SOLUZIONI DEL COMPITO DI ALGEBRA 1

16 febbraio 2018

Esercizio 1. Sia $\sigma \in S_{16}$ il prodotto di 2 3-cicli e 2 5-cicli, tutti disgiunti tra loro.

1. Descrivere $C_{S_{16}}(\sigma)$ come prodotto semidiretto;
2. mostrare che $C_{S_{16}}(\sigma)$ contiene un sottogruppo isomorfo a D_{15}.

Soluzione.

1. Supponiamo $\sigma = \tau_1\tau_2\tau_3\tau_4$, dove $\tau_1 = (1\,2\,3)$, $\tau_2 = (4\,5\,6)$, $\tau_3 = (7\,8\,9\,10\,11)$, $\tau_4 = (12\,13\,14\,15\,16)$. Il gruppo $C_{S_{16}}(\sigma)$ contiene certamente gli elementi $\tau_1, \tau_2, \tau_3, \tau_4$ che commutano tra loro e generano un gruppo N isomorfo a $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$. Inoltre il centralizzatore contiene $\mu_1 = (1\,4)(2\,5)(3\,6)$ e $\mu_2 = (7\,12)(8\,13)(9\,14)(10\,15)(11\,16)$. Infatti notiamo che μ_1 e μ_2 hanno ordine 2 e inoltre $\mu_1\tau_1\mu_1 = \tau_2$, $\mu_1\tau_2\mu_1 = \tau_1$, $\mu_2\tau_3\mu_2 = \tau_4$, $\mu_2\tau_4\mu_2 = \tau_3$, μ_1 commuta con τ_3, τ_4 e μ_2 commuta con τ_1, τ_2. Ne segue che μ_1, μ_2 commutano con σ e inoltre normalizzano N perché tramite il coniugio permutano i suoi generatori. Chiamiamo H il sottogruppo generato da μ_1, μ_2. H è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

   Notiamo che $N \cap H = \{e\}$: questo segue dal fatto che i due sottogruppi hanno ordini coprimi. Visto che i generatori di H normalizzano N e visto che l'intersezione dei due sottogruppi è banale, i due sottogruppi sono in prodotto semidiretto.

   Affermiamo che $C_{S_{16}}(\sigma)$ è isomorfo a $H \ltimes N$. Tale sottogruppo è contenuto nel centralizzatore di σ in quanto lo sono i suoi generatori. Inoltre la cardinalità di $H \ltimes N$ è $2^2 3^2 5^2$. D'altra parte la classe di coniugio di σ in S_{16} ha $\frac{1}{2}\binom{16}{5}4!\binom{11}{5}4!\frac{1}{2}\binom{6}{3}2!\binom{3}{3}2! = \frac{16!}{2^2 3^2 5^2}$ elementi, da cui segue che il suo centralizzatore deve avere la stessa cardinalità di $H \ltimes N$ e quindi i due sottogruppi coincidono.

   Le relazioni che definiscono il prodotto semidiretto sono quelle espresse dalle relazioni di coniugio e di commutazione riportate sopra.

2. L'elemento $\alpha = \tau_1\tau_2^{-1}\tau_3\tau_4^{-1}$ ha ordine 15 e appartiene al centralizzatore di σ. Anche $\beta = \mu_1\mu_2$ appartiene al centralizzatore, ha ordine 2 e per le relazioni viste nel punto precedente si ha che $\beta\alpha\beta = \alpha^{-1}$. Dunque il sottogruppo generato da α, β è isomorfo a D_{15}.

Esercizio 2. Sia G un gruppo di ordine p^2q^2 con p, q due primi distinti e supponiamo $p < q$.

1. Mostrare che G non può essere semplice.

2. Detto $n(p,q)$ il numero di gruppi di ordine p^2q^2, determinare il minimo di $n(p,q)$.

Soluzione.

1. Indichiamo con n_q il numero dei q-Sylow: sappiamo che $n_q \equiv 1 \pmod q$ e $n_q | p^2$, quindi, dato che $p < q$, si ha $n_q = 1$ oppure $n_q = p^2$. Se $n_q = 1$ il q-Sylow è normale, quindi G non è semplice. Se invece $n_q = p^2$ deve essere $q | p^2 - 1 = (p-1)(p+1)$ e, poichè $q > p$, l'unica possibilità è che $q = p+1$ e quindi $p = 2$ e $q = 3$. Anche in questo caso si prova che G non è semplice: infatti G ha 4 3-Sylow e l'azione su di essi per coniugio dà un omomorfismo non banale $\varphi\colon G \to S_4$. Se G fosse semplice φ sarebbe iniettivo, ma questo non è possibile perché $|G| = 4 \cdot 9 = 36$ mentre $|S_4| = 24$.

