Gara di Gruppi 2020, Proposte di Soluzione

A Notiamo innanzitutto che, se G è un gruppo finito e N è normale in G, il teorema di corrispondenza induce una mappa

$$\mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G/N)$$

descritta da $P \mapsto PN/N$, in quanto $PN/N \simeq P/P \cap N$ è un p-gruppo e $[G/N : PN/N] = [G : PN]$ non è divisibile per p. La tesi richiesta al punto **1.** si ottiene mostrando che tale mappa è surgettiva: d'altra parte, se PN/N è un p-Sylow di G/N, con $P \in \mathrm{Syl}_p(G)$, per il secondo teorema di Sylow ogni altro p-Sylow di G/N è della forma $(PN/N)^{gN} = P^g N/N$ per qualche $g \in G$, e pertanto è immagine di un p-Sylow di G tramite la mappa descritta sopra.

Per dimostrare il punto **2.**, consideriamo invece l'azione per coniugio di G sui suoi p-Sylow: poiché essa induce un omomorfismo $G \to S_n$, è sufficiente mostrare che è fedele. In particolare, se K è il suo nucleo, basta far vedere che la mappa $\mathrm{Syl}_p(G) \to \mathrm{Syl}_p(G/K)$ indotta dal teorema di corrispondenza è iniettiva: ne segue, poiché G è p-decrescente, che $K = 1$ (se K fosse non banale, non potrebbe esistere una bigezione come quella appena trovata). Pertanto, supponiamo che $PK/K = QK/K$, con P, Q due p-Sylow di G: si ha allora $PK = QK$. D'altra parte, K agisce banalmente su P e Q, e pertanto $PK = QK$ è contenuto in $N_G(P)$: pertanto, Q normalizza P, da cui immediatamente $Q = P$ per il secondo teorema di Sylow.

Infine, passando al punto **3.**, per quanto detto si ha subito che, se G è p-decrescente e $|G| = n!$, con $n = n_p(G)$, vale $G \simeq S_n$. Ora, per $n \leqslant 3$ si ha che S_n è p-decrescente se e solo se $p = 2, n = 3$; viceversa, per $n > 3$, S_n è banalmente p-decrescente per ogni p. Posto che S_3 è evidentemente uno dei gruppi richiesti, perché S_n compaia tra i gruppi cercati per $n > 3$ serve che valga $n_p(S_n) = n$ per qualche p. D'altra parte, se questo è il caso e $P \in \mathrm{Syl}_p(S_n)$, il suo normalizzatore $N = N_{S_n}(P)$ ha indice n in S_n: l'azione di S_n sui laterali di N è però un omomorfismo $S_n \to S_n$, chiaramente iniettivo perché l'azione è transitiva su n punti e S_n non ha sottogruppi normali non banali di indice > 2. L'isomorfismo trovato mappa N nello stabilizzatore di 1, e pertanto mostra che $N \simeq S_{n-1}$. Dal momento che $n > 3$, è chiaro che, per ogni p, un p-Sylow di S_{n-1} non è normale: pertanto, N non può avere indice n in S_n e la condizione richiesta è assurda. In conclusione, l'unico gruppo cercato è S_3.

B Sia G un gruppo di ordine $p^3 q$ tale che $n_p = n_p(G), n_q = n_q(G) > 1$. Per il terzo teorema di Sylow, dev'essere $n_p = q$, e può valere $n_q = p, p^2, p^3$. Ora, dato che $n_p = q$, e quindi q è congruo a 1 modulo p, dev'essere $q > p$: perciò, non può valere $n_q = p$. Inoltre, se n_q fosse p^3, G avrebbe p^3 q-Sylow, e quindi $(p^3 - 1)$ q-elementi: di conseguenza, avrebbe un unico p-Sylow. Deve quindi essere $n_q = p^2$:

in tal caso, q divide $(p+1)(p-1)$ e, dato che $q > p$, si ottiene che l'unica coppia possibile è $(2,3)$. D'altra parte, S_4 è effettivamente un gruppo di ordine $24 = 2^3 \cdot 3$ privo di Sylow normali, e ciò completa il punto **4.**

