beta\}$$

$$G_2=\{1, \alpha = b^2, \beta, \gamma, b, b^3, b\beta, b\gamma = b^3\beta\}$$

$$G_3=\{1, \alpha = c^2, \beta, \gamma, c, c^3, c\beta, c\gamma = c^3\beta\}$$

Osserviamo che:

$$G \simeq \langle a \rangle\langle b \rangle \times \langle \beta \rangle$$

infatti <a><b> è normale in G (perchè ha ordine 8) e <β> è normale in G perchè è contenuto nel centro inoltre essi si intersecano banalmente perchè l'unico elemento di ordine 2 di <a><b> è $a^2=\alpha$.Ora siccome <a><b> ha un solo elemento di ordine 2 e non è abeliano l'unica possibilità è che sia isomorfo a Q_8 e pertanto:

$$G \simeq Q_8 \times \mathbb{Z}_2$$

(b) $Z(G) \simeq \mathbb{Z}_4$

In tal caso Z(G)=<α> con $\alpha \in$ G : o(α)=4.Osserviamo che nessun G_i è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ perchè quest'ultimo non ha elementi di ordine 4 quindi preso i $\in \{1,2,3\}$ G_i è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_4$ oppure $\mathbb{Z}_8$.Deduciamo i seguenti fatti:

i) Sia g $\in G_i$ i=1,2,3 allora $g^2 \in$ Z(G)

ii) Preso g $\in G_i$ e h $\in G_j$ con i,j $\in \{1,2,3\}$ distinti o([g,h])=2.

Anche adesso abbiamo da analizzare quattro possibilità.

b_1) $G_i \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$ per ogni i=1,2,3

b_2) $G_1 \simeq \mathbb{Z}_8$ e $G_i \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$ per i=2,3

b_3) $G_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$ e $G_i \simeq \mathbb{Z}_8$ per i=1,2

b_4) $G_i \simeq \mathbb{Z}_8$ per ogni i=1,2,3

Studiamo questi casi singolarmente:

b_1) Dimostriamo che G $\simeq (\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\Gamma_1} \mathbb{Z}_2$

Effettivamente guardando com'è fatto $\mathbb{Z}_4 \times \mathbb{Z}_2$ esistono a,b e c in G $\setminus$ Z(G) di ordine 2 distinti tali che:

$G_1 = \{1, \alpha, \alpha^2, \alpha^3, a, a\alpha, a\alpha^2, a\alpha^3\}$

$G_2 = \{1, \alpha, \alpha^2, \alpha^3, b, b\alpha, b\alpha^2, b\alpha^3\}$

$G_3 = \{1, \alpha, \alpha^2, \alpha^3, c, c\alpha, c\alpha^2, c\alpha^3\}$

Osserviamo che

$$\text{G} \simeq \text{<}\alpha\text{><a>} \rtimes_k \text{<b>}$$

per qualche omomorfismo k : <b> $\longrightarrow$ Aut(<α><a>).Infatti l'ordine di <α><a> è 8 (quindi è normale in G) e si interseca banalmente con <b> (se così non fosse ba avrebbe ordine 2 e questo implicherebbe ab=ba che è assurdo).Ora siccome <α><a> è abeliano di ordine 8 che non ha elementi di ordine 8 e ha elementi di ordine 4 si deduce che <α><a> è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_4$ e quindi G è isomorfo a un prodotto semidiretto non banale tra $\mathbb{Z}_2 \times \mathbb{Z}_4$ e $\mathbb{Z}_2$.Siccome sotto queste ipotesi G ha 7 elementi di ordine 2 deduciamo che:

$$\text{G} \simeq (\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\Gamma_1} \mathbb{Z}_2$$

b_2) mostriamo che tale caso non si può verificare.

Effettivamente in tal caso esiste a in G \ Z(G) di ordine 8 e b,c in G \ Z(G) di ordine 2 distinti tali che:

$G_1 = \{1, \alpha, \alpha^2, \alpha^3, a, a\alpha, a\alpha^2, a\alpha^3\}$

$G_2 = \{1, \alpha, \alpha^2, \alpha^3, b, b\alpha, b\alpha^2, b\alpha^3\}$

$G_3 = \{1, \alpha, \alpha^2, \alpha^3, c, c\alpha, c\alpha^2, c\alpha^3\}$

Consideriamo l'elemento ba. ba $\in G_3$ quindi o ha ordine 2 oppure ha ordine 4.Se avesse ordine 2 troverei ba=a^6ab e cioè a^6 = [b,a] assurdo perchè a^6 non ha ordine 2.Se invece o(ba)=4 allora $(ba)^2$ba=a^6ab e siccome $a^2 \in \{\alpha, \alpha^3\}$ implicherebbe o(α)=2 assurdo.

b_3) Mostriamo che G $\simeq \mathbb{Z}_8 \rtimes_{\Psi_1} \mathbb{Z}_2$

Abbiamo che esistono a,b in G \ Z(G) di ordine 8 e c in G \ Z(G) di ordine 2 tali che:

$G_1 = \{1, \alpha, \alpha^2, \alpha^3, a, a\alpha, a\alpha^2, a\alpha^3\}$

$G_2 = \{1, \alpha, \alpha^2, \alpha^3, b, b\alpha, b\alpha^2, b\alpha^3\}$

$G_3 = \{1, \alpha, \alpha^2, \alpha^3, c, c\alpha, c\alpha^2, c\alpha^3\}$

Osserviamo che:

$$G \simeq \langle a \rangle \rtimes_j \langle c \rangle$$

per qualche omomorfismo j: <c> $\longrightarrow$ Aut(<a>). Effettivamente <a> ha ordine 8 e quindi è normale in G e interseca banalmente <c> che ha ordine 2.Pertanto G è isomorfo a un prodotto semidiretto non banale tra $\mathbb{Z}_8$ e $\mathbb{Z}_2$ e siccome ha solo 3 elementi di ordine 2 si deduce che:

$$G \simeq (\mathbb{Z}_4 \times \mathbb{Z}_2) \rtimes_{\Gamma_1} \mathbb{Z}_2$$

b_4) Mostriamo che si arriva ad un assurdo.Effettivamente in tal caso si troverebbero a,b in G \ Z(G) distinti di ordine 8 tali che o(ba)=8 e a^2=b^2=α.Allora $(ba)^6$ba=α^2ab.Se $(ba)^2 = \alpha$ allora α^3 avrebbe ordine 2 che è assurdo se invece $(ba)^2 = \alpha^3$ troverei α di ordine 2 che è assurdo.

2) | Z(G) | = 2

Nel proseguo Z(G)=$\{1, z\}$.Ora siccome G / Z(G) non può essere ciclico e ha ordine 8 si hanno varie possibilità:

i) G / Z(G) $\simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.

ii) G / Z(G) $\simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

iii) G / Z(G) $\simeq Q_8$

iv) G / Z(G) $\simeq D_4$

analizziamole separatamente:

i) Mostriamo che si giunge ad un assurdo.Siccome $\mathbb{Z}_4 \times \mathbb{Z}_2$ ha esattamente 3 sottogruppi di ordine 4 (due dei quali contengono un solo sottogruppo di ordine 2 e il restante 3 sottogruppi di ordine 2) deduciamo che G possiede esattamente 3 sottogruppi di ordine 8 contenenti Z(G) e tali che due dei quali contengono esattamente un sottogruppo di ordine 4 contenente Z(G) e il rimanente possiede esattamente 3 sottogruppi di ordine 4 contenenti Z(G),diciamoli G_1, G_2 e G_3 rispettivamente. Osserviamo che G_1 e G_2 sono abeliani. Mostriamolo per G_1.Abbiamo che Z(G) $\leq$ Z(G_1) allora se G_1 non fosse abeliano dovrebbe contenere 3 sottogruppi di ordine 4 contenenti Z(G_1) e quindi Z(G) ma questo è assurdo per il lemma 19.

ii) Mostriamo che si arriva ad un assurdo. Sia g $\in$ G $\setminus$ Z(G). Allora gZ(G) $\neq$ Z(G) e quindi gZ(G) ha ordine 2.Allora g^2Z(G) = Z(G) e quindi $g^2 \in$ Z(G).Pertanto g^2 = 1 o g^2= z. Osserviamo che se $\forall$ g $\in$ G $\setminus$ Z(G) g^2=1 allora tutti gli elementi di G hanno ordine 2 (chiaramente escluso l'elemento neutro) e quindi G è abeliano,assurdo.Pertanto deve esistere g in G $\setminus$ Z(G) tale che g^2 = z e quindi g ha ordine 4.Consideriamo:

$$<g> = \{1, g, g^2, g^2\}$$

abbiamo:

$$\frac{<g>}{Z(G)} \leq \frac{G}{Z(G)} \text{ e } \left| \frac{<g>}{Z(G)} \right| = 2$$

quindi troviamo esattamente 3 sottogruppi di G di ordine 8 contenenti il centro, diciamoli sempre G_1,G_2 e G_3,contenenti <g>.Vale il seguente fatto:

- Se i $\neq$ j , g $\in G_i \setminus$ <g> e h $\in G_j \setminus$ <g> allora gh $\in G_k \setminus$ <g> con k $\neq$ i,j

Per il lemma 19 possiamo assumere che G_2 e G_3 non siano abeliani.Siano allora:

$$g_2 \in G_2 \setminus \text{Z(G)} : \text{g}g_2 \neq g_2\ \text{g}$$

$$g_3 \in G_3 \setminus \text{Z(G)} : \text{g}g_3 \neq g_3\ \text{g}$$

Ora siccome $\frac{G}{Z(G)}$ è abeliano allora D(G) $\leq$ Z(G) ma [g,g_2] $\neq$ 1 quindi D(G)=Z(G).Allora

$$\text{g}g_2\text{=z}g_2\text{g e g}g_3\text{=z}g_3\text{g}$$

consegue:

$$\text{g}g_2g_3\text{=}g_2g_3\text{g}$$

Quindi,per Lagrange:

$$C_{G_1}(\text{g}) = G_1$$

allora g $\in$ Z(G_1) e quindi $\{1, z, g\}$ è contenuto in Z(G_1) quindi G_1 deve essere per forza abeliano.Ora G_1 non contiene elementi di ordine 8 (perchè non li contiene G) inoltre g $\in$ G_1 : o(g)=4 quindi

$$G_1 \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$$

allora G_1 avrà la forma:

$$G_1 = \{1, g, g^2, g^3, g_1, gg_1, g^2g_1, g^3g_1\} \text{ con } o(g_1) = 4.$$

Osserviamo che se x $\in G_1 \setminus$ Z(G) e y $\in G_2 \setminus$ Z(G) allora xy=zyx.Infatti se cosi non fosse avrei che xy=yx e quindi C_{G_1}(x) = G_2 da cui | Z(G_2) | = 4 assurdo perchè G_2 è non abeliano di ordine 8. Allora presi se x $\in G_1 \setminus$ Z(G) e y $\in G_2 \setminus$ Z(G)

$$\text{gxy=gzyx=zzygx=ygx}$$

quindi y commuta con gx $\in G_1 \setminus$ Z(G) che aasurdo.

