COMPITO DI ALGEBRA 1
13 luglio 2021

Esercizio 1.
Sia G un gruppo di ordine $7^2 \cdot 13^2$.

1. Dimostrare che il centro di G ha cardinalità multipla di 7.

2. Determinare le possibili cardinalità di $Z(G)$.

SOLUZIONE. Sia n_{13} il numero di 13-Sylow di G. Si ha $n_{13} \equiv 1 \pmod{13}$ e $n_{13} \mid 7^2$, da cui $n_{13} = 1$, e quindi G contiene un unico 13-Sylow P_{13}, che è dunque normale in G. Sia inoltre P_7 un 7-Sylow di G: dato che $P_7 \cap P_{13} = \{e\}$ e $P_7 P_{13} = G$ per motivi di cardinalità, abbiamo $G \cong P_{13} \rtimes_\varphi P_7$. Osserviamo che gli unici gruppi di ordine 13^2 (a meno di isomorfismo) sono $\mathbb{Z}/13^2\mathbb{Z}$ e $(\mathbb{Z}/13\mathbb{Z})^2$: nei due casi, il gruppo $\mathrm{Aut}(P_{13})$ è isomorfo rispettivamente a $(\mathbb{Z}/13^2\mathbb{Z})^\times$ (di ordine $\varphi(169) = 12 \cdot 13$) ed a $\mathrm{GL}_2(\mathbb{F}_{13})$ (di ordine $(13^2-1)(13^2-13) = 2^5 \cdot 3^2 \cdot 7 \cdot 13$). In entrambi i casi l'omomorfismo φ, il cui dominio ha ordine 49, non può essere iniettivo: in caso contrario, l'immagine di φ sarebbe un sottogruppo di $\mathrm{Aut}(P_{13})$ di ordine 49, assurdo per il teorema di Lagrange in quanto 49 non divide $\#\,\mathrm{Aut}(P_{13})$.

1. Sia h un elemento non banale nel nucleo di φ (e dunque in particolare un elemento di P_7). Tale h commuta con tutti gli elementi di P_7 (in effetti P_7 è abeliano, perché $\#P_7$ è il quadrato di un numero primo), e commuta anche con tutti gli elementi di P_{13}: preso $p \in P_{13}$, per definizione abbiamo $hph^{-1} = \varphi(h)(p) = p$, cioè $hp = ph$. Quindi il centralizzatore di h è un sottogruppo contenente sia P_{13} che P_7, e dunque contiene l'intero G: ne segue che h commuta con tutti gli elementi di G, ovvero $h \in Z(G)$. Siccome l'ordine di h è 7 o 49 (h è un elemento non banale in un gruppo di ordine 49), abbiamo che $7 \mid \mathrm{ord}(h) \mid \#Z(G)$ come voluto.

2. La cardinalità del centro di G divide $7^2 \cdot 13^2$ ed è multipla di 7. Se $7 \cdot 13$ divide $\#Z(G)$, allora $G/Z(G)$ ha cardinalità che divide $7^2 \cdot 13^2/(7 \cdot 13) = 7 \cdot 13$. Siccome ogni gruppo di cardinalità 1, 7, 13 o $7 \cdot 13$ è ciclico (si osservi che $7 \nmid 13-1$) otteniamo che $G/Z(G)$ è ciclico, il che come noto è possibile solo se G è abeliano. Otteniamo quindi che in tal caso $\#Z(G) = 13^2 \cdot 7^2$, e tale valore è certamente realizzabile, ad esempio prendendo $G = \mathbb{Z}/7^2 13^2\mathbb{Z}$. Restano da considerare i divisori di $7^2 \cdot 13^2$ multipli di 7 e non divisibili per 13, ovvero 49 e 7. Se $\#Z(G) = 49$, allora $Z(G)$

è un 7-Sylow di G. Ma il centro di un gruppo è sempre un sottogruppo normale, e otteniamo che $G \cong P_{13} \times P_7$ è un prodotto di gruppi abeliani e quindi abeliano, assurdo (perché il centro avrebbe cardinalità $7^2 \cdot 13^2$ e non 7^2). Mostriamo infine che $Z(G)$ può avere cardinalità 7: visto che abbiamo escluso tutte le altre cardinalità, è sufficiente esibire un gruppo di ordine $7^2 \cdot 13^2$ non abeliano. Un tale gruppo è ad esempio $((\mathbb{Z}/13\mathbb{Z})^2 \rtimes_\psi \mathbb{Z}/7\mathbb{Z}) \times \mathbb{Z}/7\mathbb{Z}$, dove ψ manda un generatore di $\mathbb{Z}/7\mathbb{Z}$ in un elemento di ordine 7 di $\mathrm{GL}_2(\mathbb{F}_{13})$, che esiste per il teorema di Cauchy. In tale gruppo l'azione di coniugio è non banale, quindi il gruppo non è abeliano, e per quanto già detto la cardinalità del suo centro non può essere altro che 7. Concludendo, $Z(G)$ può avere cardinalità 7 o $7^2 \cdot 13^2$.