2. Per prima cosa osservo che se G ha ordine p^2q^2 allora i suoi Sylow sono abeliani perché hanno ordine il quadrato di un primo. Se indichiamo con P il p-Sylow e con Q il q-Sylow si ha

$$P \cong \begin{cases} \mathbb{Z}/p^2\mathbb{Z} \\ \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \end{cases} \qquad Q \cong \begin{cases} \mathbb{Z}/q^2\mathbb{Z} \\ \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \end{cases}$$

Dato che ogni gruppo abeliano è prodotto diretto dei suoi Sylow, per ogni p, q ci sono esattamente 4 gruppi abeliani di ordine p^2q^2. Vediamo che possiamo scegliere p e q in modo tale che non ci siano altri gruppi di ordine p^2q^2. Nella prima parte abbiamo visto che, se escludiamo il caso $(p,q) = (2,3)$, il q-Sylow è normale; supponendo quindi $(p,q) \neq (2,3)$ si ha $G \cong Q \rtimes_\varphi P$. Vogliamo vedere che si possono scegliere p, q in modo che gli unici prodotti semidiretti siano quelli diretti. Questo succede se l'unico possibile omomorfismo $\varphi\colon P \to \mathrm{Aut}(Q)$ è quello banale, cioè se $\mathrm{Aut}(Q)$ non ha elementi di ordine p. Ora

$$|\mathrm{Aut}(Q)| = \begin{cases} |\mathrm{Aut}(\mathbb{Z}/q^2\mathbb{Z})| = \Phi(q^2) = q(q-1) \\ |\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z})| = (q^2-1)(q^2-q) \end{cases}$$

quindi se $p \nmid q^2 - 1$ l'unica azione di P su Q è quella banale e i prodotti sono tutti diretti, cioè $n(p,q) = 4$. Questo si verifica ad esempio per $p = 5$ e $q = 7$ dato che $5 \nmid 7^2 - 1$.

Esercizio 3. Sia $A = \mathbb{Z}[\sqrt{2}]$ e per ogni $\alpha = a + \sqrt{2}b \in A$ poniamo $N(\alpha) = a^2 - 2b^2$.

1. α è invertibile se e solo se $N(\alpha) = \pm 1$;

2. Contare gli ideali di A che contengono 7.

3. Mostrare che esistono P, Q ideali primi distinti di A tali che $P \cap \mathbb{Z} = Q \cap \mathbb{Z}$;

4. Mostrare che l'ideale $5A$ è primo.

Soluzione.

1. Notiamo che N è moltiplicativa. Per vederlo possiamo ad esempio considerare l'inclusione $A \subset \mathbb{Q}[\sqrt{2}]$. Chiaramente $N(\alpha) = \alpha\bar{\alpha}$ dove $\bar{\alpha}$ è il coniugato di α rispetto all'unico automorfismo non banale di $\mathbb{Q}[\sqrt{2}]$. Poiché gli automorfismi di un campo sono moltiplicativi ne segue che lo è anche N.

   Notiamo ora che per $\alpha \in A$ $N(\alpha)$ è sempre intero e dunque se α è invertibile in A allora la sua norma $N(\alpha)$ deve essere invertibile in $\mathbb{Z}$, in quanto se $\alpha\beta = 1$ si ha che $N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$.

   Viceversa se $N(\alpha) = \pm 1$ allora $\alpha\bar{\alpha} = \pm 1$ e quindi $\pm\bar{\alpha}$ è l'inverso di α.