iii) Mostriamo che si arriva ad un assurdo.Effettivamente Q_8 possiede esattamente 3 sottogruppi di ordine 4 ognuno dei quali ha esattamente un sottogruppo di ordine 2.Quindi esistono G_1,G_2 e G_3 sottogruppi di G di ordine 8 contenenti Z(G) che ammettono esattamente un sottogruppo di ordine 4 contenente Z(G).Allora G_1,G_2 e G_3 devono essere abeliani (infatti se G_i,i=1,2,3, non è abeliano allora Z(G_i)=Z(G) quindi ho un solo sottogruppo di ordine 4 in G_i che lo contiene ma questo è assurdo per com'è fatto D_4 e Q_8)

iv) G / Z(G) $\simeq D_4$

Per come è fatto D_4 esistono G_1,G_2 e G_3 sottogruppi di G di ordine 8 contenenti Z(G) tali che G_1 ha un solo sottogruppo di ordine 4 contenente Z(G) mentre G_2 e G_3 hanno 3 sottogruppi di ordine 4 contenenti Z(G).Osserviamo che G_1 è abeliano e quindi G_2 e G_3 non possono essere abeliani.Abbiamo allora Z(G)=Z(G_2)=Z(G_3).Mostriamo ora che:

$$\text{Z(G)} < \text{D(G)}$$

Effettivamente se $G_2 \simeq D_4$ consideriamo:

$$\text{F} : D_4 \longrightarrow G_2$$

isomorfismo.Allora essendo r^2=sr$s^{-1}r^{-1}$ si ha:

$$\text{z=F}(r^2)\text{=F(sr}s^{-1}r^{-1}\text{)=ab}a^{-1}b^{-1} \text{ con a = F(s) e b=F(r)}$$

consegue che z ∈ D(G).Similmente se $G_2 \simeq Q_8$=<i,j> consideriamo:

$$\text{M} : Q_8 \longrightarrow G_2$$

isomorfismo.Siccome -I=ij$i^{-1}j^{-1}$ si ha:

$$\text{z=M(-I)=M(ij}i^{-1}j^{-1}\text{)=cd}c^{-1}d^{-1} \text{ con c=M(i) e d=M(j)}$$

consegue che z ∈ D(G).Siccome G / Z(G) è non abeliano l'inclusione è stretta.Ora osserviamo che s e rs sono elementi di D_4 che non commutano quindi esistono $g_2 \in G_2$ e $g_3 \in G_3$ tali che:

$$g_2\text{Z(G)}g_3\text{Z(G)} \neq g_3\text{Z(G)}g_2\text{Z(G)}$$

Allora se:

$$\{Z(G), g'Z(G)\}\text{=Z(G/Z(G))=D(G/Z(G))}$$

si ottiene:

$$g_2g_3\text{Z(G)}=g_3g_2\text{g'Z(G)}$$

e quindi esiste $z_0 \in$ Z(G) tale che

$$g_2g_3\text{=}g_3g_2\text{g'}z_0$$

quindi g'$z_0 \in$ D(G) consegue che g' ∈ D(G).Pertanto:

$$\{1, g', z, g'z\} \subset \text{D(G)}$$

Mostriamo che $\{1, g', z, g'z\}$ = D(G). Iniziamo ad osservare che $\{1, g', z, g'z\}$ è un sottogruppo normale di G e quindi ha senso considerare il quoziente:

$$\text{G / } \{1, g', z, g'z\}$$

che ha ordine 4 e quindi è abeliano e allora:

$$\text{D(G)} \leq \{1, g', z, g'z\}$$

consegue:

$$\text{D(G)= } \{1, g', z, g'z\}$$

Adesso si osservi che D(G) < G_i i=1,2,3, essendo G / G_i di ordine 2 e quindi abeliano ed inoltre per ogni i $\neq$ j G_iG_j=G, $\mid G_i \cap G_j \mid$ = 4 ed essendo D(G) $\leq G_i \cap G_j$ si ha D(G)=G_i $\cap$ G_j.Proviamo ora che $G_1 \simeq \mathbb{Z}_8$.Sappiamo che G_1 è un gruppo di ordine 8 abeliano che ha un sottogruppo di ordine 4 contenente Z(G).Siccome $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ è tale che ogni sottogruppo di ordine 2 è contenuto in 3 sottogruppi di ordine 4 troviamo che G_1 non può essere isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.Supponiamo ora per assurdo che $G_1 \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$.Il sottogruppo di ordine 4 che contiene Z(G) è D(G) e quindi D(G) non è isomorfo a $\mathbb{Z}_4$ e quindi D(G) $\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.Ora siccome Q_8 non possiede sottogruppi di ordine 4 isomorfi a $\mathbb{Z}_2$ $\times$ $\mathbb{Z}_2$ si ha necessariamente che G_2, $G_3 \simeq D_4$.Allora sia g_2 in G_2 di ordine 2.Per ogni g_1 in G_1 il commutatore [g_1,g_2] ha ordine 4 che è assurdo.Quindi $G_1 \simeq \mathbb{Z}_8$.Deduciamo che D(G) $\simeq \mathbb{Z}_4$ e allora D(G)=<g'>.Esistera a in G $\setminus$ D(G) di ordine 8 tale che:

$$G_1 = \{1, g', z, g'^3, a, ...\}$$

Distinguiamo le varie possibilità:

i) G_2, $G_3 \simeq D_4$. Mostriamo che G $\simeq \mathbb{Z}_8 \rtimes_{\Psi_2} \mathbb{Z}_2$.

Esistono b e c in G $\setminus$ D(G) di ordine 2 distinti tali che:

$$G_2 = \{1, g', z, g'^3, b, ...\}$$

$$G_3 = \{1, g', z, g'^3, c, ...\}$$

Osserviamo che

$$\text{G} \simeq \text{<a>} \rtimes_h \text{<b>} \text{ per qualche omomorfismo h.}$$

Allora siccome G ha 9 elementi di ordine 2 si ottiene:

$$G \simeq \mathbb{Z}_8 \rtimes_{\Psi_2} \mathbb{Z}_2.$$

2) $G_2 \simeq D_4$, $G_3 \simeq Q_8$. Mostriamo che $G \simeq \mathbb{Z}_8 \rtimes_{\Psi_3} \mathbb{Z}_2$

Esistono b e c in G \ D(G) di ordine 2 e 4 rispettivamente tali che:

$G_2 = \{1, g', z, g'^3, b, ...\}$

$G_3 = \{1, g', z, g'^3, c, ...\}$

Si osserva che G $\simeq$ <a> $\rtimes_{h'}$ <b> per qualche omomorfismo h' e siccome G ha 5 elementi di ordine 2 si ha che:

$$G \simeq \mathbb{Z}_8 \rtimes_{\Psi_3} \mathbb{Z}_2$$

3) $G_2, G_3 \simeq Q_8$. Mostriamo che $G \simeq Q_{16}$

Esistono b e c in G \ D(G) di ordine 4 distinti tali che:

$G_2 = \{1, g', z, g'^3, b, ...\}$

$G_3 = \{1, g', z, g'^3, c, ...\}$

si osserva che G = <a,b> con $bab^{-1}=a^{-1}$ e quindi $G \simeq Q_{16}$ □

5.8 Gruppi di ordine 18

Iniziamo con il seguente:

Lemma 20. *Sia p un primo. Allora: (ci sono n copie di $\mathbb{Z}_p$)*

$$Aut(\mathbb{Z}_p \times ... \times \mathbb{Z}_p) \simeq GL_n(\mathbb{Z}_p)$$

Dimostrazione. Essendo p un primo $\mathbb{Z}_p$ è un campo. Allora ${\mathbb{Z}_p}^n := \mathbb{Z}_p \times ... \times \mathbb{Z}_p$ è uno spazio vettoriale su $\mathbb{Z}_p$. Quindi ha senso considerare Iso($\mathbb{Z}_p^n$) cioè l'insieme di tutte le applicazioni lineari da $\mathbb{Z}_p^n$ a $\mathbb{Z}_p^n$ biettive. Iso($\mathbb{Z}_p^n$) con l'operazione di composizione è un gruppo, mostriamo che Iso($\mathbb{Z}_p^n$) $\simeq GL_n(\mathbb{Z}_p)$. Sia B la base canonica di $\mathbb{Z}_p^n$ con B=$\{e_1, ..., e_n\}$, definiamo l'applicazione:

$$\Phi : \text{Iso}(\mathbb{Z}_p^n) \longrightarrow GL_n(\mathbb{Z}_p)$$

$$f \longmapsto M_{BB}(f)$$

dove $M_{BB}(f)$ denota come al solito la matrice associata a f rispetto alla base B.Mostriamo che Φ è un isomorfismo di gruppi. Iniziamo ad osservare che Φ è ben definita nel senso che presa f $\in$ Iso($\mathbb{Z}_p^n$) la matrice $M_{BB}(f)$ è di fatto invertibile essendo f un isomorfismo. Inoltre Φ è un omomorfismo dato che prese f e g in Iso($\mathbb{Z}_p^n$) si ha che :

$$M_{BB}(f \circ g) = M_{BB}(f)M_{BB}(g)$$

per mostrare che è biettiva iniziamo a prendere f e g $\in$ Iso($\mathbb{Z}_p^n$) tali che Φ(f)=Φ(g). Allora $M_{BB}(f) = M_{BB}(g)$ e quindi f(e_i)=g(e_i) $\forall$ i=1,...,n da cui f=g.Per mostrare che è suriettiva prendiamo A = $(a_{ij}) \in GL_n(\mathbb{Z}_p)$. Definiamo l'applicazione lineare:

$$\mathrm{F} : \mathbb{Z}_p^n \longrightarrow \mathbb{Z}_p^n$$

$$(x_1, ..., x_n) \longmapsto \mathrm{A} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

è chiaro che F è lineare, invertibile e la matrice associata ad F rispetto a B è A da cui Φ(F)=A.Pertanto Φ è un isomorfismo di gruppi. Se mostriamo che Aut($\mathbb{Z}_p^n$) = Iso($\mathbb{Z}_p^n$) abbiamo finito. Effettivamente prendiamo f $\in$ Iso($\mathbb{Z}_p^n$), dobbiamo mostrare che f $\in$ Aut($\mathbb{Z}_p^n$). Essendo f biettiva si tratta di mostrare che f è un omomorfismo di gruppi cioè che presi x e y in $\mathbb{Z}_p^n$ si ha che f(x + y)=f(x) + f(y). Ma questo si ha per l'ipotesi di linearità di f. Viceversa prendiamo g $\in$ Aut($\mathbb{Z}_p^n$) vogliamo mostrare che g $\in$ Iso($\mathbb{Z}_p^n$). Essendo g biettiva si tratta di dimostrare che g è lineare. Effettivamente presi x,y $\in \mathbb{Z}_p^n$ essendo g un omomorfismo di gruppi g(x+y)=g(x)+g(y). Inoltre se a $\in \mathbb{Z}_p$ abbiamo g(ax)=ag(x). Infatti se:

$$\mathrm{a} = [\tilde{a}]_p$$

$$\mathrm{x} = ([b_1]_p, ..., [b_n]_p)$$

$$\mathrm{g(x)} = ([c_1]_p, ..., [c_n]_p)$$

si ha che:

$$\mathrm{g(ax)}=\mathrm{g}([\tilde{a}b_1]_p, ..., [\tilde{a}b_n]_p)=\mathrm{g}(\tilde{a}[b_1]_p, ..., \tilde{a}[b_n]_p)=$$

$$\mathrm{g}([b_1]_p, ..., [b_n]_p) + ... + ([b_1]_p, ..., [b_n]_p)= (\tilde{a} \text{ volte})$$

$$([c_1]_p, ..., [c_n]_p) + ... + ([c_1]_p, ..., [c_n]_p) (\tilde{a} \text{ volte})$$

$$(\tilde{a}[c_1]_p, ..., \tilde{a}[c_n]_p) =$$

$$[\tilde{a}]_p g([b_1]_p, ..., [b_n]_p) = ag(x)$$

e quindi ha la tesi. □

Lemma 21. *Sia $\Psi \in Hom(\mathbb{Z}_2, Aut(\mathbb{Z}_3 \times \mathbb{Z}_3))$ non banale.Allora:*

$$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\Psi \mathbb{Z}_2 \simeq (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\gamma_1} \mathbb{Z}_2$$

con

$$\gamma_1([1]_2)(x,y)=(x,-y)$$

oppure:

$$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\Psi \mathbb{Z}_2 \simeq (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\gamma_2} \mathbb{Z}_2$$

con

$$\gamma_2([1]_2)(x,y)=(-x,-y)$$

e i gruppi $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\psi_1} \mathbb{Z}_2$, $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\psi_2} \mathbb{Z}_2$ non sono isomorfi perchè il primo ha 3 elementi di ordine 2, il secondo 9 elementi di ordine 2.

