COMPITO DI ALGEBRA 1
10 febbraio 2017

1. Si consideri il sottogruppo abeliano A di $\mathbb{Z}^4$ generato da

$$\begin{pmatrix} 2 \\ 4 \\ 6 \\ 8 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 4 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 8 \\ 2 \\ 8 \end{pmatrix}.$$

Si consideri inoltre il sottogruppo abeliano B di $\mathbb{Z}$ generato da 40. Consideriamo il sottogruppo $A \times B$ di $\mathbb{Z}^4 \times \mathbb{Z} = \mathbb{Z}^5$.

(a) Scrivere il quoziente $G = \mathbb{Z}^5/(A \times B)$ in una delle forme canoniche per i gruppi abeliani finitamente generati.

(b) Dire qual'è l'ordine massimo fra gli elementi della parte di torsione di G e quanti elementi hanno quell'ordine.

Traccia della soluzione:

(a) Il sottogruppo $A \times B$ di $\mathbb{Z}^5$ coincide con l'immagine dell'omomorfismo $L : \mathbb{Z}^4 \to \mathbb{Z}^5$ rappresentato rispetto alle basi standard dalla matrice

$$\begin{pmatrix} 2 & 1 & 2 & 0 \\ 4 & 3 & 8 & 0 \\ 6 & 4 & 2 & 0 \\ 8 & 2 & 8 & 0 \\ 0 & 0 & 0 & 40 \end{pmatrix}$$

Possiamo fare le mosse intere di riga e di colonna, che corrispondono rispettivamente a dei cambiamenti di base in arrivo e in partenza, e troviamo che L è rappresentato nelle nuove basi dalla matrice

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 40 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

da questo si deduce facilmente che $G = \mathbb{Z}^5/(A \times B) \cong \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_{40}$.

(b) L'ordine massimo fra gli elementi della parte di torsione è 40. Per calcolare quanti elementi hanno ordine 40 torna comodo scrivere G nell'altra forma canonica per i gruppi abeliani finitamente generati:

$$G \cong \mathbb{Z} \times (\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_8) \times \mathbb{Z}_5$$

Se un elemento di G ha coordinate (a, b, c, d, e), allora ha ordine 40 se e solo se $a = 0$, $e \neq [0]_5$ e $(b, c, d,)$ è un elemento di $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_8$ di ordine 8. Abbiamo dunque 4 scelte per e e $(2 \cdot 8 \cdot 8 - 2 \cdot 4 \cdot 4) = 96$ scelte per $(b, c, d,)$ (questo ultimo conto deriva dal considerare tutti gli elementi meno quelli che non hanno ordine 8). In totale troviamo $96 \cdot 4 = 384$ elementi di ordine 40.

2. Sia H un sottogruppo di un gruppo finito G con $H \neq G$.

(a) Mostrare un esempio in cui $H \neq \{e\}$ e l'intersezione di tutti i coniugati di H è $\{e\}$, e un esempio in cui l'intersezione di tutti i coniugati di H è $\neq \{e\}$.

(b) Dimostrare che esiste un elemento di G che non è coniugato a nessun elemento di H.

(c) Si supponga che G agisca transitivamente su un insieme S, ossia formando un'unica orbita. Mostrare che se $|S| \geq 2$ allora c'è un elemento $g \in G$ che non fissa alcun punto di S.

(d) Sia K un sottogruppo di $\mathrm{Aut}(G)$ di cardinalità coprima con la cardinalità di G. Sia $k \in K$ un elemento diverso dall'identità. Mostrare che non è possibile che per ogni classe di coniugio C in G valga che $k(C) \subseteq C$.

Soluzione:

(a) Consideriamo $G = S_3$. Il sottogruppo $H = \langle(1, 2)\rangle$ è coniugato con tutti i sottogruppi di cardinalità 2, che sono generati da una trasposizione. Sottogruppi distinti di cardinalità 2 possono condividere solo l'identità.

