SOLUZIONI DEL COMPITO DI ALGEBRA 1

20 gennaio 2017

1. (a) Sia p un primo e sia H il gruppo delle matrici 3×3 a coefficienti in $\mathbb{F}_p$ della seguente forma: $A = (a_{ij})$ tali che $\forall i$ vale $a_{ii} = 1$ e $\forall i < j$ vale $a_{ij} = 0$. Calcolare l'ordine di H e dire se è abeliano.

(b) Sia $n \in \mathbb{N}$, $n \geq 2$ tale che ogni gruppo di ordine n è abeliano. Sia $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ la fattorizzazione in primi, con $p_1, \ldots, p_m$ primi distinti. Dire per ciascuna delle seguenti affermazioni se è vera o falsa:

i. $\forall i = 1, \ldots, m$ vale $\alpha_i \in \{1, 2\}$;

ii. $\forall i, j = 1, \ldots, m$ vale $p_i \nmid (p_j - 1)$;

iii. $\forall i, j = 1, \ldots, m$ vale che se $\alpha_i = 2$ allora $p_j \nmid (p_i + 1)$.

Traccia della soluzione: → VEDI DOPO

2. Sia $n \geq 3$ un intero. Si consideri il gruppo A_n. Al variare di n trovare il più grande m intero tale che A_n contiene un sottogruppo isomorfo a S_m.

Traccia della soluzione: → VEDI DOPO

3. Sia dato il polinomio $p(x) = x^4 - 3x^2 + 4$.

(a) Calcolare il campo di spezzamento $\mathbb{K}$ di $p(x)$ su $\mathbb{Q}$;

(b) calcolare il gruppo di Galois $\mathrm{Aut}(\mathbb{K}/\mathbb{Q})$;

(c) calcolare il campo di spezzamento e il gruppo di Galois di $p(x)$ su $\mathbb{F}_7$.

Soluzione:

(a) Il campo di spezzamento deve contenere la radice quadrata del discriminante del polinomio di secondo grado $y^2 - 3y + 4$, quindi, posto $\Delta = 9 - 16 = -7$, $\sqrt{-7} \in \mathbb{K}$. Inoltre osserviamo che $[\mathbb{Q}(\sqrt{-7}) : \mathbb{Q}] = 2$ in quanto $\sqrt{-7}$ è radice di $x^2 + 7$ che essendo somma di un quadrato e un numero positivo non ha radici reali e dunque è irriducibile su $\mathbb{Q}$.

In $\mathbb{K}$ possiamo quindi scrivere

$$p(x) = \left(x^2 - \frac{3 + \sqrt{-7}}{2}\right)\left(x^2 - \frac{3 - \sqrt{-7}}{2}\right)$$

Poniamo $q_1(x) = \left(x^2 - \frac{3+\sqrt{-7}}{2}\right)$, $q_2(x) = \left(x^2 - \frac{3-\sqrt{-7}}{2}\right)$.

Affermiamo che il polinomio $q_1(x) = x^2 - \frac{3+\sqrt{-7}}{2}$ non ha radici in $\mathbb{Q}(\sqrt{-7})$, che equivale a dire che $x^2 - 6 - 2\sqrt{-7}$ non ha radici in $\mathbb{Q}(\sqrt{-7})$. Infatti, sia $x =$

$\alpha + \sqrt{-7}\beta$ un generico elemento di $\mathbb{Q}(\sqrt{-7})$, con $\alpha, \beta \in \mathbb{Q}$, supponendo che $x^2 = 6 + 2\sqrt{-7}$ avremmo

$$\begin{cases} \alpha^2 - 7\beta^2 &= 6 \\ 2\alpha\beta &= 2 \end{cases}$$

da cui segue $\beta = 1/\alpha$ e quindi, sostituendo β nella prima equazione, $\alpha^2 - 7/\alpha^2 = 6$, che non ha soluzioni in $\mathbb{Q}$ perché il polinomio associato $y^2 - 6y - 7$ ha radici $7, -1$ che non sono quadrati in $\mathbb{Q}$. Notiamo che il sistema ha (tra le altre) una soluzione data da $\alpha = i, \beta = -i$ e dunque possiamo vedere che $\omega = \frac{i+\sqrt{7}}{2}$ è una soluzione di $q_1(x)$.