Dimostrazione. Iniziamo a determinare | Hom($\mathbb{Z}_2$,Aut($\mathbb{Z}_3 \times \mathbb{Z}_3$)) | .Sia:

$$\gamma : GL_2(\mathbb{Z}_3) \longrightarrow \text{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3)$$

un isomorfismo.Definiamo l'applicazione:

$$\Phi : \text{Hom}(\mathbb{Z}_2, \text{Aut}(GL_2(\mathbb{Z}_3))) \longrightarrow \text{Hom}(\mathbb{Z}_2, \text{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3))$$

$$f \longmapsto \gamma \circ f$$

Φ è bigettiva. Quindi:

$$|\text{Hom}(\mathbb{Z}_2, \text{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3))| = |\text{Hom}(\mathbb{Z}_2, \text{Aut}(GL_2(\mathbb{Z}_3)))|$$

Ora siccome in $GL_2(\mathbb{Z}_3)$ ci sono 12 elementi di ordine 2 , diciamoli A_1,A_2,...,A_{12}, ci sono 12 omomorfismi non banali da $\mathbb{Z}_2$ a $GL_2(\mathbb{Z}_3)$,che sono Ψ_1,...,Ψ_{12} dove:

$$\Psi_i([1]_2)=A_i \text{ i=1,...,12}$$

Ora, se ,in generale, B è una matrice in $GL_2(\mathbb{Z}_3)$ di ordine 2 allora:

$$B^2=I$$

consegue che:

$$B^2\text{-I=0}$$

allora detto $m_B(t)$ il polinomio minimo di B si ha che:

$$m_B(t) \mid \text{(t-1)(t+1)}$$

quindi

$$m_B(t)\text{=t-1} \vee m_B(t)\text{=t+1} \vee m_B(t)\text{=(t-1)(t+1)}$$

pertanto B è diagonalizzabile.Inoltre:

$$0=\det(B^2\text{-I})=\det(\text{B-I})\det(\text{B+I})$$

quindi si hanno 3 casi:

- det(B-I)=0 e det(B+I) $\neq 0$

  in tal caso B ha solo l'autovalore -1 con molteplicità 2 e quindi B è simile alla matrice -I:=D_1

- det(B-I) $\neq 0$ e det(B+I)=0

  in tal caso B ha solo l'autovalore 1 con molteplicità 2 e quindi B è simile alla matrice I.Questo implica che B=I,assurdo.

- det(B-I)=det(B+I)=0

  In tal caso gli autovalori di B sono 1 e -1.Quindi B è simile alla matrice che ha nella diagonale rispettivamente $[1]_3$ e $[-1]_3$ e altrove $[0]_3$,oppure è simile alla matrice che ha nella diagonale rispettivamente $[-1]_3$ e $[1]_3$ e altrove $[0]_3$.Tuttavia queste due matrice sono simili.

  Se allora :

  $$D_2 = \begin{pmatrix} [1]_3 & [0]_3 \\ [0]_3 & [-1]_3 \end{pmatrix}$$

  si ha che B è simile a D_1 oppure B è simile a D_2

Quindi per ogni i $\in \{1, ..., 12\}$ esiste $P_i \in GL_2(\mathbb{Z}_3))$ tale che:

$$P_i^{-1}A_iP_i = D_1 \vee P_i^{-1}A_iP_i = D_2$$

A meno di cambiare il nome alle matrici possiamo assumere che le prime k ≥ 1 matrici A_i siano simili a D_1 cioè che:

$$\forall \text{ i=1,...,k } P_i^{-1}A_iP_i = D_1$$

e quindi:

$$\forall \text{ i=k+1,...,12 } P_i^{-1}A_iP_i = D_2$$

Consideriamo allora gli omomorfismi non banali da $\mathbb{Z}_2$ a Aut($\mathbb{Z}_3 \times \mathbb{Z}_3$) che sono ϕ_j = $\Phi(\Psi_j)$ j=1,...,12.Abbiamo che:

$$\forall \text{ i=1,...,k } \gamma(P_i^{-1}A_iP_i) = \gamma(D_1)$$

$$\forall \text{ j=k+1,...,12 } \gamma(P_j^{-1}A_jP_j) = \gamma(D_2)$$

cioè:

$$\forall \text{ i=1,...,k } \gamma(P_i)^{-1}\gamma(\text{A}_i)\gamma(P_i) = \gamma(D_1)$$

$$\forall \text{ j=k+1,...,12 } \gamma(P_j)^{-1}\gamma(\text{A}_j)\gamma(P_j) = \gamma(D_2)$$

Se ora:

$$D_1 = \Psi_{d1}([1]_2) \text{ e } D_2 = \Psi_{d2}([1]_2)$$

otteniamo:

$$\forall \text{ i=1,...,k } \gamma(P_i)^{-1}\gamma(\Psi_i([1]_2))\gamma(P_i) = \gamma(\Psi_{d1}([1]_2))$$

$$\forall \text{ j=k+1,...,12 } \gamma(P_j)^{-1}\gamma(\Psi_j([1]_2))\gamma(P_j) = \gamma(\Psi_{d2}([1]_2))$$

e cioè:

$$\forall \text{ i=1,...,k } \gamma(P_i)^{-1}\phi_i([1]_2)\gamma(P_i) = \phi_{d1}([1]_2)$$

$$\forall \text{ j=k+1,...,12 } \gamma(P_j)^{-1}\phi_j([1]_2)\gamma(P_j) = \phi_{d2}([1]_2)$$

quindi $\forall\ i_1, i_2 \in \{1, ..., k\}$

$$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\phi_{i_1}} \mathbb{Z}_2 \simeq (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\phi_{i_2}} \mathbb{Z}_2$$

e $\forall\ j_1, j_2 \in \{k+1, ..., 12\}$

$$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\phi_{j_1}} \mathbb{Z}_2 \simeq (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\phi_{j_2}} \mathbb{Z}_2$$

Quindi il numero di prodotti semidiretti a meno di isomorfismo tra $\mathbb{Z}_3 \times \mathbb{Z}_3$ e $\mathbb{Z}_2$ è $\leq$ 2.Tuttavia gli omomorfismi:

$$\gamma_1([1]_2)(x,y)=(x,-y)\ ,\ (x,y) \in \mathbb{Z}_3 \times \mathbb{Z}_3$$

$$\gamma_2([1]_2)(x,y)=(-x,-y)\ ,\ (x,y) \in \mathbb{Z}_3 \times \mathbb{Z}_3$$

inducono i prodotti semidiretti:

$$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\gamma_1} \mathbb{Z}_2 \text{ che ha 3 elementi di ordine 2}$$

e

$$(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\gamma_2} \mathbb{Z}_2 \text{ che ha 9 elementi di ordine 2}$$

e quindi non sono isomorfi.Segue l'asserto. □

Lemma 22. *Sia $\phi : \mathbb{Z}_2 \longrightarrow$ Aut($\mathbb{Z}_9$) un omomorfismo non banale. Allora:*

$$\mathbb{Z}_9 \rtimes_\phi \mathbb{Z}_2 \simeq D_9$$

Dimostrazione. Osserviamo che Aut($\mathbb{Z}_9$) $\simeq \mathbb{Z}_6$. Quindi siccome $\mathbb{Z}_6$ ha un solo elemento di ordine 2 si ha che c'è un solo prodotto semidiretto non banale tra $\mathbb{Z}_9$ e $\mathbb{Z}_2$ e siccome $D_9 \simeq$ <r> $\rtimes_h$ <s> per qualche omomorfismo h:<s> $\longrightarrow$ Aut(<r>) deduciamo l'asserto. □

Teorema 40. *Sia G un gruppo : | G | = 18. Allora: G $\simeq \mathbb{Z}_{18} \vee$ G $\simeq \mathbb{Z}_6 \times \mathbb{Z}_3 \vee$ G $\simeq D_9 \vee$ G $\simeq (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\phi \mathbb{Z}_2 \vee$ G $\simeq S_3 \times \mathbb{Z}_3$ dove $\phi([1]_2)(x,y)=(-x,-y) \forall\ (x,y) \in \mathbb{Z}_3 \times \mathbb{Z}_3$*

Dimostrazione. Osserviamo che 18=2·3^2.Abbiamo che $\exists$ k $\in \mathbb{N}$ tale che n_3=1+3k.Ma n_3 | 2 quindi n_3=1.Similmente $\exists$ k $\in \mathbb{N}$ tale che n_2=1+2k. Siccome n_2 deduciamo che $n_2 \in \{1, 3, 9\}$.Distinguiamo quindi i vari casi.Sia H il sottogruppo normale di G di ordine 9.Abbiamo:

- n_2=1

  allora sia K il sottogruppo normale di G di ordine 2.Siccome si interseca banalmente con H si deduce che:

  $$G \simeq H \times K$$

  e quindi:

$$G \simeq \mathbb{Z}_9 \times \mathbb{Z}_2 \simeq \mathbb{Z}_{18}$$

oppure:

$$G \simeq \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \simeq \mathbb{Z}_3 \times \mathbb{Z}_6$$

- n_2=9

  Allora G ha 9 elementi di ordine 2.Sia y $\in$ G di ordine 2,allora:

  $$G \simeq H \rtimes_h \langle y \rangle$$

  per qualche omomorfismo h : <y> $\longrightarrow$ Aut(H).Quindi se H $\simeq \mathbb{Z}_9$ alloa G è isomorfo a un prodotto semidiretto non banale tra $\mathbb{Z}_9$ e $\mathbb{Z}_2$ e quindi per il lemma anteriore si deduce che:

  $$G \simeq D_9$$

  se invece H è isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_3$ allora G è isomorfo a un prodotto semidiretto non banale tra $\mathbb{Z}_3 \times \mathbb{Z}_3$ e $\mathbb{Z}_2$.Siccome ha 9 elementi di ordine 2 per il lemma 21 deduciamo che:

  $$G \simeq (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\phi \mathbb{Z}_2$$

  dove:

  $$\phi([1]_2)(x,y)=(-x,-y)\ \forall\ (x,y) \in \mathbb{Z}_3 \times \mathbb{Z}_3$$

