Algebra 2 - Prima prova parziale - 22 novembre 2012. Tema B. 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 $G = S_6$ determinare gli ordini di $C(\alpha)$ e $N(\langle\alpha\rangle)$, dove $\alpha = (12345)$.

Gli elementi di G coniugati ad α sono tutti e soli i 5-cicli, che sono $6 \cdot 4!$ (scelgo il punto fissato in 6 modi e il 5-ciclo coinvolgente i punti mossi in 4! modi). Sappiamo che il numero di coniugati di α è uguale all'indice del centralizzante di α, e quindi avremo $6 \cdot 4! = |G : C(\alpha)| = 6!/|C(\alpha)|$, da cui $|C(\alpha)| = 6!/(6 \cdot 4!) = 5$.

Osserviamo che $\langle\alpha\rangle$ è un 5-sottogruppo di Sylow, perché la massima potenza di 5 che divide $|G| = 6!$ è 5. Ne segue, per il teorema di Sylow, che i sottogruppi di G coniugati a $\langle\alpha\rangle$ sono tutti e soli i 5-sottogruppi di Sylow. Ognuno di essi ha ordine 5, quindi contiene quattro 5-cicli ed è generato da ognuno di essi, quindi il numero di 5-sottogruppi di Sylow è $6 \cdot 4!/4 = 6 \cdot 6 = 36$. Ricordiamo ora che il numero di 5-sottogruppi di Sylow è uguale al numero di coniugati di $\langle\alpha\rangle$, che è uguale all'indice del normalizzante di $\langle\alpha\rangle$, per cui $36 = |G : N(\langle\alpha\rangle)| = 6!/|N(\langle\alpha\rangle)|$, da cui $|N(\langle\alpha\rangle)| = 6!/36 = 20$.

1.3

Quanti sono i 5-sottogruppi di Sylow di S_6?

I 5-sottogruppi di Sylow di S_6, come visto al punto precedente, sono 36.

1.4

Dare generatori per i sottogruppi $C(\alpha)$ e $N(\langle\alpha\rangle)$ di S_6.

Siccome ogni potenza di α commuta con α, abbiamo $\langle\alpha\rangle \subseteq C(\alpha)$. Ma $C(\alpha)$ ha ordine 5 (come abbiamo già osservato) e anche $\langle\alpha\rangle$ ha ordine 5, quindi necessariamente $\langle\alpha\rangle = C(\alpha)$. Quindi $C(\alpha)$ è ciclico generato da α.

Per trovare generatori per $N(\langle\alpha\rangle)$ dobbiamo trovare elementi di S_6 che mandano, tramite coniugio, $\alpha = (12345)$ in una sua potenza. Un elemento che coniuga α in $\alpha^2 = (13524)$ è scritto in notazione "funzionale" mettendo α e α^2 uno sotto l'altro:

$$(12345)$$
$$(13524)$$

La sua struttura ciclica è quindi (2354). Ne segue che (2354) normalizza $\langle\alpha\rangle$, e quindi $(2354) \in N(\langle\alpha\rangle)$. Siccome anche $\alpha \in N(\langle\alpha\rangle)$ e $o(\alpha) = 5$, $o((2354)) = 4$, e $\mathrm{MCD}(5, 4) = 1$, per il teorema di Lagrange il sottogruppo generato da α e (2354) ha ordine divisibile per $5 \cdot 4 = 20$. Siccome $|N(\langle\alpha\rangle)| = 20$, deduciamo che $N(\langle\alpha\rangle)$ è generato da α e (2354).

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'intersezione $P \cap N$ è un p-sottogruppo di Sylow di N.