2. Sia I un ideale di A contenente 7. Necessariamente I contiene l'ideale $(7) = \{7a + 7b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Dunque gli ideali di A contenenti 7 sono in corrispondenza biunivoca con gli ideali di $A/(7)$ Ora si ha $A/(7) \cong \mathbb{Z}[x]/(7, x^2 - 2) \cong \mathbb{F}_7[x](x^2 - 2)$, dove il primo isomorfismo (o meglio il suo inverso) è indotto, per passaggio al quoziente, da $p(x) \mapsto \overline{p(\sqrt{2})}$ e il secondo è quello del terzo teorema di omomorfismo. Ora, poichè 2 è un quadrato in $\mathbb{F}_7$ si ha che $x^2 - 2$ si fattorizza e $(x^2 - 2) = (x-3)(x+3)$, e i generatori dei due fattori sono coprimi. Quindi per il teorema cinese del resto $A/(7) \simeq \mathbb{F}_7[x]/(x-3) \times \mathbb{F}_7[x]/(x+3) \simeq \mathbb{F}_7 \times \mathbb{F}_7$. Sappiamo che gli ideali di un prodotto sono il prodotto degli ideali dei due fattori: in questo caso i fattori sono campi e hanno quindi solo gli ideali banali. In tutto abbiamo quindi 4 ideali nel quoziente, quindi, per il teorema di corrispondenza, 4 ideali in A che contengono 7. Anche se non richiesto, possiamo determinare questi ideali esplicitamente: due sono quelli ovvi, cioè (7) e tutto A. Determiniamo gli altri due. Notiamo che gli elementi $3-\sqrt{2}, 3+\sqrt{2}$ hanno norma 7, quindi $(3-\sqrt{2}), (3+\sqrt{2})$ sono due ideali propri di A (i generatori non sono invertibili) che contengono propriamente (7), infatti la norma di ogni elemento in (7) è un multiplo di 49, mentre $N(3-\sqrt{2}) = N(3+\sqrt{2}) = 7$ quindi $(7) \subsetneq (3+\sqrt{2}), (3-\sqrt{2}) \subsetneq A$. Infine, $(3-\sqrt{2}) + (3+\sqrt{2}) = A$ in quanto la somma di questi due ideali contiene sia 7 che $6 = 3+\sqrt{2}+3-\sqrt{2}$, quindi contiene anche 1=7-6. Ne segue che questi due ideali sono distinti.

3. Gli ideali $P = (3-\sqrt{2})$ e $Q = (3+\sqrt{2})$ del punto precedene soddisfano la richiesta. Infatti si è visto che $P \neq Q$. Inoltre $P \cap \mathbb{Z}$ deve essere un ideale di $\mathbb{Z}$ che ovviamente contiene 7 e se l'intersezione fosse strettamente più grande dell'ideale di $7\mathbb{Z}$ (che è massimale in $\mathbb{Z}$) allora dovrebbe essere tutto $\mathbb{Z}$ e quindi conterrebbe 1, cosa impossibile perché P è un ideale proprio di A. Lo stesso discorso vale anche per Q

e quindi si ha che $P \cap \mathbb{Z} = Q \cap \mathbb{Z} = 7\mathbb{Z}$.
Osservo che si poteva rispondere alla domanda senza esibire gli ideali esplicitamente: chiamo P e Q i due ideali propri trovati al punto precedente. Le loro immagini nel quoziente sono $\mathbb{F}_7 \times \{0\}$ e $\{0\} \times \mathbb{F}_7$, quindi sono ideali primi perchè danno come quoziente il campo $\mathbb{F}_7$. Ne segue che P e Q sono massimali. La loro contrazione a $\mathbb{Z}$ sarà un ideale primo che contiene 7, quindi entrambi si contraggono a $7\mathbb{Z}$.

4. Siano $\alpha, \beta \in A$ tali che $\alpha\beta \in 5A$. Allora $5 \mid N(\alpha\beta)$ e quindi a meno di scambiare α e β possiamo supporre che $5 \mid N(\alpha)$, ovvero $\alpha = a + \sqrt{2}b$ e $a^2 - 2b^2 \equiv 0 \mod 5$. Tuttavia i quadrati modulo 5 sono solo $0, 1, 4$ e il doppio di un quadrato modulo 5 può essere solo $0, 2, 3$. Perché la relazione sia verificata occorre dunque che $a \equiv b \equiv 0 \mod 5$, ovvero $\alpha \in 5A$.

Esercizio 4. Sia $a \in \mathbb{Z}$ e sia $f_a(x) = (x^{11} - 1)(x^3 - a)$. Denotiamo con K_a il campo di spezzamento del polinomio f_a su $\mathbb{Q}$. Determinare al variare di a:

1. il gruppo di Galois di K_a su $\mathbb{Q}$;
2. il numero delle sottoestensioni E di K_a normali su $\mathbb{Q}$ tali che $\mathrm{Gal}(E/\mathbb{Q})$ è abeliano.

Soluzione.

1. Indichiamo, come al solito, con ζ_n una radice n-esima primitiva dell'unità. Si ha che in $\mathbb{C}$ vale

$$x^{11} - 1 = \prod_{i=0}^{10}(x - \zeta_{11}^i) \text{ e } x^3 - a = (x - \sqrt[3]{a})(x - \zeta_3\sqrt[3]{a})(x - \zeta_3^2\sqrt[3]{a}),$$

quindi se $a \neq 0$ $K_a = \mathbb{Q}(\zeta_{11}, \zeta_3, \sqrt[3]{a})$, mentre per $a = 0$ si ottiene $K_0 = \mathbb{Q}(\zeta_{11})$. Osserviamo anche che dalle uquaglianze $\zeta_{33}^3 = \zeta_{11}$, $\zeta_{33}^{11} = \zeta_3$ e $\zeta_{11}^4\zeta_3^{-1} = \zeta_{33}$ si ottiene che $\mathbb{Q}(\zeta_{11}, \zeta_3) = \mathbb{Q}(\zeta_{33})$.