- n_2=3

  Allora G ha 3 elementi di ordine 2.Preso y in G di ordine 2:

  $$G \simeq H \rtimes_k \langle y \rangle$$

  per qualche omomorfismo k : <y> $\longrightarrow$ Aut(H).Ossserviamo che H non può essere isomorfo a $\mathbb{Z}_9$ altrimenti G sarebbe isomorfo a D_9 ma questo è assurdo perchè D_9 non ha 3 elementi di ordine 2.Quindi H $\simeq \mathbb{Z}_3 \times \mathbb{Z}_3$ e pertanto G è isomorfo a un prodotto semidiretto tra $\mathbb{Z}_3 \times \mathbb{Z}_3$ e $\mathbb{Z}_2$.Siccome G ha 3 elementi di ordine 2 deduciamo dal lemma 21 che:

$$G \simeq (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\psi \mathbb{Z}_2$$

dove:

$$\psi([1]_2)(x,y)=(x,-y)\ \forall\ (x,y) \in \mathbb{Z}_3 \times \mathbb{Z}_3$$

Quindi , in definitiva, se G è un gruppo di ordine 18 allora $G \simeq \mathbb{Z}_{18} \vee G \simeq \mathbb{Z}_6 \times \mathbb{Z}_3 \vee G \simeq D_9 \vee G \simeq (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\phi \mathbb{Z}_2 \vee G \simeq (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\psi \mathbb{Z}_2$.Ora $S_3 \times \mathbb{Z}_3$ è un gruppo di ordine 18 che può essere isomorfo solo a $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\psi \mathbb{Z}_2$ avendo $S_3 \times \mathbb{Z}_3$ 3 elementi di ordine 2 e quindi si ha la tesi. □

Osservazione 16. *Osserviamo che $\mathbb{Z}_{18}$ e $\mathbb{Z}_6 \times \mathbb{Z}_3$ sono gruppi abeliani non isomorfi. Infatti il primo ha un elemento di ordine 18, il secondo no. Inoltre i gruppi D_9 , $S_3 \times \mathbb{Z}_3$ e $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\phi \mathbb{Z}_2$ sono non abeliani non isomorfi. Infatti D_9 e $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\phi \mathbb{Z}_2$ non sono isomorfi a $S_3 \times \mathbb{Z}_3$ perchè i primi due hanno 9 elementi di ordine 2 mentre il terzo solamente 3. Infine D_9 e $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\phi \mathbb{Z}_2$ non sono isomorfi perchè D_9 possiede un elemento di ordine 9 mentre $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\phi \mathbb{Z}_2$ no. Quindi i gruppi del teorema anteriore sono tutti non isomorfi.*

5.9 Gruppi di ordine 20

Lemma 23. *Aut($\mathbb{Z}_5$)=<α> dove:*

$$\alpha : \mathbb{Z}_5 \longrightarrow \mathbb{Z}_5$$

$$[1]_5 \longmapsto [2]_5$$

Dimostrazione. Basta osservare che $\mathrm{Aut}(\mathbb{Z}_5) \simeq \mathbb{Z}_4$ e α ha ordine 4 in $\mathrm{Aut}(\mathbb{Z}_5)$ □

Lemma 24. *A meno di isomorfismo ci sono due prodotti semidiretti non banali tra $\mathbb{Z}_5$ e $\mathbb{Z}_4$ che sono:*

$$\mathbb{Z}_5 \rtimes_{\phi_1} \mathbb{Z}_4 \text{ e } \mathbb{Z}_5 \rtimes_{\phi_2} \mathbb{Z}_4$$

dove

$$\phi_1([1]_4)=\alpha \text{ e } \phi_2([1]_4)=\alpha^2$$

Dimostrazione. Gli omomorfismi non banali da $\mathbb{Z}_4$ a $\mathrm{Aut}(\mathbb{Z}_5)$ sono ϕ_1,ϕ_2 e ϕ_3 definiti:

$$\phi_1([1]_4)=\alpha$$

$$\phi_2([1]_4)=\alpha^2$$

$$\phi_3([1]_4)=\alpha^3$$

Consideriamo l'isomorfismo:

$$\mathrm{f} : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_4$$

$$[1]_4 \longmapsto [3]_4$$

allora vediamo che $\phi_3=\phi_1 \circ \mathrm{f}$, consegue:

$$\mathbb{Z}_5 \rtimes_{\phi_1} \mathbb{Z}_4 \simeq \mathbb{Z}_5 \rtimes_{\phi_3} \mathbb{Z}_4$$

con un calcolo diretto si mostra che $\mathbb{Z}_5 \rtimes_{\phi_2} \mathbb{Z}_4$ ha 3 elementi di ordine 2 mentre $\mathbb{Z}_5 \rtimes_{\phi_1} \mathbb{Z}_4$ ha 5 elementi di ordine 2 e quindi si ha la tesi. □

Lemma 25. *A meno di isomorfismo, c'è un solo prodotto semidiretto tra $\mathbb{Z}_5$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$*

Dimostrazione. Gli omomorfismi non banali da $\mathbb{Z}_2 \times \mathbb{Z}_2$ a Aut($\mathbb{Z}_5$) sono ψ_1,ψ_2 e ψ_3 definiti da:

$$\psi_1([0]_2,[1]_2)=\mathrm{Id} \text{ e } \psi_1([1]_2,[0]_2)=\alpha^2$$

$$\psi_2([0]_2,[1]_2)=\alpha^2 \text{ e } \psi_2([1]_2,[0]_2)=\mathrm{Id}$$

$$\psi_3([0]_2,[1]_2)=\alpha^2 \text{ e } \psi_3([1]_2,[0]_2)=\alpha^2$$

considerando gli isomorfismi:

$$\mathrm{f} : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$([1]_2,[0]_2) \longmapsto ([0]_2,[1]_2)$$

$$([0]_2,[1]_2) \longmapsto ([1]_2,[0]_2)$$

e

$$\mathrm{g} : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$([1]_2,[0]_2) \longmapsto ([1]_2,[1]_2)$$

$$([0]_2,[1]_2) \longmapsto ([0]_2,[1]_2)$$

si nota che

$$\psi_2=\psi_1 \circ \mathrm{f}$$

$$\psi_3=\psi_2 \circ \mathrm{g}$$

consegue:

$$\mathbb{Z}_5 \rtimes_{\psi_1} (\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_5 \rtimes_{\psi_2} (\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_5 \rtimes_{\psi_3} (\mathbb{Z}_2 \times \mathbb{Z}_2)$$

e quindi si ha la tesi. □

Teorema 41. *Sia G un gruppo :* $|\, G \,|$ *= 20, allora* $G \simeq \mathbb{Z}_{20} \vee G \simeq \mathbb{Z}_{10} \times \mathbb{Z}_2 \vee G \simeq \mathbb{Z}_5 \rtimes_{\phi_1} \mathbb{Z}_4 \vee G \simeq \mathbb{Z}_5 \rtimes_{\phi_2} \mathbb{Z}_4 \vee G \simeq \mathbb{Z}_5 \rtimes_{\psi_1} (\mathbb{Z}_2 \times \mathbb{Z}_2)$ *dove* ϕ_1,ϕ_2 *e* ψ_1 *sono definiti nei lemmi anteriori.*

Dimostrazione. Osserviamo che 20=5·2^2.Abbiamo che n_5=1 e $n_2 \in \{1, 5\}$.Sia N l'unico sottogruppo normale di G di ordine 5 abbiamo 2 possibilità:

- n_2=1

  allora detto H l'unico sottogruppo normale di G di ordine 4 si ha immediatamente che:

  $$\mathrm{G} \simeq \mathrm{N} \times \mathrm{H}$$

  e quindi:

  $$\mathrm{G} \simeq \mathbb{Z}_5 \times \mathbb{Z}_4 \simeq \mathbb{Z}_{20}$$

  oppure

  $$\mathrm{G} \simeq \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq \mathbb{Z}_{10} \times \mathbb{Z}_2$$

- n_2=5

  sia H un 2-sylow di G.Allora:

  $$\mathrm{G} \simeq \mathrm{N} \rtimes_a \mathrm{H}$$

  per qualche omomorfismo a : H $\longrightarrow$ Aut(N).Deduciamo che se H $\simeq \mathbb{Z}_4$ allora G è isomorfo a un prodotto semidiretto non banale tra $\mathbb{Z}_5$ e $\mathbb{Z}_4$ e quindi, dal lemma 24:

$$G \simeq \mathbb{Z}_5 \rtimes_{\phi_1} \mathbb{Z}_4 \vee G \simeq \mathbb{Z}_5 \rtimes_{\phi_2} \mathbb{Z}_4$$

se invece H è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ allora G è isomorfo a un prodotto semidiretto non banale tra $\mathbb{Z}_5$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$,tuttavia questi sono tutti tra loro isomorfi per il lemma 25 e quindi possiamo dire che:

$$G \simeq \mathbb{Z}_5 \rtimes_{\psi_1} (\mathbb{Z}_2 \times \mathbb{Z}_2)$$

e quindi si ha la tesi □

Osservazione 17. *Osserviamo che $\mathbb{Z}_{20}$ e $\mathbb{Z}_{10} \times \mathbb{Z}_2$ sono gruppi abeliani non isomorfi (perchè (2,10)$\neq$ 1) mentre i gruppi $\mathbb{Z}_5 \rtimes_{\phi_1} \mathbb{Z}_4$, $\mathbb{Z}_5 \rtimes_{\phi_2} \mathbb{Z}_4$ e $\mathbb{Z}_5 \rtimes_{\psi_1} (\mathbb{Z}_2 \times \mathbb{Z}_2)$ sono gruppi abeliani non isomorfi. Infatti il primo ha 5 elementi di ordine 2, il secondo 3 elementi di ordine 2 mentre l'ultimo ne ha 11.Quindi i gruppi del teorema anteriore sono tutti non isomorfi.*

5.10 Gruppi di ordine 21

Teorema 42. *Sia G un gruppo : $|G| = 21$. Allora:*

$$G \simeq \mathbb{Z}_{21} \vee G \simeq \mathbb{Z}_7 \rtimes_{\Phi} \mathbb{Z}_3$$

dove $\phi([1]_3)([1]_7) = [2]_7$

Dimostrazione. Osserviamo che 21=3 · 7 quindi deduciamo che n_7=1 e $n_3 \in \{1, 7\}$.Denotiamo con N il sottogruppo normale di ordine 7 di G, distinguiamo due casi:

1. n_3=1. Allora detto H il sottogruppo normale di G di ordine 3 si ha dal teorema numerico che:

$$G \simeq K \times H \simeq \mathbb{Z}_7 \simeq \mathbb{Z}_3 \simeq \mathbb{Z}_{21}$$

