SOLUZIONI DEL COMPITO DI ALGEBRA 1
7 settembre 2018

Esercizio 1. Determinare i sottogruppi caratteristici del gruppo $G = \mathbb{Z}/9\,\mathbb{Z} \times \mathbb{Z}/15\,\mathbb{Z}$.

Soluzione:
Possiamo riscrivere il gruppo G come prodotto $G = G_3 \times G_5$, dove $G_3 = \mathbb{Z}/3\,\mathbb{Z} \times \mathbb{Z}/9\,\mathbb{Z}$ e $G_5 = \mathbb{Z}/5\,\mathbb{Z}$. Notiamo per prima cosa che G è un gruppo abeliano e dunque prodotto dei suoi sottogruppi di Sylow, i quali sono caratteristici. Ogni sottogruppo di G a sua volta è abeliano e prodotto dei suoi sottogruppi di Sylow, i quali dovranno essere sottogruppi dei Sylow di G.
Sia dunque H un sottogruppo di G, H sarà il prodotto del suo 3-Sylow P_3 e del suo 5-Sylow P_5 e avremo che $P_3 < G_3$ e $P_5 < G_5$.
Poiché G è prodotto di sottogruppi caratteristici (i suoi sottogruppi di Sylow), avremo anche che

$$\mathrm{Aut}(G) = \mathrm{Aut}(G_3) \times \mathrm{Aut}(G_5).$$

Dunque se $H < G$ è un sottogruppo caratteristico di G, esso dovrà essere il prodotto di sottogruppi caratteristici di G_3 e di G_5. Infatti se $H = P_3 \times P_5$ è un sottogruppo caratteristico di G allora per l'azione di $\mathrm{Aut}(G)$ deve essere che anche P_3 e P_5 sono caratteristici nei rispettivi Sylow di G. Viceversa se P_3 è P_5 sono sottogruppi caratteristici di G_3 e di G_5 ne segue per la descrizione di $\mathrm{Aut}(G)$ che anche $P_3 \times P_5$ è caratteristico in G. Descriviamo dunque i sottogruppi caratteristici dei sottogruppi di Sylow di G.
Il gruppo G_3 (che ha ordine 27) ha un unico sottogruppo di ordine 1, ovvero $\{(0,0)\}$, ed un unico sottogruppo di ordine 27, ovvero G_3 stesso, e sono entrambi caratteristici.
Inoltre G_3 ha sottogruppi di ordine 3 e 9. Tra i sottogruppi di ordine 3 abbiamo che $\{0\} \times 3\,\mathbb{Z}/9Z$ è caratteristico in quanto è il nucleo della moltiplicazione per 3. Osserviamo ora che il gruppo G_3 ha il seguente automorfismo non banale:

$$\phi : (a, b) \mapsto (a, 3a + b).$$

Possiamo verificare che la mappa data sopra definisce un automorfismo di G_3 in quanto è ben definita, preserva le somme e l'ordine dei generatori $(1, 0)$ e $(0, 1)$ (questo basta per dire che ϕ è un omomorfismo) e inoltre manda il generatore $(1, 0)$ di ordine 3 al di fuori del sottogruppo generato dall'immagine del generatore $(0, 1)$ di ordine 9. Quindi ϕ è un omomorfismo surgettivo e dunque anche iniettivo. Affermiamo che non ci sono altri sottogruppi caratteristici di ordine 3. Infatti G_3 contiene altri 3 sottogruppi di ordine 3, generati rispettivamente da $(1, 0), (1, 1), (1, 2)$ e ϕ permuta ciclicamente questi elementi e dunque i gruppi che generano non possono essere caratteristici.

