Corso di Laurea in Matematica

Soluzioni esame scritto di ALGEBRA II

18 gennaio 2013

Esercizio 1. (8 punti) Siano

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Z}_7,\ a, c \neq 0 \right\} \quad \text{e} \quad N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}_7, \right\} .$$

1. Si provi che G è un gruppo e che N è un sottogruppo normale di G.
2. Determinare l'ordine nel gruppo quoziente G/N dell'elemento gN con $g = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$.
3. Si provi che l'applicazione $\phi : G \to (\mathbb{Z}/7\mathbb{Z})^\times$ definita da

$$\phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \right) = ac\ ,$$

per $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G$, è un omomorfismo.

soluzione. 1. Basta provare che G è sottogruppo del gruppo $GL(2, \mathbb{Z}_7)$ delle matrici 2×2 invertibili a coefficienti nel campo $\mathbb{Z}_7$. Ora, chiaramente, $G \neq \emptyset$; inoltre se

$$g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \quad h = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$$

sono elementi di G, si ha

$$gh = \begin{pmatrix} aa' & ab' + ba' \\ 0 & cc' \end{pmatrix} \in G \tag{1}$$

(dato che $aa', cc' \neq 0$) e

$$g^{-1} \begin{pmatrix} a^{-1} & -bc^{-1}a^{-1} \\ 0 & c^{-1} \end{pmatrix} \in G; \tag{2}$$

quindi $G \leq GL(2, \mathbb{Z}_7)$. $N \leq G$ si prova facilmente utilizzando il criterio; infatti 1_G(la matrice identica)$\in N$, e inoltre, per ogni $b, b' \in \mathbb{Z}_7$,

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b' - b \\ 0 & 1 \end{pmatrix} \in N.$$

Proseguiamo applicando il criterio di normalità; siano $g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G$ e $h = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \in N$, allora, applicando le formule in (1) e (2),

$$g^{-1}hg = \begin{pmatrix} 1 & a^{-1}cd \\ 0 & 1 \end{pmatrix} \in H.$$

Quindi $H \trianglelefteq G$.

2. Poiché $g \in N$, $gN = N = 1_{G/N}$ e quindi $|gN| = 1$.

3. Siano $g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, h = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$, elementi di G; allora, applicando l'identità (1),

$$\phi(gh) = (aa')(cc') = (ac)(a'c') = \phi(g)\phi(h).$$

Dunque, ϕ è un omomorfismo di gruppi.

Esercizio 2. Sia G un gruppo di ordine 2013.

1. Provare che G ha sottogruppi di ordine $3 \cdot 11$ e $11 \cdot 61$ e che questi sono ciclici.
2. Dimostrare che 11 divide l'ordine del centro $Z(G)$.
3. Posto $t = |\{g \in G \,:\, |g| = 3\}|$, provare che $t = 122$ oppure G è ciclico (e $t = 2$).

soluzione. 1. Si osserva, innanzi tutto, che $|G| = 2013 = 3 \cdot 11 \cdot 61$. Sia $n_{11} = n_{11}(G)$ il numero di 11-sottogruppi di Sylow di G. Per il secondo Teorema di Sylow, si ha

$$\begin{cases} n_{11} | 3 \cdot 61 = 183 \\ n_{11} \equiv 1 \pmod{11} \end{cases}$$

la sola possibilità è $n_{11} = 1$. Dunque, esiste un unico 11-sottogruppo di Sylow N di G, e $N \trianglelefteq G$. Siano ora T e P, rispettivamente, un 3-sottogruppo ed un 61-sottogruppo di Sylow di G; allora NT e NP sono sottogruppi di G (perché $N \trianglelefteq G$). Inoltre $|NT| = 3 \cdot 11$, infatti

$$|NT| = \frac{|N||T|}{|N \cap T|} = |N||T| = 11 \cdot 3,$$

e., similmente $|NP| = 61$. Quindi, NT ed NP sono i sottogruppi cercati. Ora, poiché 3 non divide $11 - 1$ si ha $n_3(NT) = 1$ per cui $NT = N \times T$ è un gruppo ciclico (è prodotto diretto di gruppi ciclici

di ordine coprimo); similmente si trova $NP = N \times P$ che, per la stessa ragione, è un gruppo ciclico.

