SOLUZIONI DEL COMPITO DI ALGEBRA 1

13 febbraio 2015

Esercizio 1.

Siano $\sigma = (1,2,3,4)$ e $\tau = (2,4)(5,6)$ permutazioni di $\mathcal{S}_6$.

a) Determinare la cardinalità di $H = \langle \sigma, \tau \rangle$ e del centralizzatore di H in $\mathcal{S}_6$.

b) Determinare il normalizzatore di H e mostrare che H è contenuto in un unico 2-Sylow di $\mathcal{S}_6$.

Soluzione esercizio 1 (a) Osserviamo che $\tau\sigma\tau^{-1} = \sigma^{-1}$, quindi $\tau \in N(\langle\sigma\rangle)$ e questo implica che $\langle\sigma\rangle\langle\tau\rangle$ è un gruppo; tale gruppo coincide con H ed è isomorfo al gruppo D_4, che ha quindi ordine 8.

È immediato vedere che $Z(H) = Z(\sigma) \cap Z(\tau)$. Sappiamo che il centralizzatore del 4 ciclo σ ha cardinalità $6!/\binom{6}{4} \cdot 3! = 8$ e si ha $Z(\sigma) = \langle \sigma, (5,6) \rangle$. Ora σ non commuta con τ ma σ^2 e $(5,6)$ commutano con τ; da questo segue che $Z(H) = \langle (1,3)(2,4), (5,6) \rangle$ che ha cardinalità 4.

(b) Osserviamo che per ogni $\gamma \in N(H)$ vale $\gamma\sigma\gamma^{-1} = \sigma$, oppure σ^{-1} (sono gli unici elementi di ordine 4 di H), quindi $N(H) \subseteq N(\langle\sigma\rangle) = Z(\langle\sigma\rangle) \cup \tau Z(\langle\sigma\rangle)$. Da questo segue che $N(H)$, che chiaramente contiene H, ha ordine 8 se coincide con H e ha ordine 16 se è strettamente più grande di H, e in tal caso coincide con $N(\langle\sigma\rangle)$. Poché chiaramente $Z(H) \subseteq N(H)$, si ha che $(5,6) \in N(H) \setminus H$ e quindi $N(H) = \langle H, (5,6) \rangle$. Questo ci dice che $N(H)$ è l'unico 2-Sylow di $\mathcal{S}_6$ che contiene H: infatti se P è un 2-Sylow che contiene H, allora $H \lhd P$, quindi $P \subseteq N(H)$ e i due gruppi coincidono per motivi di ordine.

Esercizio 2

Sia G un gruppo di ordine 300.

a) Mostrare che G non è semplice.

b) Dire se esiste un G che non contiene sottogruppi ciclici di ordine 15.

Soluzione esercizio 2 (a) Un 5-Sylow P ha cardinalità 25 ed indice 12, dunque P ha 1 o 6 coniugati. Se P è normale allora segue immediatamente che G non è semplice. Se P non è normale, allora deve avere esattamente 6 coniugati. Di conseguenza G agisce (per coniugio) transitivamente su un insieme di 6 elementi (l'insieme dei coniugati di P) e quindi esiste un omomorfismo ϕ non banale da G al gruppo di permutazioni S_6, che ha cardinalità 720. Poiché $300 \nmid 720$, $\ker\phi$ è un sottogruppo normale non banale di G.

(b) Consideriamo il gruppo $N = (\mathbb{Z}/5)^2$. Il gruppo di automorfismi di N contiene $24 \cdot 20$ elementi, dunque contiene un elemento non banale $a \in \mathrm{GL}_2(\mathbb{F}_5)$ di ordine 3. La matrice di a non può avere 1 come autovalore, altrimenti il suo polinomio caratteristico si potrebbe fattorizzare su $\mathbb{F}_5$ ed a sarebbe diagonalizzabile su $\mathbb{F}_5$, ma $3 \nmid |(\mathbb{F}_5)^*| = 4$. Dunque a fissa solo $(0,0) \in (\mathbb{Z}/5)^2$. Possiamo

allora definire $\psi : \mathbb{Z}/3 \to \mathrm{GL}_2(\mathbb{F}_5)$ con $\psi(1) := a$ ed il prodotto semidiretto

$$H := \mathbb{Z}/3 \ltimes_\psi (\mathbb{Z}/5)^2.$$

Affermiamo che H non ha sottogruppi ciclici di ordine 15. Infatti il 5-Sylow di H è normale per costruzione e preso un qualsiasi elemento b di ordine 3, esso genera un 3-Sylow la cui azione è coniugata a quella definita da ψ e dunque non commuta con nessun elemento non banale del 5-Sylow. È chiaro allora che $G = \mathbb{Z}/4 \times H$ soddisfa le richieste perchè un elemento di ordine 15 dovrebbe essere contenuto nel sottogruppo $\{0\} \times H$ isomorfo ad H.

Esercizio 3.

Sia A un dominio a fattorizzazione unica e sia P un ideale primo di A; poniamo $S_P = A \setminus P$. Mostrare che $S_P^{-1}A$ è un dominio a fattorizzazione unica.