Quindi $q_1(x)$ non ha radici in $\mathbb{Q}(\sqrt{-7})$, ma ha radici $\pm\omega$ in un'estensione di grado 2 di $\mathbb{Q}(\sqrt{-7})$. Dunque $\mathbb{F} = \mathbb{Q}(\sqrt{-7}, \omega)$ è un'estensione di $\mathbb{Q}$ di grado 4 che contiene le radici di $q_1(x)$. In particolare per il conto visto sopra possiamo dire esplicitamente che $\mathbb{F} = \mathbb{Q}(\sqrt{-7}, i)$.

Poichè il termine noto di $p(x)$ è 4, ovvero un quadrato in $\mathbb{Q}$, il campo $\mathbb{F}$ contiene anche le radici di $q_2(x) = x^2 + \frac{3-\sqrt{-7}}{2}$. Infatti, siano $\pm\tau$ le radici di $q_2(x)$, $\omega^2\tau^2 = 4$ e quindi $\omega\tau = \pm 2$ e dunque se $\omega \in \mathbb{F}$, allora anche $\tau \in \mathbb{F}$. Abbiamo quindi mostrato che $\mathbb{F} = \mathbb{K}$ è il campo di spezzamento di $p(x)$, perché è generato da una radice del polinomio $p(x)$ e da $\sqrt{\Delta}$ e contiene tutte le radici di $p(x)$. Inoltre $\mathbb{K}$ abbiamo visto che ha grado 4 su $\mathbb{Q}$.

(b) Poichè il campo di spezzamento ha grado 4 su $\mathbb{Q}$, il gruppo di Galois G avrà cardinalità esattamente 4. Dobbiamo determinare se $G \simeq \mathbb{Z}_4$ o $G \simeq \mathbb{Z}_2^2$. Notiamo che $\mathbb{K}$ contiene due sottoestensioni di grado 2 su $\mathbb{Q}$ date da $\mathbb{Q}(\sqrt{-7})$ e $\mathbb{Q}(i\sqrt{-7}) = \mathbb{Q}(\sqrt{7})$ distinte tra loro perché una reale, l'altra non reale. Dunque G deve contenere due sottogruppi distinti di indice 2 e per questo non può essere $\mathbb{Z}_4$. Ne segue che $G \simeq \mathbb{Z}_2^2$. I suoi elementi devono mandare ciascun generatore in un elemento del suo polinomio minimo, ovvero $i \mapsto \pm i$, $\sqrt{-7} \mapsto \pm\sqrt{-7}$. Quindi il gruppo è generato da:

$$\sigma : \begin{cases} \sqrt{-7} & \mapsto & \sqrt{-7} \\ i & \mapsto & -i \end{cases} \qquad \rho : \begin{cases} \sqrt{-7} & \mapsto & -\sqrt{-7} \\ i & \mapsto & i. \end{cases}$$

(c) In $\mathbb{F}_7$ il discriminante di $y^2 - 3y + 4$ è $\Delta = 9 - 16 = 0$ e quindi $p(x)$ è un quadrato: $p(x) = (x^2 - 5)$. I quadrati in $\mathbb{F}_7^*$ sono solo $1, 2, 4$ e quindi 5 non è un quadrato in $\mathbb{F}_7$. Ne segue che il campo di spezzamento di $x^2 - 5$ è l'estensione di grado 2 di $\mathbb{F}_7$. Dunque Il campo di spezzamento di $p(x)$ su $\mathbb{F}_7$ è $\mathbb{F}_{7^2}$ e poiché il grado è 2 il gruppo di Galois è $\mathbb{Z}_2$.

4. (a) Trovare un'estensione di Galois $\mathbb{E}_1$ di $\mathbb{Q}$ tale che $\mathrm{Aut}(\mathbb{E}_1/\mathbb{Q}) \simeq \mathbb{Z}_8$;

(b) trovare un elemento $\alpha \in \mathbb{C}$ tale che $\mathbb{E}_1 = \mathbb{Q}(\alpha)$;

(c) trovare un'estensione di Galois $\mathbb{E}_2$ di $\mathbb{Q}$ tale che $\mathrm{Aut}(\mathbb{E}_2)/\mathbb{Q}) \simeq \mathbb{Z}_4 \times \mathbb{Z}_8$;

(d) trovare un elemento $\beta \in \mathbb{C}$ tale che $\mathbb{E}_2 = \mathbb{Q}(\beta)$.