Il gruppo G_3 contiene solo 8 elementi di ordine 3. Dunque abbiamo che $\mathbb{Z}_3 \times 3\,\mathbb{Z}/9\,\mathbb{Z}$ è l'unico sottogruppo di ordine 9 non ciclico ed è come tale è caratteristico. Osserviamo ora che il gruppo G_3 ha il seguente automorfismo non banale:

$$\psi : (a, b) \mapsto (a + b, a).$$

Analogamenti a prima la mappa è ben definita e determina un omomorfismo surgettivo e quindi anche iniettivo. Affermiamo che non ci sono altri sottogruppi caratteristici di ordine 9. Infatti G_3 contiene 3 sottogruppi ciclici di ordine 9 generati rispettivamente da $(0, 1)$, $(1, 1)$, $(2, 1)$ e ψ permuta ciclicamente questi elementi. Pertanto i gruppi che generano non sono invarianti.
Il gruppo G_5 è ciclico di ordine primo, quindi non ha sottogruppi non banali. I suoi unici sottogruppi sono $\{0\}$ e $\mathbb{Z}/5\,\mathbb{Z}$ e sono entrambi caratteristici.
Dunque i sottogruppi caratteristici di G sono tutti i possibili prodotto tra un gruppo dell'insieme

$$\{\{(0, 0)\}, 0 \times 3\,\mathbb{Z}/9Z, \mathbb{Z}/3\,\mathbb{Z} \times 3\,\mathbb{Z}/9\,\mathbb{Z}, G_3\}$$

e un gruppo dell'insieme

$$\{\{0\}, G_5\}.$$

Esercizio 2. Diciamo che un gruppo finito G ha una *serie normale* se esiste un insieme $\mathcal{N} = \{N_1, \ldots, N_n\}$ di sottogruppi normali di G tali che vale la serie di inclusioni strette

$$N_0 = \{e\} \subsetneq N_1 \subsetneq N_2 \subsetneq \ldots \subsetneq N_n \subsetneq G = N_{n+1}.$$

Diremo che il gruppo G ha una *serie principale* se ha una serie normale che non puó essere ulteriormente raffinata aggiungendo altri sottogruppi normali di G.

1. Mostrare che ogni serie normale di G può essere raffinata ad una serie principale.

2. Mostrare che se la serie normale $\mathcal{N} = \{N_1, \ldots, N_n\}$ è principale allora i gruppi quozienti N_{i+1}/N_i non hanno sottogruppi caratteristici non banali.

3. Mostrare con un esempio che il viceversa del punto precedente è falso.

Soluzione:

1. Sia $\mathcal{N} = \{N_1, \ldots, N_k\}$ una serie normale di G. Supponiamo che $\mathcal{N}$ non sia principale e mostriamo che è possibile raffinarla ad una serie principale. Infatti se $\mathcal{N}$ non è principale esisteranno almeno due elementi consecutivi $N_i \subsetneq N_{i+1}$ di $\mathcal{N}$ tali che esiste un sottogruppo $N \lhd G$ tale che $N_i \subsetneq N \subsetneq N_{i+1}$. Abbiamo dunque ottenuto una serie la cui lunghezza è strettamente maggiore di quella di $\mathcal{N}$. Tuttavia poiché G è finito e poiché le cardinalità degli elementi di una serie normale di G sono una successione strettamente crescente e limitata da $|G|$ non sarà possibile raffinare arbitrariamente $\mathcal{N}$ e dunque il procedimento dovrà arrestarsi, ovvero arriveremo a raffinare $\mathcal{N}$ ad una serie $\mathcal{P}$ principale.

2. Sia K un sottogruppo caratteristico di N_{i+1}/N_i. Allora K è immagine al quoziente di un sottogruppo N, $N_i \subset N \subset N_{i+1}$. Vogliamo dire che N è un sottogruppo normale di G. Sia $g \in G$ e sia $\varphi_g : G \to G$ il coniugio per g. L'automorfismo φ_g preserva i sottogruppi normali N_i e N_{i+1} e dunque induce un automorfismo $\overline{\varphi}_g$ di N_{i+1}/N_i. Quindi $\overline{\varphi}_g$ manda K, che è carattersitico, in sè stesso e quindi φ_g deve mandare N in sè. Per l'arbitrarietà di g segue che N è normale e quindi, poiché $\mathcal{N}$ era principale $N = N_i$ oppure $N = N_{i+1}$, ovvero K è un sottogruppo caratteristico banale di N_{i+1}/N_i.

