COMPITO DI ALGEBRA 1

15 giugno 2021

Esercizio 1.
Sia G un gruppo finito, p un primo che divide $|G|$, e P, P' due p-Sylow di G. Dato un sottogruppo H di G, chiamiamo $N_G(H)$ il suo normalizzatore in G.

1. Dimostrare che se $P \neq P'$ i sottogruppi $N_G(P), N_G(P')$ sono coniugati ma diversi.

2. Dimostrare che $N_G(N_G(P)) = N_G(P)$.

Soluzione.

1. Dai teoremi di Sylow sappiamo che P e P' sono coniugati, ovvero esiste $g \in G$ tale che $P' = gPg^{-1}$. Affermiamo che $N_G(P') = gN_G(P)g^{-1}$, e quindi in particolare $N_G(P)$ e $N_G(P')$ sono coniugati. In effetti un elemento h sta in $N_G(P')$ se e solo se $hP'h^{-1} = P' \Leftrightarrow hgPg^{-1}h^{-1} = gPg^{-1} \Leftrightarrow g^{-1}hgP(g^{-1}hg)^{-1} = P$, cioè se e solo se $g^{-1}hg \in N_G(P)$, e infine se e solo se $h \in gN_G(P)g^{-1}$. Per la seconda affermazione, si osservi che P è l'unico p-Sylow di $N_G(P)$, perché per definizione P è normale in $N_G(P)$, e sappiamo che un p-Sylow è unico se e solo se è normale. Similmente, P' è l'unico p-Sylow di $N_G(P')$. Se per assurdo si avesse $N_G(P) = N_G(P')$ avremmo allora $P = P'$ (in quanto entrambi sarebbero l'unico p-Sylow del gruppo $N_G(P) = N_G(P')$), il che contraddice l'ipotesi.

2. Sia $H = N_G(P)$. Chiaramente si ha $H \subseteq N_G(H)$, quindi basta mostrare l'altra inclusione. Sia quindi $n \in N_G(H)$. Mostriamo che n sta anche in H, ovvero che normalizza P. Per far questo, osserviamo che nPn^{-1} è un p-Sylow di G, e che d'altro canto è contenuto in $nHn^{-1} = H$, quindi nPn^{-1} è un p-Sylow di H. Ma abbiamo già osservato che l'unico p-Sylow di H è P stesso, quindi $nPn^{-1} = P$ come voluto.

Seconda soluzione.

1. Il normalizzatore di P (rispettivamente P') è lo stabilizzatore di P (rispettivamente P') per l'azione di coniugio di G sull'insieme dei suoi p-Sylow. Siccome tale azione è transitiva per i teoremi di Sylow, gli stabilizzatori di P e P' sono coniugati. Si mostra poi come sopra che se $P \neq P'$ allora essi sono anche diversi.

2. Il contenimento $N_G(P) \subseteq N_G(N_G(P))$ è ovvio, dunque mostriamo l'altro. Sia $g \in N_G(N_G(P))$. Siccome g normalizza $N_G(P)$ abbiamo $N_G(P) = gN_G(P)g^{-1}$, e d'altro canto si ha $gN_G(P)g^{-1} = N_G(gPg^{-1})$. Allora P e gPg^{-1} sono due p-Sylow di G con lo stesso normalizzatore, per cui dal punto 1 otteniamo $P = gPg^{-1}$, cioè $g \in N_G(P)$.

Esercizio 2.
Sia G un gruppo del tipo $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes_\psi S_3$. Determinare le possibili cardinalità del centro di G al variare di ψ, mostrando in particolare che il centro non può essere banale.

Soluzione. Poniamo $V = (\mathbb{Z}/2\mathbb{Z})^3$ e $G = V \rtimes_\varphi S_3$, dove $\varphi\colon S_3 \to \mathrm{Aut}(V) \cong \mathrm{GL}_3(\mathbb{F}_2)$ è l'azione di S_3 su V che definisce il prodotto semidiretto.
Sappiamo che $S_3 = \langle \sigma, \tau \rangle$ dove σ e τ sono rispettivamente un 3-ciclo e un 2-ciclo di S_3.
Indichiamo con $\{e_1, e_2, e_3\}$ una base di V su $\mathbb{Z}/2\mathbb{Z}$.
Un elemento (v, ρ) con $v \in V$ e $\rho \in S_3$ appartiene al centro di G se e solo se $(v, \rho)(u, \eta) = (u, \eta)(v, \rho)$ per ogni $(u, \eta) \in G$. Svolgendo i prodotti otteniamo la condizione

