COMPITO DI ALGEBRA 1

12 giugno 2018

Esercizio 1a. Sia G un gruppo di ordine $693 = 3^2 \cdot 7 \cdot 11$.

1. Mostrare che G ha sottogruppi abeliani di ordine 77 e di ordine 99.
2. Dire se il centro di G può essere banale e costruire un esempio di un gruppo G non abeliano.

Soluzione:

1. Siano P,Q,R rispettivamente un 3 un 7 e un 11-Sylow. L'11-Sylow è normale in G in quanto è unico, infatti $n_{11} \equiv 1 \pmod{11}$ e $n_{11} | 3^2 \cdot 7$ ha come unica soluzione $n_{11} = 1$. Ne segue che QR è un sottogruppo di G di ordine 77 e PR è un sottogruppo di ordine 99. Tali sottogruppi sono abeliani: infatti, QR è ciclico perché si tratta di un gruppo di ordine pq ($p = 7$ e $q = 11$) con $p \nmid q - 1$. PR è un gruppo di ordine 99 e ha R come sottogruppo normale e quindi è isomorfo ad un prodotto semidiretto di un gruppo di ordine 9 (che quindi è ciclico o isomorfo a $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$) per un gruppo (ciclico) di ordine 11. Dico che il prodotto è diretto. Infatti anche il 3 Sylow è normale in PR in quanto il numero dei 3- Sylow di PR è congruo a 1 modulo 3 ed è un divisore di 11, quindi è 1. In alternativa si poteva mostrare che l'unica possibile azione di P su R è quella banale, osservando che il gruppo degli automorfismi di un gruppo di ordine 11 è ciclico di ordine 10 e in particolare non contiene elementi di ordine 3. Ne segue che il prodotto è diretto. Essendo entrambi i fattori abeliani PR è abeliano.

2. Dal punto precedente si ricava che $Z(G)$ non può essere banale in quanto $R < Z(G)$. Infatti il centralizzatore in G di R contiene sia R che P e Q (gli elementi di R commutano con quelli di P e di Q in quanto i gruppi PR e QR sono abeliani).

   Un gruppo non abeliano di ordine 693 è dato da $\mathbb{Z}/77\mathbb{Z} \rtimes_\varphi \mathbb{Z}/9Z$ dove

   $$\varphi \colon \mathbb{Z}/9\mathbb{Z} \to \mathrm{Aut}(Z/77\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/10\mathbb{Z})^*$$

   è definito da $\phi(\bar{1}) = \gamma$ dove $\gamma \in \mathrm{Aut}(Z/77\mathbb{Z})$ è un elemento di ordine 3. Questo esiste per il teorema di Cauchy in quanto 3 divide $|\mathrm{Aut}(Z/77\mathbb{Z})| = 60$. Possiamo anche esibire γ: infatti $\gamma(\bar{1}) = a$ con $a \neq \bar{1}$ e $a^3 \equiv 1 \pmod{77}$. Per risolvere passiamo al sistema

   $$\begin{cases} a^3 \equiv 1 & \pmod{7} \\ a^3 \equiv 1 & \pmod{11} \end{cases}$$

La prima equazione ha soluzioni $a \equiv 1, 2, 4 \pmod 7$ mentre la seconda ha soluzione solo $a \equiv 1 \pmod{11}$. Una soluzione diversa da 1 è ad esempio $a \equiv 23 \pmod{77}$.

Esercizio 2.

1. Sia $n = pa$, dove p è un primo e $1 \leq a < p$. Calcolare l'ordine di un p-Sylow di S_n e mostrare che un tale sottrogruppo di Sylow è abeliano.

2. Sia H un p-Sylow di S_{2p} per $p > 2$, mostrare che $Z_{S_{2p}}(H) = H$ e calcolare il numero di p-Sylow di S_{2p}.

Soluzione:

1. I p-cicli $(1,\, 2, \cdots p), (p+1,\, p+2, \cdots 2p), \ldots, ((a-1)p+1, (a-1)p+2, \cdots, ap)$ sono disgiunti e quindi commutano tra loro e generano un sottogruppo H di S_{ap} di isomorfo a $(\mathbb{Z}/p)^a$, che dunque è abeliano ed ha cardinalità p^a. Dimostriamo che questo è un p-Sylow. Infatti $(ap)! = ap \cdot (ap-1) \cdots 2 \cdot 1$ è un prodotto i cui fattori divisibili per p sono $ap, (a-1)p, \ldots, 2p, p$. Poichè $a < p$ nessuno di questi fattori è divisibile per p^2 e quindi la massima potenza di p che divide $(ap)!$ è p^a, che è proprio la cardinalità di H.

