Soluzioni esame scritto di ALGEBRA II
20 maggio 2013

Esercizio 1. Sia G un gruppo di ordine 91.

1. Si provi che G è ciclico;
2. si provi che l'applicazione $\phi : G \to G \times G$ definita da
$$\phi(g) = (g^{21}, g^{39})$$
per ogni $g \in G$, è un omomorfismo; si provi poi che ϕ è iniettiva;
3. sia $H = \{(g^a, g^b) \mid g \in G, a \in 13\mathbb{Z}, b \in 7\mathbb{Z}\} \leq G \times G$ (questo non occorre provarlo); si provi che
$$G \times G = H \times \phi(G).$$

soluzione 1. Sia ha $|G| = 91 = 13 \cdot 7$. Posto, per ciascun primo p, n_p il numero di p-sottogruppi di Sylow di G, dal teorema di Sylow segue

$$n_7 \equiv 1 \pmod 7 \quad \text{e} \quad n_7 | 13,$$

da cui $n_7 = 1$. Similmente si trova $n_{13} = 1$. Dunque G ha un unico (normale) 7-sottogruppo di Sylow P ed un unico 13-sottogruppo di Sylow Q. Poiché P e Q sono ciclici di ordine coprmo, si ha $P \cap Q = \{1\}$ e dunque

$$G = PQ \simeq P \times Q$$

è ciclico.

2. Che ϕ sia omomorfismo è immediato dato che G è commutativo. Proviamo che ϕ è iniettiva valutando il nucleo. Per $g \in G$ si ha

$$1_{G\times G} = (1, 1) = \phi(g) \;\Leftrightarrow\; g^{21} = 1 = g^{39}.$$

Poiché $(21, 39) = 3$, si conclude che $g \in ker(\phi)$ se e solo $g^3 = 1$. Ma $g \in G$ e quindi l'ordine $|g|$ divide $91 = 13 \cdot 7$. Pertanto $g^3 = 1$ forza $g = 1$. Questo prova che $ker(\phi) = \{1\}$ e dunque che ϕ è iniettiva.

3. Chiamiamo $W = G \times G$. Poiché G è commutativo anche W lo è; dunque ogni suo sottogruppo è normale. In particolare $H \trianglelefteq W$ e $\phi(G) \trianglelefteq W$.
Sia $(x_1, x_2) \in H \cap \phi(G)$; quindi $x_1 = g^{21}$ per qualche $g \in G$ e $x_1 = h^{13z}$ per qualche $h \in G$ e $z \in \mathbb{Z}$; dalla prima segue che $x_1^{13} = 1$, dalla seconda $x_1^7 = 1$. Dunque $x_1 = 1$; analogamente si prova $x_2 = 1$. Pertanto $H \cap \phi(G) = 1$.

Posto y un generatore del gruppo ciclico G si ha $H = \langle y^{13}\rangle \times \langle y^7\rangle$. Dunque $|H| = |\langle y^{13}\rangle| \cdot |\langle y^7\rangle| = 7 \cdot 13 = 91$ (e $H \simeq G$). Quindi

$$|H(\phi(G))| = |H||\phi(G)| = 91 \cdot 91 = |W|.$$

Dunque $W = H\phi(G)$; pertanto - dalla teoria - W è il prodotto diretto interno $W = H \times \phi(G)$.

Esercizio 2. Sia $A = \{1, 2, 3\}$ e $\Omega = A^A = \{f \mid f : A \to A\}$.