Per il punto **5.**, consideriamo un gruppo G di ordine 24 tale che $n_2(G), n_3(G) > 1$. Notiamo che G deve allora avere quattro 3-Sylow e tre 2-Sylow. L'azione di G sui 3-Sylow induce un omomorfismo $G \to S_4$, e il suo nucleo K è l'intersezione dei normalizzatori dei 3-Sylow di G. Siano ora P un 3-Sylow di G e $N = N_G(P)$ il suo normalizzatore in G: siccome $n_3(G) = [G : N]$, dev'essere $|N| = 6$, e pertanto $|K|$ può essere 1, 2, 3 o 6. D'altra parte, non può essere $|K| = 6$, altrimenti i normalizzatori di ognuno dei 3-Sylow di G coinciderebbero con N. Anche il caso $|K| = 3$ si esclude facilmente: in tal caso, sarebbe $K = P$, e pertanto P sarebbe contenuto in ognuno dei normalizzatori dei 3-Sylow di G, il che implicherebbe $n_3(G) = 1$. Supponiamo allora che $|K| = 2$: poiché l'unico sottogruppo di indice due di S_4 è A_4, l'azione sui 4-Sylow di G indurrebbe un isomorfismo $G/K \xrightarrow{\sim} A_4$, ma un argomento analogo a quello del quesito **2.** mostra che $n_2(G/K) = n_2(G) > 1$, mentre $n_2(A_4) = 1$, e fornisce un assurdo. In conclusione, l'azione sopra induce un isomorfismo $G \simeq S_4$, e perciò S_4 è l'unico gruppo con le proprietà cercate.

C Osserviamo preliminarmente che, se $g, h \in G$, valgono $[g,h] = [h,g]^{-1}$, e $gh = hg[g,h]$ (da cui il nome commutatore per $[g,h]$). A questo punto, per la normalità, basta notare che

$$[h,k]^g = g^{-1}h^{-1}(ghh^{-1}g^{-1})k^{-1}hkg = [g,h][h,kg] = [h,g]^{-1}[h,kg]$$

per ogni $h \in H$ e $k, g \in K$. Ciò mostra che $K \subset N_G([H,K])$: dato che $[H,K] = [K,H]$, si ottiene simmetricamente che anche K normalizza $[H,K]$, e ciò implica quanto voluto. L'uguaglianza richiesta è un po' più involuta: un'inclusione è chiara; per l'altra, si osserva che se $h \in H, k \in K$ e $g \in G$, vale

$$\begin{aligned}[hk,g] &= k^{-1}h^{-1}g^{-1}hkg = k^{-1}h^{-1}g^{-1}kh[h,k]g \\ &= k^{-1}h^{-1}g^{-1}kgh[h,k][h[h,k],g],\end{aligned}$$

dove le ultime due uguaglianze seguono commutando hk e $(h[h,k])g$ rispettivamente. A questo punto, è sufficiente esplicitare quanto scritto per rendersi conto che l'ultimo membro della catena di uguaglianze è uguale a $[k,gh][h,kg]$. La tesi segue dal fatto che due sottogruppi normali di G commutano, per cui $[K,G][H,G] = [H,G][K,G]$.

Un'idea per il punto **7.** è questa: se B è abeliano, e G è isomorfo a un prodotto semidiretto di B con un gruppo C anch'esso abeliano, il derivato G' è particolarmente semplice. Infatti, $G = BC$ e, per il punto precedente,

$$G' = [G,G] = [BC,BC] = [B,B][B,C][C,C] = [B,C].$$

Infatti, usando le osservazioni sopra si ottiene agilmente che $[B, BC] = [B, B][B, C]^C$ e $[C, BC] = [C, C][B, C]^C$, e il fatto che $[B, C]$ è normale in G fornisce la prima uguaglianza; la seconda viene invece dall'abelianità di B, C.
Fissato un gruppo abeliano A, un modo per concludere è quindi trovare gruppi abeliani B, C e un opportuno omomorfismo $\varphi : C \to \mathrm{Aut}(B)$ tali che $[B, C] < B \rtimes_\varphi C$ sia isomorfo ad A. La soluzione probabilmente più semplice si ottiene considerando $B = A_1 \times A_2$, con $A_i \simeq A$, e $C = \mathbb{Z}/2\mathbb{Z}$, con φ l'azione di C sugli indici di A_i: dal momento che, presi $a_i \in A_i$, vale

$$[(a_1, a_2), 1] = (-a_1, -a_2) \cdot (a_1, a_2)^1 = (-a_1 + a_2, -a_2 + a_1),$$

e i commutatori di questa forma sono gli unici non banali, si vede infatti che $[B, C] \simeq \Delta^- \times \{0\}$, dove Δ^- è il sottogruppo di $A \times A$ degli elementi della forma $(a, -a)$, $a \in A$. D'altra parte, $\Delta^- \times \{0\} \simeq \Delta^- \simeq A$ in modo chiaro.

