Compitino di Algebra 1
18 gennaio 2022

Esercizio 1. Sia $\sigma = (1,2,4,6,7)$, $\tau = (2,6,7,4)$ and sia $G = (\sigma, \tau)$ il sottogruppo di S_7 generato da σ e τ.

1. Calcolare $|G|$.
2. Determinare il numero di 2-Sylow di G.
3. Quanti elementi di ordine 4 sono in G?
4. Quante classi di coniugio contiene G?

Soluzione:

1. Si verifica che vale la relazione

$$\tau\sigma\tau^{-1} = (2,6,7,4)(1,2,4,6,7)(2,4,7,6) = (1,6,2,7,4) = \sigma^3 \in \langle\sigma\rangle.$$

   Posto quindi $A = \langle\sigma\rangle$ e $B = \langle\tau\rangle$ hanno ordine coprimo (5 e 4 rispettivamente) quindi $A \cap B = \{1\}$. Siccome B normalizza A segue che AB è un sottogruppo di G quindi $AB = \langle\sigma,\tau\rangle = G$. Ne segue che $|G| = |AB| = |A| \cdot |B|/|A \cap B| = |A| \cdot |B| = 5 \cdot 4 = 20$.

2. Siccome $\tau\sigma\tau^{-1} = (2,6,7,4)(1,2,4,6,7)(2,4,7,6) = (1,6,2,7,4) = \sigma^3$ non è una potenza di τ (muove 1), segue $\tau\sigma\tau^{-1} \notin B$ per cui B non è normale in G. D'altra parte è un 2-sottogruppo di Sylow di G e per il teorema di Sylow il numero di 2-sottogruppi di Sylow di G, che chiamiamo n_2, divide $|G : B| = 5$ quindi è 1 oppure 5. Di nuovo per il teorema di Sylow siccome B non è normale in G, $n_2 \neq 1$ quindi $n_2 = 5$. Quindi G ha cinque 2-sottogruppi di Sylow.

3. Siccome B è un 2-sottogruppo di Sylow ciclico di ordine 4, tutti i 2-sottogruppi di Sylow di G sono ciclici di ordine 4 (sono coniugati a B, in particolare sono isomorfi a B). Ogni 2-sottogruppo di Sylow contiene $\phi(4) = 2$ elementi di ordine 4, e ogni elemento di ordine 4 è contenuto in un unico 2-sottogruppo di Sylow (quello che genera). Siccome $n_2 = 5$ segue che G ha $5 \cdot 2 = 10$ elementi di ordine 4.

4. Contiamo intanto i coniugati di τ. Come sappiamo τ ha esattamente $|G : C_G(\tau)|$ coniugati, dove $C_G(\tau) = \{g \in G : \tau g = g\tau\}$ è il centralizzante di τ in G. Siamo ridotti a trovare tale centralizzante. Certamente $\tau \in C_G(\tau)$ (τ commuta con se stesso) quindi $B \subseteq C_G(\tau)$. Siccome B ha ordine 4 e indice 5, se $C_G(\tau) \neq B$ allora $C_G(\tau) = G$, ma quest'ultima uguaglianza non è vera perché come visto nel punto (1), σ e τ non commutano e quindi certamente $\sigma \notin C_G(\tau)$. Ne segue che $C_G(\tau) = B$ ha ordine 4, quindi τ ha $|G : C_G(\tau)| = |G|/|C_G(\tau)| = 20/4 = 5$ coniugati. Siccome G ha dieci elementi di ordine 4 (per il punto (3)), gli elementi di ordine 4 di G non sono tutti coniugati (altrimenti sarebbero tutti coniugati a τ, assurdo dato che τ ha solo cinque coniugati). Quindi G ha due classi di elementi di ordine 4, ognuna di cardinalità 5. Siccome $\tau\sigma\tau^{-1} = \sigma^3$, $\tau^k\sigma\tau^{-k} = \sigma^{3^k}$ tutti gli elementi non identici di A sono coniugati ad σ (le classi di $3^k \mod 5$ sono $1, 2, 3, 4$) quindi G ha una classe di elementi di ordine 5 che consiste dei 4 elementi $\sigma, \sigma^2, \sigma^3, \sigma^4$. C'è un unico elemento di ordine 2 in ogni 2-sottogruppo di Sylow (infatti un gruppo ciclico di ordine 4 ha un unico elemento di ordine 2) e siccome i 2-sottogruppi di Sylow sono coniugati anche gli elementi di ordine 2 risultano tutti coniugati. Riassumendo, G ha una classe di un elemento di ordine 1 (l'identità), 2 classi di 5 elementi ordine 4, una classe di quattro elementi di ordine 5 e una classe di cinque elementi di ordine 2.

