Corso di Laurea in Matematica
Algebra 1 - Soluzioni del compito del 7/2/2020

Esercizio 1.

a) Per un gruppo G fissato indichiamo con $n_k(G)$ il numero di sottogruppi di G di cardinalità k. Descrivere l'insieme dei valori che può assumere $n_{77}(G)$ al variare di G tra tutti i gruppi di ordine 154.

Soluzione: L'INSIEME È $\{1\}$.

Notiamo che $154 = 2 \cdot 7 \cdot 11$. Per i teoremi di Sylow, $n_{11} = 1$, dunque l'11-Sylow N_{11} è normale. Sia N_7 un 7-Sylow. Allora $H = N_{11}N_7$ è un s. gruppo di ordine 77, ed è normale perché ha indice 2. Poiché $7 \nmid 11-1$, H è isomorfo a $\mathbb{Z}/_{77}$. Dunque N_7 è s. gruppo caratteristico di H, che a sua volta è normale in G. Dunque N_7 è normale in G, e allora $n_7 = 1$.

Poiché un s. gruppo di G di ordine 77 deve contenere un 7-Sylow e un 11-Sylow, l'unico s. gruppo di ordine 77 di G è proprio $H = N_{11}N_7$. [ci si poteva anche più direttamente riferire a quanto abbiamo visto sui gruppi di ordine pqr]

b) Sia L un campo di spezzamento su $\mathbb{F}_5$ di $x^4 - 2x - 1$. Sia $\alpha \in L$ una radice di $x^4 - 2x - 1$. Dire quanti sono i campi K tali che

$$\mathbb{F}_5 \subsetneq K \subsetneq \mathbb{F}_5(\alpha)$$

Soluzione: 1 campo

Si verifica che $x^4 - 2x - 1$ è IRRIDUCIBILE in $\mathbb{F}_5[x]$ (non ha radici e non si fattorizza come prodotto di polinomi di grado 2).

Allora $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = 4$. Come sappiamo l'estensione $\mathbb{F}_5 \subset \mathbb{F}_5(\alpha)$ è di Galois con gruppo di Galois $\cong \mathbb{Z}/_4$.

Tale gruppo ha un unico s. gruppo proprio, che ha indice 2. Per la corrispondenza di Galois esiste dunque un unico campo K con $\mathbb{F}_5 \subsetneq K \subsetneq \mathbb{F}_5(\alpha)$ (e vale $[K : \mathbb{F}_5] = 2$). [si poteva anche concludere dicendo che $\mathbb{F}_5(\alpha) \cong \mathbb{F}_{5^4}$ e dal corso di Aritmetica sappiamo che l'unico s. campo K t.c. $\mathbb{F}_5 \subsetneq K \subsetneq \mathbb{F}_{5^4}$ è $\mathbb{F}_{5^2}$]

c) Dimostrare che A_5 è semplice.

Soluzione:

Si può ripetere la dimostrazione fatta nel Paragrafo 3,2 delle Dispense per $G(P_{20})$.

In particolare si osserva che le classi di coniugio di A_5 sono

- $\{e\}$
- la classe di $(1,2)(3,4)$, che ha cardinalità 15
- " " " $(1,2,3)$, che " " 20
- due classi costituite ciascuna da 12 5-cicli.

Poiché un s. gruppo normale se contiene un elemento contiene anche tutti i suoi coniugati, se $N \triangleleft A_5$ deve valere che $|N| = 1 + a\,15 + b\,20 + c\,12 + d\,12$ con $a, b, c, d \in \{0, 1\}$.

Le uniche scelte di a, b, c, d tali che $|N|$ divida 60 sono $a = b = c = d = 0$ $(N = \{e\})$ e $a = b = c = d = 1$ $(N = A_5)$. Dunque A_5 è semplice.

Esercizio 2. Sia G un gruppo di ordine 315 in cui il 3-Sylow non è normale.

a) Mostrare che il normalizzatore del 3-Sylow in G è sempre un sottogruppo abeliano di G.

b) Descrivere a meno di isomorfismo i possibili gruppi G siffatti.

Soluzione:

a) Sia R un 3-Sylow di G. Mostriamo intanto che il normalizzatore $N(R)$ contiene 45 elementi. Il numero dei 3-Sylow di G divide 35 ed è $\equiv 1 \bmod 3$. Le uniche possibilità sono 1 e 7, ma R non è normale. Pertanto G possiede esattamente 7 3-Sylow, e il normalizzatore di ciascuno di essi ha indice 7, e quindi ordine 45.