Infine, passando al punto **8.**, l'azione di H su H' per coniugio, che è ben definita in quanto H' è normale in H, induce un omomorfismo $H \to \mathrm{Aut}(H')$. È chiaro che tale omomorfismo mappa H' in $\mathrm{Inn}(H')$; d'altra parte, ogni omomorfismo di gruppi $H \to K$ mappa $H' \mapsto K'$, e pertanto $\mathrm{Inn}(H') < \mathrm{Aut}(H')'$. Ne segue che, se G è integrabile, $\mathrm{Inn}(G)$ è un sottogruppo di $[\mathrm{Aut}(G), \mathrm{Aut}(G)]$.
Di qui, si ottiene subito che, ad esempio, S_n non è integrabile per ogni $n > 2, n \neq 6$, in quanto $\mathrm{Aut}(S_n) \simeq S_n$ ha derivato isomorfo ad A_n, e $\mathrm{Inn}(S_n) \simeq S_n$.

In realtà, nota la caratterizzazione di $\mathrm{Aut}(S_6)$, è facile vedere che anche $\mathrm{Aut}(S_6)' \simeq A_6$, e dal fatto che $\mathrm{Inn}(S_6) \simeq S_6$ si deduce che anche S_6 non è integrabile. Anche i gruppi diedrali D_{2n} non sono integrabili per ogni $n > 2$: è facile verificare che $\mathrm{Inn}(D_{2n})$ è isomorfo a D_{2n} o a $D_{2(n-1)}$, a seconda che n sia dispari o pari; invece, $\mathrm{Aut}(D_{2n})$ è, a meno di isomorfismo, $C_n \rtimes_{id} \mathrm{Aut}(C_n)$, con C_n il gruppo ciclico di ordine n. Ne segue, dopo qualche calcolo, che il suo derivato è isomorfo a $C_n^2 = \{x^2 \mid x \in C_n\}$, e quindi ha ordine n se n è dispari, $n/2$ altrimenti.

D Ricordiamo che vale $|GL(n, p)| = \prod_{i<n}(p^n - p^i) = p^N r$ dove r non è divisibile per p e $N = \sum_{i=0}^{n-1} i = n(n-1)/2$. D'altra parte, è immediato notare che $|UT(p, n)| = p^N$: pertanto, $UT(p, n)$ è un p-Sylow di $GL(n, p)$. Osserviamo inoltre che esiste un'immersione naturale di S_n in $GL(n, p)$, che associa a $\sigma \in S_n$ la corrispondente matrice di permutazione $\left(\delta_{i,\sigma(j)}\right)$, dove δ_{ij} è la delta di Kronecker.
Se quindi P è un p-gruppo, supponiamo $|P| = n$: l'immersione di Cayley permette di identificare P con un p-Sylow di S_n: pertanto, P è isomorfo a un p-sottogruppo di $GL(n, p)$, e dal secondo teorema di Sylow si ottiene che P è isomorfo in effetti a un sottogruppo di $UT(p, n)$, e il punto **9.** è provato.

Per il punto **10.**, dimostriamo ora che C_{p^k} si immerge in $G = GL(p, p^{k-1} + 1)$. Questo equivale a trovare un elemento di ordine p^k in G. Un tale elemento è ad esempio la matrice $A = (a_{ij})$ con $a_{ii} = a_{i,i+1} = 1$ per ogni i e $a_{ij} = 0$ altrimenti (cioè, A è il blocco di Jordan relativo a 1). Per mostrare che ha l'ordine giusto,