Esercizio 2. Si consideri il sottogruppo A di $\mathbb{Z}^4$ generato da

$$(1,0,1,0),(3,2,3,0),(-1,2,1,2),(1,0,1,2).$$

1. Scrivere in una forma canonica il gruppo $\mathbb{Z}^4/A$.
2. Dire se esiste una successione esatta corta
$$0 \to A \to \mathbb{Z}^5 \to B \to 0$$
dove B è un gruppo abeliano di cardinalità 10.
3. Dire se esiste una successione esatta corta
$$0 \to A \to \mathbb{Z}^3 \to C \to 0$$
dove C è un gruppo abeliano di cardinalità 10.

NON PRESENTE NEL COMPITO: PROVATE A RISOLVERLO!

4. Costruire una estensione di Galois $\mathbb{Q} \subset E$ tale che $Aut(E/\mathbb{Q})$ sia isomorfo a $\mathbb{Z}^4/A$.

SINTESI DELLA SOLUZIONE

1) In molti hanno risolto bene questo punto:

A è lo span su $\mathbb{Z}$ delle colonne di $\begin{pmatrix} 1 & 3 & -1 & 1 \\ 0 & 2 & 2 & 0 \\ 1 & 3 & 1 & 1 \\ 0 & 0 & 2 & 2 \end{pmatrix}$

Con mosse intere di riga e di colonna si trova la forma di Smith $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$

Dunque a meno di cambiamento di base.

$$A = \mathrm{Span}\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\2\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\2\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\2\end{pmatrix}\right)$$

e $\mathbb{Z}^4/A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}_2)^3$

2) Supponiamo che esista

$$0 \to A \xrightarrow{\varphi} \mathbb{Z}^5 \xrightarrow{\psi} B \to 0$$

con $|B| = 10$.

Notiamo che A, come abbiamo visto al punto precedente, è un gruppo abeliano libero di rango 4.

Dunque φ può essere rappresentato da una matrice 5×4 (5 righe, 4 colonne). La forma di Smith di tale matrice sarà $\begin{pmatrix} d_1 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 \\ 0 & 0 & d_3 & 0 \\ 0 & 0 & 0 & d_4 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ e avrà dunque almeno una riga di zeri.

NOTA: potrebbe accadere che alcuni dei d_i siano $= 0$.

Dunque $B \cong \mathbb{Z}^5/\ker\psi \cong \mathbb{Z}^5/\operatorname{Im}\varphi \cong$

$\cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \mathbb{Z}/d_3\mathbb{Z} \times \mathbb{Z}/d_4\mathbb{Z} \times \mathbb{Z}$

che, qualunque siano i valori d_1, d_2, d_3, d_4,
è un gruppo di cardinalità infinita, in contraddizione con $|B| = 10$. Dunque NON esiste una tale successione esatta corta

3) Questo è stato risolto da molti.

Per esempio con $E = \mathbb{Q}(\zeta_{24})$ oppure $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$