Esercizio 2.
Consideriamo il gruppo $G = \mathrm{GL}_3(\mathbb{F}_3)$ e l'insieme

$$X = \{L \text{ sottospazio vettoriale di } \mathbb{F}_3^3 \text{ di dimensione } 1\}.$$

Il gruppo G agisce su X secondo la formula $g \cdot L = g(L)$, dove $g(L)$ è l'immagine del sottospazio vettoriale L tramite l'applicazione lineare corrispondente alla matrice g.

1. Dimostrare che il gruppo $\mathrm{Stab}_G(L)$ ha cardinalità indipendente da $L \in X$, e calcolare il valore comune di queste cardinalità.
2. Dimostrare che $Z(G) = \bigcap_{L \in X} \mathrm{Stab}_G(L)$.
3. Determinare il più piccolo intero positivo n per cui $G/Z(G)$ si immerge in S_n.

Soluzione. Ricordiamo che una matrice 3×3 con coefficienti in $\mathbb{F}_3$ appartiene a $\mathrm{GL}_3(\mathbb{F}_3)$ se e solo se le sue colonne sono linearmente indipendenti. Questa caratterizzazione sulla prima colonna pone come unica condizione che sia diversa da 0, sulla seconda che sia fuori dalla retta generata dal primo vettore e sulla terza che sia fuori dal piano generato dai vettori delle prime 2 colonne. Da questo otteniamo che

$$|G| = (3^3 - 1)(3^3 - 3)(3^3 - 3^2) = 26 \cdot 24 \cdot 18.$$

Una retta di $\mathbb{F}_3^3$ è generata da un vettore diverso da 0; inoltre ogni retta ha esattamente 2 basi, quindi

$$\#X = \frac{3^3 - 1}{2} = 13.$$

1. Osserviamo che l'azione di G su X è transitiva; infatti siano $L_1 = \langle v_1 \rangle$ e $L_2 = \langle v_2 \rangle$ rette di $\mathbb{F}_3^3$, vogliamo vedere che esiste $g \in G$ tale che $gL_1 = L_2$. Poiché v_1 e v_2

sono vettori non nulli, possono essere entrambi completati a base $\{v_i, w_i, z_i\}$ di $\mathbb{F}_3^3$ $(i = 1, 2)$. Sia g la matrice dell'unica applicazione lineare definita dall'assegnamento $v_1 \to v_2$, $w_1 \to w_2$, $z_1 \to z_2$; tale applicazione è chiaramente surgettiva e quindi è un automorfismo di $\mathbb{F}_3^3$, per cui $g \in G$ e chiaramente $gL_1 = L_2$. Questo mostra che per ogni $L \in X$ si ha $\mathrm{orb}_G(L) = X$ e dalla formula orbita stabilizzatore ricaviamo che per ogni $L \in X$ si ha

$$|\operatorname{Stab}_G(L)| = \frac{|G|}{|\mathrm{orb}_G(L)|} = \frac{26 \cdot 24 \cdot 18}{13} = 864.$$

2. Ricordiamo che, per ogni campo K, il centro di $\mathrm{GL}_n(K)$ è dato dalle matrici scalari, in questo caso quindi $Z(G) = \{\pm \mathrm{Id}\}$ (il centro in questo caso può essere determinato anche con un semplice calcolo esplicito). È quindi chiaro che $Z(G) \subseteq \bigcap_{L \in X} \operatorname{Stab}_G(L)$.