2. n_3=7. Allora detto H un sottogruppo di G di ordine 3 si ha che:

$$G \simeq K \rtimes_{\gamma} H$$

per qualche omomorfismo $\gamma : H \longrightarrow$ Aut(K).Da cui:

$$G \simeq \mathbb{Z}_7 \rtimes_{\tilde{\phi}} \mathbb{Z}_3$$

per qualche omomorfismo non banale $\tilde{\phi} : \mathbb{Z}_3 \longrightarrow \text{Aut}(\mathbb{Z}_7)$. Mostriamo ora che tutti i prodotti semidiretti non banali da $\mathbb{Z}_7$ a $\mathbb{Z}_3$ sono isomorfi. Iniziamo ad osservare che gli omomorfismi non banali da $\mathbb{Z}_3$ a Aut($\mathbb{Z}_7$) sono due. Infatti sia:

$$\text{F} : \mathbb{Z}_6 \longrightarrow \text{Aut}(\mathbb{Z}_7)$$

un isomorfismo. Allora la mappa:

$$\Phi : \text{Hom}(\mathbb{Z}_3,\mathbb{Z}_6) \longrightarrow \text{Hom}(\mathbb{Z}_3,\text{Aut}(\mathbb{Z}_7))$$

$$\text{f} \longmapsto \text{F} \circ \text{f}$$

è una biezione. Osserviamo che gli omomorfismi non banali da $\mathbb{Z}_3$ a $\mathbb{Z}_6$ sono 2, precisamente:

$$\text{h},\tilde{h} : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_6$$

con h($[1]_3$)=$[2]_6$ e $\tilde{h}([1]_3)=[4]_6$ quindi gli omomorfismi non banali da $\mathbb{Z}_3$ a Aut($\mathbb{Z}_7$) sono Φ(h) e $\Phi(\tilde{h})$. Ora siccome:

$$\tilde{h} = \text{h} \circ \text{g}$$

dove:

$$\text{g} : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$$

$$[1]_3 \longmapsto [2]_3$$

deduciamo che:

$$\Phi(\tilde{h}) = \Phi(\text{h}) \circ \text{g}$$

e quindi tutti i semidiretti non banali da $\mathbb{Z}_7$ a $\mathbb{Z}_3$ sono isomorfi.Siccome $\mathbb{Z}_7 \rtimes_\Phi \mathbb{Z}_3$ con $\phi([1]_3)([1]_7) = [2]_7$è un prodotto semidiretto non banale si ha la tesi

□

Osservazione 18. *I gruppi che compaiono nel teorema anteriore sono non isomorfi. Infatti* $\mathbb{Z}_{21}$ *è abeliano mentre* $\mathbb{Z}_7 \rtimes_\Phi \mathbb{Z}_3$ *non è abeliano.*

5.11 Gruppi di ordine 24

Lemma 26. *(Lemma NC) Sia G un gruppo e H ≤ G. Allora:*

1. $C_G(H) \trianglelefteq N_G(H)$
2. $\frac{N_G(H)}{C_G(H)} \simeq$ *K con K ≤ Aut(H)*

Dimostrazione. Definiamo l'applicazione:

$$\phi : N_G(H) \longrightarrow \text{Aut(H)}$$

$$\text{x} \longmapsto \phi\text{(x)}$$

dove ϕ(x)(h) = xhx^{-1} $\forall$ h $\in$ H.Iniziamo a vedere che ϕ è un omomorfismo. Chiaramente ϕ è ben definita.Per vedere che è un omomorfismo siano x e y $\in N_G(H)$ e h $\in$ H, dimostriamo che ϕ(xy)(h) =(ϕ(x) $\circ$ ϕ(y))(h). Effettivamente:

$$(\ \phi\text{(x)} \circ \phi\text{(y)}\ )\text{(h)} = \phi\text{(x)(yh}y^{-1}\text{)=xyh(xy)}^{-1} = \phi\text{(xy)(h)}.$$

Ora dimostriamo che Kerϕ = $C_G(H)$. Effettivamente:

$$\text{x} \in \text{Ker}\phi \iff \text{xh}x^{-1}\text{=h } \forall \text{ h} \in \text{H} \iff \text{xh=hx } \forall \text{ h} \in \text{H} \iff \text{x} \in C_G(H)$$

pertanto il primo punto è dimostrato.Adesso, per il primo teorema di isomorfismo si ha che:

$$\frac{N_G(H)}{C_G(H)} = \frac{N_G(H)}{Ker\phi} \simeq \phi(N_G(H)) \leq \text{Aut(H)}$$

e quindi si ha la tesi.

□

Lemma 27. *Sia G un gruppo e a,b ∈ G di ordine finito : ab=ba e (o(a),o(b))=1 Allora:*

$$o(ab)=o(a)o(b)$$

Dimostrazione. Iniziamo ad osservare che

$$(ab)^{o(a)o(b)} = a^{o(a)o(b)}b^{o(a)o(b)}=(a^{o(a)})^{o(b)}(b^{o(b)})^{o(a)}=1$$

ora sia k un naturale tale che $(ab)^k$=1, dimostriamo che k $\geq$ o(a)o(b). Siccome (o(a),o(b))=1 si ha che m.c.m(o(a),o(b))=o(a)o(b). Quindi se mostriamo che k è un multiplo di o(a) e di o(b) avremmo finito. Effettivamente:

$$(ab)^k\text{=1} \rightarrow (ab)^{ko(b)}\text{=1} \rightarrow a^{ko(b)}\text{=1} \rightarrow \text{o(a) | ko(b)} \rightarrow \text{o(a) | k}$$

similmente:

$$(ab)^k\text{=1} \rightarrow (ab)^{ko(a)}\text{=1} \rightarrow b^{ko(a)}\text{=1} \rightarrow \text{o(b)} \mid \text{ko(a)} \rightarrow \text{o(b)} \mid \text{k}$$

e quindi la tesi.

□

Lemma 28. *Sia G un gruppo finito e p un primo : p | | G |. Detto P un p-sylow di G si ha che:*

$$N_G(P) = N_G(N_G(P))$$

Dimostrazione. Sappiamo che $N_G(P) \leq N_G(N_G(P))$. Dimostriamo che $N_G(N_G(P)) \leq N_G(P)$.Sia quindi x $\in N_G(N_G(P))$, dimostriamo che P^x = P.Abbiamo:

$$P^x \leq N_G(P)^x = N_G(P)$$

Quindi P^x è un p-sylow di $N_G(P)$, così come P, e quindi, siccome tutti i p-sylow sono coniugati, esiste y $\in N_G(P)$ tale che

$$P^x = P^y = \text{P}$$

e quindi la tesi □

Lemma 29. *Sia G un gruppo : | G | = 24 , n_3=4 e n_2=3. Allora:*

$$G \simeq S_4$$

Dimostrazione. Iniziamo ad osservare che, essendo n_3=4 e n_2=3,G non possiede elementi di ordine 6. Sia ora A := Syl_3(G) = $\{H_1, ..., H_4\}$. G agisce su A tramite la mappa:

$$\Phi : \text{G} \longrightarrow S_A$$

$$\text{g} \longmapsto \Phi(\text{g})$$

dove Φ(g)(H_i)=$g^{-1}H_ig$ i=1,...,4. Essendo $S_A \simeq S_4$ se mostriamo che Φ è un isomorfismo abbiamo concluso. Essendo Φ un omomorfismo è sufficiente mostrare che Φ è biettiva. Inoltre siccome dominio e codominio sono insiemi finiti della stessa cardinalità è sufficiente far vedere che Φ è iniettiva. Sia P un 3-sylow di G. Osserviamo che se g $\in$ KerΦ allora P = $g^{-1}Pg$ e quindi g $\in N_G(P)$. Consegue che:

$$\text{Ker}\Phi \leq N_G(P) \rightarrow |\text{Ker}\Phi| \mid |N_G(P)|$$

ma dal secondo teorema di Sylow:

$$4 = n_3(G) = [G : N_G(P)] = \frac{24}{|\ N_G(P)\ |}$$

da cui :

$$|N_G(P)| = 6.$$

ma allora

$$|\mathrm{Ker}\Phi| \in \{1, 2, 3, 6\}$$

Ora $|N_G(P)| = 6$ quindi $N_G(P) \simeq S_3$ quindi $N_G(P)$ non ha sottogruppi normali di ordine 2. Pertanto non può accadere che $|\mathrm{Ker}\Phi| = 2$. Supponiamo ora per assurdo che $|\mathrm{Ker}\Phi| = 6$, allora $\mathrm{Ker}\Phi = N_G(P)$. Quindi essendo $\mathrm{Ker}\Phi$ normale in G si avrebbe G = $N_G(Ker\Phi)$=$N_G(N_G(P))$. Ma dal lemma anteriore $N_G(N_G(P)) = N_G(P)$ e quindi si avrebbe G = $N_G(P)$ assurdo.Infine se per assurdo $|\mathrm{Ker}\Phi| = 3$ allora per il lemma NC si avrebbe:

$$\frac{G}{C_G(Ker\Phi)} = \frac{N_G(Ker\Phi)}{C_G(Ker\Phi)} \simeq \mathrm{K}$$

dove $\mathrm{K} \leq \mathrm{Aut}(\mathrm{Ker}\Phi) \simeq \mathrm{Aut}(\mathbb{Z}_3) \simeq \mathbb{Z}_2$. Di conseguenza se K è il sottogruppo banale allora $C_G(Ker\Phi)$=G e quindi esiste x in $C_G(Ker\Phi)$ di ordine 2 (per il lemma di Cauchy), se invece K ha ordine 2 allora $C_G(Ker\Phi)$ ha ordine 12 e sempre per il lemma di Cauchy esiste un elemento in $C_G(Ker\Phi)$ di ordine 2. Quindi esiste y $\in C_G(Ker\Phi)$ di ordine 2. Ma allora preso z $\in \mathrm{Ker}\Phi$ di ordine 3 si ha : o(zy)=6 (infatti z e y commutano , hanno entrambi ordine finito con ordini coprimi) e quindi esiste un elemento in G di ordine 6, assurdo.Pertanto $|\mathrm{Ker}\Phi| = 1$ e si ha la tesi. □

Lemma 30. *Aut(Q_8)* $\simeq S_4$

Dimostrazione. Basta osservare che Aut(Q_8) ha 24 elementi , n_3=4 e n_2=3 (ad esempio si può usare GAP per verificarlo) □

Lemma 31. *A meno di isomorfismi c'è un unico prodotto semidiretto non banale tra Q_8 e $\mathbb{Z}_3$*

.