scriviamo $A = I + N$, dove I è l'identità di G, e $N = \left(\delta_{i+1,j}\right)$. Dal momento che i coefficienti sono elementi di $\mathbb{F}_p$, vale $A^{p^k} = I^{p^k} + N^{p^k}$; d'altra parte, $N^{p^k} = 0$, per cui l'ordine di A divide p^k, e viceversa $N^{p^{k-1}} = \left(\delta_{i+p^{k-1},j}\right) \neq 0$, da cui A ha ordine esattamente p^k.
Facciamo vedere che, in effetti, *ogni* p-gruppo abeliano P di ordine p^k si immerge in G. Per il teorema di struttura dei gruppi abeliani finiti, un tale P è della forma $C_{p^{k_1}} \oplus \cdots \oplus C_{p^{k_t}}$ per qualche t. Per ogni $i = 1, \dots, t$, sia I_i la matrice di taglia $p^{k_i - 1} + 1$ corrispondente all'identità, e sia J_i il blocco di Jordan relativo a 1 di taglia $p^{k_i-1} + 1$. Consideriamo allora le matrici

$$B_i = \begin{pmatrix} I_1 &&&&&&&&& \\ & \ddots &&&&&&&& \\ && I_{i-1} &&&&&&& \\ &&& J_i &&&&&& \\ &&&& I_{i+1} &&&&& \\ &&&&& \ddots &&&& \\ &&&&&& I_t &&& \\ &&&&&&& 1 && \\ &&&&&&&& \ddots & \\ &&&&&&&&& 1 \end{pmatrix} \in G.$$

Notiamo che sono ben definite in quanto, effettivamente,

$$\sum_{i=1}^{t} (p^{k_i-1} + 1) \leqslant \prod_{i=1}^{t} p^{k_i-1} + 1,$$

come si mostra facilmente per induzione. È immediato, usando la struttura a blocchi delle B_i, concludere che $\langle B_i \mid i = 1, \dots, t\rangle$ è isomorfo a P.

E Sia $M = \prod_i H_i$ un H-prodotto massimale in G: per mostrare il punto **10.** è sufficiente far vedere che, per ogni automorfismo $\varphi \in \mathrm{Aut}(G)$, si ha $\varphi(H_i) < M$ al variare di i, dal momento che $\varphi(M) = \langle \varphi(H_i) \mid i\rangle$.
Per dimostrarlo, notiamo che $\varphi(H_i) \cap M \neq 1$, perché altrimenti M sarebbe facilmente estendibile a un H-prodotto massimale strettamente più grande, in quanto $\varphi(H_i)$ è ancora normale in G poiché φ è un automorfismo.
D'altra parte, se $\varphi(H_i) \cap M$ è strettamente contenuto in $\varphi(H_i)$ (il che è equivalente a dire che non è interamente contenuto in M), è un sottogruppo normale non banale di $\varphi(H_i)$: ciò è tuttavia impossibile, in quanto $\varphi(H_i)$ è isomorfo a un sottogruppo normale minimale di ordine minimo, e pertanto è anch'esso normale minimale in G.

Osserviamo ora che, da quanto mostrato, segue che un gruppo G privo di sottogruppi caratteristici non banali è prodotto diretto di gruppi semplici isomorfi. Se, infatti, $M < G$ è un H-prodotto massimale con H nelle ipotesi del punto precedente, allora $G = M$. Inoltre, H dev'essere semplice: se $N < H$ è normale in H, allora è normale in $G = H \times \prod_{i>1} H_i$, il che implica che $N = 1$ o $N = H$ per minimalità di H.

Per risolvere i punti **12.** e **13.**, notiamo innanzitutto che N^* ha una struttura piuttosto semplice: è in effetti prodotto diretto di alcuni dei sottogruppi normali minimali di G. Infatti, se N_i sono alcuni di essi e N' è un altro di tali sottogruppi, per minimalità $N' \cap \langle N_i \mid i \rangle$ dev'essere 1 o l'intero N', e l'osservazione appena fatta segue dalla caratterizzazione dei prodotti diretti interni. Inoltre, osserviamo che un sottogruppo normale minimale di G non ha sottogruppi caratteristici non banali, dal momento che se $K < H < G$ con K caratteristico in H e H normale in G, allora K è normale in G.

