Algebra 2 - Prima prova parziale - 22 novembre 2012. Tema A. Risoluzione.

1

Siano a un elemento e H un sottogruppo del gruppo G.

1.1

Si definiscano $C(a)$, il centralizzante di a in G, e $N(H)$, il normalizzante di H in G.

Il centralizzante di a in G è

$$C(a) := \{g \in G \mid ga = ag\} = \{g \in G \mid gag^{-1} = a\} = \{g \in G \mid g^{-1}ag = a\}.$$

Il normalizzante di H in G è

$$N(H) := \{g \in G \mid g^{-1}Hg = H\} = \{g \in G \mid gH = Hg\}.$$

1.2

Nel gruppo simmetrico $G = S_5$ determinare gli ordini di $C(\gamma)$ e $N(\langle\gamma\rangle)$, dove $\gamma = (123)$.

Gli elementi di G coniugati a γ sono tutti e soli i 3-cicli, che sono $5 \cdot 4 \cdot 3/3$ (per il ciclo $(a\,b\,c)$ scelgo a in 5 modi, b in 4, c in 3 e tengo conto che ho 3 possibili scelte dell'elemento da cui iniziare la scrittura). Sappiamo che il numero di coniugati di γ è uguale all'indice del centralizzante di γ, e quindi avremo $20 = |G : C(\gamma)| = 5!/|C(\gamma)|$, da cui $|C(\gamma)| = 5!/20 = 6$.

Osserviamo che $\langle\gamma\rangle$ è un 3-sottogruppo di Sylow, perché la massima potenza di 3 che divide $|G| = 5!$ è 3. Ne segue, per il teorema di Sylow, che i sottogruppi di G coniugati a $\langle\gamma\rangle$ sono tutti e soli i 3-sottogruppi di Sylow. Ognuno di essi ha ordine 3, quindi contiene due 3-cicli ed è generato da ognuno di essi, quindi il numero di 3-sottogruppi di Sylow è $20/2 = 10$. Ricordiamo ora che il numero di 3-sottogruppi di Sylow è uguale al numero di coniugati di $\langle\gamma\rangle$, che è uguale all'indice del normalizzante di $\langle\gamma\rangle$, per cui $10 = |G : N(\langle\gamma\rangle)| = 5!/|N(\langle\gamma\rangle)|$, da cui $|N(\langle\gamma\rangle)| = 5!/10 = 12$.

1.3

Quanti sono i 3-sottogruppi di Sylow di S_5?

I 3-sottogruppi di Sylow di S_5, come visto al punto precedente, sono 10.

1.4

Dare generatori per i sottogruppi $C(\gamma)$ e $N(\langle\gamma\rangle)$ di S_5.

Siccome ogni potenza di γ commuta con γ, abbiamo $\langle\gamma\rangle \subseteq C(\gamma)$. Anche (45) commuta con γ (sono disgiunte), quindi $C(\gamma) \geq \langle\gamma, (45)\rangle$. Ma $C(\gamma)$ ha ordine

6 (come abbiamo già osservato) e $\langle\gamma,(45)\rangle$ ha ordine almeno $3\cdot 2 = 6$, quindi necessariamente $\langle\gamma,(45)\rangle = C(\gamma)$.

Per trovare generatori per $N(\langle\gamma\rangle)$ dobbiamo trovare elementi di S_5 che mandano, tramite coniugio, $\gamma = (123)$ in una sua potenza. Un elemento che coniuga γ in $\gamma^{-1} = (132)$ è scritto in notazione "funzionale" mettendo γ e γ^{-1} uno sotto l'altro:

$$(123)$$

$$(132)$$

La sua struttura ciclica è quindi (23). Ne segue che (23) normalizza $\langle\gamma\rangle$, e quindi $(23) \in N(\langle\gamma\rangle)$. Siccome anche $C(\gamma) \leq N(\langle\gamma\rangle)$ e $|C(\gamma)| = 6$, $o((23)) = 2$, e $(23) \notin C(\gamma)$, per il teorema di Lagrange il sottogruppo generato da $C(\gamma)$ e (23) ha ordine almeno 12. Siccome $|N(\langle\gamma\rangle)| = 12$, deduciamo che $N(\langle\gamma\rangle)$ è generato da γ, (45) e (23).