1. Si provi che porre, per ogni $(\alpha, \beta) \in S_3 \times S_3$ e ogni $f \in \Omega$,

   $$(\alpha, \beta) \cdot f = \alpha \circ f \circ \beta^{-1}$$

   definisce un azione del gruppo $G = S_3 \times S_3$ su Ω;

2. Si determini lo stabilizzatore in G dell'applicazione identica ι_A e quello della funzione costante c_1 (definita da $c_1(x) = 1$ per ogni $x \in A$); si dica quanti elementi contengono le orbite di ι_A e di c_1.

soluzione 1. Le proprietà che assicurano che quella data è un'azione di $G = S_3 \times S_3$ su Ω sono facilmente verificate: per ogni $(\alpha, \beta), (\gamma, \delta) \in G$ ed ogni $f \in \Omega$,

$$\begin{aligned}(\alpha, \beta) \cdot ((\gamma, \delta) \cdot f) &= (\alpha, \beta) \cdot (\gamma \circ f \circ \delta^{-1}) = (\alpha \circ \gamma) \circ f \circ (\delta^{-1} \circ \beta^{-1}) = \\ &= (\alpha\gamma) \circ f \circ (\beta\delta)^{-1} = (\alpha\gamma, \beta\delta) \cdot f = (\alpha, \beta)(\gamma, \delta) \cdot f\end{aligned}$$

$1_G \cdot f = (\iota_A, \iota_A) \cdot f = \iota_A \circ f \circ \iota_A = f.$

2. Si noti che per ogni $\beta \in S_3$, $c_1 \circ \beta = c_1$. Quindi, per $(\alpha, \beta) \in G$ si ha

$$\begin{aligned}(\alpha, \beta) \cdot \iota_A &= \alpha \circ \iota_A \circ \beta^{-1} = \alpha \circ \beta^{-1} \\ (\alpha, \beta) \cdot c_1 &= \alpha \circ c_1 \circ \beta^{-1} = \alpha \circ c_1 = c_{\alpha(1)}\end{aligned}$$

Dunque, denotando con H e con K lo stabilizzatore in G, rispettivamente di ι_A e di c_1, si ha

$$\begin{aligned}H &= \{(\alpha, \alpha) \mid \alpha \in S_3\} \\ K &= \{(\alpha, \beta) \in G \mid \alpha(1) = 1\}\end{aligned}$$

Per la formula orbita-stabilizzatore ed il Teorema di Lagrange

$$\begin{aligned}|O_G(\iota_A)| &= [G : H] = |G|/|H| = 36/6 = 6. \\ |O_G(c_1)| &= [G : K] = |G|/|K| = 36/12 = 3\end{aligned}$$

Esercizio 3. Siano ζ ed ω, rispettivamente, una radice primitive terza e quinta dell'unità in $\mathbb{C}$.

1. Si provi che $\mathbb{Q}[\zeta, \omega]|\mathbb{Q}$ è un'estensione di Galois e si determini l'ordine del suo gruppo di Galois;
2. si provi che $\mathbb{Q}[5\zeta + 3\omega]$ è un'estensione normale di $\mathbb{Q}$;
3. si dica se $\mathbb{Q}[\zeta\omega] = \mathbb{Q}[\zeta, \omega]$.

soluzione 1. $\mathbb{Q}[\zeta]$ e $\mathbb{Q}[\omega]$ sono, rispettivamente, il campo di spezzamento del polinomio $x^3 - 1 \in \mathbb{Q}[x]$ e del polinomio $x^5 - 1 \in \mathbb{Q}[x]$. Dunque, $E = \mathbb{Q}[\zeta, \omega]$ è il campo di spezzamento del polinomio $(x^3 - 1)(x^5 - 1)$. Pertanto, $E|\mathbb{Q}$ è un'estensione normale e dunque (poiché è certamente finita e separabile) di Galois. Per determinarne il grado, osserviamo che, poiché i polinomi minimi su $\mathbb{Q}$ di ζ e di ω sono, rispettivamente $x^2 + x + 1$ e $x^4 + x^3 + x^2 + x + 1$; per cui $[\mathbb{Q}[\zeta] : \mathbb{Q}] = 2$ e $[\mathbb{Q}[\omega] : \mathbb{Q}] = 4$. Dunque per la formula dei gradi

$$[E : \mathbb{Q}] = [\mathbb{Q}[\omega, \zeta] : \mathbb{Q}[\omega]][\mathbb{Q}[\omega] : \mathbb{Q}] \in \{4, 8\}.$$