   D'altra parte, sia $g \in \bigcap_{L \in X} \operatorname{Stab}_G(L)$ e sia $\mathcal{B} = \{v_1, v_2, v_3\}$ una base di $\mathbb{F}_3^3$. Definiamo $L_i = \langle v_i \rangle$, per $i = 1, 2, 3$ e $L = \langle v_1 + v_2 + v_3 \rangle$. Dato che g stabilizza L_1, L_2 e L_3, si ha $g(v_i) = \pm v_i$ quindi rispetto alla base $\mathcal{B}$ si ha

$$g = \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \pm 1 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix}.$$

   Inoltre g stabilizza anche L, per cui $g(v_1 + v_2 + v_3) = \pm(v_1 + v_2 + v_3)$, quindi i segni degli elementi diagonali devono essere tutti uguali, cioè $g = \pm \mathrm{Id}$ e $g \in Z(G)$.

3. Indichiamo con ϕ l'azione di G su X che stiamo considerando,

$$\phi \colon G \to S(X).$$

   Il nucleo di questa azione è

$$\ker(\phi) = \{g \in G \mid gL = L \text{ per ogni } L \in X\} = \bigcap_{L \in X} \operatorname{Stab}_G(L) = Z(G),$$

   quindi $G/Z(G)$ si immerge in $S(X) \cong S_{13}$. D'altra parte, $|G/Z(G)| = 26 \cdot 24 \cdot 18/2$ e quindi è multipla di 13. Dato che $13 | n!$ se e solo se $n \geq 13$, si ha che 13 è il minimo cercato.

   Nota: L'esercizio può essere svolto anche usando il linguaggio dei gruppi anziché quello degli spazi vettoriali. Infatti sappiamo che il gruppo $\mathbb{Z}/3\,\mathbb{Z}^3$ ha in modo naturale anche una struttura di spazio vettoriale. I suoi sottogruppi sono esattamente i sottospazi vettoriali (in particolare le rette sono i sottogruppi di ordine 3) e gli automorfismi di di gruppo sono quelli di spazio vettoriale.

Esercizio 3.
Sia A l'anello $\mathbb{Z}[i]$.

1. Calcolare la cardinalità e la caratteristica dell'anello $A/(i+18)$.
2. Determinare gli ideali primi di A che contengono $(i+18)$.

SOLUZIONE.

1. Come noto dalla teoria, la cardinalità di $A/(i+18)$ è la norma quadra di $i+18$, ovvero $1^2+18^2 = 325 = 5^2 \cdot 13$. Per definizione, la caratteristica di $A/(i+18)$ è il minimo intero positivo n tale che $\underbrace{1+\cdots+1}_{n \text{ volte}} = 0$ in $A/(i+18)$. Data la definizione di anello quoziente, questo è il minimo $n > 0$ tale che $n \in (i+18)$. Consideriamo allora il generico elemento dell'ideale $(i+18)$, ovvero
$$(i+18)(a+bi) = 18a - b + i(a+18b).$$
Un elemento di questo tipo è un intero se e solo se $a = -18b$, e in tal caso è uguale a $18a - b = -(1^2+18^2)b$. Concludiamo che gli interi in $(i+18)$ sono esattamente i multipli di 325, e quindi che questa è la caratteristica di $A/(i+18)$.

2. Gli ideali primi di A contenenti $(i+18)$ sono in bigezione con gli ideali primi del quoziente $B = A/(i+18)$. Dal punto precedente segue che $A/(i+18) \cong \mathbb{Z}/325\mathbb{Z}$: in effetti, l'omomorfismo di caratteristica $\mathbb{Z} \to A/(i+18)$ induce un omomorfismo iniettivo $\mathbb{Z}/325\mathbb{Z} \to A/(i+18)$, che essendo definito fra anelli della medesima cardinalità è un isomorfismo. Un ideale P di $B \cong \mathbb{Z}/325\mathbb{Z}$ è in particolare un sottogruppo additivo, dunque della forma (d) per qualche $d \mid 325$. Inoltre, $B/P \cong \mathbb{Z}/d\mathbb{Z}$, quindi (d) è primo se e solo se $\mathbb{Z}/d\mathbb{Z}$ è un dominio, se e solo se (d) è primo in $\mathbb{Z}$. Siccome $d \mid 325 = 5^2 \cdot 13$, le uniche possibilità sono $d = 5$ e $d = 13$. Per corrispondenza otteniamo allora gli ideali primi cercati, $(i+18, 5)$ e $(i+18, 13)$.

   Nota. Gli ideali di A sono tutti principali. Anche se non era richiesto, si può verificare facilmente che $(i+18, 5) = (i-2)$ e $(i+18, 13) = (2+3i)$.

