SOLUZIONI DEL COMPITO DI ALGEBRA 1

12 giugno 2015

Esercizio 1.
Sia G un gruppo finito e sia $G' = [G, G]$ il suo sottogruppo dei derivati.
a) Mostrare che se M è un sottogruppo massimale di G allora

$$Z(G) \leq M \text{ oppure } G' \leq M.$$

b) Dare un esempio di un gruppo non abeliano G e di un suo sottogruppo massimale M tale che $G' \subseteq M$ e $Z(G) \not\subset M$.

Soluzione esercizio 1: a) Sappiamo che per ogni sottoguppo H di G, $Z(G)H$ è un sottogruppo di G (in quanto il centro è un sottogruppo normale) che contiene H. In particolare, se M è un sottogruppo massimale di G, dalla relazione $M \subseteq Z(G)M \subseteq G$ si ha che $M = Z(G)M$ oppure $Z(G)M = G$. Chairamente $M = Z(G)M$ se e solo se $Z(G) \subseteq M$, quindi se $Z(G) \not\subset M$ vale $Z(G)M = G$. In questo caso vogliamo mostrare che $G' \subseteq M$ e per questo basta verificare che per ogni $x, y \in G$ il commutatore di x, y appartiene a M. Poché $G = Z(G)M$ si ha $x = zm$ e $y = wn$ con $z, w \in Z(G)$ e $m, n \in M$: si ha $xyx^{-1}y^{-1} = zmwn(zm)^{-1}(wn)^{-1} = mnm^{-1}n^{-1} \in M$.
b) Sia $G = \mathcal{S}_3 \times \mathbb{Z}/2\mathbb{Z}$, allora $Z(G) = \{id\} \times \mathbb{Z}/2\mathbb{Z}$ e $G' = (\mathcal{S}_3)' \times (\mathbb{Z}/2\mathbb{Z})' = \mathcal{A}_3 \times \{0\}$. Allora il sottogruppo $M = \mathcal{S}_3 \times \{0\}$ è massimale ($G/M \cong \mathbb{Z}/2\mathbb{Z}$) e verifica quanto richesto.

Esercizio 2.
a) Mostrare che $\mathrm{SL}_2(\mathbb{F}_5)$ contiene un sottogruppo isomorfo a Q_8
b) Dimostrare che S_5 non è isomorfo a $\mathrm{SL}_2(\mathbb{F}_5)$.

Soluzione esercizio 2:
a) L'elemento i in Q_8 ha ordine 4 e non è centrale, mentre il suo quadrato è centrale. Notiamo che gli elementi 2 e 3 in $\mathbb{F}_5$ hanno ordine moltiplicativo 4 e quindi la matrice diagonale

$$A_i := \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$$

ha ordine 4 (ed inoltre non è centrale in $\mathrm{SL}_2(\mathbb{F}_5)$, mentre il suo quadrato, che è $-\mathrm{Id}$, è centrale). Il normalizzatore di A_i in $\mathrm{SL}_2(\mathbb{F}_5)$ è costituito da matrici diagonali (che dunque commutano con A_i) e da matrici della forma

$$\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$$

Tra queste abbiamo

$$A_j := \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$$

di ordine 4, con quadrato $-\mathrm{Id}$. Inoltre

$$A_i \cdot A_j = \begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix}$$

che di nuovo ha ordine 4 ed ha quadrato $-\mathrm{Id}$, dunque poniamo $A_k := A_i \cdot A_j$. Si vede che le matrici A_i, A_j, A_k soddisfano le stesse relazioni di i, j, k in Q_8 e dunque A_i e A_j generano un sottogruppo di $\mathrm{SL}_2(\mathbb{F}_5)$ isomorfo a Q_8.
b) Il gruppo S_5 ha ordine 120 e dunque i suoi 2-Sylow hanno ordine 8. In particolare sono tutti coniugati del sottogruppo H generato da $(1,2)$ e $(1,2,3,4)$ che è isomorfo a D_4.
Il gruppo $\mathrm{SL}_2(\mathbb{F}_5)$ ha ordine $24 \cdot 20/4 = 120$ e dunque i suoi 2-Sylow hanno ordine 8. Abbiamo notato in a) che un sottogruppo di $\mathrm{SL}_2(\mathbb{F}_5)$ è isomorfo a Q_8.
I gruppi D_4 e Q_8 non sono isomorfi: infatti Q_8 ha un solo elemento di ordine 2, mentre D_4 ne ha 5. Ne segue che anche S_5 e $\mathrm{SL}_2(\mathbb{F}_5)$ non possono essere isomorfi, perché non sono isomorfi i loro 2-Sylow.

