Il grado di $\alpha + \beta$

LEMMA 1. Dati due insiemi A e B, con $|A| = m$ e $|B| = n$ coprimi, e due azioni $G \times A \to A$ e $G \times B \to B$ transitive, l'azione di G su $A \times B$ data da $g \cdot (a, b) := (g \cdot a, g \cdot b)$ è transitiva.

Dimostrazione. Abbiamo $|G(a,b)| = [G : G_{(a,b)}]$ e $G_{(a,b)} = G_a \cap G_b$ (con Gx e G_x indichiamo orbita e stabilizzatore di x). Ma $[G : G_a] = |Ga| = m$ e $[G : G_b] = |Gb| = n$, quindi sappiamo che $\operatorname{lcm}(m, n) \mid [G : G_a \cap G_b] \leq mn$, cioè $[G : G_a \cap G_b] = mn$. Segue che $|G(a,b)| = mn = |A \times B|$. □

LEMMA 2. Se $A = \{\alpha_1, \ldots, \alpha_m\}$ e $B = \{\beta_1, \ldots, \beta_n\}$ sono due insiemi di algebrici, con $(m, n) = 1$, e G è un gruppo finito di automorfismi per $\mathbb{Q}(A, B)/\mathbb{Q}$ che agisce transitivamente sugli elementi di A e di B (chiusi rispetto alla sua azione), allora $\alpha_1 + \beta_1 = \alpha_k + \beta_\ell$ non ha soluzioni non banali.

Dimostrazione. Possiamo supporre che la tesi sia falsa per un certo $|G|$ minimo. Se $m = 1$ o $n = 1$ non c'è niente da dimostrare, quindi supponiamo $m, n > 1$. Siano $W_a := \langle A \rangle_{\mathbb{Q}}$ e $W_b := \langle B \rangle_{\mathbb{Q}}$ i $\mathbb{Q}$-sottospazi generati da A e B e $U := W_a \cap W_b$. Osserviamo che, per ogni $g \in G$, è $g(U) = U$. Poniamo $\alpha := \alpha_1$, $\beta := \beta_1$ e $\alpha' := \alpha_k$, $\beta' := \beta_\ell$. Consideriamo ora l'azione di G sui laterali $\{U + \alpha_i\}$ e $\{U + \beta_j\}$: siano G_a lo stabilizzatore di $U + \alpha$ e G_b quello di $U + \beta$. Detto $A_0 := A \cap (U + \alpha)$, è $\alpha_i \in A_0 \Leftrightarrow U + \alpha = U + \alpha_i$, quindi $g(\alpha) \in A_0 \Leftrightarrow g \in G_a$ e A_0 è l'orbita di α in A sotto l'azione di $G_a \subseteq G$. Inoltre $\alpha' - \alpha = \beta - \beta' \in U$, da cui $\alpha' \in A_0$ e $U + \alpha = U + \alpha'$.

Definendo B_0 in modo analogo, $G_0 := G_a \cap G_b$ è transitivo su A_0 e B_0: infatti, dato $\alpha_i \in A_0$, grazie al Lemma 1 esiste $g \in G$ che soddisfa $g(\alpha) = \alpha_i$ e $g(\beta) = \beta$; è $g \in G_\beta \subseteq G_b$ e $g(U + \alpha) = U + \alpha_i = U + \alpha$, perciò è anche $g \in G_a$, ovvero $g \in G_0$ (la transitività su B_0 si ottiene in modo analogo). Infine $|A_0| = [G_a : (G_a)_\alpha] = [G_a : G_\alpha] \mid [G : G_\alpha] = |A|$, da cui $(|A_0|, |B_0|) = 1$. Siamo nelle ipotesi di partenza con G_0, A_0 e B_0 al posto di G, A e B.

Per l'ipotesi di minimalità deve essere $G_0 = G$, da cui $A_0 = G_a\alpha = G\alpha = A$ e $B_0 = B$. Ma allora $\sum \beta_j = u + n\beta$, con $u \in U$, cioè $u = \sum \lambda_i \alpha_i$. Applicando tutti gli automorfismi in G_β e sommando (e ricordando che G_β agisce transitivamente su A),

$$|G_\beta| \sum_j \beta_j = \sum_i \lambda_i \sum_{g \in G_\beta} g(\alpha_i) + n|G_\beta|\beta = \sum_k \lambda_k \frac{|G_\beta|}{m} \sum_i \alpha_i + n|G_\beta|\beta.$$

Ma $\sum \beta_j$ e $\sum \alpha_i$ sono lasciati fissi da tutto G, perciò lo stesso vale per β. Deduciamo che $n = 1$, assurdo. □

TEOREMA. Date due radici α e β di $p(x)$ e $q(x)$, polinomi in $\mathbb{Q}[x]$ irriducibili di grado m e n rispettivamente, la somma $\alpha + \beta$ ha grado mn.

Dimostrazione. Sia $\mathbb{K}$ il campo di spezzamento di $p(x)q(x)$ e sia $G := \operatorname{Gal}(\mathbb{K}/\mathbb{Q})$. Chiamiamo A e B gli insiemi delle radici di $p(x)$ e $q(x)$, come nel Lemma 2. Per il Lemma 1 G è transitivo sulle coppie (α_i, β_j), quindi ogni $\alpha_i + \beta_j$ appartiene all'orbita di $\alpha + \beta$ tramite l'azione di G. Per il Lemma 2, al variare di (i, j) queste somme sono tutte distinte, ma questo implica che il polinomio minimo di $\alpha + \beta$ ha grado almeno mn. □