$$(v + \varphi_\rho(u), \rho\eta) = (u + \varphi_\eta(v), \eta\rho) \quad \forall (u, \eta) \in G,$$

da cui si ha $\rho\eta = \eta\rho$ per ogni $\eta \in S_3$ e, avendo S_3 centro banale, necessariamente $\rho = id$.
La condizione sulla prima componente diventa quindi $\varphi_\eta(v) = v$ per ogni $\eta \in S_3$, cioè

$$Z(G) = \{(v, \mathrm{id}) \mid \mathrm{Stab}(v) = S_3\}$$

(dove $\mathrm{Stab}(v)$ è lo stabilizzatore di v sotto l'azione di S_3 data da φ); in particolare $Z(G)$ è isomorfo a un sottogruppo di V e quindi il suo ordine può essere solo un divisore di 2^3.
Il caso $|Z(G)| = 8$ è realizzato da $G = V \times S_3$.
Sia $G = V \rtimes_\varphi S_3$, dove φ è definita da

$$\varphi(\sigma) = \mathrm{Id}, \quad \text{e} \quad \varphi(\tau) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

(notiamo che φ è ben definita da questo assegnamento perché $\varphi(\tau)$ ha ordine 2 e vale $\varphi(\tau)\varphi(\sigma)\varphi(\tau)^{-1}) = \varphi(\sigma)^{-1}$). Considerando i punti fissi di $\varphi(\tau)$ è semplice verificare che $Z(G) = \langle e_1, e_2 + e_3 \rangle$ e quindi ha ordine 4.
Consideriamo ora l'azione di S_3 su V per permutazione degli elementi della base. Questo corrisponde alla scelta

$$\varphi(\sigma) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{e} \quad \varphi(\tau) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

che chiaramente definisce un'immersione di S_3 in $\mathrm{GL}_3(\mathbb{F}_2)$. In questo caso l'unico vettore non nullo stabilizzato sia da $\varphi(\sigma)$ che da $\varphi(\tau)$ è $e_1 + e_2 + e_3$, quindi $Z(G) = \langle e_1 + e_2 + e_3 \rangle$ ha ordine 2.
Infine supponiamo per assurdo che per un certa scelta di φ il centro di G sia banale. Consideriamo la partizione di V in orbite data dall'azione di S_3 via φ:

$$V = \bigsqcup_{v \in R} \mathrm{orb}(v)$$

dove R e un insieme di rappresentanti delle orbite. Dato che gli elementi con orbita banale sono quelli del centro, passando alle cardinalità si ha:

$$8 = |V| = 1 + \sum_{v \in R \setminus \{id\}} \frac{|S_3|}{|\operatorname{Stab}(v)|}.$$

La cardinalità di $\operatorname{Stab}(v)$ può essere 1, 2 o 3, quindi gli addendi della sommatoria possono essere 6, 3 o 2. Si vede facilmente che l'unica possibilità per l'equazione sopra è

$$8 = 1 + 2 + 2 + 3.$$

Questo direbbe che 2 orbite non banali hanno stabilizzatore di ordine 3, e quindi generato da σ. Equivalentemente, σ stabilizza 4 elementi oltre all'identità, e quindi necessariamente $\ker(\varphi(\sigma) - 1) = V$ (si osservi che $\ker(\varphi(\sigma) - 1)$ è un $\mathbb{F}_2$-sottospazio vettoriale di V con almeno 5 elementi). Questo però non è possibile, perché vorrebbe dire che $\varphi(\sigma)$ è l'identità, e cioè che stabilizza ogni elemento di V: ci deve però essere un'orbita di ordine 3, e σ non può stare nello stabilizzatore degli elementi di quell'orbita.

Esercizio 3. Siano S e T le parti moltiplicative di $\mathbb{Z}[x]$ definite da $S = \mathbb{Z}[x] \setminus (x)$ e $T = \mathbb{Z}[x] \setminus (x + 1)$. Poniamo $A = S^{-1}\,\mathbb{Z}[x] \times T^{-1}\,\mathbb{Z}[x]$.

1. Caratterizzare gli elementi invertibili di A.
2. Mostrare che gli ideali di A sono tutti principali e descrivere ogni ideale mediante un generatore.