Mostriamo dunque che N (R) è abeliano. Infatti $N(R)$ è un gruppo di ordine 45, nel quale R è normale. Inoltre il numero dei 5-Sylow di $N(R)$ divide 9 ed è $\equiv 1 \bmod 5$. Il 5-Sylow è quindi unico, e necessariamente normale. Allora $N(R)$ è prodotto diretto di R con il suo unico 5-Sylow. Questi sottogruppi hanno ordine 9 e 5, e sono entrambi abeliani. Allora anche il loro prodotto diretto è quindi abeliano.

b) Mostriamo intanto che il 5-Sylow di G è normale. Soluzione: Consideriamo un sottogruppo H di ordine 5 contenuto in $N(R)$. A causa dell'abelianità di $N(R)$, H è normale in $N(R)$, e quindi il suo normalizzatore contiene almeno i 45 elementi in $N(R)$. Ad ogni modo, H è un 5-Sylow di G, e il numero dei 5-Sylow di G divide 63 ed è $\equiv 1 \bmod 5$. Le uniche possibilità sono 1 e 21. Tuttavia, se un 5-Sylow possiede 21 coniugati, è normalizzato da un sottogruppo di indice 21, e quindi di ordine 15, che è troppo piccolo per contenere i 45 elementi mostrati prima. L'unica altra possibilità è che H sia normale in G.

Possiamo ora vedere che G contiene un sottogruppo ciclico di ordine 35. Infatti basta moltiplicare H per un sottogruppo $K < G$ di ordine 7. La normalità di H costringe HK, che contiene 35 elementi, ad essere un sottogruppo di G. Un gruppo di ordine $35 = 5 \cdot 7$ è ciclico poiché 5 non divide $7 - 1$.

Possiamo vedere inoltre che anche il 7-Sylow di G è normale. Per farlo ripetiamo il ragionamento precedente. K è un 7-Sylow di G, ed è contenuto nel sottogruppo HK di ordine 35, che lo normalizza per abelianità. Il normalizzatore di K ha allora indice $\leq 315/35 = 9$. Tuttavia il numero dei 7-Sylow in G divide 45, è $\equiv 1 \bmod 7$ ed è ≤ 9. L'unica possibilità è 1, e l'unicità del 7-Sylow impone la sua normalità.

A quali gruppi può essere isomorfo G? Abbiamo visto che G è prodotto semidiretto del sottogruppo normale di ordine 35 con il sottogruppo R, che sappiamo essere non normale e di ordine 9; si tratta pertanto di un prodotto semidiretto non banale. R è isomorfo a $\mathbb{Z}_9$ oppure a $\mathbb{Z}_3 \times \mathbb{Z}_3$, mentre il gruppo di ordine 35 è necessariamente ciclico. Nei due casi, dobbiamo costruire omomorfismi $\varphi : \mathbb{Z}_9 \to \mathrm{Aut}(\mathbb{Z}_{35}) \simeq \mathbb{Z}_6 \times \mathbb{Z}_4$, oppure $\varphi : \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_{35})$, rispettivamente. Se φ è non banale, la sua immagine, che ha ordine un divisore di 9, deve essere contenuta nel primo fattore diretto in entrambi i casi, ed è univocamente determinata ($\mathbb{Z}_6$ possiede un solo sottogruppo di ordine 3). Possiamo allora scegliere il generatore di $\mathbb{Z}_9$ in modo che venga mandato da φ nel generatore fissato del sottogruppo di ordine 3 in $\mathbb{Z}_6$; nell'altro caso, possiamo scegliere due generatori di $\mathbb{Z}_3 \times \mathbb{Z}_3$ in modo che il primo venga mandato da φ nel generatore fissato del sottogruppo di ordine 3 in $\mathbb{Z}_6$, e il secondo appartenga al nucleo. G è pertanto isomorfo ad uno dei seguenti due gruppi: $(\mathbb{Z}_7 \rtimes \mathbb{Z}_9) \times \mathbb{Z}_5$ nel primo caso, e $(\mathbb{Z}_7 \rtimes \mathbb{Z}_3) \times (\mathbb{Z}_3 \times \mathbb{Z}_5)$ nel secondo. I due gruppi sono non isomorfi perché sono tra loro non isomorfi i loro 3-Sylow.