Consideriamo ora $G = S_3$ e $H = A_3$. In questo caso H è normale e quindi coincide con tutti i suoi coniugati e l'intersezione è dunque sempre H.

(b) Il numero di coniugati di H è pari a $|G/N(H)|$ e poiché $H < N(H)$ si ha che $|G/N(H)| \leq |G/H|$. Complessivamente i coniugati di H, contando gli elementi con le ripetizioni, contengono $|G/N(H)| \cdot |H|$ elementi e abbiamo visto che $|G/N(H)| \cdot |H| \leq |G/H| \cdot |H| = |G|$. Inoltre se H è un sottogruppo proprio normale allora H coincide con l'unione dei suoi coniugati ed è un sottoinsieme proprio di G. Se H non è normale allora ha almeno due coniugati e poiché questi condividono almeno l'identità, allora la cardinalità dell'unione dei conoigati di H è strettamente minore di $|G/N(H)| \cdot |H| \leq |G|$. In entrambi i casi ne segue che almeno un elemento di G non sta nell'unione dei coniugati di H.

(c) Chiamiamo H lo stabilizzatore di un elemento $s \in S$. Poiché l'azione di G è transitiva, abbiamo che $|S| = |G/H|$ e gli stabilizzatori degli elementi di S (che è fatto da un'unica G-orbita) sono tutti coniugati a H. Dunque per quanto visto nel punto (b) esiste almeno un elemento di G che non sta in nessun coniugato di H, ovvero che non fissa nessun elemento di S.

(d) Sia $m \neq 1$ l'ordine di k: osserviamo che m divide la cardinalità di K e dunque è coprimo con $|G|$. Sia p un primo che divide m. Allora l'automorfismo $\gamma = k^{\frac{m}{p}}$ ha ordine p. Se valesse che per ogni classe di coniugio C in G $k(C) \subseteq C$ allora avremmo anche $\gamma(C) \subseteq C$.

Ogni classe di coniugio di G ha cardinalità che divide la cardinalità di G (infatti la cardinalità della classe di coniugio di $g \in G$ è pari a $|G/C(g)|$). In particolare tale cardinalità è prima con p.

Fissiamo una classe di coniugio C di G. Le orbite di γ in C hanno cardinalità 1 oppure p, e non possono essere tutte di cardinalità p, altrimenti $p \mid |C|$. Quindi in ogni classe C esiste una γ-orbita con un solo elemento. Sia H il sottogruppo di G dato dai punti fissi di γ. Abbiamo ottenuto che H interseca ogni classe di coniugio di G, il che implica, per quanto visto nel punto (b), che $H = G$.

Questo è assurdo perché γ non è l'identità di $\mathrm{Aut}(G)$.

3. Sia $f(x) := x^3 + 9x^2 + 27x + 76$. Sia $\mathbb{K}$ il campo di spezzamento di $f(x)$ su $\mathbb{Q}$.

(a) Mostrare che $f(x)$ è un polinomio irriducibile su $\mathbb{Q}$ e calcolare il grado $[\mathbb{K} : \mathbb{Q}]$.

(b) Determinare il gruppo di Galois G di $\mathbb{K}$ su $\mathbb{Q}$. Dire se è un gruppo abeliano.

(c) Determinare le sottoestensioni di $\mathbb{K}$. Tra queste indicare quali sono di Galois.

Soluzione:

