ALGEBRA 2 — Primo esame scritto
22 Giugno 2012
soluzioni

(1) • Mostrare che il gruppo diedrale dell'esagono D_6 è isomorfo a $\mathrm{D}_3 \times \mathrm{C}_2$.

Soluzione: Sia ρ la rotazione di 60 gradi, e s il ribaltamento rispetto ad una diagonale massima dell'esagono. Sappiamo che $G = \mathrm{D}_6 = \langle \rho, s \rangle$, e che $\rho^6 = 1 = s^2, s\rho s^{-1} = \rho^{-1}$.
Il sottogruppo $H = \langle \rho^2, s \rangle$ conserva uno dei triangoli equilateri inscritti nell'esagono, e contiene 6 elementi. E' pertanto isomorfo a D_3; ha indice 2, ed è quindi normale. Il sottogruppo $K = \langle \rho^3 \rangle$ ha ordine 2, e coincide col centro di G. E' pertanto normale. L'intersezione $H \cap K$ contiene la sola identità, e il prodotto HK possiede allora $|H||K|/|H \cap K| = 6 \cdot 2/1 = 12$ elementi. Concludiamo che $H, K \lhd G$, $H \cap K = \{\mathrm{id}\}$, $HK = G$. Pertanto $G = H \times K$. Poiché $H \simeq \mathrm{D}_3$, $K \simeq \mathrm{C}_2$, otteniamo $G \simeq \mathrm{D}_3 \times \mathrm{C}_2$.

• Mostrare che il gruppo diedrale dell'ottagono D_8 non è isomorfo a $\mathrm{D}_4 \times \mathrm{C}_2$.

Soluzione: D_8 possiede elementi di ordine 8, mentre $\mathrm{D}_4 \times \mathrm{C}_2$ non ne ha.

(2) G è un gruppo di ordine $315 = 3^2 \cdot 5 \cdot 7$ e R è un suo 3-Sylow non normale.

- Mostrare che il normalizzatore $N(R)$ contiene 45 elementi.

  Soluzione: Il numero dei 3-Sylow di G divide 35 ed è $\equiv 1 \mod 3$. Le uniche possibilità sono 1 e 7, ma R non è normale. Pertanto G possiede esattamente 7 3-Sylow, e il normalizzatore di ciascuno di essi ha indice 7, e quindi ordine 45.

- Mostrare che $N(R)$ è abeliano.

  Soluzione: $N(R)$ è un gruppo di ordine 45, nel quale R è normale. Inoltre il numero dei 5-Sylow di $N(R)$ divide 9 ed è $\equiv 1 \mod 5$. Il 5-Sylow è quindi unico, e necessariamente normale. Allora $N(R)$ è prodotto diretto di R con il suo unico 5-Sylow. Questi sottogruppi hanno ordine 9 e 5, e sono entrambi abeliani. Allora anche il loro prodotto diretto è abeliano

- Mostrare che il 5-Sylow di G è normale.
  Soluzione: Consideriamo un sottogruppo H di ordine 5 contenuto in $N(R)$. A causa dell'abelianità di $N(R)$, H è normale in $N(R)$, e quindi il suo normalizzatore contiene almeno i 45 elementi in $N(R)$.
  Ad ogni modo, H è un 5-Sylow di G, e il numero dei 5-Sylow di G divide 63 ed è $\equiv 1 \mod 5$. Le uniche possibilità sono 1 e 21. Tuttavia, se G possiede 21 coniugati, è normalizzato da un sottogruppo di indice 21, e quindi di ordine 15, che è troppo piccolo per contenere i 45 elementi mostrati prima. L'unica altra possibilità è che H sia normale in G.

- Mostrare che G contiene un sottogruppo ciclico di ordine 35.

  Soluzione: Basta moltiplicare H per un sottogruppo $K < G$ di ordine 7. La normalità di H costringe HK, che contiene 35 elementi, ad essere un sottogruppo di G. Un gruppo di ordine $35 = 5 \cdot 7$ è ciclico poiché 5 non divide $7 - 1$.

- Mostrare che anche il 7-Sylow di G è normale.

  Soluzione: Possiamo ripetere il ragionamento precedente. K è un 7-Sylow di G, ed è contenuto nel sottogruppo HK di ordine 35, che lo normalizza per abelianità. Il normalizzatore di K ha allora indice $\leq 315/35 = 9$. Tuttavia il numero dei 7-Sylow in G divide 45, è $\equiv 1 \mod 7$ ed è ≤ 9. L'unica possibilità è 1, e l'unicità del 7-Sylow impone la sua normalità.

- A quali gruppi può essere isomorfo G? Individuarli tutti a meno di isomorfismo.