   SOLUZIONE ALTERNATIVA. Come noto, gli ideali di A sono tutti principali, e quelli che contengono $(i+18)$ sono quelli della forma $(a+bi)$ per cui $i+18 \in (a+bi)$, ovvero $a+bi \mid i+18$. Osservando che $(i+18)(-i+18) = 325 = 5^2 \cdot 13 = (2+i)^2(2-i)^2(2+3i)(2-3i)$ è facile trovare la fattorizzazione in irriducibili $i+18 = (2-i)^2 \cdot (2+3i)$. Ricordando poi che A è un UFD, per determinare gli ideali primi $(a+bi)$ che contengono $(i+18)$ dobbiamo trovare gli elementi primi $a+bi$ che dividono $i+18 = (2-i)^2 \cdot (2+3i)$. Data l'unicità della fattorizzazione, tali elementi sono $2-i$ e $2+3i$, e gli ideali richiesti sono quindi $(2-i)$ e $(2+3i)$.

Esercizio 4.
Sia $K = \mathbb{Q}(i, \sqrt[7]{5})$ e indichiamo con L la più piccola estensione di K che sia normale su $\mathbb{Q}$.

1. Determinare, a meno di isomorfismo, il gruppo di Galois di $L/\mathbb{Q}$.

2. Determinare un elemento primitivo di $K/\mathbb{Q}$.

SOLUZIONE. Ricordiamo che il polinomio minimo di i su $\mathbb{Q}$ è x^2+1 e osserviamo che quello di $\sqrt[7]{5}$ è x^7-5, in quanto si annulla in $\sqrt[7]{5}$ ed è irriducibile su $\mathbb{Z}$ per il Criterio di Eisenstein rispetto al primo 5, quindi anche su $\mathbb{Q}$ in virtù del Lemma di Gauss. Quanto detto implica che $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ e $[\mathbb{Q}(\sqrt[7]{5}) : \mathbb{Q}] = 7$, e dato che $(2, 7) = 1$ otteniamo che $[K : \mathbb{Q}] = 14$.

1. La più piccola estensione di K normale su $\mathbb{Q}$ deve contenere tutte le radici di x^7-5, quindi deve contenere il campo $\mathbb{Q}(i, \sqrt[7]{5}, \zeta_7)$. D'altra parte questo campo è il campo di spezzamento su $\mathbb{Q}$ di $(x^2-1)(x^7-5)$, quindi è un'estensione normale di $\mathbb{Q}$, di conseguenza $\mathbb{Q}(i, \sqrt[7]{5}, \zeta_7) = L$.

   Sappiamo che $\mathbb{Q}(i, \zeta_7) = \mathbb{Q}(\zeta_{28})$ quindi $L = \mathbb{Q}(\zeta_{28})\,\mathbb{Q}(\sqrt[7]{5})$. Ora $[\mathbb{Q}(\zeta_{28}) : \mathbb{Q}] = \varphi(28) = 12$ e $[\mathbb{Q}(\sqrt[7]{5}) : \mathbb{Q}] = 7$, quindi, dato che $(12, 7) = 1$, si ha $[L : \mathbb{Q}] = 12 \cdot 7 = 84$. D'alta parte L è anche il composto di $\mathbb{Q}(i)$ e di $\mathbb{Q}(\sqrt[7]{5}, \zeta_7)$ che sono estensioni normali di $\mathbb{Q}$. Poiché $\mathbb{Q}(i) \cap \mathbb{Q}(\sqrt[7]{5}, \zeta_7) = \mathbb{Q}$ (questo si ricava dal fatto che il grado del composto è il prodotto dei gradi), dalla teoria svolta si ottiene:

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt[7]{5}, \zeta_7)/\mathbb{Q}).$$

   Ora $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\,\mathbb{Z}$, mentre si può dimostrare che

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[7]{5}, \zeta_7)/\mathbb{Q}) \cong \mathbb{Z}/7\,\mathbb{Z} \rtimes (\mathbb{Z}/7\,\mathbb{Z})^*.$$

