COMPITO DI ALGEBRA 1
13 settembre 2019
Soluzioni

1. Sia G un gruppo di ordine $2 \cdot 3 \cdot 7$ e sia $g \in G$ un elemento di ordine 14. Supponiamo che G non contenga elementi di ordine 6.

(a) Dimostrare che $\langle g \rangle$ non è normale in G.

(b) Dimostrare che $\langle g^2 \rangle$ è contenuto nel centro di G.

Soluzione.

(a) Supponiamo per assurdo che $\langle g \rangle$ sia normale in G. Osserviamo che $\langle g \rangle$ contiene un unico sottogruppo H di ordine 2, che è quindi caratteristico in $\langle g \rangle$. Siccome un sottogruppo caratteristico di un sottogruppo normale di G è normale in G, H è normale in G. Come noto, questo vuol dire che l'elemento $h \in H$ diverso dall'identità è centrale in G. Detto $b \in G$ un elemento di ordine 3, che esiste per il teorema di Cauchy, usando il fatto che h è centrale in G è immediato verificare che hb ha ordine 6, assurdo.

(a) Soluzione alternativa. Supponiamo per assurdo che $\langle g \rangle$ sia normale in G. Consideriamo $h = g^7$, che è un elemento di ordine 2. Usando la normalità di $\langle g \rangle$ in G otteniamo che per ogni $a \in G$ si ha $aha^{-1} = ag^7a^{-1} = g^k$ per un qualche k. D'altro canto, l'ordine di aha^{-1} deve essere uguale a 2, e quindi necessariamente $k = 7$: in altri termini, $aha^{-1} = h$ per ogni $a \in G$, e quindi h è nel centro di G. Sia allora $b \in G$ un elemento di ordine 3, che esiste per il teorema di Cauchy. Il sottogruppo $\langle h \rangle \cong \mathbb{Z}/2\mathbb{Z}$ normalizza $\langle b \rangle \cong \mathbb{Z}/3\mathbb{Z}$, dunque $\langle a \rangle \langle b \rangle$ è un sottogruppo di G con 6 elementi. Esso è quindi isomorfo a S_3 oppure a $\mathbb{Z}/6\mathbb{Z}$, ma d'altro canto abbiamo già visto che il suo centro è non banale (perché contiene h), e quindi si tratta necessariamente di $\mathbb{Z}/6\mathbb{Z}$. Questo però contraddice il fatto che G non contiene elementi di ordine 6, e l'assurdo mostra che $\langle g \rangle$ non può essere normale in G.

(b) Il gruppo $P_7 := \langle g^2 \rangle$ ha ordine 7, ed è quindi un 7-Sylow di G. Il numero di 7-Sylow di G è un divisore di 6 congruo a 1 modulo 7, ovvero è necessariamente 1, il che prova che il 7-Sylow P_7 è normale. Possiamo allora considerare l'omomorfismo

$$\begin{array}{rccc} \Phi : & G & \to & \mathrm{Aut}(P_7) \\ & a & \mapsto & \text{coniugio per } a \end{array}$$

Chiaramente g commuta con g^2, che è un generatore di P_7, quindi g sta nel nucleo di Φ. Ne segue che il nucleo di Φ contiene $\langle g \rangle$, che è un gruppo di ordine

14, e quindi $\ker\Phi$ è un gruppo di ordine 14 o 42 (in effetti, la sua cardinalità è un multiplo di 14 che divide 42). D'altro canto $\ker\Phi$ è un sottogruppo normale di G, quindi non può coincidere con $\langle g\rangle$ per il punto precedente: ne segue che $|\ker\Phi| = 42$, ovvero Φ è l'omomorfismo banale. Questo vuol dire che per ogni $a \in G$ il coniugio per a è l'identità su P_7, ovvero che a commuta con P_7. Questo dimostra che P_7 è nel centro di G.

2. Siano G un gruppo finito, p un numero primo che divide l'ordine del gruppo, e n_p il numero dei p-sottogruppi di Sylow di G. Dimostrare che l'insieme dei normalizzatori dei p-sottogruppi di Sylow costituisce una classe di coniugio dei sottogruppi di G che ha esattamente n_p elementi.

Soluzione. Sia P un p-sottogruppo di Sylow di G. Sappiamo dai teoremi di Sylow che tutti i p-sottogruppi di Sylow di G sono della forma gPg^{-1} per qualche $g \in G$. Dimostriamo innanzitutto che, per ogni $g \in G$, $N(P)$ e $N(gPg^{-1})$ sono sottogruppi coniugati.

