SOLUZIONI DEL COMPITO DI ALGEBRA 1

23 gennaio 2018

Esercizio 1. Sia p un primo e sia $\tau \in S_{3p}$ il prodotto di 3 p-cicli disgiunti.

1. Determinare, al variare di p, il numero delle soluzioni $\sigma \in S_{3p}$ dell'equazione $\sigma^p = \tau$.
2. Sia $p \geq 3$. Mostrare che S_{3p} ha un sottogruppo H isomorfo al gruppo diedrale D_p tale che $\tau \in H$.

Soluzione.

1. Sappiamo che in generale se α è un m-ciclo, fissato un intero n e detto d il massimo comune divisore di m e n, se scriviamo $m = dm'$ abbiamo che α^n è un prodotto di d m'-cicli disgiunti. In particolare un prodotto τ di 3 p-cicli disgiunti in S_{3p} può essere ottenuto solo come potenza p-esima di σ un $3p$-ciclo. Infatti σ deve essere sicuramente prodotto di cicli disgiunti di lunghezza multipla di p. Tuttavia un p-ciclo elevato alla potenza p è una permutazione banale e quindi σ non può essere prodotto di un p-ciclo e un $2p$-ciclo. Un $3p$-ciclo elevato alla p è un prodotto di p 3-cicli disgiunti. L'equazione $\sigma^p = \tau$ si può quindi risolvere se e solo se $p = 3$.

   Supponiamo dunque $p = 3$ e, a meno di riordinare gli elementi da 1 a 9, sia $\tau = (1\,2\,3)(4\,5\,6)(7\,8\,9)$. Possiamo scrivere il 9 ciclo σ fissando come primo elemento 1: $\sigma = (1\,b_1\,c_1\,a_2\,b_2\,c_2\,a_3\,b_3\,c_3)$. Abbiamo che $\sigma^3 = (1\,a_2\,a_3)(b_1\,b_2\,b_3)(c_1\,c_2\,c_3)$ e dunque, deve essere $a_2 = 2, a_3 = 3$. Per b_1 abbiamo 6 scelte (può essere 4,5,6,7,8,9) e a questo punto b_2 e b_3 sono fissati perché sono, nell'ordine, glia ltri due elementi del 3-ciclo di b_2. Per c_1 rimangono 3 possibilita' (gli elementi dell'unico 3 ciclo non scelto) e la scelta di c_1 determina quelle di c_2 e c_3. Quindi per $p = 3$ abbiamo 18 soluzioni.

2. A meno di rinumerare gli elementi da 1 a $3p$ possiamo supporre

$$\tau = (1\,2\,\cdots\,p)(p+1\,\cdots\,2p)(2p+1\,\cdots\,3p).$$

   Si ha che τ ha ordine p ed è coniugato in S_{3p} con τ^{-1} tramite una permutazione ρ di ordine 2. Infatti ogni p-ciclo è coniugato con il suo inverso tramite una permutazione di ordine 2 che sposta solo alcuni degli elementi spostati dal p-ciclo e nessun altro. Infatti $(1\,2\,\cdots\,p)$ è coniugato con $(1\ p\ p–1\ \cdots\ 2)$ tramite la permutazione $(2\ p)(3\ p–1)\cdots(\frac{p-1}{2}\ \frac{p+1}{2})$.

   Possiamo quindi considerare il sottogruppo $H = \langle \tau, \rho \rangle$: per dimotrare che H è isomorfo a D_p basta osservare che $H \cong \langle \tau \rangle \rtimes_\psi \langle \rho \rangle$ dove $\psi_\rho(\tau) = \tau^{-1}$.

Esercizio 2. Sia G un gruppo di ordine 1045.