per esempio

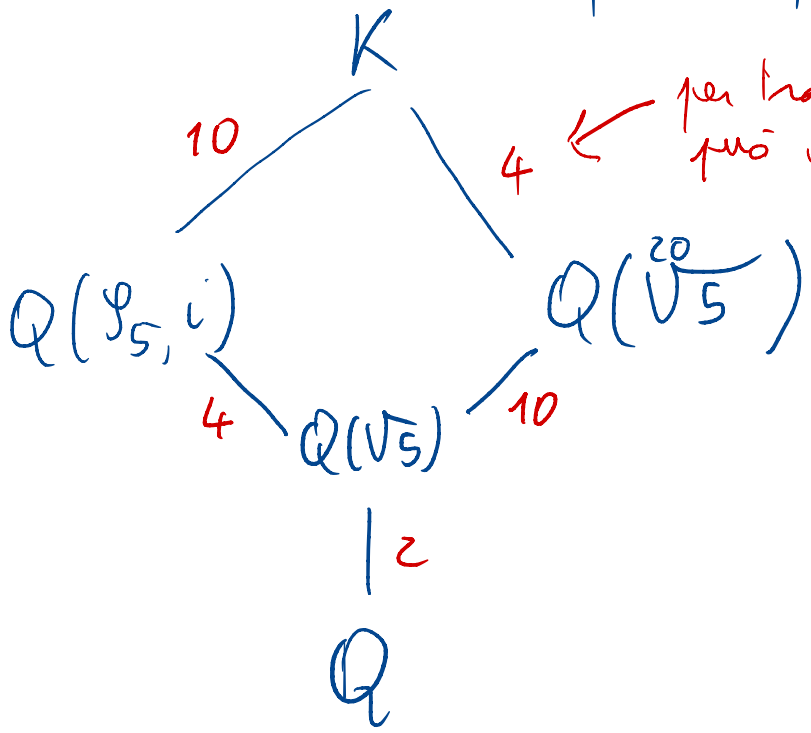
$$\mathrm{Aut}\left(\mathbb{Q}(\zeta_{24})/\mathbb{Q}\right) \cong \mathrm{Aut}\left(\mathbb{Q}(\zeta_8)/\mathbb{Q}\right) \times \mathrm{Aut}\left(\mathbb{Q}(\zeta_3)/\mathbb{Q}\right)$$

$$\cong \mathbb{Z}_8^* \times \mathbb{Z}_3^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Esercizio 3. Si consideri il campo $K = \mathbb{Q}(\sqrt[20]{5}, \zeta_5, i)$.

1. Calcolare $[K : \mathbb{Q}]$ e dimostrare che l'estensione $\mathbb{Q} \subset K$ è di Galois.
2. Descrivere il gruppo di Galois $Aut(K/Q)$ ed esibire dei generatori.

1) Questa prima parte è stata risolta da un buon numero di studenti, usando per esempio il diagramma



per trovare questo 4 si può usare per esempio il primo "lemma del diamante"

e ricavando che $[K : Q] = 80$.

L'estensione è di Galois perché campo di spezzamento di $x^{20} - 5$.

2) Presentiamo il gruppo di Galois $G = Aut(K/Q)$.

Chiamiamo intanto $G' = \mathrm{Aut}\left(K/\mathbb{Q}(\sqrt{5})\right)$

e dimostriamo per prima cosa G' che è s. gruppo di G di indice 2.

Il polinomio $x^{20}-5$ si fattorizza su $\mathbb{Q}(\zeta_5, i)$ come $(x^{10}-\sqrt{5})(x^{10}+\sqrt{5})$.

Notiamo che $\sqrt[20]{5}$ è radice di $x^{10}-\sqrt{5}$ e che $x^{10}-\sqrt{5}$ è IRRID in $\mathbb{Q}(\zeta_5, i)[x]$, visto che l'estensione $\mathbb{Q}(\zeta_5, i) \subseteq K$ ha grado 10.

Allora $\exists\ \rho \in \mathrm{Aut}\left(K/\mathbb{Q}(\zeta_5, i)\right)$ tale che

$$\rho\left(\sqrt[20]{5}\right) = \sqrt[20]{5}\ \zeta_{10}$$

perché manda $\sqrt[20]{5}$ in un'altra radice del suo polinomio minimo su $\mathbb{Q}(\zeta_5, i)$.

Si osserva che $\rho^2\left(\sqrt[20]{5}\right) = \sqrt[20]{5}\ \zeta_{10}^2$ e così via si osserva che $o(\rho) = 10$.

Ora studiamo $\mathrm{Aut}\left(\frac{\mathbb{Q}(\zeta_5, i)}{\mathbb{Q}}\right)$.

