Corso di Laurea in Matematica
Algebra 1 - Soluzioni del Compito del 17/01/2020

Esercizio 1)

a) Contare il numero di elementi di ordine 3 in in $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{18} \times \mathbb{Z}_{81}$.

Soluzione: Gli elementi il cui ordine sia un divisore di 3 (1 o 3) sono le 4-uple in cui il minimo comune multiplo degli ordini è 1 o 3. In $\mathbb{Z}_2$ c'è un elemento di ordine 1 e 0 di ordine 3. In $\mathbb{Z}_6, \mathbb{Z}_{18}, \mathbb{Z}_{81}$ vi sono 3 elementi il cui ordine divide 3. Dunque in totale abbiamo 27 elementi. Uno di essi è l'elemento neutro. Quelli di ordine esattamente 3 sono dunque 26.

b) Contare il numero di sottogruppi di ordine 9 in $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{18} \times \mathbb{Z}_{81}$.

Soluzione: I gruppi di ordine 9 sono isomorfi a $\mathbb{Z}_3^2$ o a $\mathbb{Z}_9$. Gli elementi di ordine divisore di 9 sono ottenuti (come nel punto precedente) con 1 scelta nel primo fattore, 3 scelte nel secondo, 9 nel terzo e nel quarto. Dunque abbiamo $3 \cdot 9 \cdot 9 = 243$ elementi di ordine divisore di 9 e dunque $243 - 27 = 216$ elementi di ordine 9. Ogni sottogruppo isomorfo a $\mathbb{Z}_9$ è generato da un elemento di ordine 9 e contiene esattamente $\varphi(9) = 6$ elementi di ordine 9. Dunque i sottogruppi isomorfi a $\mathbb{Z}_9$ sono $216/6 = 36$. Per contare i sottogruppi isomorfi a $\mathbb{Z}_3^2$ contiamo le coppie di elementi di ordine 3, tali per cui il secondo elemento non appartiene al sottogruppo generato dal primo: abbiamo dunque $26 \cdot (26 - 2)$ coppie. Per ogni sottogruppo isormorfo a $\mathbb{Z}_3^2$ esistono $8 \cdot 6$ tali coppie che lo generano, dunque i sottogruppi isomorfi a $\mathbb{Z}_3^2$ sono $(26 \cdot 24)/(8 \cdot 6) = 13$.

c) Qual è il numero di sottogruppi di ordine 10 in S_5?

Soluzione: In S_5 un elemento di ordine 5 è necessariamente un 5-ciclo e non ci sono elementi di ordine 2 che commutano con lui, dunque un sottogruppo di S_5 di ordine 10 è isomorfo a D_5. Per contare tali sottogruppi possiamo intanto contare i 5-cicli in S_5 e, per un fissato 5-ciclo, contare gli elementi di ordine 2 nel suo normalizzatore (per quanto osservato, ognuno di questi coniugherà il 5-ciclo con il suo inverso). Ogni tale coppia (5-ciclo)-(2-ciclo nel normalizzatore) genererà un sottogruppo isomorfo a D_5 e d'altra parte in D_5 ci sono 4 elementi di ordine 5 e 5 elementi di ordine 2 che coniugano ogni elemento di ordine 5 con il suo inverso, dunque $4 \cdot 5 = 20$ coppie distinte genereranno lo stesso sottogruppo isomorfo a D_5. I 5-cicli di S_5 sono 4! Per un fissato 5 ciclo $\sigma \in S_5$ abbiamo 5 elementi nel suo centralizzatore; inoltre abbiamo la successione di omomorfismi $Z_{S_5}(\sigma) \hookrightarrow N_{S_5}(\sigma) \twoheadrightarrow \mathrm{Aut}(\langle\sigma\rangle)$ in cui il primo omomorfismo è iniettivo, il secondo è suriettivo e l'immagine del primo omomorfismo è il nucleo del secondo; ne segue che la controimmagine dell'automorfismo di $\langle\sigma\rangle$ che manda σ nel suo inverso è fatta di 5 elementi. Dunque le coppie cercate sono $4! \cdot 5$ e il numero di sottogruppi di ordine 5 è pari a $(4! \cdot 5)/(4 \cdot 5) = 6$.

d) Sia H un sottogruppo di ordine 4 di A_5. Quanti elementi ha il normalizzatore (in A_5) di H?