Ora, $\omega \in \mathbb{C}$ è radice primitiva 5^a dell'unità e il gruppo di Galois dell'estensione ciclotomica $\mathbb{Q}[\omega]|\mathbb{Q}$ è ciclico di ordine 4. Per la corrispondenza di Galois e la teoria di gruppi ciclici finiti, si deduce che esiste un solo campo intermedio $\mathbb{Q} \subseteq L \subseteq \mathbb{Q}[\omega]$ con $[L : \mathbb{Q}] = 2$. Inoltre $L = Inv_{\mathbb{Q}[\omega]}(\gamma)$ dove γ è il coniugio complesso (ristretto a $\mathbb{Q}[\omega]$), quindi $L = \mathbb{Q}[\omega] \cap \mathbb{R}$ (di fatto, si prova che $L = \mathbb{Q}[\omega + \overline{\omega}] = \mathbb{Q}[\omega + \omega^4] = \mathbb{Q}[\cos \frac{2\pi}{5}]$).
Se fosse $[E : \mathbb{Q}] = 4$, allora $E = \mathbb{Q}[\omega]$ e $\zeta \in \mathbb{Q}[\omega]$, dunque (essendo unico camp[o intermedio di grado 2) $\mathbb{Q}[\zeta] = L$, il che è assurdo perché $\zeta \notin \mathbb{R}$. Quindi, $[E : \mathbb{Q}] = 8$ e, poiché $E|\mathbb{Q}$ è di Galois, $|Gal(E|\mathbb{Q})| = 8$.

2. Sia ζ che ω sono radici 15-esime dell'unità (non primitive). Dunque, posto η radice primitiva 15-esima dell'unità (nel punto seguente si vedrà che è possibile prendere $\eta = \zeta\omega$) si ha $E \subseteq Q[\eta]$ (infatti, $E = \mathbb{Q}[\eta]$, ma questo al momento non è necessario). Poiché $\mathbb{Q}[\eta]$ è un'estensione ciclotomica di $\mathbb{Q}$, il suo gruppo di Galois è abeliano, quindi ogni suo sottogruppo è normale; dunque, ogni campo intermedio è estensione normale di $\mathbb{Q}$. In particolare $\mathbb{Q}[5\zeta + 3\omega]$ è un'estensione normale di $\mathbb{Q}$.

3. Chiaramente $\mathbb{Q}[\zeta\omega] \subseteq \mathbb{Q}[\zeta, \omega]$. Per l'inclusione inversa, basterà osservare come

$$(\zeta\omega)^{10} = \zeta^{10}\omega^{10} = \zeta^{10} = \zeta \qquad (\zeta\omega)^{21} = \zeta^{21}\omega^{21} = \omega^{21} = \omega.$$

Quindi $\{\zeta, \omega\} \subseteq \mathbb{Q}[\zeta\omega]$ e pertanto $\mathbb{Q}[\zeta, \omega] \subseteq \mathbb{Q}[\zeta\omega]$.

Esercizio 4. Sia $E|F$ un'estensione di Galois. Fissato $u \in E$, siano $f \in F[x]$ il polinomio minimo di u su F e $w \in E$ un'altra radice di f; si provi che se $F[u] \neq F[w]$ allora il gruppo $Gal(E|F)$ non è abeliano.

soluzione. Supponiamo che $G = Gal(E|F)$ sia abeliano; allora ogni suo sotogruppo è normale. Per il Teorema di corrispondenza di Galois (parte 3) si conclude che per ogni campo L, con $F \leq L \leq E$, l'estensione $L|F$ è normale. In particolare $F[u]|F$ è normale, dunque $F[u]$, cintenendone una, contiene tutte le radici del polinomio irriduciibile f. In particolare $w \in F[u]$ e dunque $F[u] = F[w]$.