   Infatti $\mathrm{Gal}(\mathbb{Q}(\sqrt[7]{5}, \zeta_7)/\mathbb{Q})$ è un gruppo non abeliano di ordine $\frac{\#\,\mathrm{Gal}(L/\mathbb{Q})}{\#\,\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})} = 42$. In particolare, tutti i 42 assegnamenti della forma $\zeta_7 \mapsto \zeta_7^i$, $\sqrt[7]{5} \mapsto \zeta_7^j \sqrt[7]{5}$ per $i = 1, \ldots, 6$, $j = 0, \ldots, 6$ si estendono ad automorfismi di $\mathbb{Q}(\sqrt[7]{5}, \zeta_7)/\mathbb{Q}$. Il 7-sottogruppo di Sylow P che fissa $\mathbb{Q}(\zeta_7)$ è normale (perché lo è $\mathbb{Q}(\zeta_7)/\mathbb{Q}$) ed è generato dall'automorfismo

$$\rho : \begin{cases} \zeta_7 \to \zeta_7 \\ \sqrt[7]{5} \to \zeta_7 \sqrt[7]{5}. \end{cases}$$

   D'altra parte, dato che $[\mathbb{Q}(\sqrt[7]{5}, \zeta_7) : \mathbb{Q}(\sqrt[7]{5})] = [\mathbb{Q}(\zeta_7) : \mathbb{Q}]$, si ha che

$$H = \mathrm{Gal}(\mathbb{Q}(\sqrt[7]{5}, \zeta_7)/\,\mathbb{Q}(\sqrt[7]{5})) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_7)/\,\mathbb{Q}) \cong (\mathbb{Z}/7\,\mathbb{Z})^*$$

ed è immediato verificare che

$$\eta : \begin{cases} \zeta_7 \to \zeta_7^3 \\ \sqrt[7]{5} \to \sqrt[7]{5} \end{cases}$$

ha grado 6 ed è quindi un generatore di H. Da questo otteniamo che $\mathrm{Gal}(\mathbb{Q}(\sqrt[7]{5}, \zeta_7)/\mathbb{Q})$ è isomorfo ad un prodotto semidiretto di H e P. Dato che

$$\eta\rho\eta^{-1}(\sqrt[7]{5}) = \zeta_7^3\sqrt[7]{5} = \rho^3(\sqrt[7]{5}),$$

si ottiene

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[7]{5}, \zeta_7)/\mathbb{Q}) \cong \mathbb{Z}/7\mathbb{Z} \rtimes_\psi (\mathbb{Z}/7\mathbb{Z})^*$$

dove $\psi\colon (\mathbb{Z}/7\mathbb{Z})^* \mapsto \mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$ è definita da $\bar{3} \to (\bar{1} \to \bar{3})$.

2. Sia $\alpha \in K$. α è un elemento primitivo di $K/\mathbb{Q}$ se $K = \mathbb{Q}(\alpha)$; questo equivale a dire che il polinomio minimo di α su $\mathbb{Q}$ ha grado 14, o ancora che α ha 14 coniugati su $\mathbb{Q}$.

   Consideriamo le immersioni di $K/\mathbb{Q}$ definite dagli assegnamenti

$$\sigma_{lj} : \begin{cases} i \to (-1)^l i \\ \sqrt[7]{5} \to \zeta_7^j\sqrt[7]{5} \end{cases}$$

   dove $\zeta_7 \in \mathbb{C}$ è una radice settima primitiva di 1, $l = 0, 1$ e $j = 0, \ldots, 6$. Il fatto che questi assegnamenti si estendano a tutto K segue immediatamente dal fatto che sono restrizioni di elementi del gruppo di Galois di $L/\mathbb{Q}$. Queste 14 immersioni sono distinte su K e quindi sono tutte le immersioni di $K/\mathbb{Q}$ che sappiamo essere tante quanto il grado.

   Scegliamo $\alpha = i + \sqrt[7]{5}$ e mostriamo che le immagini di α mediante le immersioni σ_{lj} sono tutte distinte. Infatti $\sigma_{lj}(\alpha) = \sigma_{hk}(\alpha)$ se e solo se

$$(-1)^l i + \zeta_7^j\sqrt[7]{5} = (-1)^h i + \zeta_7^k\sqrt[7]{5}.$$

   Se $l = h$ questo dà $\zeta_7^j\sqrt[7]{5} = \zeta_7^k\sqrt[7]{5}$ da cui $j = k$. Se $l \neq h$ otteniamo $(-1)^l 2i = \sqrt[7]{5}(\zeta_7^k - \zeta_7^j) \in \mathbb{Q}(i) \cap \mathbb{Q}(\sqrt[7]{5}, \zeta_7) = \mathbb{Q}$ ma i due membri non sono razionali, quindi questa uguaglianza non è possibile.

   Questo mostra che α ha 14 coniugati, quindi è un elemento primitivo di $K/\mathbb{Q}$.