SOLUZIONI DEL COMPITO DI ALGEBRA 1

14 luglio 2015

Esercizio 1.

Sia G un gruppo finito; ricordiamo che l'esponente di G è il minimo intero positivo d tale che $x^d = 1\ \forall x \in G$.

a) Dimostrare che l'esponente di G è uguale all' ordine di G se e solo se tutti i sottogruppi di Sylow di G sono ciclici.

b) Dimostrare che se G è abeliano l'esponente di G concide con il massimo ordine di un elemento di G.

Soluzione esercizio 1: Soluzione Esercizio 1.

a) Sia H_p un p-Sylow di G e sia $p^a = |H_p|$ la massima potenza di p che divide l'ordine di G. $\forall g \in H_p$ vale che $g^{p^a} = e$. Inoltre, se H_p è ciclico, sia g_p un generatore di H_p, e dunque g_p di ordine p^a, si ha che

$$g_p^d = e \Leftrightarrow p^a \mid d$$

e dunque p^a divide l'esponente di G. Ne segue che se ogni p-Sylow è ciclico, per ogni primo p che divide l'ordine di G si ha che $|H_p|$ divide l'esponente di G. Sappiamo già dal teorema di Lagrange che $\forall g \in G, g^{|G|} = e$. Dunque, poiché l'ordine di G è il prodotto degli ordini dei suoi p-Sylow, l'esponente di G coincide con l'ordine di G.

Viceversa, supponiamo che l'esponente di G coincida con l'ordine di G. Vogliamo dimostrare che ogni p-Sylow di G è ciclico. Notiamo che l'esponente di G è il minimo comune multiplo degli ordini degli elementi di G. Dunque, per ogni primo p, se p^a divide l'esponente di G, G contiene un elemento g il cui ordine è diviso da p^a e quindi $g^{\mathrm{ord}(g)/p^a}$ è un elemento di ordine p^a. In particolare se p^a è l'ordine di un p-Sylow, G contiene un elementi di ordine p^a e quindi un p-Sylow è ciclico e dunque, poichè sono tutti coniugati tra loro, tutti i p-Sylow sono ciclici.

b) Chiaramente l'ordine di un elemento di G è sempre minore o uguale all'esponente di G.

Per ogni primo p che divide $|G|$, sia $p^{a(p)}$ il massimo ordine di un sottogruppo ciclico del p-Sylow. Vogliamo mostrare che l'esponente di G è

$$\prod_{p|\mathrm{ord}(G)} p^{a(p)}$$

e che questo è anche il massimo ordine di un suo elemento. Poiché G è abeliano, è il prodotto diretto dei suoi sottogruppi di Sylow:

$$G = P_1 \times \cdots \times P_h$$

Dunque ogni elemento $g \in G$ non è altro che il prodotto delle sue componenti nei Sylow

$$g = (g_1, \ldots, g_h)$$

ed il suo ordine è il minimo comune multiplo degli ordini delle sue componenti nei Sylow, e quindi è il prodotto degli ordini delle sue componenti, perché gli ordini sono potenze di primi distinti.
Dunque l'ordine di un elemento $g \in G$ è un divisore di $p_1^{a(p_1)} \cdots p_h^{a(p_h)}$, dove $p_1, \ldots, p_h$ sono i primi che dividono l'ordine di G.
L'ordine $p_1^{a(p_1)} \cdots p_h^{a(p_h)}$ è effettivamente ottenuto se per ogni primo p che divide l'ordine di G scegliamo come g_i un generatore di un sottogruppo ciclico di ordine $p_i^{a(p_i)}$ e prendiamo $g = (g_1, \ldots, g_h)$. Quindi ordine ed esponente di G coincidono e sono pari a $p_1^{a(p_1)} \cdots p_h^{a(p_h)}$.

Esercizio 2.
a) Dimostrare che S_7 non ha sottogruppi abeliani di ordine 16 né di ordine 14.
b) Dimostrare che i possibili ordini di un sottogruppo abeliano di S_7 sono 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12.