Ne segue che un sottogruppo N normale minimale di G è prodotto diretto di gruppi semplici isomorfi e, pertanto, dev'essere $N^*(G) \simeq A \times H$, dove $A = \prod_i A_i$ e ognuno degli A_i è abeliano elementare, cioè della forma $C_p \times \cdots \times C_p$ per qualche p, e H è prodotto diretto di gruppi semplici non abeliani. Viceversa, è evidente che, se $G = A \times H$ con A, H siffatti, vale $G = N^*(G)$.

Se G è risolubile, ognuno di essi dev'essere risolubile, N è in effetti prodotto diretto di un numero finito di gruppi ciclici di ordine primo (cioè, come si dice, è *abeliano elementare*). Poiché $N^* = \prod_i N_i$ per certi N_i normali minimali, si ottiene che N^* è prodotto finito di gruppi abeliani elementari e, in particolare, è abeliano. Al contrario, nel caso in cui ogni sottogruppo normale non banale di G non sia risolubile, N^* è un prodotto diretto della forma $\prod_j H_j^{\alpha_j}$, con gli H_j semplici non abeliani e gli $\alpha_j \in \mathbb{N}$. Ne segue subito che nessun elemento di N^* centralizza l'intero N^*. Di conseguenza, $C_G(N^*) \cap N^* = C_{N^*}(N^*) = 1$; d'altra parte, N^* è normale in G, e pertanto lo è anche il suo centralizzatore in G. Ma allora, per com'è definito N^*, si ottiene $C_G(N^*) = 1$: altrimenti, $C_G(N^*)$ conterrebbe un sottogruppo normale minimale non banale, e intersecherebbe N^* in modo altrettanto non banale.

FSia H un sottogruppo infinito di G: mostriamo che $H \setminus \sigma H$ è finito. Se $x \in \sigma H \setminus H$, $\langle x \rangle$ è un sottogruppo evidentemente non fissato da σ: per ipotesi, c'è un numero finito di tali sottogruppi; inoltre, se C è un gruppo ciclico, il numero di elementi y di C tali che $\langle y \rangle = C$ è finito (è $\varphi(n)$ se C ha ordine n, 2 se C è infinito): ciò dimostra quanto asserito. Di conseguenza, $\sigma H \cap H$ è infinito, e dal fatto che $\sigma H \setminus H$ è unione delle classi laterali non banali di $\sigma H \cap H$ si conclude subito che $\sigma H = H$, e il punto **14.** è dimostrato.

Per l'ultimo quesito, ragioniamo come segue. Per ipotesi, esiste un sottogruppo $K_0 < G$ non normale; il suo normalizzatore $F_0 = N_G(K_0)$ è tale che K_0 è normale in F_0, e inoltre ha indice finito in G. Infatti, dal punto precedente segue subito che, nelle ipotesi attuali, i sottogruppi infiniti di G sono normali, in quanto ogni $\sigma \in \mathrm{Inn}(G)$ fissa quasi tutti i sottogruppi di G; d'altra parte, K_0 può avere solo un numero finito di coniugati distinti, e questo implica che F_0 è infinito, dato che $[G : F_0]$ è esattamente il numero di tali coniugati.

Ora, o F_0 ha tutti i sottogruppi normali, e in tal caso abbiamo concluso, oppure esiste $K_1 < F_0$ che non è normale in F_0. Per lo stesso ragionamento appena fatto (notiamo che F_0 rispetta ancora le ipotesi fatte su G), se poniamo $F_1 = N_{F_0}(K_1)$, otteniamo che F_1 ha indice finito in F_0 e K_1 è normale in F_1. Continuando induttivamente, troviamo sottogruppi F_i inscatolati tali che $[F_i : F_{i+1}]$ è finito e K_{i+1} è normale in F_{i+1} ma non in F_i: se è vero che tale costruzione deve terminare dopo un numero finito di passi, diciamo n, abbiamo concluso, dato che l'F_n così ottenuto ha indice finito in G, ed è quindi normale in G, ha tutti i sottogruppi normali (altrimenti potremmo iterare la costruzione) e, per costruzione, $K_n < F_n$ non è normale in G. D'altra parte, i K_i sono tutti distinti, dato che K_i non è normale in F_j per ogni $j < i$: di conseguenza, ne troviamo in numero finito. Ponendo allora $K = K_n$ e $F = F_n$, il quesito **15.** è concluso.