Dimostrazione. Un omomorfismo non banale tra $\mathbb{Z}_3$ e Aut(Q_8) è completamente determinato dove mappa $[1]_3$. L'immagine deve avere ordine 3. Ora in Aut(Q_8) ci sono esattamente 8 elementi di ordine 3 (perchè in S_4 ci sono 8 elementi di ordine 3) quindi ci sono 8 prodotti semidiretti non banali tra Q_8 e $\mathbb{Z}_3$, consideriamone due distinti, $Q_8 \rtimes_{\Psi_1} \mathbb{Z}_3$ e $Q_8 \rtimes_{\Psi_2} \mathbb{Z}_3$,

mostriamo che $Q_8 \rtimes_{\Psi_1} \mathbb{Z}_3 \simeq Q_8 \rtimes_{\Psi_2} \mathbb{Z}_3$. Siccome tutti gli elementi di ordine 3 in S_4 sono coniugati $\Psi_1([1]_3)$ e $\Psi_2([1]_3)$ sono coniugati cioè esiste α in Aut(Q_8) tale che:

$$\alpha \circ \Psi_1([1]_3)\ \alpha^{-1} = \Psi_2([1]_3)$$

deduciamo che :

$$Q_8 \rtimes_{\Psi_1} \mathbb{Z}_3 \simeq Q_8 \rtimes_{\Psi_2} \mathbb{Z}_3$$

e cioè la tesi □

Osservazione 19. *Si osservi che un prodotto semidiretto non banale tra $\mathbb{Z}_3$ e Q_8 è dato da $Q_8 \rtimes_{\gamma_1} \mathbb{Z}_3$ dove $\gamma_1([1]_3)$(i)=j e $\gamma_1([1]_3)$(j)=k*

Lemma 32. *A meno di isomorfismi c'è un unico prodotto semidiretto non banale tra $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ e $\mathbb{Z}_3$*

Dimostrazione. Un omomorfismo non banale tra $\mathbb{Z}_3$ e Aut($\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$) è completamente determinato dove mappa $[1]_3$. L'immagine deve avere ordine 3. Ora in Aut($\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$) ci sono esattamente 56 elementi di ordine 3 (perchè in $GL_3(\mathbb{Z}_2)$ ci sono 56 elementi di ordine 3) quindi ci sono 56 prodotti semidiretti non banali tra $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ e $\mathbb{Z}_3$, consideriamone due distinti,$(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Psi_1} \mathbb{Z}_3$ e $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Psi_2} \mathbb{Z}_3$, mostriamo che $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Psi_1} \mathbb{Z}_3 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Psi_2} \mathbb{Z}_3$. Siccome tutti gli elementi di ordine 3 in $GL_3(\mathbb{Z}_2)$ sono coniugati $\Psi_1([1]_3)$ e $\Psi_2([1]_3)$ sono coniugati cioè esiste α in Aut($\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$) tale che:

$$\alpha \circ \Psi_1([1]_3)\ \alpha^{-1} = \Psi_2([1]_3)$$

deduciamo che :

$$(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Psi_1} \mathbb{Z}_3 \simeq (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\Psi_2} \mathbb{Z}_3$$

e cioè la tesi □

Osservazione 20. *Si osservi che un prodotto semidiretto non banale tra $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ e $\mathbb{Z}_3$ è dato da $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\gamma_2} \mathbb{Z}_3$ dove $\gamma_2([1]_2, [0]_2, [0]_2)$=$([0]_2, [1]_2, [0]_2)$, $\gamma_2([0]_2, [1]_2, [0]_2)$=$([0]_2, [0]_2, [1]_2)$ e $\gamma_2([0]_2, [0]_2, [1]_2)$=$([1]_2, [0]_2, [0]_2)$*

Osservazione 21. *Osserviamo che Aut($\mathbb{Z}_3$) =$\{Id, \phi_1\}$ dove $\phi_1([1]_3) = [2]_3$*

Lemma 33. *C'è un solo prodotto semidiretto non banale tra $\mathbb{Z}_3$ e $\mathbb{Z}_8$. Questo è $\mathbb{Z}_3 \rtimes_{\gamma_3} \mathbb{Z}_8$ dove $\gamma_3([1]_8)$=ϕ_1*

Dimostrazione. Basta osservare che l'unico omomorfismo non banale da $\mathbb{Z}_8$ a Aut($\mathbb{Z}_3$) è proprio γ_3. □

Lemma 34. *A meno di isomorfismo ci sono due prodotti semidiretti non banali tra* $\mathbb{Z}_3$ *e* $\mathbb{Z}_4 \times \mathbb{Z}_2$

Dimostrazione. Osserviamo che gli omomorfismi non banali da $\mathbb{Z}_4 \times \mathbb{Z}_2$ a Aut($\mathbb{Z}_3$) sono:

$$f_1 : \mathbb{Z}_4 \times \mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$([1]_4, [0]_2) \longmapsto \text{Id}$$

$$([0]_4, [1]_2) \longmapsto \phi_1$$

$$f_2 : \mathbb{Z}_4 \times \mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$([1]_4, [0]_2) \longmapsto \phi_1$$

$$([0]_4, [1]_2) \longmapsto \text{Id}$$

$$f_3 : \mathbb{Z}_4 \times \mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$([1]_4, [0]_2) \longmapsto \phi_1$$

$$([0]_4, [1]_2) \longmapsto \phi_1$$

Ora poichè $f_2 = f_1 \circ$ g dove g è l'isomorfismo:

$$\text{g} : \mathbb{Z}_4 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \times \mathbb{Z}_2$$

$$([1]_4, [0]_2) \longmapsto ([0]_4, [1]_2)$$

$$([0]_4, [1]_2) \longmapsto ([1]_4, [0]_2)$$

si ha che:

$$\mathbb{Z}_3 \rtimes_{f_1} (\mathbb{Z}_4 \times \mathbb{Z}_2) \simeq \mathbb{Z}_3 \rtimes_{f_2} (\mathbb{Z}_4 \times \mathbb{Z}_2)$$

mentre

$$\mathbb{Z}_3 \rtimes_{f_2} (\mathbb{Z}_4 \times \mathbb{Z}_2) \text{ non è isomorfo a } \mathbb{Z}_3 \rtimes_{f_3} (\mathbb{Z}_4 \times \mathbb{Z}_2)$$

dato che il primo ha 7 elementi di ordine 2 il secondo 5 □

Lemma 35. *A meno di isomorfismi c'è un solo prodotto semidiretto non banale tra* $\mathbb{Z}_3$ *e* $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Dimostrazione. I prodotti semidiretti non banali tra $\mathbb{Z}_3$ e $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ sono $\mathbb{Z}_3 \rtimes_{h_i} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$ i=1,...,7 dove:

$$h_1 : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$([1]_2, [0]_2, [0]_2) \longmapsto \text{Id}$$

$$([0]_2, [1]_2, [0]_2) \longmapsto \text{Id}$$

$$([0]_2, [0]_2, [1]_2) \longmapsto \phi_1$$

$$h_2 : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$([1]_2, [0]_2, [0]_2) \longmapsto \text{Id}$$

$$([0]_2, [1]_2, [0]_2) \longmapsto \phi_1$$

$$([0]_2, [0]_2, [1]_2) \longmapsto \text{Id}$$

$$h_3 : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$([1]_2, [0]_2, [0]_2) \longmapsto \text{Id}$$

$$([0]_2, [1]_2, [0]_2) \longmapsto \phi_1$$

$$([0]_2, [0]_2, [1]_2) \longmapsto \phi_1$$

$$h_4 : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$([1]_2, [0]_2, [0]_2) \longmapsto \phi_1$$

$$([0]_2, [1]_2, [0]_2) \longmapsto \text{Id}$$

$$([0]_2, [0]_2, [1]_2) \longmapsto \text{Id}$$

$$h_5 : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$([1]_2, [0]_2, [0]_2) \longmapsto \phi_1$$

$$([0]_2, [1]_2, [0]_2) \longmapsto \text{Id}$$

$$([0]_2, [0]_2, [1]_2) \longmapsto \phi_1$$

$$h_6 : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$([1]_2, [0]_2, [0]_2) \longmapsto \phi_1$$

$$([0]_2, [1]_2, [0]_2) \longmapsto \phi_1$$

$$([0]_2, [0]_2, [1]_2) \longmapsto \text{Id}$$

$$h_7 : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$([1]_2, [0]_2, [0]_2) \longmapsto \phi_1$$

$$([0]_2, [1]_2, [0]_2) \longmapsto \phi_1$$

$$([0]_2, [0]_2, [1]_2) \longmapsto \phi_1$$

Ora, è immediato vedere che:

$$\mathbb{Z}_3 \rtimes_{h_1} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_3 \rtimes_{h_2} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_3 \rtimes_{h_4} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$$

e che:

$$\mathbb{Z}_3 \rtimes_{h_3} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_3 \rtimes_{h_5} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_3 \rtimes_{h_6} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$$

mostriamo che:

$$\mathbb{Z}_3 \rtimes_{h_1} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_3 \rtimes_{h_3} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$$

e che:

$$\mathbb{Z}_3 \rtimes_{h_6} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_3 \rtimes_{h_7} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$$

Effettivamente $\forall$ x $\in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ si ha che:

$$\phi_1 \circ h_1(x) \circ \phi_1 = h_3(\beta(x))$$

dove:

$$\beta : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$([1]_2, [0]_2, [0]_2) \longmapsto ([1]_2, [0]_2, [0]_2)$$

$$([0]_2, [1]_2, [0]_2) \longmapsto ([0]_2, [1]_2, [1]_2)$$

$$([0]_2, [0]_2, [1]_2) \longmapsto ([0]_2, [0]_2, [1]_2)$$

che è un isomorfismo. Quindi

$$\mathbb{Z}_3 \rtimes_{h_1} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_3 \rtimes_{h_3} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$$

Similmente $\forall$ x $\in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ si ha che:

$$\phi_1 \circ h_6(x) \circ \phi_1 = h_7(\beta_1(x))$$

dove:

$$\beta_1 : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$([1]_2, [0]_2, [0]_2) \longmapsto ([1]_2, [0]_2, [0]_2)$$

$$([0]_2, [1]_2, [0]_2) \longmapsto ([0]_2, [1]_2, [0]_2)$$

$$([0]_2, [0]_2, [1]_2) \longmapsto ([0]_2, [1]_2, [1]_2)$$

che è un isomorfismo. Quindi

$$\mathbb{Z}_3 \rtimes_{h_6} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_3 \rtimes_{h_7} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$$

e quindi si ha la tesi. □

Lemma 36. *A meno di isomorfismo c'è un solo prodotto semididretto non banale tra $\mathbb{Z}_3$ e Q_8.*

Dimostrazione. I prodotti semidiretti non banali tra $\mathbb{Z}_3$ e Q_8 sono $\mathbb{Z}_3 \rtimes_{g_i} Q_8$ i=1,2,3 dove:

$$g_1 : Q_8 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$\text{i} \longmapsto \text{Id}$$

$$\text{j} \longmapsto \phi_1$$

$$g_2 : Q_8 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$\text{i} \longmapsto \phi_1$$

$$\text{j} \longmapsto \text{Id}$$

$$g_3 : Q_8 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$\text{i} \longmapsto \phi_1$$

$$\text{j} \longmapsto \phi_1$$

Ovviamente $\mathbb{Z}_3 \rtimes_{g_1} Q_8 \simeq \mathbb{Z}_3 \rtimes_{g_2} Q_8$. Per vedere che:

$$\mathbb{Z}_3 \rtimes_{g_2} Q_8 \simeq \mathbb{Z}_3 \rtimes_{g_3} Q_8$$

è sufficiente osservare che $\forall$ x $\in Q_8$:

$$\phi_1 \circ g_2(x) \circ \phi_1 = g_3(\beta_2(x))$$

dove β_2 è l'isomorfismo:

$$\beta_2 : Q_8 \longrightarrow Q_8$$

$$\text{i} \longmapsto \text{i}$$

$$\text{j} \longmapsto \text{k}$$

e quindi si ha la tesi. □

Lemma 37. *A meno di isomorfismi ci sono due prodotti semidiretti non banali tra $\mathbb{Z}_3$ e D_4.*