Esercizio 3.
Sia A l'anello $\mathbb{Z}[\sqrt{13}]$.
a) Verificare che $18 + 5\sqrt{13}$ invertibile e che A^* é infinito.
b) Verificare che gli elementi $2, 3 + \sqrt{13}$ sono irriducibili in A.
c) Dimostrare che l'anello A non è a fattorizzazione unica.

Soluzione esercizio 3:
a) Consideriamo in A il coniugio

$$A \ni u = a + b\sqrt{13} \mapsto \overline{u} = a - b\sqrt{13} \in A.$$

Questo è un automorfismo dell'anello A. Possiamo quindi definire la norma

$$A \ni u = a + b\sqrt{13} \mapsto a^2 - 13b^2 \in \mathbb{Z}.$$

Poiché il coniugio è un automorfismo è facile vedere che $N(uv) = N(u)N(v)$ per ogni $u, v \in A$. Si può facilmente calcolare che $N(18+5\sqrt{13}) = -1$ e dunque, posto $w = 18+5\sqrt{13}$, $w \cdot (-\overline{w}) = 1$ e dunque w è invertibile in A.
Inoltre w è un numero reale maggiore di 1 e quindi tutte le potenze di w sono distinte. Per cui gli elementi della forma w^n, $-w^n$, per $n \in \mathbb{Z}$ sono tutti distinti e invertibili. Ne segue che A^* è infinito.
b) Notiamo che $N(2) = 4$ e $N(3+\sqrt{13}) = -4$. Dunque se 2 o $3+\sqrt{13}$ fossero riducibili dovrebbe esistere un elemento di A con norma 2. Sia $u = a + b\sqrt{13}$ e supponiamo $N(u) \equiv 0 \pmod 2$. Allora $a^2 \equiv b^2 \pmod 2$ e dunque a e b sono entrambi pari o entrambi dispari. In entrambi i casi si ha che $a^2 \equiv b^2 \pmod 4$. Inoltre $13 \equiv 1 \pmod 4$ e quindi $4 \mid N(u) = a^2 - 13b^2$. Quindi non può esistere un elemento di A di norma 2 e dunque $2, 3 + \sqrt{13}$ sono irriducibili in A.
c) Vale l'uguaglianza

$$2^2 = (3 + \sqrt{13})(-3 + \sqrt{13}) = 4.$$

Tuttavia per il punto b) tutti i fattori sono irriducibili e 2 non è associato a $3+\sqrt{13}$ (infatti tutti gli elementi di A associati a 2 devono essere della forma $u = a + b\sqrt{13}$ con a e b pari).

Esercizio 4.
Sia K il campo di spezzamento su $\mathbb{Q}$ del polinomio $f(x) = x^5 - 5$.
a) Determinare il grado di $K/\mathbb{Q}$.
b) Determinare tutte le sottoestensioni di $K/\mathbb{Q}$ individuando quelle normali su $\mathbb{Q}$.