Soluzione esercizio 2: (a) Un gruppo abeliano di ordine 14 è ciclico (14 è libero da quadrati) e quindi generato da una permutazione di ordine 14, ma non ne esistono in S_7 (dovrebbe contenere un 14 ciclo o un 7 ciclo e un 2 ciclo disgiunti...impossibile) quindi S_7 non ha sottogruppi abeliani di ordine 14. Un sottogruppo di ordine 16 di S_7 è un suo 2-Sylow: basta quindi mostrare che i 2-Sylow di S_7 non sono abeliani. Questo può essere mostrato in vari modi, ad esempio osservando che S_4 (e quindi anche S_7) ha un sottogruppo isomorfo a D_4 che essendo un 2-gruppo è contenuto in un 2-Sylow, che quindi non può essere abeliano. poiché tutti i 2-Sylow sono coniugati, non ci sono sottogruppi abeliani di ordine 16.
(b) Chiaramente in S_7 esistono sottogruppi ciclici (e quindi abeliani) di ordine m per $m = 1, 2, 3, 4, 5, 6, 7, 10, 12$ che sono generati da permutazioni di ordine m. Possiamo costruire sottogruppi abeliani di ordine 8 e 9, ad esempio $\langle (1,2,3,4), (5,6) \rangle$ e $\langle (1,2,3), (4,5,6) \rangle$ (per giustificare che l'ordine è proprio quello detto occorre osservare che i generatori commutano ....perché?). Vogliamo mostrare che non ci sono altri ordini possibili.
Osserviamo che, dato che S_7 non ha sottogruppi abeliani di ordine 16, non ne ha neppure di ordine multiplo di 16. Inoltre se H è un sottogruppo abeliano di S_7 e $7 \mid |H|$ allora H contiene un 7-ciclo σ e $H \subseteq Z_{S_7}(\sigma)$; poichè $|Z_{S_7}(\sigma)| = 7$ ne segue che $|H| = 7$. Analogamente se $5 \mid |H|$ allora H deve essere contenuto ne centralizzatore di un 5-ciclo che ha ordine 10, quindi H può avere ordine 5 o 10 che sono ordini già considerati.
Mettendo insieme tutte le informazioni ottenute e il fatto che $|S_7| = 2^4 \cdot 3^2 \cdot 5 \cdot 7$ abbiamo che rimangono da considerare i possibili ordini $2^3 \cdot 3, , 2 \cdot 3^2, 2^2 \cdot 3^2, 2^3 \cdot 3^2$. Osserviamo che non esistono sottogruppi abeliani di ordine 18 (e quindi neppure di ordine 36 e 72): infatti un tale sottogruppo se esistesse sarebbe contenuto nel centralizzatore di una permutazione τ di ordine 2 (2 ciclo , 2+2 ciclo oppure 2+2+2 ciclo) ma un calcolo diretto mostra che $9 \nmid |Z_{S_7}(\tau)|$. Rimane da considerare il caso di sottogruppi di ordine 24 e questi si possono escludere osservando che un gruppo abeliano di ordine 24 deve contenere un elemento γ di ordine 6, cioè un 6-ciclo oppure una permutazione di tipo 3+2, e dovrebbe essere contenuto nel suo centralizzatore, ma in entrambi i casi si ha che $24 \nmid |Z_{S_7}(\gamma)|$.

Esercizio 3.
a) Descrivere l'insieme degli interi a per cui l'ideale $I = (7, x^2 + a)$ è primo in $\mathbb{Z}[x]$.
b) Indichiamo con S la parte moltiplicativa $\mathbb{Z}[x] - (7, x^2 + 4)$. Per quali valori del parametro $\lambda \in \mathbb{Z}$ il polinomio $f_\lambda(x) = x^4 + \lambda x^2 + 5$ è invertibile in $S^{-1}\mathbb{Z}[x]$?

Soluzione esercizio 3: a) L'ideale $I = (7, x^2 + a)$ è primo se e solo se $\mathbb{Z}[x]/I$ è un dominio. Scriviamo $\mathbb{Z}_7$ per indicare l'anello quoziente $\mathbb{Z}/7\mathbb{Z}$. Poichè