Soluzione: Sappiamo che A_5 è semplice, ha ordine $2^2 \cdot 3 \cdot 5$. Un sottogruppo di ordine 4 é dunque un 2-Sylow ed è (coniugato all')immagine di un 2-Sylow di A_4 tramite un'inclusione $A_4 \hookrightarrow A_5$. In A_4 vi sono solo 3 elementi di ordine 2 (i 2-2-cicli) e dunque il 2-Sylow di A_4 è normale, ovvero il suo normalizzatore è tutto A_4, che ha ordine 12. Ne segue che il normalizzatore del 2-Sylow in A_5 conterrà l'immagine (o un suo coniugato) di A_4 tramite la stessa inclusione e deve avere ordine 12 o un multiplo di 12. I multipli di 12 che dividono $|A_5| = 60$ sono 12 e 60, ma poiché A_5 non è semplice deve essere necessariamente che il normalizzatore di un sottogruppo di ordine 4 in A_5 ha 12 elementi.

Esercizio 2. Sia N un gruppo di ordine p^α e H un gruppo di ordine q^β, con $\alpha \geq 1, \beta \geq 1$.

a) Si consideri un prodotto semidiretto $G = N \rtimes_\varphi H$. Sia $\overline{N} = \{(n, e) \mid n \in N\}$ e $\overline{H} = \{(e, h) \mid h \in H\}$. Inoltre per ogni sottogruppo M di H definiamo analogamente

$\overline{M} < \overline{H}$. Dimostrare che che $\overline{\ker\varphi} = \overline{H} \cap C(\overline{N})$, dove $C(\cdot)$ indica il centralizzatore di un sottogruppo di G.

b) Si considerino due prodotti semidiretti $G_1 = N \rtimes_{\varphi_1} H$ e $G_2 = N \rtimes_{\varphi_2} H$. Sia $f : G_1 \to G_2$ un isomorfismo. Analogamente a sopra chiamiamo $\overline{N}_i$ e $\overline{H}_i$ rispettivamente le copia di N ed H in G_i. Spiegare perché $f(\overline{N}_1) = \overline{N}_2$ e $f(\overline{H}_1)$ è un coniugato di $\overline{H}_2$.

c) Con la notazione del punto b), dimostrare che se G_1 è isomorfo a G_2 allora $\ker(\varphi_1)$ è isomorfo a $\ker(\varphi_2)$.

Soluzione: Per la parte a), consideriamo che $(e, h) \in \overline{\ker\varphi}$ se e solo se per ogni $n \in N$, $\varphi(h)(n) = n$. Questo accade se e solo se per ogni $n \in N$,

$$(n, h) = (\varphi(h)(n), h)$$

ossia se e solo se per ogni $n \in N$

$$(n, e)(e, h) = (e, h)(n, e)$$

che equivale a dire che $(e, h) \in C(\overline{N}) \cap \overline{H}$.

Per la parte b) basta osservare che $\overline{N}_1$ è l'unico p-Sylow di G_1 (dato che è normale) e analogamente $\overline{N}_2$ è l'unico p-Sylow di G_2. Dunque per ragioni di cardinalità $f(\overline{N}_1) = \overline{N}_2$. Invece $\overline{H}_1$ è un q-Sylow di G_1, dunque $f(\overline{H}_1)$ è un q-Sylow di G_2, e pertanto, per il secondo teorema di Sylow, visto che anche $\overline{H}_2$ è un q Sylow di G_2, esiste $g \in G_2$ tale che $f(\overline{H}_1) = g\overline{H}_2 g^{-1}$.

Per la parte c), cominciamo con l'osservare che

$$f(\overline{Ker\varphi_1}) = f(\overline{H}_1 \cap C(\overline{N}_1)) = f(\overline{H}_1) \cap f(C(\overline{N}_1)) = g\overline{H}_2 g^{-1} \cap C(f(\overline{N}_1)) = g\overline{H}_2 g^{-1} \cap C(\overline{N}_2)$$

dove nell'ultimo passaggio abbiamo usato la parte b). Se dimostriamo che $gC(\overline{N}_2)g^{-1} = C(\overline{N}_2)$ allora possiamo concludere perché

$$f(\overline{Ker\varphi_1}) = g\overline{H}_2 g^{-1} \cap C(\overline{N}_2) = g\overline{H}_2 g^{-1} \cap gC(\overline{N}_2)g^{-1} = g(\overline{H}_2 \cap C(\overline{N}_2))g^{-1} = g\ \overline{Ker\varphi_2}\ g^-1$$

dove nell'ultimo passaggio abbiamo usato la parte a). Da questa uguaglianza segue che $\overline{Ker\varphi_1}$ e $\overline{Ker\varphi_2}$ sono isomorfi e pertanto lo sono anche $Ker\varphi_1$ e $Ker\varphi_2$.

