SVOLGIMENTO DEL COMPITO DI ALGEBRA 2 DEL 12/11/2013 (PRIMO COMPITINO).

Nel seguito verrà svolto il Tema A e in ogni esercizio sarà specificata l'eventuale differenza col Tema B. Tale differenza è in ogni caso minima e la risoluzione si può adattare facilmente al tema B, con le seguenti specifiche: l'esercizio 2 è risolto per entrambi i temi, ed è specificato il risultato dell'esercizio 3 punto (c) del Tema B.

1 Esercizio 1

Sia G un p-gruppo finito e sia N un sottogruppo normale di G. Mostrare che se $N \neq \{1\}$ allora $N \cap Z(G) \neq \{1\}$.

Siccome N è normale in G, G agisce su N per coniugio. Siano $O_1, \dots, O_k$ le orbite di tale azione. Allora N è l'unione disgiunta di $O_1, \dots, O_k$ e quindi (*) $|N| = |O_1| + \ldots + |O_k|$. Se x appartiene a un'orbita O_i allora O_i non è altro che la classe di coniugio di x in G. Quindi dire che $O_i = \{x\}$ è come dire che x, che sta in N, appartiene al centro di G. Quindi $O_i = \{x\}$ se e solo se $x \in N \cap Z(G)$. Raggruppando nell'uguaglianza (*) le orbite con un solo elemento, siano esse $O_1, \dots, O_t$, otteniamo quindi (**) $|N| = |N \cap Z(G)| + \sum_{i=t+1}^{k} |O_i|$. Ne segue che $|O_i|$ è diverso da 1 per ogni $i = t+1, \dots, k$. Essendo orbite per l'azione del p-gruppo G, la loro cardinalità, dovendo dividere $|G|$ (essendo l'indice dello stabilizzatore di un elemento dell'orbita) dev'essere una potenza di p, in particolare p divide $|O_i|$ per ogni $i = t+1, \dots, k$. Siccome $N \neq \{1\}$ è un sottogruppo di G, che è un p-gruppo, $|N|$ è una potenza di p diversa da 1, in particolare p divide $|N|$ e quindi da (**) segue che p divide anche $|N \cap Z(G)|$. In particolare $N \cap Z(G) \neq \{1\}$.

2 Esercizio 2

Versione Tema A. Sia $G = \langle g \rangle$ un gruppo ciclico di ordine 90 e siano $H = \langle g^{12} \rangle$ e $K = \langle g^{80} \rangle$.

(a) Determinare $|H|$ e $|K|$.

Si ha $|H| = |\langle g^{12} \rangle| = o(g^{12}) = o(g)/(12, o(g)) = 90/(12, 90) = 90/6 = 15$, $|K| = |\langle g^{80} \rangle| = o(g^{80}) = o(g)/(80, o(g)) = 90/(80, 90) = 90/10 = 9$.

(b) Trovare l'ordine e un generatore per $H \cap K$ e per $\langle H, K \rangle$.

Osserviamo che un elemento di $\langle g^a \rangle \cap \langle g^b \rangle$ è del tipo g^m con m multiplo sia di a che di b, cioè multiplo di $mcm(a, b)$, per cui $\langle g^a \rangle \cap \langle g^b \rangle = \langle g^{mcm(a,b)} \rangle$. Osserviamo inoltre che un elemento di $\langle g^a, g^b \rangle$ è del tipo $g^{ax} g^{by} = g^{ax+by}$ al variare di $x, y \in \mathbb{Z}$ e cioè, per l'algoritmo di Euclide, del tipo g^d dove $d = (a, b)$ è il massimo comun divisore di a, b.

Ne segue nel nostro caso che $\langle g^{12}\rangle \cap \langle g^{80}\rangle = \langle g^{mcm(12,80)}\rangle = \langle g^{240}\rangle = \langle g^{(240,90)}\rangle = \langle g^{30}\rangle$ ha ordine $o(g^{30}) = 90/(90,30) = 3$ e $\langle g^{12}, g^{80}\rangle = \langle g^{(12,80)}\rangle = \langle g^{4}\rangle$ ha ordine $o(g^4) = 90/(90,4) = 45$.

(c) Quanti elementi di ordine 15 contiene G?