2

Siano G un gruppo finito, p un primo, N un sottogruppo normale di G.

2.1

Provare che per ogni p-sottogruppo di Sylow di G l'immagine PN/N è un p-sottogruppo di Sylow di G/N.

Anzitutto PN è un sottogruppo di G perchè N è normale, e contiene P. Siccome $PN/N \cong P/P\cap N$ è isomorfo ad un quoziente di P e P è un p-gruppo, per il teorema di Lagrange anche PN/N è un p-gruppo. Per concludere che PN/N è un p-sottogruppo di Sylow di G/N dobbiamo quindi dimostrare che $|G/N : PN/N|$ non è divisibile per p. Ma sappiamo che $|G/N : PN/N| = |G : PN|$ e che $|G : PN| \cdot |PN : P| = |G : P|$. Poichè P è un p-sottogruppo di Sylow di G l'indice $|G : P|$ è primo con p, e dunque anche $|G/N : PN/N|$ non è divisibile per p.

2.2

È vero che il numero dei p-sottogruppi di Sylow di G/N è minore o uguale del numero dei p-sottogruppi di Sylow di G?

Mostriamo che la risposta è sì. Ogni sottogruppo di G/N, per il teorema di corrispondenza, è della forma H/N con H sottogruppo di G contenente N. Supponiamo che H/N sia un p-sottogruppo di Sylow di G/N. Allora $|G : H| = |G/N : H/N|$ non è divisibile per p, cioè la massima potenza di p che divide $|H|$ coincide con la massima potenza di p che divide $|G|$, e un p-sottogruppo di Sylow P di H è un p-sottogruppo di Sylow di G. Per la prima parte dell'esercizio PN/N è un p-sottogruppo di Sylow di G/N, ed essendo $PN/N \leq H/N$ risulta

$H/N = PN/N$. Quindi la funzione

$$\mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G/N),\ P \mapsto PN/N$$

è ben definita (per il punto precedente) e suriettiva. Questo prova l'asserto.

3

Si consideri l'omomorfismo di anelli

$$\eta : \mathbb{Z}[X] \to \mathbb{Z},\ \eta(f) := f(2).$$

3.1

Verificare che $\ker(\eta) = (x-2)$.

- Mostriamo che $\ker(\eta) \subseteq (x-2)$. Se $f(x) \in \ker(\eta)$ allora $f(2) = 0$. Effettuando la divisione con resto di $f(x)$ con $x-2$ in $\mathbb{Z}[X]$ (si può fare perché $x-2$ è monico) otteniamo polinomi $g(x), r(x) \in \mathbb{Z}[X]$ con $r(x) = r \in \mathbb{Z}$ tali che $f(x) = g(x)(x-2) + r$. Da $f(2) = 0$ otteniamo $0 = f(2) = g(2) \cdot 0 + r = r$, per cui $r = 0$, cioè $f(x) = g(x)(x-2)$ e quindi $f(x) \in (x-2)$.

- Mostriamo che $(x-2) \subseteq \ker(\eta)$. Se $f(x) \in (x-2)$ allora esiste $g(x) \in \mathbb{Z}[X]$ con $f(x) = (x-2)g(x)$, da cui $f(2) = 0 \cdot g(2) = 0$ e quindi $f(x) \in \ker(\eta)$.

3.2

Dimostrare che per ogni primo p l'ideale $(p, x-2)$ è un ideale massimale di $\mathbb{Z}[X]$.

Consideriamo l'omomorfismo di anelli

$$\gamma : \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z},\ \gamma(f(x)) := f(2) + p\mathbb{Z}.$$

Si tratta della composizione di η con la proiezione canonica $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Il suo nucleo è

$$\ker(\gamma) = \{f(x) \in \mathbb{Z}[X] \mid f(2) + p\mathbb{Z} = p\mathbb{Z}\} = \{f(x) \in \mathbb{Z}[X] \mid p | f(2)\}.$$

Dimostriamo che $\ker(\gamma) = (p, x-2)$.