Resta dunque da dimostrare che $gC(\overline{N}_2)g^{-1} = C(\overline{N}_2)$. Per ragioni di cardinalità basta dimostrare una sola inclusione, per esempio $gC(\overline{N}_2)g^{-1} \subseteq C(\overline{N}_2)$. Sia $x \in C(\overline{N}_2)$ e sia $n \in \overline{N}_2$. Vale che $(gxg^{-1})n = gx(g^{-1}ng)g^{-1}$. Poiché N_2 è normale in G_2 allora $g^{-1}ng \in \overline{N}_2$ per cui x commuta con questo elemento. Dunque

$$(gxg^{-1})n = gx(g^{-1}ng)g^{-1} = g(g^{-1}ng)xg^{-1} = n(gxg^{-1})$$

e, visto che ciò vale per ogni $n \in \overline{N}_2$, si conclude che $gxg^{-1} \in C(\overline{N}_2)$ e questo prova l'inclusione di cui avevamo bisogno.

Esercizio 3.

a) Calcolare il grado dell'estensione di campi

$$\mathbb{C}(X_1, \ldots, X_n) \supset \mathbb{C}(X_1^{d_1}, \ldots, X_n^{d_n}),$$

dove $X_1, \ldots, X_n$ sono variabili e $d_1, \ldots, d_n$ sono interi positivi.

b) Trovare il grado dell'estensione di campi $[\mathbb{C}(X,Y) : \mathbb{C}(X^2Y^6, X^4Y^{21})]$, dove X, Y sono variabili.

c) Mostrare che l'estensione $\mathbb{C}(X^2Y^6, X^4Y^{21}) \subset \mathbb{C}(X,Y)$ è di Galois e descrivere il suo gruppo di Galois.

Soluzione:

a) Dato un campo $K \supset \mathbb{C}$, affermiamo che l'estensione $[K(X) : K(X^d)]$ ha grado d. Ne seguirà per induzione su n che l'estensione indicata nell'esercizio ha grado $d_1 \cdots d_n$.
Per dimostrare quanto affermato notiamo che il polinomio nella variabile t dato da $p(t) = t^d - X^d$ è un polinomio a coefficienti in $K(X^d)$ di grado d. Pertanto l'estensione considerata ha grado al più d.
D'altra parte la funzione $\varphi : K(X) \to K(X)$ data da $\varphi : f(X)/g(X) \mapsto f(\zeta_d X)/g(\zeta_d X)$ è un automorfismo del campo $K(X)$ di ordine d che chiaramente fissa il sottocampo $K(X^d)$. Inoltre l'orbita di X rispetto al gruppo generato da φ è costituita da d elementi, dunque il grado di X su $K(X^d)$ è almeno d. Con questo abbiamo concluso la dimostrazione di quanto affermato all'inizio.

b) Dette A, B due variabili, notiamo che il campo $K(A,B)$ è uguale al campo $K(A, A^nB)$, con n intero, e al campo $K(AB^m, B)$ con m intero. Pertanto abbiamo le uguaglianze

$$K(X^2Y^6, X^4Y^{21}) = K(X^2Y^6, X^{-2}Y^3) = K(X^6, X^{-2}Y^3)$$

e ponendo $X^{-1}Y = W$ (e quindi $K(X,Y) = K(X,W)$) otteniamo

$$K(X^6, X^{-2}Y^3) = K(X^6, XW^3) = K(W^{-18}, XW^3)$$

e infine ponendo $XW^3 = Z$ (e quindi $K(X,W) = K(Z,W)$) otteniamo

$$K(W^{-18}, XW^3) = K(W^{-18}, Z) = K(W^{18}, Z).$$

Ne segue che $[K(X,Y) : K(X^2Y^6, X^4Y^{21})] = [K(Z,W) : K(W^{18}, Z)] = 18$, dove l'ultima uguaglianza segue dal punto precedente.

c) L'automorfismo φ di $K(Z,W)$ che manda $(Z,W) \mapsto (Z, \zeta_{18}W)$ ha ordine 18 e contiene $K(Z, W^{18})$ nel suo campo fisso. Poiché $W = X^{-1}Y, Z = X^{-2}Y^3$, e dunque $X = ZW^{-3}$ e $Y = WX = ZW^{-2}$ l'azione di φ sugli elementi X, Y è data da:

$$\varphi(X) = \zeta_6^{-1}X, \qquad \varphi(Y) = \zeta_9^{-1}Y.$$

Visto che il grado dell'estensione è esattamente 18 possiamo concludere che l'estensione considerata è di Galois e che φ genera il gruppo di Galois dell'estensione che pertanto è ciclico di ordine 18, dunque $\mathrm{Gal}(K(X,Y)/K(X^2Y^6, X^4Y^{21})) \simeq \mathbb{Z}_{18}$.