Di sicuro tutti gli elementi di G di ordine 15 stanno nell'unico sottogruppo di G di ordine 15 (G è ciclico), quindi sono tanti quanti gli elementi di ordine 15 in un gruppo ciclico di ordine 15, che sappiamo essere $\varphi(15) = 8$. Più esplicitamente, l'unico sottogruppo di G di ordine 15 è $\langle g^6\rangle$ e quindi gli elementi di G di ordine 15 sono del tipo g^{6k} con k tra 1 e 15 e coprimo con 15, cioè $k \in \{1, 2, 4, 7, 8, 11, 13, 14\}$.

(d) Quanti elementi di ordine 15 contiene il gruppo $H \times K$?

Si ha $H \cong C_{15}$ e $K \cong C_9$. Un elemento $(a, b) \in H \times K$ ha ordine $mcm(o(a), o(b))$. Infatti $(a, b)^n = (1, 1)$, cioè $(a^n, b^n) = (1, 1)$, cioè $a^n = 1 = b^n$, se e solo se $o(a), o(b)$ dividono n, se e solo se $mcm(o(a), o(b))$ divide n. Quindi (a, b) ha ordine 15 se e solo se $mcm(o(a), o(b)) = 15$. D'altra parte $o(a)$ divide $|H| = 15$ e $o(b)$ divide $|K| = 9$. Quindi le possibilità sono le seguenti: $o(a) = 15$ e $o(b) \in \{1, 3\}$ oppure $o(a) = 5$ e $o(b) = 3$. Nel primo caso abbiamo $\varphi(15) = 8$ scelte per a e $1 + \varphi(3) = 3$ scelte per b, nel secondo caso abbiamo $\varphi(5) = 4$ scelte per a e $\varphi(3) = 2$ scelte per b. In totale abbiamo quindi $8 \cdot 3 + 4 \cdot 2 = 32$ elementi di $H \times K$ di ordine 15.

Versione Tema B. Sia G un gruppo ciclico di ordine 120 e siano $H = \langle g^{18}\rangle$ e $K = \langle g^{28}\rangle$.

(a) Determinare $|H|$ e $|K|$.

Si ha $|H| = |\langle g^{18}\rangle| = o(g^{18}) = o(g)/(18, o(g)) = 120/(18, 120) = 120/6 = 20$, $|K| = |\langle g^{28}\rangle| = o(g^{28}) = o(g)/(28, o(g)) = 120/(28, 120) = 120/4 = 30$.

(b) Trovare l'ordine e un generatore per $H \cap K$ e per $\langle H, K\rangle$.

Osserviamo che un elemento di $\langle g^a\rangle \cap \langle g^b\rangle$ è del tipo g^m con m multiplo sia di a che di b, cioè multiplo di $mcm(a, b)$, per cui $\langle g^a\rangle \cap \langle g^b\rangle = \langle g^{mcm(a,b)}\rangle$. Osserviamo inoltre che un elemento di $\langle g^a, g^b\rangle$ è del tipo $g^{ax}g^{by} = g^{ax+by}$ al variare di $x, y \in \mathbb{Z}$ e cioè, per l'algoritmo di Euclide, del tipo g^d dove $d = (a, b)$ è il massimo comun divisore di a, b.

Ne segue nel nostro caso che $\langle g^{18}\rangle \cap \langle g^{28}\rangle = \langle g^{mcm(18,28)}\rangle = \langle g^{252}\rangle = \langle g^{(252,120)}\rangle = \langle g^{12}\rangle$ ha ordine $o(g^{12}) = 120/(120, 12) = 120/12 = 10$ e $\langle g^{18}, g^{28}\rangle = \langle g^{(18,28)}\rangle = \langle g^2\rangle$ ha ordine $o(g^2) = 120/(120, 2) = 120/2 = 60$.

(c) Quanti elementi di ordine 15 contiene G?

Di sicuro tutti gli elementi di G di ordine 15 stanno nell'unico sottogruppo di G di ordine 15 (G è ciclico), quindi sono tanti quanti gli elementi di ordine 15 in un gruppo di ordine 15, che sappiamo essere $\varphi(15) = 8$. Più esplicitamente, l'unico sottogruppo di G di ordine 15 è $\langle g^8\rangle$ e quindi gli elementi di G di ordine 15 sono del tipo g^{8k} con k tra 1 e 15 e coprimo con 15, cioè $k \in \{1, 2, 4, 7, 8, 11, 13, 14\}$.

(d) Quanti elementi di ordine 15 contiene il gruppo $H \times K$?