Siccome $P \cap N \leq P$ e P è un p-gruppo, per il teorema di Lagrange anche $P \cap N$ è un p-gruppo. Per concludere che $P \cap N$ è un p-sottogruppo di Sylow di N dobbiamo quindi dimostrare che $|N|/|P \cap N| = |N : P \cap N|$ non è divisibile per p. Ma sappiamo che $|PN| = |P| \cdot |N|/|P \cap N|$ e quindi

$$\frac{|N|}{|P \cap N|} = \frac{1}{|P|} \frac{|P| \cdot |N|}{|P \cap N|} = \frac{|PN|}{|P|}.$$

Siccome N è normale in G, $PN \leq G$ e quindi per il teorema di Lagrange $|PN|$ divide $|G|$. Ne segue che $|N|/|P \cap N| = |PN|/|P|$ divide $|G|/|P|$, che non è divisibile per p perché P è un p-sottogruppo di Sylow di G. Quindi nemmeno $|N|/|P \cap N|$ è divisibile per p.

2.2

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

Mostriamo che la risposta è sì. Sia Q un p-sottogruppo di Sylow di N. Allora Q è un p-sottogruppo di G, quindi è contenuto in un p-sottogruppo di Sylow P di G. Ora siccome $P \cap N \leq P$ e P è un p-gruppo, per il teorema di Lagrange anche $P \cap N$ è un p-gruppo. Quindi $P \cap N$ è un p-sottogruppo di N contenente Q, che è un p-sottogruppo di Sylow di N. Ne segue che $P \cap N = Q$, e quindi la funzione

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

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

3

Si consideri l'omomorfismo di anelli

$$\eta : \mathbb{Z}[X] \to \mathbb{Z},\ \eta(f) := f(-1).$$

3.1

Verificare che $\ker(\eta) = (x+1)$**.**

- Mostriamo che $\ker(\eta) \subseteq (x+1)$. Se $f(x) \in \ker(\eta)$ allora $f(-1) = 0$. Effettuando la divisione con resto di $f(x)$ con $x+1$ in $\mathbb{Z}[X]$ (si può fare perché $x+1$ è monico) otteniamo polinomi $g(x), r(x) \in \mathbb{Z}[X]$ con $r(x) = r \in \mathbb{Z}$ tali che $f(x) = g(x)(x+1) + r$. Da $f(-1) = 0$ otteniamo $0 = f(-1) = g(-1) \cdot 0 + r = r$, per cui $r = 0$, cioè $f(x) = g(x)(x+1)$ e quindi $f(x) \in (x+1)$.
- Mostriamo che $(x+1) \subseteq \ker(\eta)$. Se $f(x) \in (x+1)$ allora esiste $g(x) \in \mathbb{Z}[X]$ con $f(x) = (x+1)g(x)$, da cui $f(-1) = 0 \cdot g(-1) = 0$ e quindi $f(x) \in \ker(\eta)$.

3.2

Dimostrare che per ogni primo p **l'ideale** $(p, x+1)$ **è un ideale massimale di** $\mathbb{Z}[X]$**.**

Consideriamo l'omomorfismo di anelli

$$\gamma : \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z},\ \gamma(f(x)) := f(-1) + p\mathbb{Z}.$$

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

$$\ker(\gamma) = \{f(x) \in \mathbb{Z}[X] \mid f(-1) + p\mathbb{Z} = p\mathbb{Z}\} = \{f(x) \in \mathbb{Z}[X] \mid p | f(-1)\}.$$

Dimostriamo che $\ker(\gamma) = (p, x+1)$.

- Mostriamo che $\ker(\gamma) \subseteq (p, x+1)$. Sia $f(x) \in \ker(\gamma)$. Allora p divide $f(-1)$, quindi esiste $c \in \mathbb{Z}$ con $f(-1) = pc$. Ne segue che il polinomio $f(x) - pc$ ammette -1 come zero, quindi effettuando la divisione con resto come sopra riusciamo a scrivere $f(x) - pc = (x+1)g(x)$ per qualche $g(x) \in \mathbb{Z}[X]$. Ma allora $f(x) = g(x)(x+1) + pc \in (p, x+1)$.
- Mostriamo che $(p, x+1) \subseteq \ker(\gamma)$. Sia $a(x) = f(x)p + g(x)(x+1)$ un generico elemento di $(p, x+1)$, con $f(x), g(x) \in \mathbb{Z}[X]$. Si ha $a(-1) = f(-1)p + g(x) \cdot 0 = f(-1)p \in p\mathbb{Z}$, 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 $\mathbb{Z}[X]/(p, x+1) \cong \mathbb{Z}/p\mathbb{Z}$ è un campo, e quindi $(p, x+1)$ 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 $(p, x+1)$ con p primo.