Soluzione. Osserviamo per prima cosa che sia S che T sono effettivamente parti moltiplicative del dominio di integrità $\mathbb{Z}[x]$, in quanto entrambi gli insiemi sono il complementare di un ideale primo.

1. Ricordiamo che gli elementi invertibili di un prodotto diretto di anelli sono le coppie con entrambe le componenti invertibili. Caratterizziamo quindi gli elementi invertibili dei due fattori. Gli elementi di $S^{-1}\mathbb{Z}[x]$ sono del tipo $\alpha = \frac{p(x)}{s(x)}$ con $p(x) \in \mathbb{Z}[x]$ e $s(x) \in S$; quest'ultima condizione è verificata se e solo se $s(x) \in \mathbb{Z}[x]$ e $s(0) \neq 0$. L'elemento α è invertibile se è diverso da 0 e se $\alpha^{-1} = \frac{s(x)}{p(x)}$, che è il suo inverso in $\mathbb{Q}(x)$, appartiene a $S^{-1}\mathbb{Z}[x]$, cioè ammette une scrittura $\frac{a(x)}{s_1(x)}$ con denominatore in S. Ora $\frac{s(x)}{p(x)} = \frac{a(x)}{s_1(x)}$ se e solo se $p(x)a(x) = s_1(x)s(x)$ e, valutando in 0, si ottiene $p(0) \neq 0$. Questo mostra che gli elementi invertibili di $S^{-1}\mathbb{Z}[x]$ sono quelli del tipo $\alpha = \frac{p(x)}{s(x)}$ con $p(x), s(x) \in S$.

   Analogamente gli elementi invertibili di $T^{-1}\mathbb{Z}[x]$ sono del tipo $\beta = \frac{q(x)}{t(x)}$ con $q(x)$, $t(x) \in T$. Quindi $\left(\frac{p(x)}{s(x)}, \frac{q(x)}{t(x)}\right)$ è invertibile in A se e solo se $p(0) \neq 0$ e $q(-1) \neq 0$.

2. Ricordiamo che gli ideali di un prodotto diretto di anelli $A_1 \times A_2$ sono del tipo $I_1 \times I_2$ con I_i ideale di A_i ($i = 1, 2$). Quindi anche in questo caso si tratta di analizzare le due componenti.

   L'ideale banale (0) è il prodotto dei due ideali banali. Gli altri ideali propri di $S^{-1}\mathbb{Z}[x]$ sono del tipo $S^{-1}I$ con I ideale di $\mathbb{Z}[x]$ con $I \cap S = \emptyset$: questo è equivalente a dire che $I \subseteq (x)$, quindi gli elementi di $S^{-1}I$ possono essere scritti come $x^n \frac{p(x)}{s(x)}$ con $n \geq 1$ e $p(0) \neq 0$. Dalla parte (1) sappiamo che l'elemento $\frac{p(x)}{s(x)}$ è invertibile, quindi possiamo scegliere come generatori di $S^{-1}I$ elementi del tipo x^n con $n \geq 1$. È quindi evidente che $S^{-1}I = (x^{n_0})$ dove $n_0 = \min\{n \mid x^n \in S^{-1}I\}$. Infine, anche l'ideale (1) di $S^{-1}\mathbb{Z}[x]$ è della stessa forma, con $n_0 = 0$.

   Analogamente gli ideali propri e non banali di $T^{-1}\mathbb{Z}[x]$ sono del tipo $T^{-1}J$, con J ideale di $\mathbb{Z}[x]$ contenuto in $(x+1)$. Ne segue che gli elementi di $T^{-1}J$ possono essere scritti come $(x+1)^m \frac{q(x)}{t(x)}$ con $m \geq 1$ e $q(-1) \neq 0$, quindi, dato che $\frac{q(x)}{t(x)}$ è invertibile in $T^{-1}\mathbb{Z}[x]$, possiamo scegliere come generatori di $T^{-1}J$ elementi del tipo $(x+1)^m$ con $m \geq 1$. Come sopra otteniamo che $T^{-1}I = ((x+1)^{m_0})$ dove $m_0 = \min\{n \mid (x+1)^n \in T^{-1}J\}$, incluso il caso $m_0 = 0$.

   Possiamo concludere che gli ideali di $A = S^{-1}\mathbb{Z}[x] \times T^{-1}\mathbb{Z}[x]$ sono quelli del tipo $(x^n) \times ((x+1)^m)$ con $n, m \in \mathbb{N}$, oltre all'ideale (0).