$$\mathbb{Z}[x]/(7, x^2 + a) \cong \mathbb{Z}_7[x]/(x^2 + a)$$

allora I è primo in $\mathbb{Z}[x]$ se e solo se (x^2+a) è primo in $\mathbb{Z}_7[x]$. Poiché $\mathbb{Z}_7[x]$ è PID, l'ideale (x^2+a) è primo se e solo se $x^2 + a$ è irriducibile, ovvero se $-a$ non è un quadrato in $\mathbb{Z}_7$. I quadrati in $\mathbb{Z}_7$ sono $0, 1, 2, 4$, (e i loro opposti sono $0, 3, 5, 6$) e quindi I è primo se è solo se a è congruo modulo 7 ad uno dei seguenti numeri: $1, 2, 4$.
b) Osserviamo che l'anello $\mathbb{Z}[x]$ è un dominio, I è un ideale primo e S non contiene 0. Dunque il polinomio $f_\lambda(x)$ è invertibile in $S^{-1}\mathbb{Z}[x]$ se e solo se esiste $\alpha/\beta \in S^{-1}\mathbb{Z}[x]$ tale che $f_\lambda(x)\alpha/\beta = 1$, ovvero ($\mathbb{Z}[x]$ è un dominio)

$$f_\lambda(x)\alpha = \beta, \text{ con } \beta \in S$$

ovvero $f_\lambda(x)\alpha \notin I$ e poiché I è primo, questo vale se e solo se $f_\lambda(x) \notin I$. Quest'ultimo fatto equivale a dire che $f_\lambda(x) \neq 0$ in $\mathbb{Z}[x]/I$ ovvero $f_\lambda(x) \neq 0$ in $\mathbb{Z}_7[x]/(x^2+4)$ ovvero $(-4)^2+\lambda(-4)+5 \neq 0$ in $\mathbb{Z}_7$. Quest'ultima disuguaglianza è equivalente a

$$21 \not\equiv 4\lambda \pmod 7$$

ovvero

$$\lambda \not\equiv 0 \pmod 7.$$

Esercizio 4.
Sia $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{2})$.
a) Determinare un elemento primitivo di $K/\mathbb{Q}$.
b) Sia L la più piccola estensione di K che è normale su $\mathbb{Q}$. Determinare il gruppo di Galois di $L/\mathbb{Q}$.

Soluzione esercizio 4: a): Il polinomio minimo di $\sqrt[3]{2}$ su $\mathbb{Q}$ è $x^3 - 2$ e quello di $\sqrt{2}$ è $x^2 - 2$ (entrambi sono irriducibili per il criterio di Eisenstein): ne segue che $K/\mathbb{Q}$ è il composto di una sua sottoestensione di grado 3 e di una di grado 2, quindi $6 \mid [K : \mathbb{Q}] \leq 6$ cioè ha grado 6. Dico che l'elemento $\alpha = \sqrt[6]{2}$ è un generatore di $K/\mathbb{Q}$. Infatti, $\alpha = \sqrt{2}/\sqrt[3]{2} \in K$, inoltre ha grado 6 in quanto il suo polinomio minimo è $x^6 - 2$ (è di Eisenstein rispetto a $p = 2$), quindi $K = \mathbb{Q}(\alpha)$.
b) La più piccola estensione L di K che sia normale su $\mathbb{Q}$ coincide con il campo di spezzamento dei generatori di K su $\mathbb{Q}$ (e quindi di α): infatti un'estensione normale contiene il campo di spezzamento dei polinomi minimi di tutti gli elementi e, viceversa, un campo di spezzamento è un'estensione normale. Questo assicura che $L = \mathbb{Q}(\{\sqrt[6]{2}\zeta_6^i\}_{i=0,\dots,5}) = \mathbb{Q}(\sqrt[6]{2}, \zeta_6)$ (vanno verificati

i due contenimenti). Costruiamo gli elementi del gruppo di Galois di $L/\mathbb{Q}$: sia $\varphi \in \mathrm{Gal}(L\mathbb{Q})$, allora $\varphi(\sqrt[6]{2}) = \sqrt[6]{2}\zeta_3^i$ e $\varphi(\zeta_6) = \zeta_6^j$ con $i \in \{0, 1, \ldots, 5\}$e $(j, 6) = 1$: chiamiamo tale elemento γ_{ij}. Allora $\mathrm{Gal}(L/\mathbb{Q}) = \langle \gamma_{1,1}, \gamma_{0,5} \rangle$ (come si scrive il generico γ_{ij} in termini dei generatori?). Per verifica diretta si prova che $\gamma_{1,1}$ ha ordine 6, $\gamma_{0,5}$ ha ordine 2 e che $\gamma_{0,5}\gamma_{ij}\gamma_{0,5} = \gamma_{ij}^{-1}$. Ne segue che $\mathrm{Gal}(L/\mathbb{Q}) \cong D_6$ (in questa dimostrazione ho tralasciato un po' di dettagli in quanto sono stati visti a lezione)