Soluzione esercizio 4: Le radici del polinomio $f(x)$ sono $\sqrt[5]{5}\zeta_5^i$ per $i = 0, 1, 2, 3, 4$, il campo di spezzamento è quindi $K = \mathbb{Q}(\sqrt[5]{5}\zeta_5^i \,|\, i = 0, 1, 2, 3, 4) = \mathbb{Q}(\sqrt{5}, \zeta_5)$. Osserviamo che:
• $[\mathbb{Q}(\sqrt[5]{5}) : \mathbb{Q}] = 5$, infatti $f(x)$ è irriducibile per il criterio di Eisenstein applicato con $p = 5$, quindi è il polinomio minimo di $\sqrt[5]{5}$.
• $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$, perché sappiamo che il polinomio minimo di ζ_5 è $\frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1$.
Poiché $\mathbb{Q}(\sqrt[5]{5}), \mathbb{Q}(\zeta_5) \subset K$ dalla regola del grado nelle torri si ha che sia 5 che 4 dividono $[K : \mathbb{Q}]$, quindi $20 \,|\, [K : \mathbb{Q}]$. D'altra parte il grado di ζ_5 su $\mathbb{Q}(\sqrt[5]{5})$ è chiaramente minore o uguale al suo grado su $\mathbb{Q}$ che è 4, quindi $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[5]{5})][\mathbb{Q}(\sqrt[5]{5}) : \mathbb{Q}] \leq 20$ e quindi otteniamo $[K : \mathbb{Q}] = 20$.
Sia $G = \mathrm{Gal}(K/\mathbb{Q})$; usando il teorema di corrispondenza di Galois, dall'analisi delle sottoestensioni si ottiene che G ha un sottogruppo normale N di ordine 5 (quello che fissa $\mathbb{Q}(\zeta_5)$): N è l'unico 5-Sylow di G e $G/N \cong \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$. Da questo segue che i 2-Sylow di G sono ciclici e quindi isomorfi a $\mathbb{Z}/4\mathbb{Z}$ (se ci sono elementi di ordine 4 nel quoziente, a maggior ragione ce ne sono in G). Se indichiamo con S un 2-Sylow si ha che G è un prodotto semidiretto di N e di S ed è quindi isomorfo a $\mathbb{Z}/5\mathbb{Z} \rtimes_\psi \mathbb{Z}/4\mathbb{Z}$ per un opportuno ψ. Descriviamo ora le sottoestensioni dividendole per grado e usando il teorema di corrispondenza:
• Ci sono le sottoestensioni banali $\mathbb{Q}$ e K che sono di Galois.
• Le sottoestensioni di ordine 4 sono quelle fissate dai sottogruppi di ordine 5, che sono i 5-Sylow di G: di questi ne esiste uno solo, quindi l'unica sottoestensione di grado 4 è $\mathbb{Q}(\zeta_5)$ che è normale.
• Le sottoestensioni di grado 5 sono fissate dai sottogruppi di ordine 4, cioè dai 2-Sylow: è facile vedere che $n_2 = 5$, quindi ci sono 5 sottoestensioni (tutte non normali) di grado 5 su $\mathbb{Q}$. Poiché le estensioni $\mathbb{Q}(\sqrt[5]{5}\zeta_5^i)$ sono 5 e sono tra loro distinte (se fosse $\mathbb{Q}(\sqrt[5]{5}\zeta_5^i) = \mathbb{Q}(\sqrt[5]{5}\zeta_5^j)$ per $i \neq j$ si avrebbe $\zeta_5 \in \mathbb{Q}(\sqrt[5]{5})$), queste sono esattamente quelle cercate.
• Le sottoestensioni di grado 2 sono fissate da eventuali sottogruppi di ordine 10 di G. Mostramo che ce n'è una sola: un sottogruppo di ordine 10 contiene necessariamente il 5-Sylow N, quindi una sottoestensione di ordine 2 su $\mathbb{Q}$ deve essere contenuta $K^N = \mathbb{Q}(\zeta_5)$: qui di sottoestensioni di grado 2 su $\mathbb{Q}$ c'e solo $\mathbb{Q}(\zeta_5 + \zeta_5^{-1})$ che è di Galois su $\mathbb{Q}$.
• Le sottoestensioni di grado 10 sono fissate da sottogruppi di ordine 2 e di questi ce ne sono 5. Innanzitutto osserviamo che le estensioni $\mathbb{Q}(\zeta_5 + \zeta_5^{-1}, \sqrt[5]{5}\zeta_5^i)$ sono 5 estensioni di grado 10 tutte distinte (che il grado sia 10 è un calcolo immediato, per vedere che sono distinte fraziono come per le estensioni grado 5). Devo dire che non ce ne sono altre, e questo lo ottengo osservando che in G ci sono al più 5 elementi di ordine 2 (infatti ci sono 4 elementi di ordine 5, 10 elementi di ordine 4 e l'identità). Le estensioni trovate non sono normali perché il polinomio $f(x)$ ha un'unica radice in ognuno di tali campi. Infatti un campo che contiene due radici di $f(x)$ deve contenere tutto K.