2. Usiamo le notazioni introdotte al punto precedente.
N (avendo ordine primo) è ciclico; sia $N = \langle g \rangle$ e sia $C = C_G(g)$ il suo centralizzante; poniamo poi $n = |C_G(g)|$. Poiché $C_G(g) \leq G$, n divide $|G| = 2013$. Inoltre, chiaramente, $N \leq C_G(g)$ e quindi $11|n$. Ma abbiamo provato al punto precedente che anche T e P sono contenuti in $C_G(g)$; quindi sia $|T| = 3$ che $|P| = 61$ dividono n. Ne consegue che $n = 11 \cdot 3 \cdot 61 = 2013 = |G|$ e quindi che $C_G(g) = G$. Ciò equivale a $g \in Z(G)$. Dunque $N = \langle g \rangle \leq Z(G)$ e pertanto l'ordine del centro $Z(G)$ è multiplo di 11.

3. Osserviamo che, per ogni $x \in G$, $x \in \{g \in G \ : \ |g| = 3\}$ se e soltanto se $\langle x \rangle$ è un 3-sottogruppo di Sylow di G. Ora ogni 3-sottogruppo di Sylow T di G ha due generatori e intersezione banale con ogni altro 3-sottogruppo di Sylow diverso da T. Pertanto

$$t = 2 \cdot n_3(G)$$

(al solito, $n_3(G)$ denota il numero di 3-sottogruppi di Sylow di G). Dal secondo Teorema di Sylow segue

$$\begin{cases} .n_3(G) \text{ divide } 11 \cdot 61 = 671 \\ n_3 \equiv 1 \pmod 3 \end{cases}$$

Quindi $n_3(G) \in \{1, 61\}$. Pertanto, se $t \neq 122$ si ha $t = 2$ e $n_3(G) = 1$. Dunque, in questo caso, G ha un unico 3-sottogruppo di Sylow T; $T \trianglelefteq G$ e T è ciclico. Ma, ancora per il Teorema di Sylow, si osserva che $n_{61}(G) = 1$, ovvero che G ha un unico 61-sottogruppo di Sylow P, che è ciclico. Abbiamo poi già provato (punto 1.) che G ha un unico 11-sottogruppo di Sylow N (che è ciclico). Ne consegue che $G \simeq T \times N \times P$ è il prodotto diretto di gruppi ciclici i cui ordini sono a sue a due coprimi, ed è quindi ciclico.

Esercizio 3. (12 punti) Sia $\omega \in \mathbb{C}$ una radice primitiva 9-esima dell'unità.

1. Trovare il polinomio minimo di ω su $\mathbb{Q}$.
2. Posto $E = \mathbb{Q}[\omega]$, provare che $E|\mathbb{Q}$ è normale e determinare il gruppo $G = Gal(E|\mathbb{Q})$.
3. Trovare (come combinazione lineare di potenze di ω) elementi $u, v \in E$ tali che $[\mathbb{Q}[u] : \mathbb{Q}] = 3$ e $[\mathbb{Q}[v] : \mathbb{Q}] = 2$.
4. Posto $\Omega = \{\omega^i \ : \ 0 \leq i \leq 8\}$ l'insieme delle radici di $x^9 - 1$, si dica quante sono le orbite di G su Ω.

soluzione. 1. e 2. Le radici del polinomio $x^9 - 1$ sono le potenze ω^i con $i = 0, \ldots, 8$ (che sono tutte distinte), quindi $E = \mathbb{Q}[\omega]$ è il campo di spezzamento su $\mathbb{Q}$ del polinomio $x^9 - 1$. Dunque $E|\mathbb{Q}$ è un'estensione finita e normale. Poiché $\mathbb{Q}$ ha caratteristica 0, tale estensione è di Galois.