(a) Ponendo $y = x + 3$ otteniamo

$$f(x) = y^3 + 49 = g(y)$$

e quindi il campo di spezzamento di $f(x)$ è $\mathbb{K} = \mathbb{Q}(\zeta_3, \sqrt[3]{-49})$. Il campo $\mathbb{K}$ contiene un elemento di grado 2 (ζ_3, di grado $\phi(3) = 2$) ed un elemento di grado 3 ($\sqrt[3]{-49} = -\sqrt[3]{49}$ e $7/\sqrt[3]{49} = \sqrt[3]{7}$ radice del polinomio $x^3 - 7$, irriducibile per Eisenstein, quindi $\mathbb{Q}(\sqrt[3]{49}) = \mathbb{Q}(\sqrt[3]{7})$ ha grado 3), dunque il grado $[\mathbb{K} : \mathbb{Q}]$ deve essere multiplo di 6. D'altra parte $\mathbb{K}$ è campo di spezzamento di un polinomio di grado 3, dunque il suo grado su $\mathbb{Q}$ è al più $3!$. Quindi $[\mathbb{K} : \mathbb{Q}] = 6$. Ne segue anche che $g(y)$ deve essere irriducibile. Infatti in caso contrario l'estensione avrebbe grado al più 2.

(b) $\mathbb{K}$ è il campo di spezzamento di un polinomio di grado 3, quindi il suo gruppo di Galois G si immerge in S_3. Poiché il grado di $\mathbb{K}$ su $\mathbb{Q}$ è proprio 6, tale è anche la cardinalità del gruppo di Galois G, che quindi deve essere isomorfo a S_3.

Tale gruppo chiaramente non è abeliano (due 2-cicli distinti in S_3 non commutano). Si sarebbe potuto mostrare che il gruppo di Galois di $\mathbb{K}$ su $\mathbb{Q}$ non è abeliano anche osservando che $\mathbb{Q}(\sqrt[3]{7})$ è un'estensione di $\mathbb{Q}$ di grado 3 contenuta in $\mathbb{K}$, ma non è normale in quanto non contiene tutte le radici del polinomio minimo di $\sqrt[3]{7}$ perché è un'estensione reale, dunque il sottogruppo di G che la fissa non è normale e quindi G non è abeliano.

(c) Ovviamente $\mathbb{K}$ contiene $\mathbb{Q}$ e $\mathbb{K}$ come sottoestensioni banali. Il gruppo S_3 ha 4 sottogruppi propri. A ciascuno corrisponde una sottoestensione propria data dal corrispondente campo fisso.

Il sottogruppo $H_1 = A_3 = \langle(1, 2, 3)\rangle$ che è normale ed è l'unico che ha indice 2 e quindi fissa un campo di grado 2 su $\mathbb{Q}$. Poiché $\mathbb{Q}(\zeta_3) = \mathbb{Q}(i\sqrt{3})$ è un'estensione di grado 2 su $\mathbb{Q}$ contenuta in $\mathbb{K}$, deve essere il campo fisso di H_1.

I tre sottogruppi $H_2 = \langle(1, 2)\rangle$, $H_3 = \langle(1, 3)\rangle$ e $H_4 = \langle(2, 3)\rangle$ hanno indice 3 in G e dunque fissano ciascuna un sottocampo di grado 3 su $\mathbb{Q}$. Poichè gli elementi di S_3 agiscono su $\mathbb{K}$ permutanto le radici di $g(y)$, ovvero $-\sqrt[3]{49}$, $-\zeta_3\sqrt[3]{49}$, $-\zeta_3^2\sqrt[3]{49}$, i tre generatori dei tre sottogruppi H_2, H_3, H_4 fissano ciascuna una delle tre radici. Quindi i tre campi fissi di H_2, H_3, H_4 contengono rispettivamente una delle tre radici. Ciascuna di queste però ha grado esattamente 3 su $\mathbb{Q}$, in quanto ha polinomio minimo $g(y)$, che abbiamo notato essere irriducibile. Ne segue che i tre sottocampi fissi sono $\mathbb{Q}(\sqrt[3]{49}) = \mathbb{Q}(\sqrt[3]{7})$, $\mathbb{Q}(\zeta_3\sqrt[3]{49}) = \mathbb{Q}(\zeta_3^2\sqrt[3]{7})$, $\mathbb{Q}(\zeta_3^2\sqrt[3]{49}) = \mathbb{Q}(\zeta_3\sqrt[3]{49})$. Questi sono ovviamente distinti perché fissati da sottogruppi distinti.