ALGEBRA 2 — Terzo esame scritto
3 settembre 2012
soluzioni

(1)
- [4pt] Esistono omomorfismi suriettivi $\mathrm{S}_4 \to \mathrm{S}_3$? Se sì, quanti sono?
Soluzione: Il (primo?) teorema di isomorfismo ci informa che se $\phi : G \to H$ è un omomorfismo di gruppi, allora l'immagine di ϕ è isomorfa a $G/\ker\phi$. Il nucleo di un omomorfismo suriettivo $\phi : \mathrm{S}_4 \to \mathrm{S}_3$ deve allora avere ordine $|\,\mathrm{S}_4\,|/|\,\mathrm{S}_3\,| = 24/6 = 4$, ed effettivamente S_4 possiede un sottogruppo normale di tale ordine: V_4.
Dal momento che S_4/V_4 non possiede elementi di ordine 6, non è ciclico, ed è quindi isomorfo a S_3. Ogni isomorfismo $f : \mathrm{S}_4/V_4 \to \mathrm{S}_3$ si solleva dunque ad un unico omomorfismo suriettivo $\phi = f \circ \pi$, dove $\pi : \mathrm{S}_4 \to \mathrm{S}_4/V_4$ è la proiezione al quoziente. Contare gli isomorfimi $\mathrm{S}_4/V_4 \to \mathrm{S}_3$ non è difficile: è equivalente a contare gli isomorfismi di S_3 con se stesso. Abbiamo visto a lezione che gli automorfismi di S_3 sono sei, tutti interni. Pertanto gli omomorfismi suriettivi $\mathrm{S}_4 \to \mathrm{S}_3$ sono in totale sei.

- [4pt] Esistono omomorfismi suriettivi $\mathrm{S}_5 \to \mathrm{S}_4$? Se sì, quanti sono?
Soluzione: Per il ragionamento precedente, se $\phi : \mathrm{S}_5 \to \mathrm{S}_4$ è un omomorfismo suriettivo, $\ker\phi$ deve avere ordine $|\,\mathrm{S}_5\,|/|\,\mathrm{S}_4\,| = 120/24 = 5$. Tuttavia, S_5 non possiede sottogruppi normali di ordine 5, poiché il suo unico sottogruppo normale non banale è A_5, come abbiamo visto a lezione.

(2) G è un gruppo di ordine 374.

- [2pt] Mostrare che G è prodotto semidiretto di un sottogruppo di ordine 2 e di un sottogruppo normale ciclico di ordine 187.
  Soluzione: L'esistenza di un sottogruppo normale N di ordine 187 si può mostrare in vari modi: innanzitutto abbiamo visto a lezione, sfruttando l'immersione di Cayley, che un gruppo di ordine $2d$, con d dispari, possiede sempre un sottogruppo di indice 2. Alternativamente, per il teorema di Sylow, in un gruppo di ordine $374 = 2{\cdot}11{\cdot}17$, il 17-Sylow è sicuramente normale, in quanto 1 è l'unico divisore di $2 \cdot 11$ congruo ad $1 \mod 17$. Moltiplicandolo per uno qualsiasi degli 11-Sylow, si ottiene un sottogruppo di ordine $11 \cdot 17/1 = 187$, in quanto l'intersezione tra un sottogruppo di ordine 11 e uno di ordine 17 ha ordine che li divide entrambi, ed è quindi necessariamente banale. Un sottogruppo di ordine 187 ha indice 2, ed è quindi normale. Un gruppo di ordine $187 = 11 \cdot 17$ è ciclico, poiché $11 < 17$ sono primi distinti, e 11 non divide $17 - 1$.
  Il teorema di Sylow, o anche solo quello di Cauchy, ci garantiscono l'esistenza di almeno un sottogruppo H di ordine 2. G è allora prodotto semidiretto di H e N poiché $H \cap N$ ha ordine 1 per il motivo indicato prima, e allora $|HN| = |H||N|/|H \cap N| = 2 \cdot 187/1 = 374$ mostra che $HN = G$.

- [3pt] Esibire quattro gruppi di ordine 374, a 2 a 2 non isomorfi, e spiegare perché non lo siano.
  Soluzione: I gruppi $\mathrm{C}_{374}, \mathrm{D}_{187}, \mathrm{C}_{11} \times \mathrm{D}_{17}, \mathrm{C}_{17} \times \mathrm{D}_{11}$ hanno tutti ordine 187, ma hanno centri di ordini diversi, e non sono quindi isomorfi.