Soluzione esercizio 3 Poniamo $A_P = S_P^{-1}A$; sappiamo che A_P è un dominio. Per prima cosa caratterizziamo gli elementi *invertibili* e gli elementi *irriducibili* di A_P. Si ha:

$$\frac{a}{s} \in A_P \text{ è invertibile} \quad \iff \quad a \in S_P.$$

Infatti, $\Leftarrow$ è ovvia in quanto se $a \in S$, allora $\frac{s}{a} \in A_P$ ed è chiaramente l'inverso di A. Viceversa, se $\frac{a}{s}$ è invertibile esiste $\frac{b}{t} \in A_P$ tale che $\frac{a}{s}\frac{b}{t} = \frac{1}{1}$, quindi $ab = st \in S_P$, cioè $ab \notin P$, da cui $a \notin P$.

$$\frac{a}{s} \in A_P \text{ è irriducibile} \quad \iff \quad a = \pi u \text{ con } u \in S_P \text{ e } \pi \in P, \text{elemento irriducibile in } A.$$

($\Leftarrow$) Sia $a = \pi u$, e supponiamo $\frac{a}{s} = \frac{b}{t}\frac{c}{v}$ in A_P, allora $\pi utv = bcs$ e quindi $\pi | bcs$: essendo π irriducibile (e quindi primo) in A si ha $\pi | b$ oppure $\pi | c$ (chiaramente $\pi \not| s$), cioè $b = \pi\beta$ oppure $c = \pi\gamma$. Se $b = \pi\beta$ otteniamo $utv = \beta cs$ da cui si ricava che $c \notin P$ e quindi $\frac{c}{s}$ è invertibile in A_P. Analogamente si può ragionare su c.
($\Rightarrow$) Supponiamo $\frac{a}{s}$ irriducibile in A_P e sia $a = \pi_1 \cdots \pi_k$ la fattorizzazione in irriducibili in A con $\pi_i \in P$ per $i = 1, \dots r$ e $\pi_i \notin P$ per $r < i \leq k$. Abbiamo che $\frac{\pi_i}{1}$ è irriducibile per $i \leq r$ e invertibile per $r < i \leq k$. Se fosse $r \geq 1$ avrei che $\frac{\pi_1}{1}$ e $\frac{\pi_2}{1}$ sono fattori non banale di $\frac{a}{s}$, infatti entrambi dividono $\frac{a}{s}$ e non sono invertibili; questo nega però l'irriducibilità di $\frac{a}{s}$, da cui $r = 1$.
Vediamo ora che ogni elemento non invertibile di A_P si scrive in modo unico come prodotto di irriducibili. Sia $\frac{a}{s}$ un elemento non invertibile allora $a \in P$; per quanto detto sopra in A vale $a = \pi_1 \cdots \pi_r t$ con $t \notin P$, $\pi_i \in P$ irriducibile in A e $r \geq 1$. Allora $\frac{a}{s} = \frac{\pi_1}{1} \cdots \frac{\pi_r}{1}\frac{t}{s}$ è una fattorizzazione in A_P (gli elementi $\frac{\pi_i}{1}$ sono irriducibili e $\frac{t}{s}$ è invertibile).
Supponiamo ora che un elemento di A_P abbia due fattorizzazioni: allora a meno di moltiplicare per elementi invertibili si ha un'uguaglianza del tipo: $\frac{\pi_1}{1} \cdots \frac{\pi_r}{1} = \frac{p_1}{1} \cdots \frac{p_k}{1}\frac{u}{v}$ con $\pi_i, p_j \in P$ irriducibili in A per ogni $i = 1, \dots r$ e per ogni $j = 1, \dots k$, e $u, v \notin P$. Allora se $v = \rho_1 \cdots \rho_l$ e $u = q_1 \dots q_h$ sono le fattorizzazioni in irriducibili di u e v, in A vale l'uguaglianza $\pi_1 \cdots \pi_r \rho_1 \cdots \rho_l = p_1 \cdots p_k q_1 \dots q_h$: per l'unicità della fattorizzazione in A, i fattori che compaiono ai due membri devono essere due a due associati, ma allora i π_i e i p_j devono essere associati tra loro perché gli altri fattori non appartengono a P. Ne segue che la fattorizzazione è unica anche in A_P.

Esercizio 4.
Sia $\alpha = \sqrt[3]{3} + \sqrt{5} \in \mathbb{C}$.
a) Mostare che $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{3}, \sqrt{5})$.
b) Determinare il campo di spezzamento K e il gruppo di Galois del polinomio minimo di α su $\mathbb{Q}$.
c) Descrivere le sottoestensioni di K che sono di Galois su $\mathbb{Q}$ e il cui gruppo di Galois è abeliano.