Dimostrazione. I prodotti semidiretti non banali tra $\mathbb{Z}_3$ e D_4 sono dati da $\mathbb{Z}_3 \rtimes_{l_i} D_4$ i=1,2,3 dove:

$$l_1 : D_4 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$\text{r} \longmapsto \text{Id}$$

$$\text{s} \longmapsto \phi_1$$

$$l_2 : D_4 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$\text{r} \longmapsto \phi_1$$

$$\text{s} \longmapsto \text{Id}$$

$$l_3 : D_4 \longrightarrow \text{Aut}(\mathbb{Z}_3)$$

$$\text{r} \longmapsto \phi_1$$

$$\text{s} \longmapsto \phi_1$$

Ora. chiaramente:

$$\mathbb{Z}_3 \rtimes_{l_1} D_4 \simeq \mathbb{Z}_3 \rtimes_{l_2} D_4$$

mentre

$$\mathbb{Z}_3 \rtimes_{l_2} D_4 \text{ non è isomorfo a } \mathbb{Z}_3 \rtimes_{l_3} D_4$$

perchè $\mathbb{Z}_3 \rtimes_{l_2} D_4$ ha 11 elementi di ordine 2 mentre $\mathbb{Z}_3 \rtimes_{l_3} D_4$ ha 9 elementi di ordine 2. Quindi si ha la tesi. □

Lemma 38. *C'è un unico prodotto semidiretto tra $\mathbb{Z}_8$ e $\mathbb{Z}_3$, ed è quello banale*

Dimostrazione. Consideriamo un prodotto semidiretto tra $\mathbb{Z}_8$ e $\mathbb{Z}_3$ diciamo $\mathbb{Z}_8 \rtimes_\phi \mathbb{Z}_3$. ϕ è un omomorfismo da $\mathbb{Z}_3$ a Aut($\mathbb{Z}_8$). Ora ϕ è l'omomorfismo banale se mappa $[1]_3$ nell'identita di $\mathbb{Z}_8$. Effettivamente:

$$\text{o}(\phi([1]_3)) \mid 3 \rightarrow \text{o}(\phi([1]_3))=1 \vee \text{o}(\phi([1]_3))=3$$

ma Aut($\mathbb{Z}_8$) ha 4 elementi quindi non può esistere in Aut($\mathbb{Z}_8$) un elemento di ordine 3. Quindi o($\phi([1]_3)$)=1 da cui $\phi([1]_3)$=Id e quindi ϕ è l'omomorfismo banale. Conseguentemente il prodotto semidiretto $\mathbb{Z}_8 \rtimes_\phi \mathbb{Z}_3$ è banale.

□

Lemma 39. *C'è un unico prodotto semidiretto tra $\mathbb{Z}_4 \times \mathbb{Z}_2$ e $\mathbb{Z}_3$, ed è quello banale.*

Dimostrazione. Consideriamo un prodotto semidiretto tra $\mathbb{Z}_4 \times \mathbb{Z}_2$ e $\mathbb{Z}_3$ diciamo ($\mathbb{Z}_4 \times \mathbb{Z}_2$) $\rtimes_\psi \mathbb{Z}_3$. ψ è un omomorfismo da $\mathbb{Z}_3$ a Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$). Ora ψ è l'omomorfismo banale se mappa $[1]_3$ nell'identita di $\mathbb{Z}_4 \times \mathbb{Z}_2$. Effettivamente:

$$\text{o}(\psi([1]_3)) \mid 3 \rightarrow \text{o}(\psi([1]_3))=1 \vee \text{o}(\phi([1]_3))=3$$

ma Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) ha 8 elementi quindi non può esistere in Aut($\mathbb{Z}_4 \times \mathbb{Z}_2$) un elemento di ordine 3. Quindi o($\psi([1]_3)$)=1 da cui $\psi([1]_3)$=Id e quindi ψ è l'omomorfismo banale. Conseguentemente il prodotto semidiretto ($\mathbb{Z}_4 \times \mathbb{Z}_2$) $\rtimes_\psi \mathbb{Z}_3$ è banale. □

Lemma 40. *Aut(D_4) ha 8 elementi*

Dimostrazione. Un isomorfismo ϕ da D_4 a D_4 è completamente determinato dove mappa i generatori r ed s. Ora o(ϕ(r)) = 4 quindi, siccome in D_4 ci sono 2 elementi di ordine 4, abbiamo solo due scelte per ϕ(r). Similmente o(ϕ(s)) = 2 quindi, siccome in D_4 ci sono 5 elementi di ordine 2, abbiamo 5 scelte per ϕ(s). Deduciamo che , al massimo, ci sono 10 elementi in Aut(D_4). Ora consideriamo gli automorfismi interni di D_4, Inn(D_4). Adesso:

$$\frac{D_4}{Z(D_4)} \simeq \text{Inn}(D_4)$$

ma

$$\mid \frac{D_4}{Z(D_4)} \mid = \frac{8}{2} = 4$$

allora, siccome $\frac{D_4}{Z(D_4)}$ non può essere ciclico:

$$\frac{D_4}{Z(D_4)} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

quindi Inn(D_4) ha 4 elementi e tutti questi elementi (eccetto l'elemento neutro) hanno ordine 2. Dal fatto che ha 4 elementi deduciamo che (essendo un sottogruppo di Aut(D_4)) :

$$| \text{Aut}(D_4) | \in \{4, 8\}.$$

Tuttavia non può avere ordine 4 altrimenti:

$$\text{Aut}(D_4) = \text{Inn}(D_4)$$

e quindi tutti gli elementi di Aut(D_4) hanno ordine 2, ma questo è falso. Ad esempio l'isomorfismo:

$$\text{f} : D_4 \longrightarrow D_4$$

$$\text{r} \longmapsto \text{r}$$

$$\text{s} \longmapsto \text{sr}$$

ha ordine 4. Quindi si ha la tesi □

Lemma 41. *C'è un unico prodotto semidiretto tra D_4 e $\mathbb{Z}_3$, ed è quello banale.*

Dimostrazione. Consideriamo un prodotto semidiretto tra D_4 e $\mathbb{Z}_3$ diciamo $D_4 \rtimes_\gamma \mathbb{Z}_3$. γ è un omomorfismo da $\mathbb{Z}_3$ a Aut(D_4). Ora γ è l'omomorfismo banale se mappa $[1]_3$ nell'identita di D_4 . Effettivamente:

$$\text{o}(\gamma([1]_3)) \mid 3 \rightarrow \text{o}(\gamma([1]_3))=1 \vee \text{o}(\gamma([1]_3))=3$$

ma Aut(D_4) ha 8 elementi quindi non può esistere in Aut(D_4) un elemento di ordine 3. Quindi o($\gamma([1]_3)$)=1 da cui $\gamma([1]_3)$=Id e quindi γ è l'omomorfismo banale. Conseguentemente il prodotto semidiretto $D_4 \rtimes_\gamma \mathbb{Z}_3$ è banale. □

Teorema 43. *Sia G un gruppo : $|G|$ = 24. Allora G è isomorfo ad uno dei gruppi sotto elencati.*

- $\mathbb{Z}_{24}$
- $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2$
- $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathbb{Z}_3 \times Q_8$
- $\mathbb{Z}_3 \times D_4$

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_{\gamma_2} \mathbb{Z}_3$
- $Q_8 \rtimes_{\gamma_1} \mathbb{Z}_3$
- $\mathbb{Z}_3 \rtimes_{\gamma_3} \mathbb{Z}_8$
- $\mathbb{Z}_3 \rtimes_{f_1} (\mathbb{Z}_4 \times \mathbb{Z}_2)$
- $\mathbb{Z}_3 \rtimes_{f_3} (\mathbb{Z}_4 \times \mathbb{Z}_2)$
- $\mathbb{Z}_3 \rtimes_{h_1} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$
- $\mathbb{Z}_3 \rtimes_{g_1} Q_8$
- $\mathbb{Z}_3 \rtimes_{l_1} D_4$
- $\mathbb{Z}_3 \rtimes_{l_3} D_4$
- S_4

dove γ_1,γ_2,γ_3,f_1,f_3,h_1,g_1,l_1 e l_3 sono definiti nei lemmi e nelle osservazioni precedenti

Dimostrazione. Osserviamo che 24=3 $\cdot$ 2^3. Quindi $n_3 \in \{1, 4\}$ e $n_2 \in \{1, 3\}$. Distinguiamo i vari casi.

- n_2=n_3=1 .Allora detto H il sottogruppo normale di G di ordine 3 e K il sottogruppo normale di G di ordine 8, si ha, per il teorema numerico, che G $\simeq$ H $\times$ K. Dal teorema di classificazione per i gruppi di ordine 8 deduciamo che:

$$\text{G} \simeq \mathbb{Z}_3 \times \mathbb{Z}_8 \simeq \mathbb{Z}_{24} \vee \text{G} \simeq \mathbb{Z}_3 \times (\mathbb{Z}_4 \times \mathbb{Z}_2) \vee \text{G} \simeq \mathbb{Z}_3 \times (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \vee \text{G} \simeq \mathbb{Z}_3 \times Q_8 \vee \text{G} \simeq \mathbb{Z}_3 \times D_4$$

- n_2=1,n_3=4 . Allora detto H il sottogruppo normale di G di ordine 8 e K un sottogruppo di G di ordine 3 si ha, per il teorema di riconoscimento per i prodotti semidiretti, che G $\simeq$ H $\rtimes_a$ $\mathbb{Z}_3$ per qualche a : $\mathbb{Z}_3 \longrightarrow$ Aut(H) omomorfismo. Quindi se :

  1. H $\simeq$ $\mathbb{Z}_8$ per il lemma 38 G $\simeq$ $\mathbb{Z}_8 \times \mathbb{Z}_3$
  2. H $\simeq$ $\mathbb{Z}_4 \times \mathbb{Z}_2$ per il lemma 39 G $\simeq$ $(\mathbb{Z}_4 \times \mathbb{Z}_2) \times \mathbb{Z}_3$
  3. H $\simeq$ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ per il lemma 32 e l'osservazione 20 G $\simeq$ ($\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$) $\rtimes_{\gamma_2}$ $\mathbb{Z}_3$

4. H $\simeq Q_8$ per il lemma 31 e l'osservazione 19 G $\simeq Q_8 \rtimes_{\gamma_1} \mathbb{Z}_3$
5. H $\simeq D_4$ per il lemma 41 G $\simeq D_4 \times \mathbb{Z}_3$.

- n_2=3,n_3=1. Allora detto H il sottogruppo normale di G di ordine 3 e K un sottogruppo di G di ordine 8 si ha che G $\simeq \mathbb{Z}_3 \rtimes_b$ K per qualche omomorfismo b : K $\longrightarrow$ Aut($\mathbb{Z}_3$).Quindi se:

  1. K $\simeq \mathbb{Z}_8$ per il lemma 33 G $\simeq \mathbb{Z}_3 \rtimes_{\gamma_3} \mathbb{Z}_8$
  2. K $\simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ per il lemma 34 G $\simeq \mathbb{Z}_3 \rtimes_{f_1} (\mathbb{Z}_4 \times \mathbb{Z}_2) \vee$ G $\simeq \mathbb{Z}_3 \rtimes_{f_3} (\mathbb{Z}_4 \times \mathbb{Z}_2)$
  3. K $\simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ per il lemma 35 G $\simeq \mathbb{Z}_3 \rtimes_{h_1} (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$
  4. K $\simeq Q_8$ per il lemma 36 G $\simeq \mathbb{Z}_3 \rtimes_{g_1} Q_8$
  5. K $\simeq D_4$ per il lemma 37 G $\simeq \mathbb{Z}_3 \rtimes_{l_1} D_4 \vee$ G $\simeq \mathbb{Z}_3 \rtimes_{l_3} D_4$

- n_3 = 4 , n_2 = 3. Allora per il lemma 29 G $\simeq S_4$.