  Soluzione: G è prodotto semidiretto del sottogruppo normale di ordine 35 con il sottogruppo R, che sappiamo essere non normale e di ordine 9; si tratta pertanto di un prodotto semidiretto non banale. R è isomorfo a C_9 oppure a $\mathrm{C}_3 \times \mathrm{C}_3$, mentre il gruppo di ordine 35 è necessariamente ciclico.
  Nei due casi, dobbiamo costruire omomorfismi $\phi : \mathrm{C}_9 \to \mathrm{Aut}(\mathrm{C}_{35}) \simeq \mathrm{C}_6 \times \mathrm{C}_4$, oppure $\phi : \mathrm{C}_3 \times \mathrm{C}_3 \to \mathrm{Aut}(\mathrm{C}_{35})$, rispettivamente. Se ϕ è non banale, la sua immagine, che ha ordine un divisore di 9, deve essere contenuta nel primo fattore diretto in entrambi i casi, ed è univocamente determinata (C_6 possiede un solo sottogruppo di ordine 3). Possiamo allora scegliere il generatore di C_9 in modo che venga applicato da ϕ nel generatore fissato di $\mathrm{C}_3 < \mathrm{C}_6$; nell'altro caso, possiamo scegliere due generatori di $\mathrm{C}_3 \times \mathrm{C}_3$ in modo che il primo venga applicato da ϕ nel generatore fissa di C_3, e il secondo appartenga al nucleo. G è pertanto isomorfo ad uno dei seguenti due gruppi: $(\mathrm{C}_7 \ltimes \mathrm{C}_9) \times \mathrm{C}_5$ nel primo caso, e $(\mathrm{C}_7 \ltimes \mathrm{C}_3) \times (\mathrm{C}_3 \times \mathrm{C}_5)$ nel secondo.

(3) Se $g(x) = x^6 + 3 \in \mathbb{Q}[x]$, sia α una radice complessa di $g(x)$, e poniamo $L = \mathbb{Q}(\alpha)$.

- Mostrare che L contiene la radice sesta dell'unità $\zeta = \frac{1}{2} + \frac{\sqrt{-3}}{2}$.

  Soluzione: $\alpha^3 = \pm\sqrt{-3}$.

- Mostrare che L è il campo di spezzamento di $g(x)$. Qual è il grado di L come estensione di $\mathbb{Q}$?

  Soluzione: Poiché $\zeta = \frac{1}{2} + \frac{\sqrt{-3}}{2}$ è una radice sesta primitiva dell'unità, il campo $\mathbb{Q}(\alpha)$ contiene tutte e sei le radici complesse $\zeta^i\alpha, i = 0, \ldots, 5$, di $g(x)$. Il polinomio $g(x)$ è irriducibile per il criterio di Eisenstein, e quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$.

- Dire quante e quali sono le estensioni intermedie $\mathbb{Q} \subset E \subset L$ tali che $[E : \mathbb{Q}] = 2$.

  Soluzione: L è il campo di spezzamento di un polinomio separabile (siamo in caratteristica 0) e quindi è un'estensione di Galois di $\mathbb{Q}$. Poiché $[L : \mathbb{Q}] = 6$, il gruppo $\mathrm{Gal}(L/\mathbb{Q})$ ha ordine 6. A prescindere dal fatto che sia ciclico o isomorfo a S_3, possiede un solo sottogruppo[1] di indice 2, e quindi vi è una sola estensione intermedia di grado 2 su $\mathbb{Q}$. Non può che trattarsi di $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta)$.

- Determinare $\mathrm{Gal}(L/\mathbb{Q})$ a meno di isomorfismo.

  Soluzione: Gli elementi di $\mathrm{Gal}(L/\mathbb{Q})$ sono determinati dalla loro azione su α. Inoltre, $\phi(\alpha)$ può essere soltanto una delle sei radici $\zeta^i\alpha$. E' utile osservare che $\phi(\alpha^3) = \zeta^{3i}\alpha^3$ e quindi $\phi(\sqrt{-3}) = \pm\sqrt{-3}$, a seconda che i sia pari oppure dispari; nei due casi abbiamo quindi $\phi(\zeta) = \zeta^{\pm 1}$. Indichiamo con ϕ_i l'automorfismo che applica α in $\zeta^i\alpha$. Chiaramente, ϕ_0 è l'identità. Per quanto riguarda ϕ_1, si ha $\phi_1(\alpha) = \zeta_\alpha$, $\phi_1(\zeta\alpha) = \phi_1(\zeta)\phi_1(\alpha) = \zeta^{-1}\zeta\alpha = \alpha$. ϕ_1^2 fissa allora α, e coincide con l'identità. Concludiamo che ϕ_1 ha ordine 2.
  Ripetendo questo ragionamento, si vede che ϕ_3 scambia α con $\zeta^3\alpha$. Di conseguenza anche ϕ_3 ha ordine 2. Il gruppo G, di ordine 6, possiede pertanto almeno due elementi di ordine 2, e non può quindi essere ciclico.