1. Dimostrare che il 19 Sylow di G è contenuto nel centro e determinare i possibili valori della cardinalità di $Z(G)$.

2. Mostrare che esiste un omomorfismo non banale $f\colon G \to \mathbb{Z}/154\mathbb{Z}$ se e solo se G è ciclico.

Soluzione:

1. $1045 = 19 \cdot 11 \cdot 5$; indichiamo con P, Q, R rispettivamente il 19-Sylow, l'11-Sylow e il 5-Sylow di G e con $p, q, r \in G$ i loro generatori (i Sylow sono ciclici perché hanno ordine primo). Il Teorema di Sylow garantisce che $P \triangleleft G$, infatti il numero dei 19-Sylow n_{19} è un divisore di 55 ed è congruo a 1 modulo 19, quindi $n_{19} = 1$. Da questo segue che $H = PQ$ e $K = PR$ sono sottogruppi di G. Inoltre $|H| = 19 \cdot 11$ e $|K| = 19 \cdot 5$, quindi entrambi sono gruppi ciclici per la teoria svolta, in quanto $11 \nmid 19 - 1$ e $5 \nmid 19 - 1$. Da questo segue che gli elementi del gruppo P commutano sia con gli elementi di Q che con gli elementi di R, cioè $P, Q, R \subseteq Z(P)$ da cui $Z(P) = G$ e $P \subseteq Z(G)$.

   Da questa relazione, usando il fatto che se G non è abeliano allora $G/Z(G)$ non è ciclico, si ottiene che $Z(G) = G$ oppure, se G non è abeliano, $Z(G) = P$. Per mostrare che entrambi i casi si verificano, occorre esibire un gruppo non abeliano di ordine 1045. Per questo consideriamo il gruppo $G = \mathbb{Z}/209\mathbb{Z} \rtimes_\varphi \mathbb{Z}/5\mathbb{Z}$ dove $\varphi\colon \mathbb{Z}/5\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/209\mathbb{Z})$ è un omomorfismo. Il gruppo G così costruito è non abeliano se e solo se φ è non banale. Osserviamo che $\mathrm{Aut}(\mathbb{Z}/209\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}/19\mathbb{Z}) \times \mathrm{Aut}(\mathbb{Z}/11\mathbb{Z}) \cong (\mathbb{Z}/19\mathbb{Z})^* \times (\mathbb{Z}/11\mathbb{Z})^*$ è un gruppo di ordine 180 e quindi contiene elementi di ordine 5. Ne segue che, se definiamo $\varphi(\bar{1}) = \beta$ dove β è un automorfismo di $\mathbb{Z}/209\mathbb{Z}$ di ordine 5, si ottiene un gruppo non abeliano, che quindi ha centro di ordine 19.

2. Se esiste un omomorfismo $f\colon G \to \mathbb{Z}/154\mathbb{Z}$, allora $G/\ker(f)$ è isomorfo ad un sottogruppo di $\mathbb{Z}/154\mathbb{Z}$ e, dato che $154 = 11 \cdot 7 \cdot 2$, se f è non banale l'unica possibilità è $|G/\ker(f)| = 11$.

   Se G è ciclico generato da un suo elemento g possiamo definire f mandando g in un elemento di ordine 11 di $\mathbb{Z}/154\mathbb{Z}$, ad esempio nella classe di 14. Viceversa, se esiste f allora $K = \ker(f)$ è un sottogruppo normale di G di ordine $5 \cdot 19$ e, per motivi di ordine, è ciclico. Ne segue che $G \cong K \rtimes_\psi Q$, con $\psi\colon Q \to \mathrm{Aut}(K)$. Ma poiché Q ha ordine 11 che è coprimo con l'ordine di $\mathrm{Aut}(K)$ che è $\Phi(5) \cdot \Phi(19)$, si ottiene che l'unica possibilità è che ψ sia l'omomorfismo banale, cioè $G \cong K \times Q \cong \mathbb{Z}/95\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \cong \mathbb{Z}/1045\mathbb{Z}$.

Esercizio 3. Sia A un anello commutativo con identità. Un ideale proprio Q di A si dice *primario* se

$$\forall x, y \in A \text{ tali che } xy \in Q \text{ e } \ x \notin Q \Rightarrow y^n \in Q \text{ per qualche } \ n \in \mathbb{N}.$$

1. Mostrare che un ideale Q di A è primario se e solo se in A/Q ogni divisore di zero è nilpotente.

2. Determinare gli ideali primari di $\mathbb{Z}[i]$ e quelli di $\mathbb{Z} \times \mathbb{Z}$.

Soluzione:

1. In A/Q ogni divisore di zero è nilpotente se e solo se $\forall \bar{x}, \bar{y} \in A/Q$ tali che $\bar{x} \neq \bar{0}$ e $\bar{x}\bar{y} = \bar{0}$ si ha $\bar{y}^n = -\bar{0}$ per qualche n. Questo è equivalente a dire che $\forall x, y \in A$ tali che $xy \in Q$ e $x \notin Q$ si ha che $y^n \in Q$ per qualche n, cioè Q è primario.