Esercizio 4.
Sia K il campo di spezzamento su $\mathbb{Q}$ del polinomio $f(x) = (x^3 - 2)(x^3 - 3)$. È noto che $[K : \mathbb{Q}] = 18$.

1. Descrivere il gruppo di Galois di $K/\mathbb{Q}$ come prodotto semidiretto di gruppi abeliani.

2. Mostrare che le sottoestensioni L di K contenenti $\mathbb{Q}(\zeta_3)$ e tali che $[L : \mathbb{Q}(\zeta_3)] = 3$ sono tutte del tipo $\mathbb{Q}(\zeta_3, \sqrt[3]{d})$ e descriverle dando per ognuna un valore di d.

Soluzione. Per $a = 2, 3$ sia $K_a = \mathbb{Q}(\zeta_3, \sqrt[3]{a})$ il campo di spezzamento su $\mathbb{Q}$ di $x^3 - a$. Per tali a il polinomio $x^3 - a$ è irriducibile su $\mathbb{Q}$ (Eisenstein al primo a), dunque i campi K_a hanno grado 6 su $\mathbb{Q}$ (sono il composto di $\mathbb{Q}(\sqrt[3]{a})$, di grado 3, e $\mathbb{Q}(\zeta_3)$, di grado 2). L'estensione $K_a/\mathbb{Q}(\zeta_3)$ è di Galois e di grado 3, quindi il suo gruppo di Galois è isomorfo a $\mathbb{Z}/3\mathbb{Z}$.

1. K è il composto di K_2 e K_3, ed è quindi uguale a $\mathbb{Q}(\zeta_3, \sqrt[3]{2}, \sqrt[3]{3})$. Consideriamo ora il seguente diagramma di campi:

$$\begin{tikzcd}
 & K \arrow[dl, dash] \arrow[dr, dash] & \\
K_2 \arrow[dr, dash] & & K_3 \arrow[dl, dash] \\
 & \mathbb{Q}(\zeta_3) \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

Dalla teoria sappiamo che $K/\mathbb{Q}$ è un'estensione di Galois, così come lo è $K/\mathbb{Q}(\zeta_3)$. Siccome $K/\mathbb{Q}(\zeta_3)$ è il composto delle estensioni $K_2/\mathbb{Q}(\zeta_3)$ e $K_3/\mathbb{Q}(\zeta_3)$, il gruppo $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3))$ è isomorfo ad un sottogruppo di $\mathrm{Gal}(K_2/\mathbb{Q}(\zeta_3)) \times \mathrm{Gal}(K_3/\mathbb{Q}(\zeta_3)) \cong (\mathbb{Z}/3\mathbb{Z})^2$. Dal testo sappiamo che $[K : \mathbb{Q}(\zeta_3)] = \frac{[K:\mathbb{Q}]}{[\mathbb{Q}(\zeta_3):\mathbb{Q}]} = 9$, per cui $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3))$ ha ordine 9, e quindi è isomorfo a $(\mathbb{Z}/3\mathbb{Z})^2$. Un qualsiasi $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(\zeta_3))$ è completamente determinato dalle immagini $\sigma(\sqrt[3]{a})$ per $a = 2, 3$. D'altro canto, $\sigma(\sqrt[3]{a})$ dev'essere una radice del polinomio $x^3 - a$, e quindi della forma $\sqrt[3]{a} \cdot \zeta_3^i$ per un certo $i \in \{0, 1, 2\}$. Siano allora i_2, i_3 tali che

$$\sigma(\sqrt[3]{2}) = \zeta_3^{i_2} \sqrt[3]{2}, \quad \sigma(\sqrt[3]{3}) = \zeta_3^{i_3} \sqrt[3]{3}.$$

È immediato osservare che

$$\begin{array}{ccc} \mathrm{Gal}(K/\mathbb{Q}(\zeta_3)) & \to & (\mathbb{Z}/3\mathbb{Z})^2 \\ \sigma & \mapsto & (i_2, i_3) \end{array} \tag{1}$$

è un isomorfismo di gruppi (è iniettivo fra gruppi della stessa cardinalità). Descriviamo ora la struttura di prodotto semidiretto di $\mathrm{Gal}(K/\mathbb{Q})$. Il sottogruppo $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3))$ di

