ALGEBRA 2 — Secondo esame scritto
20 luglio 2012
soluzioni

(1) Se $H < G$, allora $C(H) = \{g \in G \,|\, gh = hg$ per ogni $h \in H\}$ è il *centralizzatore* di H.

- [3pt] Mostrare che $C(H)$ è un sottogruppo di G. *Soluzione:* Innanzitutto, l'identità commuta sicuramente con ogni elemento di H, e quindi $\mathrm{id} \in C(H)$. Inoltre, se $x, y \in C(H)$, allora $xh = hx, yh = hy$ per ogni $h \in H$; pertanto
$$(xy)h = x(yh) = x(hy) = (xh)y = (hx)y = h(xy),$$
da cui $xy \in C(H)$. Alla stessa maniera, da $xh = hx$ segue $hx^{-1} = x^{-1}h$ moltiplicando a destra e a sinistra per h^{-1}. Pertanto $x \in C(H)$ implica $x^{-1} \in C(H)$. In conclusione $C(H)$ è un sottoinsieme non vuoto di G chiuso rispetto a prodotto e inverso, ed è pertanto un sottogruppo.
Si poteva procedere anche indirettamente: $C(H)$ è l'intersezione dei centralizzatori degli elementi di H. Poiché il centralizzatore di un elemento è sempre un sottogruppo (lo abbiamo visto a lezione) e l'intersezione di sottogruppi è un sottogruppo, $C(H)$ non può che essere un sottogruppo.

- [4pt] Mostrare che se $H \lhd G$, allora $C(H) \lhd G$.
Soluzione: E' sufficiente mostrare che se $xinC(H), g \in G$, allora $gxg^{-1} \in C(H)$. In effetti, se $x \in C(H)$ e $h \in H \lhd G$, abbiamo
$$gxg^{-1}h = gx(g^{-1}hg)g^{-1} = g(g^{-1}hg)xg^{-1} = hgxg^{-1},$$
dove, grazie alla normalità di H, sappiamo che x commuta con $g^{-1}hg \in g^{-1}Hg = H$.
Vi erano altre maniere di procedere, tutte equivalenti. La più rapida è forse notare che se $H \lhd G$, allora ogni elemento $g \in G$ induce un automorfismo (non necessariamente interno) di H dato da $T_g : h \mapsto ghg^{-1}$. L'applicazione
$$G \ni g \mapsto T_g \in \mathrm{Aut}(G)$$
è un omomorfismo, e il suo nucleo è $C(H)$, che deve quindi essere normale.

(2) Si consideri la permutazione $\sigma = (1\,5\,2\,9\,7)$ nel gruppo simmetrico A_9.

- [2pt] Calcolare il numero dei coniugati di σ in A_9.
  Soluzione: Sappiamo bene che in un gruppo simmetrico, due elementi sono coniugati se e solo se hanno la stessa struttura ciclica. Questo è in generale nei gruppi alterni, ma abbiamo visto a lezione che continua a valere per le classi di coniugio di elementi che commutano, nel gruppo simmetrico, con almeno una permutazione dispari. Nel nostro caso, σ commuta ad esempio con $(3\,4)$, e quindi i suoi coniugati in A_9 sono tutti e soli i 5-cicli.
  Il conto è adesso facile: i 5-cicli in A_9 sono esattamente
  $$\binom{9}{5} \cdot 4! = 9 \cdot 8 \cdot 7 \cdot 6 = 3024.$$

- [2pt] Calcolare l'ordine del normalizzatore N in A_9 del sottogruppo $H = (\sigma)$.
  Soluzione: Il sottogruppo H è un 5-Sylow di A_9, e i 5-Sylow sono tutti coniugati tra loro. Il loro numero coincide con l'indice del normalizzatore $N = N(H)$. Contare i 5-Sylow è facile: sappiamo per il punto precedente che il numero di elementi di ordine 5 in A_9 è 3024, e ciascun 5-Sylow ne contiene esattamente 4. Inoltre, ogni elemento di ordine 5 genera un 5-Sylow, e due 5-Sylow distinti si intersecano nella sola identità. Il numero di 5-Sylow è quindi pari a $3024/4 = 9 \cdot 7 \cdot 6 \cdot 2 = 756$.
  Poiché $[\mathrm{A}_9 : N] = 756$, avremo
  $$|N| = \frac{9!}{2} \cdot \frac{1}{756} = \frac{9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{9 \cdot 7 \cdot 6 \cdot 4} = 8 \cdot 5 \cdot 3 \cdot 2 = 240.$$