Per il teorema di corrispondenza, gli ideali di $\mathbb{Z}[X]$ contenenti $\ker(\eta) = (x+1)$ sono in corrispondenza biunivoca con gli ideali di $\mathbb{Z}[X]/(x+1) \cong \mathbb{Z}$, cioè di $\mathbb{Z}$, e la corrispondenza è data da

$$\mathbb{Z}[X] \supseteq I \mapsto \{f(-1) \mid f(x) \in I\},$$

la sua inversa è data da

$$\mathbb{Z} \supseteq J = n\mathbb{Z} \mapsto \{f(x) \in \mathbb{Z}[X] \mid f(-1) \in n\mathbb{Z}\} = (n, x+1).$$

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 $(p, x+1) \neq (q, x+1)$.

Se fosse $(p, x+1) = (q, x+1)$ allora si avrebbe

$$\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}[X]/(p, x+1) = \mathbb{Z}[X]/(q, x+1) \cong \mathbb{Z}/q\mathbb{Z},$$

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

Un altro modo era il seguente. Se fosse $(p, x+1) = (q, x+1)$ allora si avrebbe $p \in (q, x+1)$, quindi esisterebbero $f(x), g(x) \in \mathbb{Z}[X]$ con $p = qf(x)+(x-2)g(x)$. Valutando in $x = 2$ (!) otteniamo allora $p = qf(2) \in q\mathbb{Z}$, assurdo.

4

Si consideri il gruppo di matrici

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

4.1

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

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

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

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

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 $g = \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \in G$. Il suo inverso è dato da $g^{-1} = \begin{pmatrix} a & 0 \\ -ba & 1 \end{pmatrix}$. Dato $x \in S$ si ha

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

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 $g = \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \in G$ e $h = \begin{pmatrix} c & 0 \\ d & 1 \end{pmatrix} \in G$. Effettuando i prodotti gh, hg vediamo che la condizione $gh = hg$ diventa

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

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 $g = \begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix} \in G$ e $h = \begin{pmatrix} c & 0 \\ d & 1 \end{pmatrix} \in G$. Ricordando che $a^2 = c^2 = 1$, un semplice conto dimostra che

$$g^{-1}h^{-1}gh = \begin{pmatrix} 1 & 0 \\ -b-ad+bc+d & 1 \end{pmatrix}.$$

Quindi la condizione che $g^{-1}h^{-1}gh \in H(\mathbb{Z})$ per ogni $h \in G$ diventa la seguente: $-b-ad+bc+d \in \mathbb{Z}$ 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 $-b-ad+bc+d \in \mathbb{Z}$ è verificata per ogni $c \in \{-1,1\}$, $d \in \mathbb{Q}$. Di conseguenza

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

Andiamo a vedere quando due classi $gH(\mathbb{Z}), hH(\mathbb{Z}) \in Z(G/H(\mathbb{Z}))$ sono uguali. Siano $n,m \in \mathbb{Z}$ con $\begin{pmatrix} 1 & 0 \\ n/2 & 1 \end{pmatrix} H(\mathbb{Z}) = \begin{pmatrix} 1 & 0 \\ m/2 & 1 \end{pmatrix} H(\mathbb{Z})$. Questo accade se e solo se $\begin{pmatrix} 1 & 0 \\ -m/2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ n/2 & 1 \end{pmatrix} \in H(\mathbb{Z})$, cioè se e solo se $-m/2+n/2 \in \mathbb{Z}$, in altre parole $n-m$ è pari. Ne segue che $Z(G/H(\mathbb{Z}))$ consiste di due elementi:

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