- Mostriamo che $\ker(\gamma) \subseteq (p, x-2)$. Sia $f(x) \in \ker(\gamma)$. Allora p divide $f(2)$, quindi esiste $c \in \mathbb{Z}$ con $f(2) = pc$. Ne segue che il polinomio $f(x) - pc$ ammette 2 come zero, quindi effettuando la divisione con resto come sopra riusciamo a scrivere $f(x) - pc = (x-2)g(x)$ per qualche $g(x) \in \mathbb{Z}[X]$. Ma allora $f(x) = g(x)(x-2) + pc \in (p, x-2)$.

- Mostriamo che $(p, x-2) \subseteq \ker(\gamma)$. Sia $a(x) = f(x)p + g(x)(x-2)$ un generico elemento di $(p, x-2)$, con $f(x), g(x) \in \mathbb{Z}[X]$. Si ha $a(2) = f(2)p + g(2) \cdot 0 = f(2)p \in p\mathbb{Z}$, da cui $a(x) \in \ker(\gamma)$.

L'omomorfismo γ è suriettivo in quanto se $n + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}$ allora $\gamma(n) = n + p\mathbb{Z}$. Segue dal teorema di isomorfismo per gli anelli che $\mathbb{Z}[X]/(p, x-2) \cong \mathbb{Z}/p\mathbb{Z}$ è un campo, e quindi $(p, x-2)$ è un ideale massimale di $\mathbb{Z}[X]$.

3.3

Dimostrare che ogni ideale massimale di $\mathbb{Z}[X]$ contenente $\ker(\eta)$ è del tipo $(p, x-2)$ con p primo.

Per il teorema di corrispondenza, gli ideali di $\mathbb{Z}[X]$ contenenti $\ker(\eta) = (x-2)$ sono in corrispondenza biunivoca con gli ideali di $\mathbb{Z}[X]/(x-2) \cong \mathbb{Z}$, cioè di $\mathbb{Z}$, e la corrispondenza è data da

$$\mathbb{Z}[X] \trianglerighteq I \mapsto \{f(2) \mid f(x) \in I\},$$

la sua inversa è data da

$$\mathbb{Z} \trianglerighteq J = n\mathbb{Z} \mapsto \{f(x) \in \mathbb{Z}[X] \mid f(2) \in n\mathbb{Z}\} = (n, x-2).$$

Resta da osservare che la corrispondenza preserva la massimalità. Facciamolo in generale. Sia A un anello commutativo unitario e siano I, J suoi ideali con $I \subseteq J$. Allora per il terzo teorema di isomorfismo per gli anelli si ha $A/J \cong (A/I)/(J/I)$ e quindi A/J è un campo se e solo se $(A/I)/(J/I)$ è un campo, in altre parole J è massimale in A se e solo se J/I è massimale in A/I.

3.4

Verificare che se p, q sono primi distinti allora $(p, x-2) \neq (q, x-2)$.

Se fosse $(p, x-2) = (q, x-2)$ allora si avrebbe

$$\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[X]/(p, x-2) = \mathbb{Z}[X]/(q, x-2) \cong \mathbb{Z}/q\mathbb{Z},$$

assurdo perché $|\mathbb{Z}/p\mathbb{Z}| = p \neq q = |\mathbb{Z}/q\mathbb{Z}|$.

4

Si consideri il gruppo di matrici

$$G = \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \{1, -1\},\ b \in \mathbb{Q}\}.$$

4.1

Si dimostri che per ogni sottogruppo S del gruppo additivo di $\mathbb{Q}$ l'insieme

$$H(S) = \{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in S\}$$

è un sottogruppo normale di G.