Soluzione:

(a) e (b) *[Seguiamo quanto già visto a esercitazione.]* Sia $\mathbb{K} = \mathbb{Q}(\zeta_{17})$. Sappiamo che $G = \mathrm{Aut}(\mathbb{Q}(\zeta_{17})/\mathbb{Q})$ è isomorfo a $\mathbb{Z}_{16}$, ma in $\mathbb{Z}_{16}$ vi è un sottogruppo H di indice 8, abbiamo dunque che il sottocampo $\mathbb{E}_1$ di $\mathbb{K}$ fissato da H è una estensione di Galois (tutti i sottogruppi di un gruppo abeliano sono normali) di $\mathbb{Q}$ tale che $\mathrm{Aut}(\mathbb{K}^H/\mathbb{Q}) = G/H \simeq \mathbb{Z}_8$. Un elemento di ordine 2 in G è definito da $\phi : \zeta_{17} \mapsto \zeta_{17}^{-1}$. Prendiamo quindi $\alpha = \zeta_{17} + \zeta_{17}^{-1} \in \mathbb{K}^H$; possiamo considerare che in $\mathbb{Q}(\alpha)[x]$ il polinomio $x^2 - \alpha x + 1$ annulla ζ_{17}, quindi $[\mathbb{K} : \mathbb{Q}(\alpha)] \leq 2$. Inoltre per costruzione $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta_{17})^H$ e dunque ha grado al più 8 su $\mathbb{Q}$. Dalla torre di estensioni segue $\mathbb{E}_1 = \mathbb{Q}(\alpha) = \mathbb{K}^H$ e che il grado di $\mathbb{E}_1$ su $\mathbb{Q}$ è esattamente 8.

(c) e (d) Abbiamo già visto a lezione, da un risultato generale per le estensioni ciclotomiche, che $\mathrm{Aut}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \simeq \mathbb{Z}_5^* = \mathbb{Z}_4$.

Come visto a lezione, poichè 5 e 17 sono primi distinti e quindi in particolare sono numeri coprimi, $\mathbb{Q}(\zeta_5, \zeta_{17}) = \mathbb{Q}(\zeta_{5\cdot 17})$ ed è un'estensione di Galois di $\mathbb{Q}$ di grado $\phi(5)\phi(17) = 4{\cdot}16$. Inoltre, sempre per quanto visto a lezione, anche $\mathbb{Q}(\zeta_5)$ e $\mathbb{Q}(\zeta_{17})$ sono estensioni di Galois di $\mathbb{Q}$ e $\mathbb{Q}(\zeta_5) \cap \mathbb{Q}(\zeta_{17}) = \mathbb{Q}$. Il gruppo di automorfismi $\mathrm{Aut}(\mathbb{Q}(\zeta_5, \zeta_{17})/\mathbb{Q})$ è dato dunque dal prodotto $G' = \mathbb{Z}_4 \times \mathbb{Z}_{16}$, abeliano e quindi con tutti i sottogruppi normali (e tutti i sottocampi che sono estensioni di Galois di $\mathbb{Q}$). Inoltre nel prodotto il fattore $\mathbb{Z}_4$ è inteso agire banalmente su $\mathbb{Q}(\zeta_{17})$ e il fattore $\mathbb{Z}_{16}$ è inteso agire banalmente su $\mathbb{Q}(\zeta_5)$. Sia $\mathbb{E}_2$ il campo fisso del sottogruppo $H' = \{0\} \times \{0, 8\}$, il suo gruppo di Galois su $\mathbb{Q}$ è quindi isomorfo a $G'/H' \simeq \mathbb{Z}_4 \times \mathbb{Z}_8$. Per quanto detto su come agiscono i due fattori di G' e per quanto visto nel punto precedente, il campo fisso di H' è $\mathbb{Q}(\zeta_5, \alpha)$.

Consideriamo l'elemento $\beta = \zeta_5\alpha$. Affermiamo che $\mathbb{Q}(\beta) = \mathbb{Q}(\zeta_5, \alpha)$. Infatti $\mathbb{Q}(\beta) \subset \mathbb{Q}(\zeta_5, \alpha)$. Inoltre $\beta^5 = \alpha^5$ genera $\mathbb{Q}(\alpha^5)$ che è una sottoestensione di $\mathbb{Q}(\alpha)$. Se non fosse che $\alpha \in \mathbb{Q}(\alpha^5)$ allora $x^5 - \alpha^5$ si fattorizzerebbe in $\mathbb{Q}(\alpha^5)$ con un fattore irriducibile di grado dispari maggiore di 1. In particolare il grado del suo campo di spezzamento, ovvero $\mathbb{Q}(\alpha, \zeta_5)$, dovrebbe avere un grado su $\mathbb{Q}(\alpha^5)$ diviso da un numero dispari, ma questo non è possibile perchè il suo grado è $4{\cdot}8$, cioé potenza di 2 e quindi per la torre di estensioni $\mathbb{Q}(\alpha, \zeta_5) \supset \mathbb{Q}(\alpha) \supset \mathbb{Q}(\alpha^5) \supset \mathbb{Q}$ anche il grado dell'estensione $\mathbb{Q}(\alpha) \supset \mathbb{Q}(\alpha^5)$ è potenza di 2. Dunque $\mathbb{Q}(\beta) \supset \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\zeta_5, \alpha)$. Quindi, $\mathbb{Q}(\beta) = \mathbb{E}_2$ e $\mathrm{Aut}(\mathbb{E}_2/\mathbb{Q}) = \mathbb{Z}_4 \times \mathbb{Z}_8$.