- [2pt] Mostrare che N contiene almeno un sottogruppo di ordine 20.
  Soluzione: Il sottogruppo H, di ordine 5, è sicuramente normale nel suo normalizzatore N. Se troviamo in N un sottogruppo K di ordine 4, il prodotto NK sarà un sottogruppo di N di ordine 20. Ad ogni modo, ciascun 2-Sylow di N contiene 16 elementi, e possiede quindi un sottogruppo di ordine 4, dal momento che ogni p-gruppo possiede sottogruppi di qualsiasi ordine possibile.

- [2pt] Mostrare che N contiene almeno un sottogruppo abeliano di ordine 20.
  Soluzione: Come nel punto precedente, basta trovare un sottogruppo di N di ordine 4 che commuti con H. Questo si può fare in maniera diretta, notando che $\{\mathrm{id}, (34)(68), (36)(48), (38)(46)\}$ è un tale sottogruppo, oppure indirettamente. In effetti, dal calcolo del numero dei coniugati di σ possiamo facilmente ricavare l'ordine del suo centralizzatore, che è
  $$|(C(\sigma)| = \frac{9!}{2} \frac{1}{9 \cdot 8 \cdot 7 \cdot 6} = \frac{5!}{2} = 60.$$
  Ma allora il 2-Sylow di $C(\sigma)$ contiene 4 elementi che commutano con σ e quindi centralizzano $H = (\sigma)$.

(3) • [3 pt] Calcolare il polinomio minimo di $\gamma = \sqrt{2} + \sqrt[4]{8}$ su $\mathbb{Q}$.
Soluzione: Notiamo subito che $\gamma \in \mathbb{Q}(\sqrt[4]{2})$, e quindi sicuramente $\mathbb{Q}(\gamma) \subset \mathbb{Q}(\sqrt[4]{2})$. Il polinomio $x^4 - 2 \in \mathbb{Q}[x]$, irriducibile per il Criterio di Eisenstein, annulla $\alpha = \sqrt[4]{2}$, e quindi $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
E′ facile trovare un polinomio razionale annullato da γ. In effetti $\gamma - \sqrt{2} = \sqrt[4]{8}$, e quadrando si ottiene

$$\gamma^2 + 2 - 2\gamma\sqrt{2} = 2\sqrt{2},$$

da cui $\gamma^2 + 2 = 2\sqrt{2}(\gamma + 1)$ e quadrando nuovamente

$$\gamma^4 + 4\gamma^2 + 4 = 8\gamma^2 + 16\gamma + 8.$$

Il polinomio $x^4 - 4x^2 - 16x - 4$ annulla quindi γ. Si può ora verificare direttamente, per forza bruta, che questo polinomio è irriducibile in $\mathbb{Q}[x]$. Tuttavia è più semplice notare che $1, \alpha, \alpha^2, \alpha^3$ formano una $\mathbb{Q}$-base di $\mathbb{Q}(\alpha)$, ed esprimere in questa base le potenze di γ. Si ha: $\gamma^0 = 1, \gamma^1 = \alpha^2 + \alpha^3, \gamma^2 = 2(1 + \alpha + \alpha^2)$ che sono evidentemente $\mathbb{Q}$-linearmente indipendenti. Pertanto il grado di γ su $\mathbb{Q}$ è superiore a 2. Dovendo dividere $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, deve essere necessariamente 4.

• [2 pt] L'estensione $\mathbb{Q} \subset \mathbb{Q}(\gamma)$ è normale?
Soluzione: Abbiamo già visto che $\mathbb{Q}(\gamma)$ coincide con $\mathbb{Q}(\alpha)$, che non può essere normale, in quanto non contiene tutte le radici di $x^4 - 2$: in effetti, due di tali radici sono immaginarie pure, mentre ogni elemento di $\mathbb{Q}(\alpha)$ è reale.