- [3pt] Spiegare perché G sia necessariamente isomorfo ad uno dei quattro gruppi elencati.
  Soluzione: G è isomorfo ad un prodotto semidiretto esterno $N \ltimes_\phi H$, dove $\phi : H \to \mathrm{Aut}(N)$ è un omomorfismo di gruppi. Poiché $N \simeq \mathrm{C}_{187}$, abbiamo $\mathrm{Aut}(N) \simeq \mathbb{Z}_{187}^\times \simeq \mathrm{C}_{10} \times \mathrm{C}_{16}$. Tale gruppo possiede esattamente tre elementi di ordine 2; poiché ϕ è determinato dall'immagine dell'elemento di ordine 2, che può soltanto essere un elemento di ordine 2 di $\mathrm{Aut}(N)$, oppure l'identità, esistono al più quattro possibili scelte per ϕ. Pertanto esistono al più quattro gruppi di ordine 374 a meno di isomorfismo; per il punto precedente, ne esistono esattamente quattro.

(3) E' dato il polinomio $f(x) = x^5 - 2 \in \mathbb{F}_7[x]$.

- [3 pt] Sia K un'estensione finita di $\mathbb{F}_7$. Mostrare che se $\omega \in K \setminus \mathbb{F}_7$ è una radice di f, allora ω ha ordine 15 nel gruppo moltiplicativo K^*.
  Soluzione: Da $\omega^5 = 2$ segue $\omega^{15} = (\omega^5)^3 = 2^3 = 8 = 1$ (ricordiamo che siamo in caratteristica 7!!!). Pertanto l'ordine moltiplicativo di ω divide 15. Sicuramente non è 1, poiché l'identità di $K^\times$ appartiene a $\mathbb{F}_7$; e non è 5, poiché $\omega^5 = 2 \neq 1$. Tuttavia, l'ordine di ω non può nemmeno essere 3: infatti se $\omega^3 = 1$, allora $\omega^6 = 1$, e quindi $\omega = \omega^6/\omega^5 = 1/2 = 4 \in \mathbb{F}_7$. Possiamo allora concludere che l'ordine di ω è 15.

- [2 pt] Mostrare che il gruppo di Galois $\mathrm{Gal}(L/\mathbb{F}_7)$ del campo di spezzamento L di f ha ordine 2 o 4.
  Soluzione: Si verifica facilmente che $f(4) = 0$, che fornisce la fattorizzazione $f(x) = (x+3) \cdot h(x)$ con $h(x) = x^4 + 4x^3 + 2x^2 + x + 4$. Sostituendo nella sua espressione, si vede che h non ha radici in $\mathbb{F}_7$ ed è pertanto irriducibile, oppure prodotto di due polinomi irriducibili di grado 2.
  Nel primo caso, il campo $\mathbb{F}_{7^4}$ è campo di spezzamento di $f(x)$, poiché ogni polinomio irriducibile in $\mathbb{F}_7[x]$ di grado divisore di 4 si spezza in $\mathbb{F}_{7^4}$, e un'estensione che contenga una radice di $f(x)$ deve avere grado almeno 4.
  Allo stesso modo, nel secondo caso, il campo $\mathbb{F}_{7^2}$ è campo di spezzamento di $f(x)$.
  Le estensioni tra campi finiti sono tutte di Galois, e quindi l'ordine del gruppo di Galois, che coincide col grado dell'estensione, è 2 oppure 4.