Si ha $H \cong C_{20}$ e $K \cong C_{30}$. Un elemento $(a, b) \in H \times K$ ha ordine $mcm(o(a), o(b))$. Infatti $(a, b)^n = (1, 1)$, cioè $(a^n, b^n) = (1, 1)$, cioè $a^n = 1 = b^n$, se e solo se $o(a), o(b)$ dividono n, se e solo se $mcm(o(a), o(b))$ divide n. Quindi (a, b) ha ordine 15 se e solo se $mcm(o(a), o(b)) = 15$. D'altra parte $o(a)$ divide $|H| = 20$ e $o(b)$ divide $|K| = 30$. Quindi le possibilità sono le seguenti: $o(a) = 1$ e $o(b) = 15$ oppure $o(a) = 5$ e $o(b) \in \{3, 15\}$. Nel primo caso abbiamo una scelta per a ($a = 1$) e $\varphi(15) = 8$ scelte per b, nel secondo caso abbiamo $\varphi(5) = 4$ scelte per a e $\varphi(3) + \varphi(15) = 2 + 8 = 10$ scelte per b. In totale abbiamo quindi $8 + 4 \cdot 10 = 48$ elementi di $H \times K$ di ordine 15.

3 Esercizio 3

Svolgeremo solo la versione Tema A. Nel Tema B cambiano solo i numeri coinvolti nel 5-ciclo e nel 3-ciclo, ma le risposte ai quesiti sono le stesse, eccetto la seguente: un β che va bene per il punto (c) nel Tema B è (5786).

Si considerino le permutazioni $\sigma = (12345)(678)$ e $\tau = (13524)(678)$.

(a) Determinare il numero di coniugati di σ nel gruppo simmetrico S_8.

In S_8 i coniugati di σ sono tutti e soli gli elementi con la sua stessa struttura ciclica, cioè struttura ciclica $(5, 3)$ (un prodotto di un 5-ciclo con un 3-ciclo a lui disgiunto). Un tale elemento è determinato dalla scelta dei 5 elementi coinvolti nel 5-ciclo in $\binom{8}{5}$ modi e dalla scelta successiva del particolare 5-ciclo in 4! modi e del particolare 3-ciclo in 2! modi (ricordo infatti che ci sono esattamente $(k-1)!$ cicli realizzabili con k elementi). In totale quindi otteniamo che σ ha $\binom{8}{5} \cdot 4! \cdot 2$ coniugati in S_8.

(b) Descrivere il centralizzante di σ in S_8, esibendone un insieme di generatori.

Abbiamo visto che σ ha $\binom{8}{5} \cdot 4! \cdot 2$ coniugati in S_8, per cui dall'equazione delle classi segue che l'ordine del centralizzante di σ in S_8 è $|C_{S_8}(\sigma)| = 8!/(\binom{8}{5} \cdot 4! \cdot 2) = 15$. D'altra parte σ ha ordine 15 e appartiene certamente a $C_{S_8}(\sigma)$ (commuta con se stesso), per cui $\langle \sigma \rangle$ è un sottogruppo di $C_{S_8}(\sigma)$, che ha ordine 15 e segue che $C_{S_8}(\sigma) = \langle \sigma \rangle$.

(c) Trovare $\beta \in S_8$ tale che $\tau = \beta \sigma \beta^{-1}$.

Un tale β si trova osservando che

$$\beta \sigma \beta^{-1} = (\beta(1)\ \beta(2)\ \beta(3)\ \beta(4)\ \beta(5)) \cdot (\beta(6)\ \beta(7)\ \beta(8)),$$

per cui basta scegliere β che manda $1 \mapsto 1$, $2 \mapsto 3$, $3 \mapsto 5$, $4 \mapsto 2$, $5 \mapsto 4$, $6 \mapsto 6$, $7 \mapsto 7$ e $8 \mapsto 8$, cioè $\beta = (2354)$.

(d) Esiste $\gamma \in A_8$ tale che $\tau = \gamma \sigma \gamma^{-1}$?

Mostriamo che la risposta è no: un tale γ è necessariamente una permutazione dispari. γ verifica $\gamma\sigma\gamma^{-1} = \tau = \beta\sigma\beta^{-1}$ da cui, moltiplicando a sinistra per β^{-1} e a destra per γ, abbiamo $\beta^{-1}\gamma\sigma = \sigma\beta^{-1}\gamma$, cioè $\beta^{-1}\gamma \in C_{S_8}(\sigma)$. Ma allora siccome $C_{S_8}(\sigma) = \langle\sigma\rangle$ si ha $\beta^{-1}\gamma \in \langle\sigma\rangle \subseteq A_8$ (osserviamo infatti che σ è una permutazione pari e quindi appartiene ad A_8). Dire che $\beta^{-1}\gamma \in A_8$ è come dire che β e γ hanno lo stesso segno, cioè sono entrambe pari oppure entrambe dispari. Siccome $\beta = (2354)$ è dispari, anche γ è dispari.