Sappiamo che ha cardinalità 8 e che è generato da σ tale che $\sigma(\zeta_5) = \zeta_5^2$ e $\sigma(i) = i$

e τ tale che $\tau(\zeta_5) = \zeta_5$ e $\tau(i) = -i$

con $o(\sigma) = 4$, $o(\tau) = 2$ e $\tau\sigma = \sigma\tau$.

(è isomorfo a $\mathbb{Z}_4 \times \mathbb{Z}_2$, come sappiamo dalla teoria).

Il s. gruppo che fissa $\mathbb{Q}(\sqrt{5})$ è (σ^2, τ)

che è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Per il primo "lemma del diamante", i gruppi

$\mathrm{Aut}\left(\frac{\mathbb{Q}(\zeta_5, i)}{\mathbb{Q}(\sqrt{5})}\right)$ e $\mathrm{Aut}\left(\frac{K}{\mathbb{Q}(\sqrt{2\rho_5})}\right)$

sono isomorfi, con isomorfismo dato dalla restrizione.

Esistono dunque Σ e $\tilde{\tau}$ $\in \mathrm{Aut}\left(\frac{K}{\mathbb{Q}(\sqrt{2\rho_5})}\right)$

tali che $\Sigma|_{\mathbb{Q}(\zeta_5, i)} = \sigma^2$ e $\tilde{\tau}|_{\mathbb{Q}(\zeta_5, i)} = \tau$.

Dall'osservazione fatta sopra sappiamo che

$o(\Sigma) = o(\check{\tau}) = 2$ e $\Sigma \check{\tau} = \check{\tau} \Sigma$.

Allora ρ, Σ e $\check{\tau}$ generano $Aut\left(K/_{Q(\sqrt{5})}\right)$

con le seguenti relazioni

1) $\Sigma \rho \Sigma = \rho^{-1}$. INFATTI:

$\Sigma \rho \Sigma(\varphi_5) = \Sigma \rho(\varphi_5^{-1}) = \Sigma(\varphi_5^{-1}) = \varphi_5 = \rho^{-1}(\varphi_5)$

$\Sigma \rho \Sigma(\iota) = \Sigma \rho(\iota) = \Sigma(\iota) = \iota = \rho^{-1}(\iota)$

$\Sigma \rho \Sigma(\sqrt[20]{5}) = \Sigma \rho(\sqrt[20]{5}) = \Sigma(\sqrt[20]{5}\ \varphi_{10}) =$

NOTIAMO ADESSO che $\varphi_{10} = (-\varphi_5)^3$, allora

$= \Sigma\left(-\sqrt[20]{5}\ \varphi_5^3\right) = -\sqrt[20]{5}\ \varphi_5^2 = \sqrt[20]{5}\ \varphi_{10}^9$

ma $\rho^{-1}(\sqrt[20]{5}) = \rho^9(\sqrt[20]{5}) = \sqrt[20]{5}\ \varphi_{10}^9$.

2) $\check{\tau} \rho \check{\tau} = \rho$

INFATTI

$$\check{\tau}\,\rho\,\check{\tau}\,(\varphi_5) = \varphi_5 = \rho(\varphi_5)$$

$$\check{\tau}\,\rho\,\check{\tau}\,(\iota) = \iota = \rho(\iota)$$

$$\check{\tau}\,\rho\,\check{\tau}\,(\sqrt[20]{5}) = \check{\tau}\,(\sqrt[20]{5}\,\varphi_{10}) = \sqrt[20]{5}\,\check{\tau}\,(-\varphi_5^3) =$$

$$= \sqrt[20]{5}\,(-\varphi_5^3) = \sqrt[20]{5}\,\varphi_{10} = \rho(\sqrt[20]{5})$$

Dunque, visto che $\check{\tau}$ commuta con ρ e con Σ,

$$G' \cong (\rho, \Sigma) \times (\check{\tau}) \cong D_{10} \times \mathbb{Z}_2.$$

Infine, che relazione c'è fra G' e G?

Sappiamo che $G' < G$ e ha indice 2.

Dunque $G = G' \cup g\,G'$ unione di 2 classi laterali.

