Corso di Algebra 2 – a.a. 2010-2011

Prova scritta del 7.2.2012

1. (a) Siano G e H gruppi finiti, e sia $f : G \to H$ un omomorfismo **suriettivo**. Mostrare che $f([G,G]) = [H,H]$ e che l'indice $\big[G : [G,G]\big]$ è maggiore o uguale a $\big[H : [H,H]\big]$.

   (b) Sia G un gruppo di ordine p^n, dove p è primo e $n \geq 2$. Mostrare che $\big[G : [G,G]\big] \geq p^2$.

2. Equazioni algebriche risolubili e non risolubili per radicali: discutere la teoria e dare esempi concreti.

3. Dato un polinomio razionale $p(x) \in \mathbb{Q}[x]$ sia K un campo di spezzamento di p su $\mathbb{Q}$. Si calcoli il grado $[K : \mathbb{Q}]$ nei seguenti casi:

   (a) $p(x) = x^3 + 3$

   (b) $p(x) = x^4 - 9$

   (c) $p(x) = x^6 - 25x^2 - 20x$

Soluzioni

1. (a) $[H,H]$ è generato dai commutatori $[h,h']$, $h, h' \in H$. Dato che f è suriettiva ci sono elementi $g, g' \in G$ tali che $h = f(g)$ e $h' = f(g')$, quindi $[h,h'] = [f(g), f(g')] = f([g,g'])$. Ne segue che $[H,H] = f([G,G])$. Dato che il nucleo dell'omomorfismo composto $G \to H \to H/[H,H]$ contiene $[G,G]$, per i teoremi di omomorfismo c'è un omomorfismo suriettivo $G/[G,G] \to H/[H,H]$. Quindi

$$\big[G : [G,G]\big] = \#\big(G/[G,G]\big) \geq \#\big(H/[H,H]\big) = \big[H : [H,H]\big]$$

   (b) Induzione su n. Se $n = 2$, G è abeliano, quindi $[G,G] = \{1\}$ ha indice p^2. Per $n > 2$, se G è abeliano non c'è niente da dimostrare. Supponiamo G non abeliano. Dato che G è un p-gruppo il suo centro Z non è banale. Ricordiamo che il quoziente di un gruppo modulo il suo centro non può essere ciclico. In particolare, Z ha indice almeno p^2. Quindi $H = G/Z$ ha ordine almeno p^2 e per ipotesi induttiva $\big[H : [H,H]\big] \geq p^2$. Usando (a) ne segue che $\big[G : [G,G]\big] \geq \big[H : [H,H]\big] \geq p^2$.

3. (a) $K = \mathbb{Q}[\zeta, \eta]$, dove ζ è una radice cubica di -3 e η è una radice cubica di 1. Dato che $x^3 + 3$ è irriducibile, perché non ha radici razionali, $[\mathbb{Q}[\zeta] : \mathbb{Q}] = 3$, mentre $[\mathbb{Q}[\eta] : \mathbb{Q}] = 2$ perché il polinomio minimo di η è il polinomio ciclotomico $x^2 + x + 1$. Dato che 3 e 2 sono primi fra loro $\big[\mathbb{Q}[\zeta, \eta] : \mathbb{Q}\big] = 6$.

   (b) $x^4 - 9 = (x^2 - 3)(x^2 + 3)$, e quindi $K = \mathbb{Q}[\sqrt{3}, \sqrt{-3}]$. Ora $\big[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}\big] = \big[\mathbb{Q}[\sqrt{-3}] : \mathbb{Q}\big] = 2$, mentre $\sqrt{-3} \notin \mathbb{R} \supset \mathbb{Q}[\sqrt{3}]$. Ne segue che $\mathbb{Q}[\sqrt{3}, \sqrt{-3}] \neq \mathbb{Q}[\sqrt{3}$, e quindi che $\big[\mathbb{Q}[\sqrt{3}, \sqrt{-3}] : \mathbb{Q}[\sqrt{3}]\big] = 2$. In conclusione

$$\big[\mathbb{Q}[\sqrt{3}, \sqrt{-3}] : \mathbb{Q}\big] = \big[\mathbb{Q}[\sqrt{3}, \sqrt{-3}] : \mathbb{Q}[\sqrt{3}]\big]\big[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}\big] = 4$$

   (c) $p(x) = x(x^5 - 25x - 20)$, quindi K è il campo di spezzamento di $q(x) = x^5 - 25x - 20$ su $\mathbb{Q}$. Il polinomio $q(x)$ è irriducibile per il criterio di Eisenstein. La funzione reale di variabile reale $x \mapsto q(x)$ ha punti stazionari nelle radici di $q'(x) = 5x^4 - 25$, cioè in $\pm\sqrt[4]{5}$,

quindi è strettamente crescente per $x < -\sqrt[4]{5}$ e per $x > \sqrt[4]{5}$, e strettamente decrescente per $-\sqrt[4]{5} < x < \sqrt[4]{5}$, e tende a $\pm\infty$ per $x \to \pm\infty$. Inoltre

$$q(-\sqrt[4]{5}) = -5\sqrt[4]{5} + 25\sqrt[4]{5} - 20 = 20(\sqrt[4]{5} - 1) > 0$$
$$q(\sqrt[4]{5}) = 5\sqrt[4]{5} - 25\sqrt[4]{5} - 20 = -20\sqrt[4]{5} - 20 < 0$$

Ne segue che il polinomio $q(x)$ ha esattamente tre radici reali, una minore di $-\sqrt[4]{5}$, una tra $-\sqrt[4]{5}$ e $\sqrt[4]{5}$ e una maggiore di $\sqrt[4]{5}$. Le rimanenti due radici sono complesse coniugate. In questa situazione si sa che il gruppo di Galois di $q(x)$ è il gruppo simmetrico S_5 (vedi sotto per una spiegazione). Quindi

$$\big[K : \mathbb{Q}\big] = \#S_5 = 5! = 120$$

L'affermazione sul gruppo di Galois si dimostra così. Il gruppo di Galois G è un sottogruppo del gruppo delle permutazioni delle radici di $q(x)$, e quindi di S_5. Dato che $q(x)$ è irriducibile G agisce transitivamente sulle radici. Inoltre G contiene il coniugio complesso, che lascia fisse le tre radici reali e scambia le due complesse. Dunque G contiene una trasposizione e dato che agisce transitivamente sulle radici deve coincidere con S_5.