Esercizio 3. Sia $\alpha = \zeta_5 + i\sqrt[4]{5}$.

a) Determinare il grado di α su $\mathbb{Q}$ e su $\mathbb{Q}[i]$.
b) Descrivere il campo di spezzamento $\mathbb{K}$ del polinomio minimo di α su $\mathbb{Q}$ esibendo dei generatori e calcolare il grado di $\mathbb{K}$ su $\mathbb{Q}$.
c) Descrivere il gruppo di Galois di $\mathbb{K}$ su $\mathbb{Q}$.

Soluzione:

a) Consideriamo le seguenti estensioni di Galois di $\mathbb{Q}$: $\mathbb{F}_1 := \mathbb{Q}[\zeta_5]$ e $\mathbb{F}_2 := \mathbb{Q}[i, \sqrt[4]{5}]$. Notiamo che $\mathbb{F}_1$ ha grado 4 su $\mathbb{Q}$ e gruppo di Galois $\mathbb{Z}_4$ perché è un'estensione ciclotomica fatta con la radice quinta dell'unità e $\mathbb{Z}_5^* \simeq \mathbb{Z}_4$. Inoltre $\mathbb{F}_2$ ha grado 8 su $\mathbb{Q}$. Infatti $\mathbb{Q}[\sqrt[4]{5}]$ è reale ha grado 4 su $\mathbb{Q}$ perché $\sqrt[4]{5}$ è radice di $x^4 - 5$, irriducibile per Eisenstein; inoltre i è annullato da $x^2 + 1$, quindi ha polinomio minimo di grado minore o uguale a 2, ma $i \notin \mathbb{Q}[\sqrt[4]{5}]$ e dunque i ha grado 2 su $\mathbb{Q}[\sqrt[4]{5}]$. Il gruppo di Galois di $\mathbb{F}_2$ su $\mathbb{Q}$ è D_4: infatti gli 8 automorfismi sono determinati dall'immagine (tra le 4 possibili) di $\sqrt[4]{5}$ e da quella (tra le 2 possibili) di i. Dunque per ogni $a = 0, 1, 2, 3$ e $b = 0, 1$ abbiamo un automorfismo definito da $\varphi_{a,b} : \begin{cases} \sqrt[4]{5} & \mapsto & i^a\sqrt[4]{5} \\ i & \mapsto & (-1)^b i. \end{cases}$ Possiamo notare che $\psi = \varphi_{1,0}$ ha ordine 4 e $\tau = \varphi_{0,1}$ e $\tau\psi\tau = \psi^{-1}$, dunque il gruppo generato è D_4.
Notiamo ora che $\mathbb{F}_1 \cap \mathbb{F}_2 = \mathbb{Q}[\sqrt{5}]$ infatti $\gamma = \zeta_5 + \zeta_5^{-1}$ è radice di $x^2 + x - 1$ e dunque $\gamma = -\frac{1 \pm \sqrt{5}}{2}$ e quindi $\mathbb{Q}[\gamma] = \mathbb{Q}[\sqrt{5}]$. Inoltre non è possibile che $\mathbb{F}_1 = \mathbb{Q}[\zeta_5] \subset \mathbb{F}_2 = \mathbb{Q}[i, \sqrt[4]{5}]$ in quanto D_4 non ha un sottogruppo normale di indice 4 che dia un quoziente isomorfo a $\mathbb{Z}_4$
Concludiamo che l'estensione $\mathbb{L} := \mathbb{Q}[\zeta_5, i, \sqrt[4]{5}]$ ha grado 16 su $\mathbb{Q}$ ed è di Galois perché composizione di estensioni di Galois.
Affermiamo che l'orbita di $\alpha = \zeta_5 + i\sqrt[4]{5}$ rispetto all'azione del gruppo di Galois di $\mathbb{L}$ su $\mathbb{Q}$ è fatta di 8 elementi. Infatti un automorfismo di $\mathbb{L}$ è determinato dall'immagine di ζ_5 (al più 4 possibili scelte), di i (al più 2 possibili scelte), e di $\sqrt[4]{5}$ (al più 4 possibili scelte), ma non tutte queste 32 scelte complessive sono realizzabili come automorfismi. Tuttavia se scegliamo prima l'immagine di $\sqrt{5} = 2\zeta_5 + 2\zeta_5^{-1} + 1$ (tra le 2 possibili scelte) allora abbiamo solo 2 scelte per l'immagine di ζ_5, 2 scelte per l'immagine di $\sqrt[4]{5}$ e 2 scelte per l'immagine di i, dunque in tutto al più 16 scelte distinte, che sono esattamente il numero di elementi del gruppo. Pertanto tali scelte sono tutte realizzate da un automorfismo di $\mathbb{L}$. Dunque se consideriamo gli automorfismi che fissano $\sqrt{5}$ vediamo che l'orbita di α contiene i quattro elementi $\zeta_5^{\pm 1} \pm i\sqrt[4]{5}$, mentre se consideriamo gli automorfismi che mandano $\sqrt{5}$ nel suo opposto vediamo che l'orbita di α contiene $\zeta_5^{\pm 2} \pm \sqrt[4]{5}$. Ne segue che α ha grado 8 su $\mathbb{Q}$.
Per quanto riguarda il grado di α su $\mathbb{Q}[i]$ notiamo intanto che per la torre di estensioni $[\mathbb{L} : \mathbb{Q}[i]] = 8$. Analogamente a prima, se consideriamo gli automorfismi di $\mathbb{L}$ che fissano i abbiamo che se fissiamo prima l'immagine di $\sqrt{5} = 2\zeta_5 + 2\zeta_5^{-1} + 1$ (tra le 2 possibili scelte) allora abbiamo solo 2 scelte che possiamo fare per l'immagine di ζ_5, 2 scelte che possiamo fare per l'immagine di $\sqrt[4]{5}$, dunque in tutto al più 8 scelte distinte, che sono esattamente il numero di elementi del gruppo. Pertanto tali scelte sono tutte realizzabili tramite un automorfismo di $\mathbb{L}$ che fissa $\mathbb{Q}[i]$ e abbiamo che l'orbita di α rispetto al gruppo degli automorfismi di $\mathbb{L}$ su $\mathbb{Q}[i]$ è costituita di nuovo da 8 elementi e quindi il grado è sempre 8.