Soluzione esercizio 4 (a) È chiaro che $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt[3]{3}, \sqrt{5})$. Per vedere il contenimento inverso notiamo intanto che $\mathbb{Q}(\sqrt[3]{3}, \sqrt{5}) = \mathbb{Q}(\alpha)[\sqrt[3]{3}]$. Il polinomio minimo di $\sqrt[3]{3}$ su $\mathbb{Q}$ è $x^3 - 3$, che ha due radici non reali, quindi il polinomio minimo di $\sqrt[3]{3}$ su $\mathbb{Q}(\alpha)$, che deve dividere $x^3 - 3$, non può avere grado 2, altrimenti una delle radici non reali dovrebbe stare in $\mathbb{Q}(\alpha)$, che è reale. Dunque il grado divide 3. D'altra parte $\mathbb{Q}(\sqrt[3]{3}, \sqrt{5}) = \mathbb{Q}(\alpha)[\sqrt{5})$ e quindi $\mathbb{Q}(\sqrt[3]{3}, \sqrt{5})$ è un'estensione di $\mathbb{Q}(\alpha)$ di grado che minore o uguale a 2. Ma allora l'unica possibilità è che il grado dell'estensione sia 1. Segue inoltre che $\mathbb{Q}(\alpha)$ ha grado 6 su $\mathbb{Q}$.
(b) Poiché il polinomio minimo di $\sqrt[3]{3}$ è $x^3 - 3$, il campo di spezzamento è dato da $F_1 = \mathbb{Q}(\sqrt[3]{3}, \zeta_3\sqrt[3]{3}, \zeta_3^2\sqrt[3]{3}) = \mathbb{Q}(\sqrt[3]{3}, \zeta_3) = \mathbb{Q}(\sqrt[3]{3}, \imath\sqrt{3}]$ che è un'estensione di Galois di $\mathbb{Q}$ di grado 6, con gruppo di Galois S_3. Inoltre $F_2 = \mathbb{Q}(\sqrt{5})$ è un'estensione di Galois di $\mathbb{Q}$ di grado 2. Dunque il campo di spezzamento di α è la chiusura di Galois di $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{3}, \sqrt{5})$ e dunque è dato da $K = \mathbb{Q}(\sqrt[3]{3}, \zeta_3, \sqrt{5})$.
Il campo K è un'estensione di $\mathbb{Q}$ di grado 12. Infatti contiene le sottoestensioni $\mathbb{F}_1$ ed $\mathbb{F}_2$ di grado rispettivamente 6 e 2 e $F_1 \cap F_2 = \mathbb{Q}$ in quanto l'unica sottoestensione di F_1 di grado 2 è $\mathbb{Q}(\zeta_3)$ che non è reale, mentre F_2 è reale. Poiché F_1 e F_2 sono entrambe normali e la loro intersezione è $\mathbb{Q}$, segue che il gruppo di Galois di K su $\mathbb{Q}$ è $G = S_3 \times \mathbb{Z}/2$.
L'elemento α ha 6 coniugati $\alpha_1, \ldots, \alpha_6$ nella forma $\pm\sqrt{5} + \zeta_3^i\sqrt[3]{3}$, $i = 0, 1, 2$. Dunque il polinomio minimo di α è dato da

$$p(x) = \prod_{i=1}^{6}(x - \alpha_i) = x^6 - 15x^4 - 6x^3 + 75x^2 - 90x - 116.$$

(c) Descriviamo i generatori di G. Il sottogruppo S_3 agisce banalmente su F_2. È generato da un elemento di ordine 2, τ, e un elemento di ordine 3, σ, che agiscono su F_1 come segue:

$$\tau(\zeta_3) = \zeta_3^2, \tau(\sqrt[3]{3}) = \sqrt[3]{3};$$

$$\sigma(\zeta_3) = \zeta_3, \sigma(\sqrt[3]{3}) = \zeta_3\sqrt[3]{3}.$$

Il sottogruppo $\mathbb{Z}/2$ corrispondente al gruppo di Galois di F_2 su $\mathbb{Q}$ agisce banalmente su F_1 ed il suo generatore ρ agisce su F_2 con $\rho(\sqrt{5}) = -\sqrt{5}$.
La corrispondenza di Galois ci dice che i sottocampi di K che sono estensioni di Galois di $\mathbb{Q}$ con gruppo di Galois abeliano sono i campi fissati dai sottogruppi normali di G che danno quoziente abeliano.
Un sottogruppo normale di G che dia quoziente deve contenere il sottogruppo dei commutatori e poiché $G = S_3 \times \mathbb{Z}/2$ il sottogruppo dei commutatori di G è dato da $G' = S_3' \times \mathbb{Z}_2' =$

$\langle\sigma\rangle \times \{e\}$. Dunque stiamo cercando le sottoestensioni di Galois del campo fisso $K^{G'} = \mathbb{Q}[\zeta_3, \sqrt{5}]$. Quest'ultimo ha gruppo di Galois $\mathbb{Z}/2 \times \mathbb{Z}/2$ (ovviamente è abeliano) e dunque tutte le sue sottoestensioni sono di Galois e sono (contando anche $K^{G'}$ e $\mathbb{Q}$ stesso) esattamente 5. Le tre non banali sono i sottocampi di $K^{G'}$ fissati da $\tau, \rho, \tau\rho$ e dunque sono: $\mathbb{Q}[\zeta_3], \mathbb{Q}[\sqrt{5}], \mathbb{Q}[\imath\sqrt{3}\sqrt{5}]$.