• [3 pt] Determinare il grado su $\mathbb{Q}$ del più piccolo campo $\mathbb{Q} \subset E \subset \mathbb{C}$ che sia un'estensione di Galois di $\mathbb{Q}$ e che contenga γ.
Soluzione: Tale campo E è il campo di spezzamento del polinomio $x^4 - 2$, e coincide quindi con $\mathbb{Q}(\pm\alpha, \pm i\alpha) = \mathbb{Q}(\alpha, i)$. Si vede facilmente che $[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)] = 2$, in quando i soddisfa $x^2 + 1$ e non appartiene a $\mathbb{Q}(\alpha) \subset \mathbb{R}$. Pertanto $[E : \mathbb{Q}] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8$.

(4) Il campo $K = \mathbb{F}_5(\alpha)$ è un'estensione finita di $\mathbb{F}_5$, e α soddisfa $\alpha^4 = 2\alpha + 1$.

- [4 pt] Mostrare che $[K : \mathbb{F}_5] = 4$.
  Soluzione: α soddisfa il polinomio $x^4 - 2x - 1 \in \mathbb{F}_5[x]$. E' necessario quindi mostrare che questo polinomio è irriducibile. Procediamo per forza bruta: se
  $$x^4 - 2x - 1 = (x^2 + ax + b)(x^2 - ax + c),$$
  allora
  $$\begin{cases} b + c = a^2 \\ a(b - c) = 2 \\ bc = 1 \end{cases} .$$
  A meno di scambiare b con c, le uniche soluzioni a $bc = 1$ sono: $b = c = \pm 1$, $b = 2, c = 3$. Nel primo caso si ottiene $a^2 = \pm 2$, che non è un quadrato in $\mathbb{F}_5$, e nel secondo si ottiene $a^2 = 0$, che contraddice la seconda equazione. Il polinomio è pertanto irriducibile.
  Esiste un altro modo di procedere, più involuto. Se il polinomio $x^4 - 2x - 1$ si fattorizza in $\mathbb{F}_5[x]$, si spezza allora nel prodotto di due irriducibili di grado 2 — si controlla infatti facilmente che $x^4 - 2x - 1$ non possiede radici in $\mathbb{F}_5$. Allora una radice α soddisfa anche uno di tali fattori di grado 2, e quindi $F(F(\alpha)) = \alpha$, dove F indica l'automorfismo di Frobenius $x \mapsto x^5$.
  Ora, si calcola facilmente $F(\alpha) = \alpha^5 = \alpha(\alpha^4) = \alpha(2\alpha + 1) = 2\alpha^2 + \alpha$, da cui
  $$F^2(\alpha) = 2(2\alpha^2 + \alpha)^2 + (2\alpha^2 + \alpha) = 8\alpha^4 + 8\alpha^3 + 4\alpha^2 + \alpha.$$
  Se $F^2(\alpha) = \alpha$, si ottiene $8\alpha^4 + 8\alpha^3 + 4\alpha^2 = 0$ e quindi α soddisfa anche $2x^2 + 2x + 1$, o la sua versione monica $x^2 + x + 3$. Possiamo allora concludere che OGNI radice di $x^4 - 2x - 1$ soddisfa $x^2 + x + 3$, e quindi che $x^4 - 2x - 1 = (x^2 + x + 3)^2$, il che è sicuramente falso. L'ipotesi che $x^4 - 2x - 1$ conduce quindi ad una contraddizione.

- [2 pt] Quante sono le soluzioni in K dell'equazione $x^2 + x + 2 = 0$?
  Soluzione:K è un'estensione di grado 4 di $\mathbb{F}_5$, e quindi ogni polinomio irriducibile di grado che divide 4 si spezza in K. Le soluzioni sono quindi 2, anche se bisognerebbe controllare che le soluzioni non coincidano (nessuno studente lo ha verificato).

- [2 pt] Elencare tutti i campi strettamente contenuti tra $\mathbb{F}_5$ e K.
  Soluzione: Una volta identificato K con $\mathbb{F}_{625}$, l'unico campo strettamente contenuto è $\mathbb{F}_{25}$.

Dipartimento di Matematica, Università degli studi di Roma – "La Sapienza"
E-mail address: dandrea@mat.uniroma1.it