Abbiamo

$$\begin{aligned} x \in N(gPg^{-1}) \;&\Leftrightarrow\; xgPg^{-1}x^{-1} = gPg^{-1} \Leftrightarrow g^{-1}xgPg^{-1}x^{-1}g = P \\ &\Leftrightarrow\; g^{-1}xgP(g^{-1}xg)^{-1} = P \Leftrightarrow g^{-1}xg \in N(P) \Leftrightarrow x \in gN(P)g^{-1}\,, \end{aligned}$$

da cui $N(gPg^{-1}) = gN(P)g^{-1}$, e dunque i normalizzatori di due p-sottogruppi di Sylow sono coniugati.

Viceversa, supponiamo che un sottogruppo H di G sia coniugato al sottogruppo $N(P)$. Allora esiste $g \in G$ per cui $H = gN(P)g^{-1}$ e, per quanto visto prima, $H = N(gPg^{-1})$.

Ne segue che i normalizzatori dei p-sottogruppi di Sylow formano una classe di coniugio, e quindi resta solo da dimostrare che questa classe di coniugio ha esattamente n_p elementi. Trattandosi di un insieme finito, è sufficiente dimostrare che, se $gPg^{-1} \neq P$, allora $N(gPg^{-1}) = gN(P)g^{-1} \neq N(P)$. Supponiamo, per assurdo, che nelle nostre ipotesi valga $gN(P)g^{-1} = N(P)$. Allora $g \in N(N(P))$. Osserviamo ora che $N(N(P)) = N(P)$; infatti, l'inclusione $N(P) \subseteq N(N(P))$ è ovvia, mentre, se $x \in N(N(P))$, allora il coniugio per x induce un automorfismo di $N(P)$; ma poiché P, essendo normale in $N(P)$, è l'unico p-sottogruppo di Sylow di $N(P)$, il coniugio per x induce anche un automorfismo di P, ossia $x \in N(P)$, da cui l'osservazione è dimostrata.

In conclusione, se $gN(P)g^{-1} = N(P)$, allora $g \in N(P)$, e dunque $gPg^{-1} = P$, contraddizione.

3. Sia A un anello commutativo con identità.

(a) Supponiamo che per ogni ideale I di A valga $\sqrt{I} = I$. Dimostrare che, se k è un intero positivo e J, L sono ideali di A per cui $J^k = L^k$, allora $J = L$.

(b) Supponiamo invece che esista un ideale I di A con $I = I^2$ e tale che $\sqrt{I} \neq I$. Dimostrare che esistono due ideali distinti di A, J e L, per cui $J^k = L^k$ per ogni $k > 1$.

(c) Dimostrare che, se $\sqrt{I} \neq I$ e la catena discendente di ideali $I \supseteq I^2 \supseteq I^3 \supseteq \dots$ è stazionaria, allora esiste un ideale I_0 di A tale che $I_0 = I_0^2$ e $\sqrt{I_0} \neq I_0$.

SOLUZIONE.

(a) Sia $I = J^k = L^k$. Dimostreremo che sia J che L sono uguali ad I, da cui la tesi. Abbiamo ovviamente $I = J^k \subseteq J$. D'altra parte, sia $x \in J$; allora $x^k \in J^k = I$, ossia $x \in \sqrt{I} = I$. Ne segue che $J = I$ e, per simmetria, anche $L = I$.

(b) Sia I un ideale tale che $I = I^2$ e $\sqrt{I} \neq I$. Sia $x \in \sqrt{I} \setminus I$, e supponiamo che $m > 1$ sia il più piccolo esponente per cui $x^m \in I$. Siano $J = (x^{m-1}) + I$, $L = I$. Allora $J \neq L$ e, poichè $x^{k(m-1)} \in I$ per ogni $k > 1$, si ha $I^k \subseteq J^k \subseteq I + I^k$. Inoltre, poiché da $I = I^2$ si deduce facilmente per induzione che $I = I^k$ per ogni $k > 1$, si ha che $J^k = L^k = I$ per ogni $k > 1$.

(c) Supponiamo che n sia un intero positivo per cui $I^n = I^{n+1} = I^{n+2} = \dots$ e poniamo $I_0 = I^n$. Allora ovviamente $I_0 = I_0^2$. Inoltre, da $I^n \subseteq I$ si ottiene immediatamente che $\sqrt{I^n} \subseteq \sqrt{I}$. Viceversa, se $x \in \sqrt{I}$, allora esiste $k > 0$ tale che $x^k \in I$, da cui $x^{kn} \in I^n$, $x \in \sqrt{I^n}$ e infine $\sqrt{I^n} = \sqrt{I}$, ossia $\sqrt{I_0} = \sqrt{I}$. La conclusione segue dal fatto che, poiché $I_0 \subseteq I$, se $x \in \sqrt{I} \setminus I$ allora a maggior ragione $x \in \sqrt{I_0} \setminus I_0$.