3. Consideriamo il gruppo $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

   La serie vuota è chiaramente normale e il quoziente $N_1/N_0 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ non ha sottogruppi caratteristici non banali, tuttavia la serie non è principale in quanto può essere raffinata a

$$\{(0,0)\} \subsetneq \{0\} \times \mathbb{Z}/2\mathbb{Z} \subsetneq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = G.$$

Esercizio 3.

1. Sia $A = \mathbb{Q}[x]$ l'anello dei polinomi in una indeterminata con coefficienti razionali. Sia $I = (x)$ e poniamo $S = A \setminus I$. Mostrare che S è una parte moltiplicativa di A e determinare ideali e ideali primi di $S^{-1}A$.

2. Sia $B = \mathbb{Z}[x]$, sia J l'deale di B generato da x e sia T la parte moltiplicativa $B \setminus J$. Determinare se esiste un isomorfismo da $S^{-1}A$ a $T^{-1}B$.

Soluzione:
(1) Per prima cosa osserviamo che $S^{-1}A = \{f(x)/g(x) \mid f(x), g(x) \in \mathbb{Q}[x],\ g(0) \neq 0\}$; infatti $g(x) \notin (x)$ se e solo se $g(0) \neq 0$. Gli ideali di $S^{-1}A$ sono del tipo $S^{-1}I$ con I ideale

di A. Poiché A è un PID, si ha $I = (f(x))$ con $f(x) \in A$. Sia $f(x) = x^n f_1(x)$ con $n \geq 0$ e $f_1(x) \in A$ con $f_1(0) \neq 0$. Allora l'elemento $f_1(x)/1$ è invertibile in $S^{-1}A$ (il suo inverso è $1/f_1(x)$) e quindi $S^{-1}I = S^{-1}(x^n)$. Questo ci dice che gli ideali di $S^{-1}A$ sono generati da x^n per qualche $n \geq 0$. Osserviamo anche che al variare di n tali ideali sono tutti distinti. Infatti $S^{-1}(x^{n+1}) \subsetneq S^{-1}(x^n)$: il contenimento è ovvio, e l'uguaglianza non vale in quanto $x^n \notin S^{-1}(x^{n+1})$ perché gli elementi di $S^{-1}(x^{n+1})$ sono del tipo $x^{n+1}f(x)/g(x)$ con $g(0) \neq 0$ e se x^n fosse di questo tipo si otterrebbe $x^{n+1}f(x) = x^n g(x)$ da cui $xf(x) = g(x)$ ma $g(0) \neq 0$.
(2) Osserviamo che $T^{-1}B = \{f(x)/g(x) \mid f(x), g(x) \in \mathbb{Z}[x];\ g(0) \neq 0\}$, quindi $T^{-1}B$ è un sottoanello di $S^{-1}A$. D'alta parte vale anche l'inclusione opposta. Infatti, sia $f(x)/g(x) \in S^{-1}A$ e siano $c, d \in \mathbb{Z}\setminus\{0\}$ tali che $cf(x) \in \mathbb{Z}[x]$ e $dg(x) \in \mathbb{Z}[x]$; allora $f(x)/g(x) = cdf(x)/cdg(x) \in T^{-1}B$. Un isomorfismo è dato quindi dalla mappa di inclusione di $T^{-1}B$ in $S^{-1}A$ che risulta anche surgettiva.

Esercizio 4. Sia p un numero primo. Poniamo $K = \mathbb{Q}(\sqrt[p]{2}, i)$.