b) Il campo di spezzamento $\mathbb{K}$ è generato dagli 8 elementi dell'orbita di α elencati al punto precedente. In particolare, visto che il campo contiene $\zeta_5 + i\sqrt[4]{5}$, $\zeta_5 - i\sqrt[4]{5}$, $\zeta_5 + \sqrt[4]{5}$, segue immediatamente che $\mathbb{K}$ contiene $\sqrt[4]{5}, i, \zeta_5$ e dunque $\mathbb{K} = \mathbb{L}$. Per quanto visto nel punto precedente dunque $\mathbb{K}$ ha grado 16 su $\mathbb{Q}$.

c) Notiamo che il sottogruppo $H = \mathrm{Gal}(\mathbb{K}/\mathbb{Q}[i]) \subset \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = G$ è un gruppo di ordine 8 che contiene 4 elementi di ordine 4 dati da

$$\begin{cases} \zeta_5 & \mapsto & \zeta_5^{\pm 2} \\ \sqrt[4]{5} & \mapsto & \pm i\sqrt[4]{5} \\ i & \mapsto & i \end{cases}$$

e 4 elementi di ordine ≤ 2 dati da

$$\begin{cases} \zeta_5 & \mapsto & \zeta_5^{\pm 1} \\ \sqrt[4]{5} & \mapsto & \pm\sqrt[4]{5} \\ i & \mapsto & i \end{cases}$$

ed è dunque isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_4$. Esso è generato da

$$\rho_1 : \begin{cases} \zeta_5 & \mapsto & \zeta_5^{-1} \\ \sqrt[4]{5} & \mapsto & \sqrt[4]{5} \\ i & \mapsto & i \end{cases}$$

e

$$\rho_2 : \begin{cases} \zeta_5 & \mapsto & \zeta_5^{2} \\ \sqrt[4]{5} & \mapsto & i\sqrt[4]{5} \\ i & \mapsto & i \end{cases}$$

di ordine rispettivamente 2 e 4 che commutano tra loro. Inoltre l'automorfismo indotto dal coniugio

$$\sigma : \begin{cases} \zeta_5 & \mapsto & \zeta_5^{-1}; \\ \sqrt[4]{5} & \mapsto & \sqrt[4]{5} \\ i & \mapsto & -i. \end{cases}$$

ha ordine 2, non è contenuto in H e valgono le relazioni $\sigma\rho_1\sigma = \rho_1$ e $\sigma\rho_2\sigma = \rho_1\rho_2^3$. Possiamo quindi descrivere il gruppo di Galois G di $\mathbb{K}$ su $\mathbb{Q}$ come $G = (\mathbb{Z}_2 \times \mathbb{Z}_4) \rtimes \mathbb{Z}_2$ dove l'azione del generatore del fattore di destra su $\mathbb{Z}_2 \times \mathbb{Z}_4$, in notazione additiva, è $(a, b) \mapsto (a + b, -b)$.