4. Sia $\alpha = \sqrt[5]{5 + \sqrt{24}} \in \mathbb{R}$.

(a) Mostrare che $\mathbb{Q}(\alpha, \zeta_5)$ è un'estensione di Galois di $\mathbb{Q}$.

(b) Per ogni intero j sia $\beta_j = \alpha\zeta_5^j + \frac{1}{\alpha\zeta_5^j}$. Determinare, in funzione di j, il polinomio minimo di β_j su $\mathbb{Q}$.

(c) Dire se $\mathbb{Q}(\alpha + 1/\alpha)$ è un'estensione di Galois di $\mathbb{Q}$.

SOLUZIONE.

(a) È sufficiente mostrare che $\mathbb{Q}(\alpha, \zeta_5)$ è il campo di spezzamento di un polinomio a coefficienti in $\mathbb{Q}$. Partendo dall'equazione $\alpha = \sqrt[5]{5 + \sqrt{24}}$ otteniamo $\alpha^5 = 5 + \sqrt{24}$, e dunque $(\alpha^5 - 5)^2 = 24$. Ne ricaviamo che α è una radice del polinomio $p(x) = x^{10} - 10x^5 + 1$ (non stiamo affermando che questo polinomio sia irriducibile). Troviamo tutte le radici di questo polinomio. Posto $y = x^5$, abbiamo che $y^2 - 10y + 1 = 0$, che ha come radici $y_1 = 5 + \sqrt{24}$ e $y_2 = 5 - \sqrt{24}$.

Osserviamo che $5-\sqrt{24}=\frac{1}{5+\sqrt{24}}$. Le radici di $p(x)$ sono le radici quinte di y_1 e $y_2=1/y_1$. Ne segue che il campo di spezzamento è $\mathbb{Q}(\sqrt[5]{y_1}\zeta_5^j, \sqrt[5]{1/y_1}\zeta_5^j \mid j = 0,\dots,4) = \mathbb{Q}(\sqrt[5]{y_1}, \zeta_5, \sqrt[5]{1/y_1}) = \mathbb{Q}(\alpha,\zeta_5)$, che è quindi un'estensione di Galois di $\mathbb{Q}$ come voluto.

(b) Si ha

$$\begin{aligned}\beta_j^5 &= \alpha^5 + 5(\alpha\zeta_5^j)^4(\alpha^{-1}\zeta_5^{-j}) + 10(\alpha\zeta_5^j)^3(\alpha^{-1}\zeta_5^{-j})^2 + 10(\alpha\zeta_5^j)^2(\alpha^{-1}\zeta_5^{-j})^3 \\ &\quad + 5(\alpha\zeta_5^j)(\alpha^{-1}\zeta_5^{-j})^4 + \alpha^{-5} = \\ &= \alpha^5+\alpha^{-5} + 5(\alpha^3\zeta_5^{3j} + \alpha^{-3}\zeta_5^{-3j}) + 10(\alpha\zeta_5^j + \alpha^{-1}\zeta_5^{-j}) \\ &= 10 + 5\left(\beta_j^3 - 3\beta_j\right) + 10\beta_j.\end{aligned}$$

Ne segue che β_j è una radice del polinomio $q(x) = x^5-5x^3+5x-10$, che è irrudicibile per il criterio di Eisenstein applicato con il primo 5. Esso è quindi il polinomio minimo cercato, indipendentemente da j.

(c) Se $\mathbb{Q}(\alpha+1/\alpha)$ fosse un'estensione di Galois di $\mathbb{Q}$, allora avrebbe la seguente proprietà: se contiene la radice di un polinomio irriducibile a coefficienti in $\mathbb{Q}$, allora le contiene tutte. Abbiamo visto al punto precedente che $\alpha+1/\alpha$ è una radice del polinomio $q(x)$, le cui altre radici sono i β_j per $j=1,2,3,4$. Tuttavia, β_1 non appartiene a $\mathbb{Q}(\alpha+1/\alpha)$: in effetti $\mathbb{Q}(\alpha+1/\alpha)$ è un sottocampo di $\mathbb{R}$, mentre $\alpha\zeta_5+\frac{1}{\alpha\zeta_5} = \sqrt[5]{5+\sqrt{24}}\cdot\zeta_5 + \sqrt[5]{5-\sqrt{24}}\cdot\overline{\zeta_5}$ non è un numero reale, perché la sua parte immaginaria è $(\sqrt[5]{5+\sqrt{24}} - \sqrt[5]{5-\sqrt{24}})y \neq 0$, dove y è la parte immaginaria di ζ_5. Ne segue che $\mathbb{Q}(\alpha+1/\alpha)$ non è un'estensione di Galois di $\mathbb{Q}$.