4 Esercizio 4

Svolgeremo solo la versione Tema A. Nel Tema B p e q sono scambiati.

Supponiamo che G sia un gruppo finito di ordine p^2q con p e q primi distinti. Denotiamo con $n_p(G)$ e $n_q(G)$ il numero dei p-sottogruppi di Sylow e dei q-sottogruppi di Sylow di G.

(a) Provare che se $n_p(G) \neq 1$ allora $p < q$.

Per il teorema di Sylow $n_p(G)$ divide l'indice di un p-Sylow, cioè $|G|/p^2 = q$, per cui siccome q è primo se $n_p(G) \neq 1$ allora $n_p(G) = q$. Per il teorema di Sylow $q = n_p(G) \equiv 1 \mod p$, cioè p divide $q-1$. In particolare $p \leq q-1$ per cui $p \leq q-1 < q$.

(b) Provare che se $n_p(G) \neq 1$ allora $n_q(G) \neq p$.

Supponiamo $n_p(G) \neq 1$. Come abbiamo già osservato, segue che $n_p(G) = q$. Se fosse $n_q(G) = p$ allora per il teorema di Sylow sarebbe $p = n_q(G) \equiv 1 \mod q$ da cui q divide $p-1$ e in particolare $q \leq p-1 < p$, assurdo: abbiamo dimostrato nel punto precedente che se $n_p(G) \neq 1$ allora $p < q$.

(c) Provare che se $n_q(G) = p^2$ allora G contiene $|G| - p^2$ elementi di ordine q.

Ogni q-Sylow ha q elementi, e siccome q è primo ogni q-Sylow è ciclico, e contiene un elemento di ordine 1 (l'identità) e $q-1$ elementi di ordine q. Siccome ogni elemento diverso da 1 in un q-Sylow genera da solo l'intero q-Sylow, segue che i $q-1$ elementi di ordine q di un dato q-Sylow non sono contenuti in nessun altro q-Sylow, e quindi il numero totale di elementi di ordine q in G è $(q-1)n_q(G)$. Se $n_q(G) = p^2$ otteniamo quindi esattamente $(q-1)p^2 = qp^2 - p^2 = |G| - p^2$ elementi di ordine q.

(d) Provare che G contiene almeno un sottogruppo di Sylow normale.

Per il teorema di Sylow, si tratta di dimostrare che uno tra $n_p(G)$ e $n_q(G)$ è uguale a 1. Supponiamo quindi per assurdo che sia $n_p(G) \neq 1 \neq n_q(G)$. Siccome $n_q(G)$ divide l'indice di un q-Sylow, cioè $p^2q/q = p^2$, segue che $n_q(G) \in \{1, p, p^2\}$. Siccome $n_q(G) \neq 1$ per ipotesi e, siccome $n_p(G) \neq 1$, $n_q(G) \neq p$ per il punto (b), per cui $n_q(G) = p^2$, quindi per il punto (c) G contiene esattamente $|G| - p^2$ elementi di ordine q. Siccome ogni p-Sylow contiene p^2 elementi, tutti di ordine diverso da q, segue che in G c'è spazio per al più un p-Sylow, e quindi, siccome ce n'è di sicuro almeno uno, segue che $n_p(G) = 1$, assurdo.

(e) Provare che G contiene almeno un sottogruppo normale di indice primo.

Se $n_p(G) = 1$ allora il p-Sylow è normale e ha indice q, primo. Supponiamo ora che sia $n_p(G) \neq 1$. Per il punto (d) segue allora che $n_q(G) = 1$. Siano P un p-Sylow di G e Q un q-Sylow di G. Allora siccome $n_q(G) = 1$, $Q \trianglelefteq G$. Ne segue che $PQ \leq G$ (un prodotto di due sottogruppi è un sottogruppo se uno dei due è normale). Inoltre PQ ha indice $|G : PQ| = p^2q/pq = p$, primo. Per concludere basta mostrare che $PQ \trianglelefteq G$. Ci sono due modi per procedere, naturalmente vanno bene entrambi.