[1] Si dice anche *"il 3-Sylow è normale"*.

(4) In questo esercizio sfruttiamo la teoria di Galois per fattorizzare il polinomio $f(x) = x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) \in \mathbb{F}_{11}[x]$.

- Mostrare che il gruppo moltiplicativo $\mathbb{F}_{11^n}^\times$ contiene elementi di ordine 7 se e solo se n è multiplo di 3.

  Soluzione: Il gruppo $\mathbb{F}_{11^n}^\times$ possiede $11^n - 1$ elementi. Per i teoremi di Cauchy e Lagrange, contiene elementi di ordine 7 se e solo se 7 divide $11^n - 1$, cioè esattamente quando $11^n \equiv 1 \mod 7$. Si vede che $[11] = [4]$ ha ordine 3 in $\mathbb{Z}/(7)^\times$, e quindi l'equazione è verificata per ogni n multiplo di 3.

- Mostrare che se $\mathbb{F}_{11^n}^\times$ contiene elementi di ordine 7, allora $f(x)$ si spezza in $\mathbb{F}_{11}[x]$ in fattori lineari. Calcolare il grado su $\mathbb{F}_{11}$ del campo di spezzamento L di $f(x)$.

  Soluzione: Se $\mathbb{F}_{11^n}^\times$ contiene un elemento di ordine 7, contiene almeno le sue sette potenze distinte. Questi sono elementi di $\mathbb{F}_{11^n}$ che soddisfano $f(x)$. Pertanto $f(x)$ ha 7 radici distinte in $\mathbb{F}_{11^n}$, e si spezza quindi nel prodotto di fattori lineari. Il minimo valore per cui questo accade è $n = 3$; possiamo concludere che $L = \mathbb{F}_{11^3}$ è il campo di spezzamento di $f(x)$, e di conseguenza $[L : \mathbb{F}_{11}] = 3$.

- Sia $1 \neq \omega \in L$, $\omega^7 = 1$. Quali sono le altre radici in L del polinomio minimo $g(x) \in \mathbb{F}_{11}[x]$ di ω?

  Soluzione: Le radici del polinomio minimo di ω sono gli elementi dell'orbita di ω sotto l'azione del gruppo di Galois. Essendo questo ciclico, e generato dal Frobenius $\alpha \mapsto \alpha^{11}$, si ottengono applicando ad ω ripetutamente il Frobenius.
  Ricordando che $\omega^7 = 1$, si ottiene $F(\omega) = \omega^{11} = \omega^4$. $F^2(\omega) = F(\omega^4) = \omega^{44} = \omega^2$. $F(\omega^3) = F(\omega^2) = \omega^{22} = \omega$. L'orbita di ω contiene quindi i tre elementi $\omega, \omega^2, \omega^4$, come doveva essere, dal momento che il gruppo di Galois è ciclico di ordine 3.

- Mostrare che $g(x)$ è della forma $x^3 + ax^2 + (a-1)x - 1, a \in \mathbb{F}_{11}$, e fattorizzare $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ nel prodotto di irriducibili di $\mathbb{F}_{11}[x]$, utilizzando l'informazione che i suoi fattori irriducibili hanno questa forma.

  Soluzione: Il polinomio minimo di ω su $\mathbb{F}_{11}$ è $(x-\omega)(x-\omega^2)(x-\omega^4) = x^3 - (\omega + \omega^2 + \omega^4)x^2 + (\omega^3 + \omega^5 + \omega^6)x - 1$. Si vede che la differenza tra il coefficiente del termine di grado 1 e quello di grado 2 vale esattamente $\omega^3 + \omega^5 + \omega^6 + \omega + \omega^2 + \omega^4 = -1$. Se a è il coefficiente di grado 2, allora $a - 1$ deve essere il coefficiente di grado 1.
  Ricapitolando, $x^7 - 1$ è prodotto di $x - 1$ e di due polinomi irriducibili di grado 3 della forma $x^3 + ax^2 + (a-1)x - 1$. Possiamo procedere per forza bruta, imponendo

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + ax^2 + (a-1)x - 1)(x^3 + bx^2 + (b-1)x - 1).$$

  Confrontando i termini di grado 5 si trova che $a + b = 1$, e da quelli di grado 4 si ottiene $ab + a - 1 + b - 1 = 1$, che diventa $ab = 2$ utilizzando $a + b = 1$. Sostituendo $b = 1 - a$ nella seconda equazione, si ottiene $a^2 - a + 2 = 0$ che ha le soluzioni $a = 5, 7$. Quindi

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + 5x^2 + 4x - 1)(x^3 + 7x^2 + 6x - 1).$$

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI ROMA – "LA SAPIENZA"
E-mail address: dandrea@mat.uniroma1.it