2. Ideali primari di $\mathbb{Z}[i]$: E' immediato vedere che (0) è un ideale primario di $\mathbb{Z}[i]$ in quanto $\mathbb{Z}[i]$ non contiene divisori di zero. Sia $I = (\alpha)$ un ideale proprio di $Z[i]$ (ricordiamo che $\mathbb{Z}[i]$ è un dominio euclideo e quindi anche PID e UFD). Se $\alpha = \beta\gamma$ con β e γ non invertibili e coprimi, allora $\beta\gamma \in I$ ma $\beta \notin I$ e $\gamma^n \notin I$ per ogni n perché $\alpha \nmid \gamma^n$. In questo caso I non è primario. Se invece α non ha due fattori non invertibili coprimi, allora $\alpha = \pi^k$ con π irriducibile in $\mathbb{Z}[i]$. In questo caso, siano $x, y \in \mathbb{Z}[i]$ tali che $x \notin I$ e $xy \in I$: questo vuol dire che $\pi^k \nmid x$ e $\pi^k \mid xy$ da cui si ha che necessariamente $\pi \mid y$ e quindi $y^k \in I$. Gli ideali primari di $\mathbb{Z}[i]$ sono quindi (0) e quelli generati da potenze di elementi irriducibili.
   Ideali primari di $\mathbb{Z} \times \mathbb{Z}$: ricordiamo che gli ideali di un prodotto diretto di anelli sono i prodotti degli ideali dei fattori, quindi gli ideali di $\mathbb{Z}\times\mathbb{Z}$ sono del tipo $m\mathbb{Z}\times n\mathbb{Z}$ e il quoziente è $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Se entrambi i fattori sono non banali l'ideale non è primario perché $(\bar{1}, \bar{0})$ è un divisore di zero ma non è nilpotente. Consideriamo quindi gli ideali del tipo $m\mathbb{Z} \times \mathbb{Z}$ o, simmetricamente, $\mathbb{Z} \times m\mathbb{Z}$: quozientando si ottiene un anello isomorfo a $\mathbb{Z}/m\mathbb{Z}$, che ha come divisori di zeri i divisori di m. Ne segue che i divisori di zero sono tutti nilpotenti se e solo se $m = 0$ o m è la potenza di un primo. Gli ideali primari di $\mathbb{Z} \times \mathbb{Z}$ sono quindi i prodotti di un ideale del tipo $p^k\mathbb{Z}$ con p primo o (0) con tutto l'anello.

Esercizio 4. Sia $p(x) = x^4 - 2x^2 - 10$ e sia E il suo campo di spezzamento su $\mathbb{Q}$.

1. Trovare dei generatori del campo di spezzamento E e calcolare il grado di $E/\mathbb{Q}$.

2. Calcolare $\mathrm{Gal}(E/\mathbb{Q})$.

3. Contare i sottocampi di E e descrivere esplicitamente quelli che sono estensioni di Galois di $\mathbb{Q}$.

Soluzione.

1. Il polinomio $p(x) = x^4 - 2x^2 - 10$ è irriducibile per Eisenstein. Posto $w_1 = \sqrt{1+\sqrt{11}}$ e $w_2 = \sqrt{1-\sqrt{11}}$ abbiamo che $p(x)$ si fattorizza come

$$\begin{aligned} p(x) &= (x^2 - 1 + \sqrt{11})(x^2 - 1 - \sqrt{11}) = \\ &= (x - w_1)(x + w_1)(x - w_2)(x + w_2) \end{aligned}$$

   e dunque il campo di spezzamento è $\mathbb{Q}[w_1, w_2]$. Possiamo notare che le inclusioni

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{11}] \subset \mathbb{Q}[w_1] \subset \mathbb{Q}[w_1, w_2]$$

   hanno tutte grado minore o uguale a 2. Inoltre sono tutte proprie. Infatti: $\sqrt{11}$ non è razionale; $w_1 = \sqrt{1+\sqrt{11}}$ ha grado 4 su $\mathbb{Q}$ in quanto è radice di $p(x)$ che è di grado 4 ed è irriducibile; $\mathbb{Q}[w_1]$ è un campo incluso in $\mathbb{R}$, mentre la radice $w_2 = \sqrt{1-\sqrt{11}}$ non è contenuta in $\mathbb{R}$ in quanto radice di un numero negativo. Il grado dell'estensione complessiva è il prodotto dei gradi e dunque il grado di $E/\mathbb{Q}$ è 8.