- Senza "cannoni". Per il teorema di corrispondenza per mostrare che $PQ \trianglelefteq G$ basta mostrare che $PQ/Q \trianglelefteq G/Q$. Ma questo è vero perché G/Q ha ordine $|G|/q = p^2$, quindi è abeliano, per cui tutti i suoi sottogruppi sono normali.
- Con "cannoni". PQ ha ordine p, e $p < q$, quindi p è il più piccolo primo che divide $|G|$. Segue che $PQ \trianglelefteq G$ per un risultato dimostrato a lezione.

5 Esercizio 5

Svolgeremo solo la versione Tema A. Nel Tema B cambia solo la posizione dell' 1 fuori dalla diagonale nella definizione di g.

Sia $G = GL(2,5)$ il gruppo delle matrici invertibili 2×2 sul campo $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ e sia $N = SL(2,5)$ il sottogruppo di G formato dalle matrici in G che hanno determinante 1.

(a) Provare che N è un sottogruppo normale di G e che G/N è ciclico di ordine 4.

Per il teorema di Binet, la funzione $\det : G \to \mathbb{F}_5^* = \mathbb{F}_5 - \{0\}$ è un omomorfismo dal gruppo G al gruppo moltiplicativo del campo con 5 elementi $\mathbb{F}_5$. Il suo nucleo è N, e det è suriettivo, infatti se $a \in \mathbb{F}_5^*$ allora $\det \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = a$. Dal teorema di isomorfismo segue allora che $G/N \cong \mathbb{F}_5^*$. Segue che G/N ha ordine $5 - 1 = 4$. Per mostrare che è ciclico basta guardare quali sono gli ordini (moltiplicativi) degli elementi di $\mathbb{F}_5^* = \{1, 2, 3, 4\}$. L'ordine di 2 è 4, infatti $2^1 = 2$, $2^2 = 4$, $2^3 = 3$ e $2^4 = 1$ (stiamo lavorando modulo 5). Quindi G/N è ciclico.

(b) Determinare gli ordini di G e di N.

Per determinare $|G|$ contiamo le possibilità per le colonne: abbiamo $5^2 - 1$ scelte per la prima colonna (non dev'essere nulla) e $5^2 - 5$ scelte per la seconda (non dev'essere un multiplo della prima), quindi $|G| = (5^2-1)(5^2-5) = 2^5 \cdot 3 \cdot 5$. Dal punto precedente $|G/N| = 4$, quindi $|N| = |G|/4 = 2^3 \cdot 3 \cdot 5$.

(c) Sia $g := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$. Determinare l'ordine di g.

Mostriamo per induzione che se n è un intero positivo allora $g^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Il caso $n = 1$ è ovvio. Ora, per l'ipotesi induttiva abbiamo $g^{n+1} = g^n g = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$. Ne segue che l'ordine di g è uguale al più piccolo intero n tale che $n \equiv 0 \mod 5$, cioè $n = 5$. Quindi g ha ordine 5 in G.

(d) Trovare il centralizzante di g in G e in N.

Una matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ centralizza g se e solo se

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

In altre parole

$$\begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}.$$

Ciò significa $a = a+c$, $a+b = b+d$, $c+d = d$, cioè $c = 0$ e $a = d$. Ne segue che il centralizzante di g in G è

$$C_G(g) = \{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \ : \ a, b \in \mathbb{F}_5, \ a \neq 0 \},$$

e ha ordine 20 (ho 4 scelte per a e 5 scelte per b). Ne segue che il centralizzante di g in N (ciò ha senso, essendo $g \in N$) è

$$C_N(g) = C_G(g) \cap N = \{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \ : \ a, b \in \mathbb{F}_5, \ a^2 = 1 \}.$$

Siccome $\mathbb{F}_5$ è un campo, $a^2 = 1$ significa che $a = \pm 1$, quindi in questo caso ho 2 scelte per a e 5 scelte per b, da cui $|C_N(g)| = 2 \cdot 5 = 10$. Da ciò deduciamo anche che g ha $|G : C_G(g)| = \frac{2^5 \cdot 3 \cdot 5}{2^2 \cdot 5} = 24$ coniugati in G e $|N : C_N(g)| = \frac{2^3 \cdot 3 \cdot 5}{2 \cdot 5} = 12$ coniugati in N.

(e) Calcolare $n_5(G)$. Quanti sono gli elementi di G di ordine 5?

Siccome la massima potenza di 5 che divide $|G|$ è 5, e $\langle g \rangle$ ha ordine 5, segue che $\langle g \rangle$ è un 5-Sylow di G. Si ha quindi che $n_5(G) = |G : N_G(\langle g \rangle)|$. Ci sono due modi per procedere.