Per completare un insieme di generatori basta descrivere un $g \in G \setminus G'$

Si tratta di trovare un automorfismo in G tale che $g(\sqrt{5}) = -\sqrt{5}$.

Consideriamo l'estensione $\mathbb{Q}(\zeta_{5,i}) \subseteq K$

Come sappiamo ha grado 10.

I polinomi $x^{10} - \sqrt{5}$ e $x^{10} + \sqrt{5}$ sono irriducibili in $\mathbb{Q}(\zeta_{5,i})[x]$ dato che K si può ottenere da $\mathbb{Q}(\zeta_{5,i})$ aggiungendo o $\sqrt[20]{5}$ che è radice di $x^{10} - \sqrt{5}$ o $\sqrt[20]{5}\, i$ che è radice di $x^{10} + \sqrt{5}$.

Sia $\sigma \in \mathrm{Aut}\left(\mathbb{Q}(\zeta_{5,i})/\mathbb{Q}\right)$ come sopra, ossia $\sigma(\zeta_5) = \zeta_5^2$ $\sigma(i) = i$.

Notiamo che σ non fissa $\sqrt{5}$ (che è invece fissato da σ^2).

Per il Teorema 14.8 delle dispense di Aritmetica esiste un sollevamento $g : K \to K$ di σ tale che $g(\sqrt[20]{5}) = \sqrt[20]{5}\, i$ (e $g_{|\mathbb{Q}(\zeta_{5,i})} = \sigma$).

Questo $g \in G \setminus G'$, come volevamo. ACCIUNTIVO: NON RICHIESTO DAL TESTO ✓

Calcoliamo le relazioni che legano g a ρ, Σ e τ.

$$g \rho g^{-1}\left(\sqrt[20]{5}\right) = g \rho\left(-\sqrt[20]{5}\, i\right) =$$

$$= g\left(-i \sqrt[20]{5}\, \zeta_{10}\right) = -i \sqrt[20]{5}\, i\, g(\zeta_{10})$$

(ora $\varphi_{10} = -\varphi_5^3$ per cui $g(\varphi_{10}) = -g(\varphi_5^3) = -\varphi_5$)

$= \sqrt[20]{5}\ \varphi_{10}^7$

$g \rho g^{-1}(i) = i$

$g \rho g^{-1}(\varphi_5) = g\ \rho(\varphi_5^3) = g(\varphi_5^3) = \varphi_5$

da cui si ricava che $g \rho g^{-1} = \rho^7$

Inoltre

$g \Sigma g^{-1}(\sqrt[20]{5}) = g \Sigma(-\sqrt[20]{5}\, i) =$

$= g(-\sqrt[20]{5}\, i) = -i \sqrt[20]{5}\, i = \sqrt[20]{5}$

$g \Sigma g^{-1}(i) = i$

$g \Sigma g^{-1}(\varphi_5) = g \Sigma(\varphi_5^3) = g(\varphi_5^{-3}) = \varphi_5^{-1}$

cioè $g \Sigma g^{-1} = \Sigma$

Infine.

$$g\,\overset{\vee}{\tau}\,g^{-1}\left(\sqrt[20]{5}\right) = g\,\overset{\vee}{\tau}\left(-\sqrt[20]{5}\,i\right) = g\left(\sqrt[20]{5}\,i\right)$$

$$= -\sqrt[20]{5} = g^2\,\overset{\vee}{\tau}\left(\sqrt[20]{5}\right)$$

$$g\,\overset{\vee}{\tau}\,g^{-1}(i) = g\,\overset{\vee}{\tau}(i) = g(-i) = -i = g^2\,\overset{\vee}{\tau}(i)$$

$$g\,\overset{\vee}{\tau}\,g^{-1}(\vartheta_5) = g\,\overset{\vee}{\tau}(\vartheta_5^3) = g(\vartheta_5^3) = \vartheta_5 = g^2\,\overset{\vee}{\tau}(\vartheta_5)$$

Da cui

$$g\,\overset{\vee}{\tau}\,g^{-1} = g^2\,\overset{\vee}{\tau} \quad \text{ossia}$$

$$\overset{\vee}{\tau}\,g^{-1} = g\,\overset{\vee}{\tau}$$