2. Sia H il gruppo descritto sopra, per $a = 2$. Condizione necessaria e sufficiente perché un elemento σ di S_{2p} appartenga a $Z_{S_{2p}}(H)$ è che σ appartenga al centralizzatore di entrambi i generatori di H: $\tau_1 = (1,\, 2, \cdots p), \tau_2 = (p+1,\, p+2, \cdots 2p)$. Il centralizzatore di τ_1 è il sottogruppo $\langle \tau_1 \rangle \times S_{p+1,\ldots,2p}$. Infatti tutti gli elementi di questo sottogruppo commutano con τ_1 e il suo indice è $\frac{(2p)!}{p \cdot p!}$ è pari al numero di p cicli in S_{2p}. Analogamente il centralizzatore di τ_2 è il sottogruppo $S_{1,2,\ldots,p} \times \langle \tau_2 \rangle$. Dunque $Z_{S_{2p}}(\tau_1) \cap Z_{S_{2p}}(\tau_2) = \langle \tau_1 \rangle \times \langle \tau_2 \rangle = H$.

   Per calcolare il numero di p-Sylow determiniamo prima la cardinalità di $N(H)$. Ogni elemento di $N(H)$ induce, per coniugio, un automorfismo di H. Tuttavia gli automorfismi di H indotti da un elemento di $N(H)$ sono tutti e soli quelli che mandano i due p-cicli τ_1 e τ_2 in altri due p-cicli che generano H. Infatti il coniugio preserva la struttura in cicli e due p-cicli che generano H devono essere necessariamente disgiunti. Infatti i p cicli di H sono tutti e soli gli elementi di $\langle \tau_1 \rangle \cup \langle \tau_2 \rangle \setminus \{e\}$ e due p-cicli che generano H non possono stare nello stesso sottogruppo ciclico. Inoltre qualsiasi coppia di p-cicli disgiunti $\nu_1 = (a_1, \cdots, a_p)$, $\nu_2 = (b_1, \cdots, b_p)$ di H è ottenibile da τ_1, τ_2 tramite il coniugio per un elemento di $N(H)$: basta considerare la permutazione che manda $1 \mapsto a_1, \ldots p \mapsto a_p, p+1 \mapsto b_1, \ldots, 2p \mapsto b_p$. Dunque gli automorfismi di H indotti da un elemento di $N(H)$ sono esattamente $2(p-1)^2$ e poiché il nucleo dell'omomorfismo $N(H) \to \mathrm{Aut}(H)$ è proprio H, segue che l'indice

di H in $N(H)$ è $2(p-1)^2$ e quindi la cardinalità di $N(H)$ è $2p^2(p-1)^2$. Il numero dei p-Sylow, che è pari all'indice di $N(H)$ in S_{2p}, è dunque $\frac{(2p)!}{2p^2(p-1)^2}$.

Esercizio 3. Consideriamo l'anello $A = \mathbb{Z}[x]/(x^3-1)$.

1. Mostrare che A non è un dominio di integrità;
2. Mostrare che A ha un quoziente isomorfo a $\mathbb{Z}$ e uno isomorfo a $\mathbb{Z}[\zeta_3]$, dove ζ_3 è una radice terza primitiva dell'unità.
3. Dare un esempio di un elemento di A che non sia né invertibile né divisore di zero.

Soluzione:

1. L'anello A non è un dominio di integrità, infatti è quoziente dell'anello $\mathbb{Z}[x]$ per l'ideale (x^3-1) che non è un ideale primo in quanto il polinomio $x^3-1 = (x-1)(x^2+x+1)$ non è irriducibile. In alternativa si poteva esibire un divisore di zero non banale: $(\overline{x-1})(\overline{x^2+x+1}) = \overline{x^3-1} = \bar{0}$, ma $\overline{x-1} \neq \bar{0}$ e $\overline{x^2+x+1} \neq \bar{0}$ in quanto $x-1$, e x^2+x+1 non appartengono all'ideale (x^3-1). Questo mostra che $\overline{x-1}$ è un divisore di zero diverso da 0.

2. Dire che A ha un quoziente isomorfo ad un anello B equivale a dire che esiste un omomorfismo surgettivo da A in B, o equivalentemente che esiste un omomorfismo surgettivo da $\mathbb{Z}[x]$ in B il cui nucleo contiene x^3-1.

   Sia $\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}$ l'omomorfismo di sostituzione che manda x in 1 (quindi $p(x) \to p(1)$ per ogni $p(x) \in \mathbb{Z}[x]$). Chiaramente φ è surgettivo e $\varphi(x^3-1) = 1^3-1 = 0$ quindi $x^3-1 \in \ker(\varphi)$.