- Troviamo il normalizzante $N_G(\langle g\rangle)$. Un elemento $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ di G normalizza $\langle g\rangle$ se e solo se manda g in una sua potenza, cioè se e solo se esiste $n \in \mathbb{F}_5$ tale che
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$
In altre parole, svolgendo i calcoli, abbiamo
$$\frac{1}{ad-bc}\begin{pmatrix} ad-bc-ac & a^2 \\ -c^2 & ad-bc+ac \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$
Un tale n esiste se e solo se $-c^2 = 0$, cioè $c = 0$. Ne segue che
$$N_G(\langle g\rangle) = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \ : \ ad \neq 0\}.$$
Ne segue che $|N_G(\langle g\rangle)| = 5 \cdot 4^2$ (ho 5 scelte per b e 4 per a e per d) e quindi $n_5(G) = |G : N_G(\langle g\rangle)| = |G|/|N_G(\langle g\rangle)| = \frac{2^5 \cdot 3 \cdot 5}{2^4 \cdot 5} = 6$.
- Osserviamo che $N_G(\langle g\rangle)$ contiene $C_G(g)$, che ha ordine 20 (punto (d)), quindi 20 divide $|N_G(\langle g\rangle)|$ che divide $|G| = 20 \cdot 24$, da cui $n_5(G) = |G : N_G(\langle g\rangle)|$ divide 24. D'altra parte per il teorema di Sylow $n_5(G) \equiv 1 \mod 5$ quindi $n_5(G) \in \{1, 6\}$. Per mostrare che $n_5(G) = 6$ basta quindi mostrare che $n_5(G) \neq 1$, cioè che $\langle g\rangle$ non è normale in G. Questo segue dal fatto che
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$
non è una potenza di g per il punto (c). Ne segue che $n_5(G) = 6$.

Siccome i 5-Sylow hanno ordine 5, primo, il numero di elementi di G di ordine 5 è $(5-1)n_5(G) = 4 \cdot 6 = 24$.

(f) Provare che tutti gli elementi di G di ordine 5 sono coniugati.

Come abbiamo visto, G ha 24 elementi di ordine 5 (punto (e)), tanti quanti i coniugati di g (punto (d)). Siccome i coniugati di g hanno lo stesso ordine di g, e g ha ordine 5, segue che i coniugati di g sono tutti e soli gli elementi di G di ordine 5, per cui tutti gli elementi di G di ordine 5 sono coniugati.

(g) È vero che tutti gli elementi di N di ordine 5 sono coniugati in N?

Osserviamo che, siccome $g \in N$, tutti i G-coniugati di g stanno in N, essendo N normale (se $x \in G$ allora $xgx^{-1} \in xNx^{-1} = N$). Siccome tutti gli elementi di G di ordine 5 sono coniugati in G, segue che stanno tutti in N. Quindi se essi fossero tutti coniugati in N allora g avrebbe 24 coniugati in N. Ma abbiamo visto nel punto (d) che g ha 12 coniugati in N. Quindi non è vero che tutti gli elementi di N di ordine 5 sono coniugati.

6 Esercizio 6

Sia G un gruppo finito contenente un sottogruppo normale N con la proprietà che tutti gli elementi di N diversi da 1 sono coniugati in G. Provare che G contiene un sottogruppo di indice $|N|-1$ e dedurne $|G| \geq |N|^2 - |N|$.

Sia $x \in N$ con $x \neq 1$. Allora per l'ipotesi ogni elemento di $N - \{1\}$ è coniugato a x in G. D'altra parte, siccome N è normale, ogni coniugato di x sta in N, infatti se $g \in G$ allora $gxg^{-1} \in gNg^{-1} = N$. Ne segue che la classe di coniugio di x in G è esattamente $N - \{1\}$. Ma sappiamo che il numero di coniugati di un elemento è uguale all'indice del suo centralizzante, quindi abbiamo $|G : C_G(x)| = |N| - 1$, per cui il sottogruppo $C_G(x)$ di G ha indice $|N| - 1$ in G. In particolare $|N| - 1$ divide $|G|$. Siccome $N \leq G$, anche $|N|$ divide $|G|$. Siccome $|N|$ e $|N|-1$ sono coprimi, anche $|N|(|N|-1) = |N|^2 - |N|$ divide $|G|$, in particolare $|N|^2 - |N| \leq |G|$.