Sappiamo poi, dal corso, che il grado del polinomio minimo di ω su $\mathbb{Q}$ coincide con il valore della funzione di Eulero $\phi(9) = 6$. Poiché, in $\mathbb{Q}[x]$, si ha la fattorizzazione che si fattorizza come

$$x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$$

ne segue che il polinomio minimo di ω è

$$f = x^6 + x^3 + 1.$$

In particolare, posto $G = Gal(E|\mathbb{Q})$, si ha $|G| = [E : \mathbb{Q}] = 6$. Sappiamo inoltre che G è abeliano (in quanto gruppo di Galois del campo di spezzamento di un polinomio del tipo $x^n - 1$), quindi G è ciclico di ordine 6.

3. Per $v \in E$ tale che $[\mathbb{Q}[v] : \mathbb{Q}] = 2$ non è difficile: infati $v = \omega^3$ è una radice primitiva terza dell'unità; il suo polinomio minimo è quindi $x^2 + x + 1$ e $[\mathbb{Q}[v] : \mathbb{Q}] = 2$.
Per quanto rigurda $u \in E$ tale che $[\mathbb{Q}[u] : \mathbb{Q}] = 3$, osserviamo che, per la corrispondenza di Galois $\mathbb{Q}[u]$ deve coincidere con il campo degli invarianti dell'unico sottogruppo di ordine 2 di $G = Gal(E|\mathbb{Q})$. Ora, il gruppo ciclico G contiene un unico elemento γ di ordine 2 di G che è la restrizione a E del coniugio complesso; cerchiamo quindi un elemento $u \in E$ tale che $\mathbb{Q}[u] = Inv(\gamma)$. Consideriamo

$$u = \omega + \omega^8 = \omega + \omega^{-1} = \omega + \overline{\omega}.$$

Allora, $u \in Inv(\gamma)$ e $u \notin \mathbb{Q}$ (se, per assurdo, $u \in \mathbb{Q}$, allora ω è radice del polinomio $x^2 - ux + 1 \in \mathbb{Q}[x]$); poiché $[Inv(\gamma) : \mathbb{Q}] = [G : \langle\gamma\rangle] = 3$, per la formula dei gradi si ha $Q[u] = Inv(\gamma)$ (in particolare $[\mathbb{Q}[u] : \mathbb{Q}] = 3$). Infine, da $\omega^6 + \omega^3 + 1 = 0$ segue $\omega^8 = -\omega^5 - \omega^2$, dunque $u = \omega - \omega^2 - \omega^5$.

4. $\Omega = \{\omega^i \ : \ 0 \leq i \leq 8\}$ è l'insieme delle radici di $x^9 - 1$. Le orbite di $G = Gal(\mathbb{Q}[\omega]|\mathbb{Q})$ su Ω corrispondono ai faoori irriducibili di tale polinomio, che sono $x - 1$, $x^2 + x + 1$ e $x^6 + x^3 + 1$. Infatti, per ciascuno di tali fattori G fissa l'insieme delle radici, e poiché questi fattori sono irriducibili, G permuta transitivamente le loro radici; esplicitamente, le tre orbite sono

$$\{1\}, \quad \{\omega^3, \omega^6\}, \quad \{\omega, \omega^2, \omega^4, \omega^5, \omega^7, \omega^8\}.$$

Esercizio 4. (4 punti Sia $E|F$ un'estensione di campi e sia $a \in E$ tale che $[F(a) : F] = pq$ con p, q primi, $p < q$. Provare che

$$F[a^{p-1} + a] = F[a]$$

.

soluzione. Poiché $a^{p-1} + a \in F[a]$ si ha subito l'inclusione

$$F[a^{p-1} + a] \subseteq F[a].$$

Sia $d = [F[a^{p-1} + a] : F]$. Posto $b = a^{p-1} + a$, osserviamo che a è radice del polinomio $x^{p-1} + x - b \in F[b]$ e quindi che

$$[F[a] : F[b]] \leq p - 1.$$

Ora, per la formula dei gradi,

$$pq = [F[a] : F[b]][F[b] : F] \leq (p-1)d < pd$$

dunque $d > q$. Poiché, sempre per la formula dei gradi, d divide pq e, per ipotesi, $p < q$, l'unica possibilità è $d = pq$. Quindi

$$[F[b] : F] = pq = [F[a] : F]$$

e siccome $F[b] \leq F[a]$ si conclude che $F[b] = F[a]$, che è ciò che si voleva.