   Analogamente possiamo definire $\psi\colon \mathbb{Z}[x] \to \mathbb{Z}[\zeta_3]$ mandando x in ζ_3. È evidente che l'omomorfismo è surgettivo perché $\psi(a+bx) = a+b\zeta_3$ e al variare di a, b in $\mathbb{Z}$ questi elementi descrivono tutto $\mathbb{Z}[\zeta_3]$. Inoltre $\psi(x^2+x+1) = 0$, quindi $x^2+x+1 \in \ker(\psi)$.

3. La classe $\overline{x+1}$ non è invertibile, infatti se lo fosse anche la sua immagine mediante un omomorfismo di anelli lo sarebbe, mentre $\varphi(x+1) = 2$ non è inveribile in $\mathbb{Z}$. Inoltre $\overline{x+1}$ non è un divisore di zero perché se $(\overline{x+1})\overline{p(x)} = \bar{0}$ per un certo $\overline{p(x)} \in A$, allora $x^3-1 \mid (x+1)p(x)$ in $\mathbb{Z}[x]$, e quindi in $\mathbb{Q}[x]$. Ma x^3-1 e $x+1$ sono coprimi in $\mathbb{Q}[x]$, quindi $x^3-1 \mid p(x)$ in $\mathbb{Q}[x]$ e anche in $\mathbb{Z}[x]$ per il Lemma di Gauss. Ne segue che $\overline{p(x)} = 0$, quindi $\overline{x+1}$ non è un divisore di zero.

Esercizio 4. Siano $\mathbb{F}$ il campo di spezzamento di x^3-3 ed $\mathbb{K}$ il campo di spezzamento di x^6+3 su $\mathbb{Q}$.

1. Determinare se $\mathbb{F} \subset \mathbb{K}$ e se $\mathbb{K} \subset \mathbb{F}$.

2. Calcolare il gruppo di Galois di $\mathbb{K}$ su $\mathbb{Q}$.

Soluzione:

1. Le radici di $x^3 - 3$ sono $\sqrt[3]{3}, \zeta_3\sqrt[3]{3}, \zeta_3^2\sqrt[3]{3}$ e dunque $\mathbb{F}$ è generato da $\sqrt[3]{3}, \zeta_3$. Analogamente le radici di $x^6 + 3$ sono $\sqrt[6]{-3}, \zeta_6\sqrt[6]{-3}, \ldots, \zeta_6^5\sqrt[6]{-3}$ e dunque $\mathbb{K}$ è generato da $\sqrt[6]{-3}, \zeta_6$. Notiamo che ζ_3 è radice del polinomio irriducibile $x^2 + x + 1$ e ζ_6 è radice di $x^2 - x + 1$, dunque entrambe le radici dell'unità generano su $\mathbb{Q}$ l'estensione quadratica $\mathbb{Q}[i\sqrt{3}] = \mathbb{Q}[\zeta_3] = \mathbb{Q}[\zeta_6]$.

   Vale dunque che $\mathbb{F} = \mathbb{Q}[\sqrt[3]{3}, \zeta_3] = \mathbb{Q}[\sqrt[3]{3}, i\sqrt{3}] = \mathbb{Q}[\frac{i\sqrt{3}}{\sqrt[3]{3}}, i\sqrt{3}]$. Notiamo che $\alpha = \frac{i\sqrt{3}}{\sqrt[3]{3}}$ è una radice di $x^6 + 3$: infatti $\alpha^6 = \frac{-3^3}{3^2} = -3$. Dunque $\alpha \in \mathbb{K}$ e $\mathbb{Q}[\alpha, i\sqrt{3}] = \mathbb{Q}[\alpha, \zeta_6]$ è il campo di spezzamento di $x^6 + 3$ e abbiamo mostrato che $\mathbb{F} = \mathbb{K}$.

2. Il polinomio $x^3 - 3$ è irriducibile su $\mathbb{Q}$ per Eisenstein e pertanto è il polinomio minimo di $\sqrt[3]{3}$. Il campo $\mathbb{F}$ contiene la sottoestensione $\mathbb{Q}[\zeta_3]$ di grado 2 su $\mathbb{Q}$ e la sottoestensione $\mathbb{Q}[\sqrt[3]{3}]$ di grado 3 su $\mathbb{Q}$ (in quanto generata da un elemento il qui polinomio minimo ha grado 3). Dunque $\mathbb{F}$ ha grado 6 su $\mathbb{Q}$ ed il suo gruppo di Galois, che tramite l'azione di permutazione indotta sulle radici di $x^3 - 3$ deve essere isomorfo ad un sottogruppo di S_3, ha ordine 6 ed è pertanto isomorfo all'intero S_3.