1. Determinare i valori di p per i quali K è un'estensione normale di $\mathbb{Q}$.

2. Sia E la più piccola estensione di K normale su $\mathbb{Q}$. Determinare il gruppo di Galois di $E/\mathbb{Q}$.

Soluzione: (1) K è normale su $\mathbb{Q}$ se e solo se è campo di spezzamento dei polinomi minimi dei suoi generatori, cioè dei polinomi $x^p - 2$ e $x^2 + 1$ (il polinomio $x^p - 2$ è irriducibile per Eisenstein). È immediato verificare che questo è equivalente a dire che $K/\mathbb{Q}$ è normale se e solo se $\zeta_p \in K$, dove con ζ_p indichiamo come al solito una radice p-esima primitiva di 1.
Ora $[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = p$ e inoltre $i \notin \mathbb{Q}(\sqrt[p]{2})$ in quanto questa estensione è reale. Ne segue che $[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt[p]{2})(i) : \mathbb{Q}(\sqrt[p]{2})][\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = 2p$. Condizione necessaria affinché $\zeta_p \in K$ è che $p - 1 = [\mathbb{Q}(\zeta_p) : \mathbb{Q}]$ divida $2p = [K : \mathbb{Q}]$. Da questo si ricava che le uniche possibilità sono $p = 2$ o 3.
Per $p = 2$ l'estensione è chiaramente normale perché $\zeta_2 = -1 \in K$.
Per $p = 3$ invece l'estensione non è normale in quanto $\zeta_3 \notin K$. Infatti, $\zeta_3 \in K$ se e solo se $\sqrt{-3} \in K$ e se così fosse si avrebbe $\mathbb{Q}(i, \sqrt{-3}) \subseteq K$. Questo però non è possibile perché l'estensione $\mathbb{Q}(i, \sqrt{-3}) = \mathbb{Q}(i, \sqrt{3})$ ha grado 4 su $\mathbb{Q}$ (infatti $i \notin \mathbb{Q}(\sqrt{3})$ che è reale) e 4 non divide il grado di $K/\mathbb{Q}$ che è 6.
(2) Per $p = 2$ si ha $E = K$ che a sua volta è il composto delle due estensioni normali $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(i)$. Poiché queste due estensioni si intersecano banalmente, vale

$$\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Per $p \geq 3$ si ha $E = K(\zeta_p) = \mathbb{Q}(\sqrt[p]{2}, \zeta_p)\,\mathbb{Q}(i)$. Ora $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ e $\mathbb{Q}(i)$ sono estensioni di Galois di $\mathbb{Q}$; studiamole singolarmente. $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)/\mathbb{Q}$ è il composto di $\mathbb{Q}(\sqrt[p]{2})$ che ha grado p su $\mathbb{Q}$ e $\mathbb{Q}(\zeta_p)$ che ha grado $p-1$ su $\mathbb{Q}$; poiché $(p, p-1) = 1$ si ottiene $[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] = p(p-1)$. Inoltre $G_1 = \mathrm{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta_p)/\mathbb{Q}) = \{\varphi_{,i,j} \mid i = 0, \ldots, p-1;\ j = 1 \ldots, p-1\}$ dove $\varphi_{ij}(\sqrt[p]{2}) = \zeta_p^i \sqrt[p]{2}$ e $\varphi_{i,j}(\zeta_p) = \zeta_p^j$. È semplice vedere che $\{\varphi_{i,1} \mid i = 0, \ldots, p-1\}$ è un sottogruppo normale di G_1 isomorfo a $\mathbb{Z}/p\mathbb{Z}$, che $\{\varphi_{0,j} \mid j = 1, \ldots, p-1\}$ è un sottogruppo normale di G_1 isomorfo a $(\mathbb{Z}/p\mathbb{Z})^*$ e che $G_1 \cong \mathbb{Z}/p\mathbb{Z} \rtimes_\psi (\mathbb{Z}/p\mathbb{Z})^*$ dove $\psi(j)(i) = ji$ (infatti $\varphi_{0,j} \circ \varphi_{i,1} \circ \varphi_{0,j}^{-1} = \varphi_{ji,1}$).
Chiaramente il gruppo di Galois G_2 di $\mathbb{Q}(i)/\mathbb{Q}$ è isomorfo a $\mathbb{Z}/2\mathbb{Z}$. Inoltre $\mathbb{Q}(i) \cap \mathbb{Q}(\sqrt[p]{2}, \zeta_p) = \mathbb{Q}$ in quanto $i \notin \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$: infatti altrimenti $\zeta_{4p} \in \mathbb{Q}(\sqrt[p]{2}, \zeta_p)$, ma questo elemento ha grado $\phi(4p) = 2(p-1)$ che non divide $p(p-1)$. Ne segue che

$$\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta_p)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong G_1 \times G_2.$$