2. Il gruppo di Galois G di $E/\mathbb{Q}$ è un gruppo di ordine 8 i cui elementi sono determinati dalla permutazione indotta sulle radici di $p(x)$ e dunque si include in S_4. L'ordine di S_4 è 24 e quindi i suoi 2-Sylow hanno ordine 8 e in particolare G è un suo 2-Sylow. Poiché è possibile includere il gruppo diedrale D_4 in S_4 (ad esempio mandando una rotazione di ordine 4 nel 4-ciclo $(1\,2\,3\,4)$ e una riflessione nella permutazione $(2\,4)$) ne segue che i 2-Sylow di S_4, che sono tutti coniugati tra loro, sono tutti isomorfi a D_4. Quindi G è isomorfo a D_4.

3. I sottocampi di E sono in corrispondenza con i sottogruppi di D_4, che possiamo contare. Poniamo

$$D_4 = \langle \sigma, \tau \mid \sigma^4 = \tau^2 = \tau\sigma\tau\sigma = e \rangle.$$

   I sottogruppi di D_4 sono dunque: $\{e\}$, che ha indice 8, $\langle\tau\rangle$, $\langle\sigma\tau\rangle$ $\langle\sigma^2\tau\rangle$ $\langle\sigma^3\tau\rangle$, $\langle\sigma^2\rangle$, che hanno indice 4, $\langle\sigma\rangle$, $\langle\sigma^2, \tau\rangle$, $\langle\sigma^2, \sigma\tau\rangle$, che hanno tutti indice 2, D_4 stesso. Dunque, contando anche $\mathbb{Q}$ e lo stesso E, i sottocampi di E sono in totale 10.

   Tra i sottogruppi elencati, quelli normali, oltre a quelli banali, sono: $\langle\sigma^2\rangle$, che è il centro di D_4 e $\langle\sigma\rangle$, $\langle\sigma^2, \tau\rangle$, $\langle\sigma^2, \sigma\tau\rangle$, che sono normali in quanto hanno indice 2. I sottogruppi di ordine 2 generati da una riflessione non sono normali in quanto contengono solo una riflessione e l'identità, ma in D_4 tutte le riflessioni sono coniugate

tra loro. Vi sono dunque 4 sottocampi di E (senza contare E e $\mathbb{Q}$) che sono estensioni di Galois di $\mathbb{Q}$. Di questi 3 hanno grado 2 su $\mathbb{Q}$ ed una a grado 4. Notiamo che $w_1 w_2 = \sqrt{-10}$ è contenuto in E, dunque E contiene i sottocampi

$$\mathbb{Q}[\sqrt{11}], \mathbb{Q}[\sqrt{-10}], \mathbb{Q}[\sqrt{-110}], \mathbb{Q}[\sqrt{11}, \sqrt{-10}]$$

che sono tutte estensioni di Galois distinte. Per vederlo possiamo ad esempio osservare che $\sqrt{-10} \notin \mathbb{Q}[\sqrt{11}]$ in quanto $\mathbb{Q}[\sqrt{11}]$ è un'estensione reale di $\mathbb{Q}$, mentre $\sqrt{-10}$ non è reale. Ne segue che $\mathbb{Q}[\sqrt{11}]$ e $\mathbb{Q}[\sqrt{-10}]$ sono estensioni di grado 2 distinte di $\mathbb{Q}$ e dunque anche $\mathbb{Q}[\sqrt{-110}]$ è distinta da entrambe perchè se contenesse una delle due conterrebbe anche il generatore dell'altra. Infine $\mathbb{Q}[\sqrt{11}, \sqrt{-10}]$ è distinta da tutte e tre le precedenti perché essendo generata da due di esse ha grado 4 su $\mathbb{Q}$. Queste quattro sono dunque le estensioni cercate.