- [3 pt] Determinare la struttura di $\mathrm{Gal}(L/\mathbb{F}_7)$.
  Soluzione: Il gruppo di Galois di ogni estensione tra campi finiti è ciclico, ed è generato dal Frobenius. Rimane soltanto da capire se l'ordine di tale gruppo ciclico è 2 o 4, cioè se il polinomio $h(x)$ è riducibile o irriducibile. Questo può essere fatto in maniera diretta per forza bruta (ricordate che i coefficienti della fattorizzazione vanno cercati in $\mathbb{F}_7$, e non in $\mathbb{Z}$!!!), ma preferisco farlo in maniera indiretta.
  Abbiamo visto nel primo punto che ogni campo che contiene una radice ω del polinomio $h(x)$ possiede un elemento di ordine moltiplicativo 15. Per questo motivo, se L è il campo di spezzamento di $f(x)$, il gruppo moltiplicativo $L^\times$ deve avere ordine multiplo di 15 per il Teorema di Lagrange. Tuttavia $\mathbb{F}_{49}^\times$ possiede 48 elementi, che non è multiplo di 15. L'unica possibilità è che $h(x)$ sia irriducibile, e che $\mathrm{Gal}(L/\mathbb{F}_7)$ sia isomorfo a C_4.
  Non rimaniamo ora sorpresi dal fatto che $|\mathbb{F}_{7^4}^\times| = 7^4 - 1 = 2400$ è effettivamente divisibile per 15.

(4) Se α, β, γ le tre radici complesse del polinomio $g(x) = x^3 + x - 3$, sia $F = \mathbb{Q}(\alpha, \beta, \gamma)$.

- [4 pt] Dire quanti sono i campi strettamente compresi tra $\mathbb{Q}$ e F.
  Soluzione: Il polinomio $g'(x) = 3x^2 + 1$ è sempre positivo sui reali, e pertanto $g(x)$, visto come funzione reale, è crescente. Di conseguenza, $g(x)$ possiede un'unica radice reale, e due radici complesse coniugate non reali. Inoltre, $g(x)$ è irriducibile in $\mathbb{Q}[x]$, poiché gli unici candidati ad essere radici razionali — $\pm 1, \pm 3$ — non lo soddisfano. Siano α la radice reale di g e $\beta, \gamma = \overline{\beta}$ le altre radici.
  Poiché $g(x) \in \mathbb{Q}[x]$ è irriducibile, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Inoltre $\beta \notin \mathbb{Q}(\alpha)$, dal momento che $\mathbb{Q}(\alpha) \subset \mathbb{R}$ e $\beta \notin \mathbb{R}$. Pertanto $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$ è diverso da 1, e quindi inevitabilmente uguale a 2. Poiché $\gamma = 3/\alpha\beta$, $F = \mathbb{Q}(\alpha, \beta)$ ha grado
  $$[F : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6.$$
  F è quindi un'estensione di Galois di $\mathbb{Q}$ con gruppo di Galois di ordine 6 che permuta fedelmente le tre radici α, β, γ; di conseguenza $\mathrm{Gal}(F/\mathbb{Q}) \simeq \mathrm{S}_3$. Per la corrispondenza di Galois, vi è un campo strettamente compreso tra $\mathbb{Q}$ e F per ogni sottogruppo non banale di S_3. Questi ultimi sono quattro: i tre 2-Sylow e l'unico 3-Sylow.
  Per onor di cronaca, i campi corrispondenti ai primi tre sottogruppi sono $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$, $\mathbb{Q}(\gamma)$; l'estensione quadratica $\mathbb{Q}(\sqrt{-247})$ corrispondente al 3-Sylow è più complicata da individuare, e nell'economia dell'esercizio non ci interessa farlo.

- [4 pt] Dire quanti e quali di tali campi sono completamente contenuti in $\mathbb{R}$.
  Soluzione: Dobbiamo dire quali dei quattro campi individuati sono completamente contenuti in $\mathbb{R}$. Notiamo che un numero complesso è reale se e solo se è fissato dalla coniugazione complessa. Inoltre, la coniugazione complessa c è/induce uno degli elementi di $\mathrm{Gal}(F/\mathbb{Q})$. Gli elementi reali di F sono quindi quelli del campo fisso $F^{(c)}$ del sottogruppo generato da c, che ha ordine 2 in quanto $c^2 = \mathrm{id}$.
  $F \cap \mathbb{R}$ è quindi un'estensione di $\mathbb{Q}$ di grado 3, e contiene sicuramente $\mathbb{Q}(\alpha)$: non può che coincidere con $\mathbb{Q}(\alpha)$. Ogni estensione intermedia completamente reale è dunque contenuta in $\mathbb{Q}(\alpha)$, che ha grado 3. Il suo grado deve allora dividere 3. In conclusione, l'unico campo completamente reale, intermedio tra $\mathbb{Q}$ e F, è $\mathbb{Q}(\alpha)$.

Nella risoluzione di ciascun punto potete dare per buoni i punti precedenti.

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