Chiaramente $H(S)$ contiene la matrice identica (basta scegliere $x = 0$), e se $x, y \in S$ si ha $x + y \in S$, essendo S un sottogruppo additivo di $\mathbb{Q}$, e quindi

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix} \in H(S).$$

Scegliendo $y = -x$ vediamo da qui che ogni elemento in $H(S)$ ha l'inverso in $H(S)$. Queste osservazioni dimostrano che $H(S)$ è un sottogruppo di G. Mostriamo che è normale. Sia $g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$. Il suo inverso è dato da $g^{-1} = \begin{pmatrix} a & -ba \\ 0 & 1 \end{pmatrix}$. Dato $x \in S$ si ha

$$\begin{aligned} g^{-1} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g &= \begin{pmatrix} a & -ba \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \\ &= \begin{pmatrix} a & ax - ba \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & xa \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Siccome $xa \in \{x, -x\}$ si ha $xa \in S$ (perché S è un sottogruppo additivo di $\mathbb{Q}$) e quindi otteniamo $H(S) \trianglelefteq G$.

4.2

Si verifichi che il centro di G è identico.

Il centro di G è dato da quegli elementi $g \in G$ tali che $gh = hg$ per ogni $h \in G$. Scriviamo $g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$ e $h = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \in G$. Effettuando i prodotti gh, hg vediamo che la condizione $gh = hg$ diventa

$$\begin{pmatrix} ac & bc + d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad + b \\ 0 & 1 \end{pmatrix}.$$

Otteniamo $bc + d = ad + b$, e questo deve essere vero per ogni $h \in G$, cioè per ogni $c \in \{1, -1\}$, $d \in \mathbb{Q}$. Scegliendo $d = 0$ e $c = -1$ otteniamo $b = -b$, cioè $b = 0$. Ma allora $d = ad$ per ogni $d \in \{-1, 1\}$, e scegliendo $d = 1$ otteniamo $a = 1$. Quindi $g = 1$.

4.3

Si elenchino gli elementi del centro di $G/H(\mathbb{Z})$.

Il centro di $G/H(\mathbb{Z})$ è dato da quegli elementi $gH(\mathbb{Z}) \in G/H(\mathbb{Z})$ tali che $ghH(\mathbb{Z}) = hgH(\mathbb{Z})$, cioè $g^{-1}h^{-1}gh \in H(\mathbb{Z})$, per ogni $h \in G$. Scriviamo $g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$ e $h = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \in G$. Ricordando che $a^2 = c^2 = 1$, un semplice conto dimostra che

$$g^{-1}h^{-1}gh = \begin{pmatrix} 1 & cd + acb - acd - ba \\ 0 & 1 \end{pmatrix}.$$

Quindi la condizione che $g^{-1}h^{-1}gh \in H(\mathbb{Z})$ per ogni $h \in G$ diventa la seguente: $cd + acb - acd - ba \in \mathbb{Z}$ per ogni $c \in \{1, -1\}$, $d \in \mathbb{Q}$. Scegliendo $c = 1$ otteniamo che $(1 - a)d \in \mathbb{Z}$ per ogni $d \in \mathbb{Q}$, e questo è possibile solo se $a = 1$ (se $a = -1$ allora $2d \in \mathbb{Z}$ per ogni $d \in \mathbb{Q}$, e questo è chiaramente falso, basta scegliere $d = 1/3$), quindi deduciamo che $a = 1$ e $b(c - 1) \in \mathbb{Z}$ per ogni $c \in \{1, -1\}$. In particolare scegliendo $c = -1$ otteniamo $2b \in \mathbb{Z}$. D'altra parte, se $a = 1$ e $2b \in \mathbb{Z}$ allora la condizione $cd + acb - acd - ba \in \mathbb{Z}$ è verificata per ogni $c \in \{-1, 1\}$, $d \in \mathbb{Q}$. Di conseguenza

$$Z(G/H(\mathbb{Z})) = \{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} H(\mathbb{Z}) \in G/H(\mathbb{Z}) \mid b \in \frac{1}{2}\mathbb{Z}\}.$$

Sia allora $b = \frac{n}{2}$ con $n \in \mathbb{Z}$. Se n è pari $gH(\mathbb{Z}) = H(\mathbb{Z})$. Se n è dispari, $n = 2k + 1$ con $k \in \mathbb{Z}$, allora $b = \frac{1}{2} + k$ e $gH(\mathbb{Z}) = \begin{pmatrix} 1 & 1/2 \\ 0 & 1 \end{pmatrix} H(\mathbb{Z})$. Questi sono i due elementi del centro di $G/H(\mathbb{Z})$.