Consideriamo dapprima il caso $\underline{a = 0:}$ il gruppo di Galois richiesto è noto dalla teoria ed è $\mathrm{Gal}(\mathbb{Q}(\zeta_{11}/\mathbb{Q}) \cong (\mathbb{Z}/11\mathbb{Z})^*$.
Supponiamo nel seguito $a \neq 0$. Dalla teoria sappiamo che $[\mathbb{Q}(\zeta_{33}) : \mathbb{Q}] = \Phi(33) = 20$. Inoltre $[\mathbb{Q}(\sqrt[3]{a}) : \mathbb{Q}] = 1$ se a è un cubo in $\mathbb{Z}$, mentre $[\mathbb{Q}(\sqrt[3]{a}) : \mathbb{Q}] = 3$ se non lo è: infatti se $\sqrt[3]{a} \notin \mathbb{Q}$ (o equivalentemente $\sqrt[3]{a} \notin \mathbb{Z}$), allora il polinomio $x^3 - a$ non ha radici razionali (le altre due radici di $x^3 - a$ sono non reali e quindi sicuramente non razionali), e, avendo grado 3, è irriducibile. Ne segue che in questo caso $x^3 - a$ è il polinomio minimo di $\sqrt[3]{a}$.

Se $\underline{a \text{ è il cubo di un intero} \neq 0}$ abbiamo quindi che $K_a = \mathbb{Q}(\zeta_{33})$ e

$$\mathrm{Gal}(K_a/\mathbb{Q}) \cong (\mathbb{Z}/33\mathbb{Z})^* \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Se invece $\underline{a \text{ non è un cubo}}$ in $\mathbb{Z}$, poichè $(20, 3) = 1$ otteniamo che $[K_a : \mathbb{Q}] = 60$ e la teoria assicura che

$$\mathrm{Gal}(K_a/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{11}/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{a}) \cong \mathbb{Z}/10\mathbb{Z} \times S_3.$$

2. Le sottoestensioni E normali su $\mathbb{Q}$ sono quelle fissate da sottogruppi normali H di $\mathrm{Gal}(K_a/\mathbb{Q})$ e si ha che $\mathrm{Gal}(E/Q) \cong \mathrm{Gal}(K_a/\mathbb{Q})/H$ è abeliano se e solo se H contiene il derivato di $\mathrm{Gal}(K_a/\mathbb{Q})$.

   Se $\underline{a = 0}$ $\mathrm{Gal}(\mathbb{Q}(\zeta_{11}/\mathbb{Q}) \cong (\mathbb{Z}/11\mathbb{Z})^* \cong \mathbb{Z}/10\mathbb{Z}$ ed essendo ciclico ha solo sottogruppi normali con quoziente ciclico. I sottogruppo di $\mathbb{Z}/10\mathbb{Z}$ sono tanti quanti i divisori di 10, cioè 4 e quindi le sottoestensioni ceracte sono 4.

   Se $\underline{a \text{ è un cubo} \neq 0,}$ $\mathrm{Gal}(K_a/\mathbb{Q}) \cong (\mathbb{Z}/33\mathbb{Z})^* \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, quindi tutti i suoi sottogruppi sono normali e tutti i suoi quozienti sono abeliani: dobbiamo quindi contare tutte le sottoestensioni o , equivalentemente, tutti i sottogruppi di $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. È semplice vedere che ci sono un unico sottogruppo di ordine 1, 3 sottogruppi di ordine 2, 1 di ordine 4 (il 2-Sylov) 1 di ordine 5 (il 5-Sylow), 3 di ordine 10 (ci sono vari modi per contarli: posso osservare che sono ciclici e contare gli elementi di ordine 10, che sono 12, e dividere per $\Phi(10) = 4$, oppure notare che i ogni sottogruppo di ordine 10 deve contenere il 5-Sylow e quindi ce ne sono tanti quanti i sottogruppi di ordine 2 del quoziente modulo il 5-Sylow che è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) e 1 di ordine 20. In totale sono quindi 1+3+1+1+3+1=10.

   Se $\underline{a \text{ non è un cubo}}$ $\mathrm{Gal}(K_a/\mathbb{Q}) \cong \mathbb{Z}/10\mathbb{Z} \times S_3$ che ha come sottogruppo derivato $\{\bar{0}\} \times A_3$. Le sottoestensioni cercate sono quindi tante quanti i sottogruppi di $(\mathbb{Z}/10\mathbb{Z} \times S_3)/(\{\bar{0}\} \times A_3) \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, e abbiamo già visto che sono 10.