Traccia sol. es 1.

a) Il gruppo ha ordine p^3 e non è abeliano come mostra il seguente esempio:

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

b) Le tre affermazioni sono tutte vere.

Se vale $\alpha_i \geq 3$ per qualche i, allora $p_i^3 \mid n$ e dunque abbiamo il gruppo non abeliano $A \times \mathbb{Z}_{\frac{n}{p_i^3}}$ dove A è un gruppo non abeliano di ordine p_i^3 (vedi esempio del punto a)).

Se $r = 1$ non abbiamo altro da dimostrare.

Se $r \geq 2$ ed esistono p e q primi distinti che dividono n, tali che $p \mid q-1$, allora facciamo come sopra con $B \times \mathbb{Z}_{\frac{n}{pq}}$ dove B è un gruppo non abeliano

di ordine pq (che sappiamo che esiste dalla teoria).

Infine, se esistono p e q primi distinti tali che $p^2 q \mid n$ e $q \mid p+1$, costruiamo un gruppo C di ordine $p^2 q$ non abeliano e concludiamo considerando $C \times \mathbb{Z}_{n/p^2 q}$.

Per costruire C osserviamo che

$$|\mathrm{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p)| = |GL(\mathbb{Z}_p^2)| = (p^2-1)(p^2-p) =$$
$$= (p-1)^2 p (p+1)$$

In particolare $q \mid |\mathrm{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p)|$.

Allora $\exists\ \tau : \mathbb{Z}_q \longrightarrow \mathrm{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p)$

omomorfismo non banale (per Cauchy esiste in $\mathrm{Aut}(\mathbb{Z}_p \times \mathbb{Z}_p)$ un elemento γ di ordine q, e possiamo definire τ mediante $\tau(1) = \gamma$).

Il gruppo $C = (\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes_\tau \mathbb{Z}_q$

non è abeliano (RIPASSO: in generale se A_1 e A_2 sono gruppi abeliani $\neq \{e\}$ e $\tau : A_1 \to \mathrm{Aut}(A_2)$ non è banale, allora $A_2 \rtimes_\tau A_1$ non è abeliano perché .... CONTINUATE VOI!)

Traccia sol. es. 2.

Innanzitutto si osserva che per ogni n c'è una immersione $S_n \hookrightarrow A_{n+2}$ data da

se σ è pari: $\sigma \longrightarrow \sigma$

se σ è dispari: $\sigma \longrightarrow \sigma \cdot (n+1, n+2)$

dove il σ che compare a destra è l'elemento di A_{n+2} che permuta gli elementi di $\{1, \dots, n\}$ esattamente come il σ a sinistra e inoltre lascia fissi $n+1$ e $n+2$.

Mostriamo adesso che per $n \geq 4$ non è possibile che $S_n \hookrightarrow A_{n+1}$.

Infatti: se avessimo una simile immersione, chiamiamo H l'immagine di S_n.

Allora A_{n+1} agisce sui laterali di H dando origine ad un omomorfismo

$$A_{n+1} \xrightarrow{\varphi} S_{\text{indice di } H \text{ in } A_{n+1}} = S_{\frac{n+1}{2}}$$

da qui già si osserva che n deve essere dispari

Ora, visto che $n+1 \geq 5$, sappiamo che A_{n+1} è semplice.

Dunque $\ker \varphi = \begin{cases} A_{n+1} \\ \{e\} \end{cases}$ ← IMPOSSIBILE perché l'azione sui laterali non è banale.

Allora $\ker \varphi = \{e\}$, ASSURDO perché $\frac{(n+1)!}{2} > \left(\frac{n+1}{2}\right)!$ nel nostro caso in cui $n \geq 4$.

Si conclude l'esercizio studiando i casi $n = 1, 2, 3$:

S_1 si immerge in A_1 (è dunque un caso speciale)

S_2 non si immerge in A_3

S_3 non si immerge in A_4