□

5.12 Gruppi di ordine 27

Siccome 27 = 3^3 con 3 primo si deduce che se G è un gruppo di ordine 27 allora G è isomorfo ad uno dei seguenti gruppi:

$$\mathbb{Z}_{27}, \mathbb{Z}_9 \times \mathbb{Z}_3, \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3, \text{Heis}(\mathbb{Z}_3), D_3$$

e si osservi che tali gruppi sono tutti non isomorfi per quanto detto nell'osservazione 12

5.13 Gruppi di ordine 28

Lemma 42. *C'è un solo prodotto semidiretto non banale tra $\mathbb{Z}_7$ e $\mathbb{Z}_4$*

Dimostrazione. Basta osservare che un omomorfismo non banale da $\mathbb{Z}_4$ a Aut($\mathbb{Z}_7$) è completamente determinato da dove mappa $[1]_4$. Siccome l'ordine dell'immagine di $[1]_4$ deve dividere 4 l'unica possibilità è che l'immagine abbia ordine 2 (non può avere ordine 4 perchè in Aut($\mathbb{Z}_7$) non ci sono elementi di ordine 4), ma in Aut($\mathbb{Z}_7$) c'è solo un elemento di ordine 2 (perchè è isomorfo a $\mathbb{Z}_6$) □

Osservazione 22. *Si osservi che il prodotto semidiretto non banale tra* $\mathbb{Z}_7$ *e* $\mathbb{Z}_4$ *è* $\mathbb{Z}_7 \rtimes_k \mathbb{Z}_4$ *dove k(*$[1]_4$*)(*$[1]_7$*)=*$[6]_7$

Lemma 43. *Tutti i prodotti semidiretti non banali tra* $\mathbb{Z}_7$ *e* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *sono isomorfi.*

Dimostrazione. Sia $\gamma : \mathbb{Z}_6 \longrightarrow \text{Aut}(\mathbb{Z}_7)$ un isomorfismo. Allora l'applicazione:

$$\text{F} : \text{Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2,\mathbb{Z}_6) \longrightarrow \text{Hom}(\mathbb{Z}_2 \times \mathbb{Z}_2,\text{Aut}(\mathbb{Z}_7))$$

$$\text{f} \longmapsto \gamma \circ \text{f}$$

è una biezione. Osserviamo che gli omomorfismi non banali da $\mathbb{Z}_2 \times \mathbb{Z}_2$ a $\mathbb{Z}_6$ sono dati da:

$$\phi_1 : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_6$$

$$([1]_2, [0]_2) \longmapsto [0]_6$$

$$([0]_2, [1]_2) \longmapsto [3]_6$$

$$\phi_2 : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_6$$

$$([1]_2, [0]_2) \longmapsto [3]_6$$

$$([0]_2, [1]_2) \longmapsto [0]_6$$

$$\phi_3 : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_6$$

$$([1]_2, [0]_2) \longmapsto [3]_6$$

$$([0]_2, [1]_2) \longmapsto [3]_6$$

quindi gli omomorfismi non banali da $\mathbb{Z}_2 \times \mathbb{Z}_2$ a Aut($\mathbb{Z}_7$) sono : F(ϕ_i) per i=1,2,3 Allora essendo:

$$\phi_2=\phi_1 \circ \text{g}$$

con

$$\text{g} : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$([1]_2, [0]_2) \longmapsto ([0]_2, [1]_2)$$

$$([0]_2, [1]_2) \longmapsto ([1]_2, [0]_2)$$

e

$$\phi_3=\phi_2 \circ \mathrm{h}$$

con

$$\mathrm{h} : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$([1]_2, [0]_2) \longmapsto ([1]_2, [0]_2)$$

$$([0]_2, [1]_2) \longmapsto ([1]_2, [1]_2)$$

otteniamo che:

$$\mathrm{F}(\phi_2)=\mathrm{F}(\phi_1) \circ \mathrm{g}$$

$$\mathrm{F}(\phi_3)=\mathrm{F}(\phi_2) \circ \mathrm{h}$$

con g,h isomorfismi, e quindi si ha:

$$\mathbb{Z}_7 \rtimes_{F(\phi_1)} (\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_7 \rtimes_{F(\phi_2)} (\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq \mathbb{Z}_7 \rtimes_{F(\phi_3)} (\mathbb{Z}_2 \times \mathbb{Z}_2)$$

e quindi si ha la tesi □

Teorema 44. *Sia G un gruppo :* $|\ G\ |$ *= 28. Allora:*

$$G \simeq \mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \vee G \simeq \mathbb{Z}_7 \times \mathbb{Z}_4 \vee G \simeq D_{14} \vee G \simeq \mathbb{Z}_7 \rtimes_k \mathbb{Z}_4.$$

dove k è definito nell'osservazione 22

Dimostrazione. Osserviamo che 28=$2^2 \cdot 7$. Deduciamo che n_7 = 1 mentre $n_2 \in \{1, 7\}$. Sia K il sottogruppo normale di G di ordine 7. Distinguiamo due casi:

1. n_2=1 . Allora detto H il sottogruppo normale di G di ordine 4 si ha dal teorema numerico che:

   $$\mathrm{G} \simeq \mathrm{K} \times \mathrm{H}$$

   quindi:

   $$\mathrm{G} \simeq \mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \vee \mathrm{G} \simeq \mathbb{Z}_7 \times \mathbb{Z}_4$$

2. n_2=7. Sia allora H un sottogruppo di G di ordine 4. Allora:

   $$\mathrm{G} \simeq \mathrm{K} \rtimes_\gamma \mathrm{H}$$

per qualche omomorfismo γ : H $\longrightarrow$ Aut(K).Quindi se H è isomorfo a $\mathbb{Z}_4$ allora

$$G \simeq \mathbb{Z}_7 \rtimes_k \mathbb{Z}_4$$

se invece H è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ allora H è isomorfo a un prodotto semidiretto non banale tra $\mathbb{Z}_7$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$, ma questi ultimi sono tutti isomorfi quindi possiamo scrivere:

$$G \simeq \mathbb{Z}_7 \rtimes_q (\mathbb{Z}_2 \times \mathbb{Z}_2)$$

per qualche omomorfismo non banale q : $\mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow$ Aut($\mathbb{Z}_7$)

Quindi se G è un gruppo di ordine 28 allora G $\simeq \mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \vee$ G $\simeq \mathbb{Z}_7 \times \mathbb{Z}_4 \vee$ G $\simeq \mathbb{Z}_7 \rtimes_q (\mathbb{Z}_2 \times \mathbb{Z}_2) \vee$ G $\simeq \mathbb{Z}_7 \rtimes_k \mathbb{Z}_4$. Adesso D_{14} è un gruppo di ordine 28 non abeliano con 15 elementi di ordine 2. Siccome $\mathbb{Z}_7 \rtimes_k \mathbb{Z}_4$ non ha 15 elementi di ordine 2 deduciamo che D_{14} $\simeq \mathbb{Z}_7 \rtimes_q (\mathbb{Z}_2 \times \mathbb{Z}_2)$ e quindi si ha la tesi. □

5.14 Gruppi di ordine 30

Teorema 45. *Sia G un gruppo di ordine 30. Allora:*

$$G \simeq \mathbb{Z}_{30} \vee G \simeq D_{15} \vee G \simeq \mathbb{Z}_5 \times S_3 \vee G \simeq \mathbb{Z}_3 \times D_5$$

Dimostrazione. Osserviamo che 30 = 2 · 3 · 5. Allora $n_3 \in \{1, 10\}$ e $n_5 \in \{1, 6\}$. Ora non può capitare che n_3=10 e n_5=6. Infatti altrimenti ci sarebbero 20 elementi di ordine 3 e 24 elementi di ordine 5 contro l'ipotesi che G ha 30 elementi.Quindi se H è un 3-sylow e K un 5-sylow uno dei due è normale in G e quindi possiamo supporre che HK sia un sottogruppo di G. Osserviamo che | HK | = 15 e , avendo indice 2 in G, HK $\triangleleft$ G. Quindi esiste N $\triangleleft$ G : | N | = 15. Sia ora W un 2-sylow di G.Abbiamo che:

$$G \simeq N \rtimes_\Psi W$$

per qualche omomorfismo Ψ : W $\longrightarrow$ Aut(N).Allora:

$$G \simeq \mathbb{Z}_{15} \rtimes_\Phi \mathbb{Z}_2$$

per qualche omomorfismo $\Phi : \mathbb{Z}_2 \longrightarrow$ Aut($\mathbb{Z}_{15}$).Adesso:

$$\text{Aut}(\mathbb{Z}_{15}) \simeq \text{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_5) \simeq \text{Aut}(\mathbb{Z}_3) \times \text{Aut}(\mathbb{Z}_5) \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$$

Adesso in $\mathbb{Z}_2 \times \mathbb{Z}_4$ ci sono 3 elementi di ordine 2 quindi G può essere isomorfo al massimo a quattro prodotti semidiretti tra $\mathbb{Z}_{15}$ e $\mathbb{Z}_2$. Ora siccome i gruppi $\mathbb{Z}_{30}$, D_{15} , $\mathbb{Z}_5 \times S_3$, $\mathbb{Z}_3 \times D_5$ sono tutti non isomorfi (il primo è abeliano mentre i restanti tre non sono abeliani. Per vedere che i restanti 3 non sono isomorfi possiamo contare gli elementi di ordine 2. D_{15} ha 15 elementi di ordine 2 , $\mathbb{Z}_5 \times S_3$ ha 3 elementi di ordine 2 mentre $\mathbb{Z}_3 \times D_5$ ha 5 elementi di ordine 2) si ha la tesi. □

Bibliografia

[1] D. Dikranjan e M. L. Lucido, Aritmetica e Algebra, Liguori Editore;

[2] I. N. Herstein, Algebra, Editori Riuniti (2003);

[3] http://math.uchicago.edu/ may/REU2016/REUPapers/Idelhaj.pdf

[4] https://kconrad.math.uconn.edu/blurbs/grouptheory/group16.pdf

[5] http://buzzard.ups.edu/courses/2012spring/projects/clausen-groups-16-ups-434-2012.pdf

[6] https://web.math.utk.edu/ finotti/f06/m455/g18.pdf

[7] https://kconrad.math.uconn.edu/blurbs/grouptheory/group12.pdf

[8] https://math.stackexchange.com/questions/tagged/group-theory

[9] https://kconrad.math.uconn.edu/blurbs/grouptheory/semidirect-product.pdf

[10] https://kconrad.math.uconn.edu/blurbs/grouptheory/genquat.pdf