$\mathrm{Gal}(K/\mathbb{Q})$ è normale (ha indice 2). Sia $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ la restrizione a K del coniugio complesso, che è un elemento di ordine 2. Nel gruppo $\mathrm{Gal}(K/\mathbb{Q})$ abbiamo il sottogruppo normale $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3)) \cong (\mathbb{Z}/3\mathbb{Z})^2$ e il sottogruppo $\langle\tau\rangle \cong \mathbb{Z}/2\mathbb{Z}$, che – per ragioni di cardinalità – si intersecano banalmente e generano $\mathrm{Gal}(K/\mathbb{Q})$. Otteniamo quindi

$$\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^2 \rtimes_\psi \mathbb{Z}/2\mathbb{Z}.$$

Resta solo da descrivere ψ, ovvero l'azione del coniugio per τ sul sottogruppo $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3))$. Data σ in questo sottogruppo, corrispondente a $(i_2, i_3) \in (\mathbb{Z}/3\mathbb{Z})^2$, si ha

$$\tau\sigma\tau^{-1}(\sqrt[3]{a}) = \tau\sigma(\sqrt[3]{a}) = \tau\left(\zeta_3^{i_a}\sqrt[3]{a}\right) = \zeta_3^{-i_a}\sqrt[3]{a},$$

dunque (sotto l'isomorfismo (1)) $\tau\sigma\tau^{-1}$ corrisponde a $(-i_2, -i_3)$. Concludiamo quindi che ψ manda un generatore di $\mathbb{Z}/2\mathbb{Z}$ nell'automorfismo di $(\mathbb{Z}/3\mathbb{Z})^2$ dato da $x \mapsto -x$.

2. Le sottoestensioni L volute corrispondono, per teoria di Galois, ai sottogruppi di $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3))$ di indice 3. Dato che $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3)) \cong (\mathbb{Z}/3\mathbb{Z})^2$, i sottogruppi di indice 3 sono i sottogruppi di ordine 3, che sono $\frac{3^2-1}{\varphi(3)} = 4$, ovvero i sottogruppi generati da $(1,0), (1,1), (1,2)$ e $(0,1)$. Siano $\sigma_1, \dots, \sigma_4$ gli elementi di $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3))$ che corrispondono a queste coppie tramite l'isomorfismo (1). Per definizione σ_1 fissa $\sqrt[3]{3}$ e σ_4 fissa $\sqrt[3]{2}$, per cui le corrispondenti estensioni sono K_3 e K_2 (che sappiamo già avere grado 3 su $\mathbb{Q}(\zeta_3)$). Osserviamo ora che σ_2 fissa $\sqrt[3]{12}$: infatti

$$\sigma_2(\sqrt[3]{12}) = \sigma_2(\sqrt[3]{2}^2 \cdot \sqrt[3]{3}) = \sigma_2(\sqrt[3]{2})^2 \cdot \sigma_2(\sqrt[3]{3}) = (\sqrt[3]{2} \cdot \zeta_3^1)^2 \cdot \sqrt[3]{3} \cdot \zeta_3^1 = \sqrt[3]{2}^2 \cdot \sqrt[3]{3} = \sqrt[3]{12}.$$

Ne segue che l'estensione $\mathbb{Q}(\zeta_3, \sqrt[3]{12})$ (che ha grado 6 su $\mathbb{Q}$: si noti che $x^3 - 12$ è irriducible per Eisenstein al primo 3) è fissata da $\langle\sigma_2\rangle$, ovvero $\mathbb{Q}(\zeta_3, \sqrt[3]{12}) \subseteq K^{\langle\sigma_2\rangle}$. Siccome $[\mathbb{Q}(\zeta_3, \sqrt[3]{12}) : \mathbb{Q}(\zeta_3)] = 3 = [\mathrm{Gal}(K/\mathbb{Q}(\zeta_3)) : \langle\sigma_2\rangle]$ abbiamo proprio $\mathbb{Q}(\zeta_3, \sqrt[3]{12}) = K^{\langle\sigma_2\rangle}$. Infine, per un calcolo analogo al precedente σ_3 fissa $\sqrt[3]{6}$ (infatti $\sigma_3(\sqrt[3]{2})\sigma_3(\sqrt[3]{3}) = \sqrt[3]{2}\zeta_3\sqrt[3]{2}\zeta_3^2 = \sqrt[3]{6}$), e come sopra si deduce che l'estensione corrispondente è $\mathbb{Q}(\zeta_3, \sqrt[3]{6})$. Le estensioni cercate sono dunque 4, e corrispondono ai valori $d = 2, 3, 6, 12$.