(*December 27, 2011*)

Linear independence of roots

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

It is natural to believe that $\sqrt{7} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and that $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$, and natural to hope for a simple causal mechanism behind such facts. Small versions of such questions permit direct manipulative resolution, but the best context for larger versions of such questions is not immediately clear.

[Robinson 2011] gives a straightforward argument, and suggests extensions to higher-order roots, which is the point of the present discussion. It is not surprising that such questions were addressed many decades ago, and, indeed, [Dubuque 2011] quotes reviews of sources dating to at least [Hasse 1933].

Fix $2 \le \ell \in \mathbb{Z}$, and let k be a field of characteristic not dividing ℓ, with k containing a primitive ℓ^{th} root of unity. Let $a_1, \ldots, a_n \in k^\times$, and $\alpha_j = \sqrt[\ell]{a_j}$ in a finite Galois extension K of k.

Suppose that, for any pair of indices $i \neq j$, there is $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma(\alpha_i)/\alpha_i \neq \sigma(\alpha_j)/\alpha_j$.

Since $\sigma(\alpha_i) = \omega_i \cdot \alpha_i$ for some ℓ^{th} root of unity ω_i (depending on σ), the hypothesis is equivalent to a_i/a_j not being an n^{th} power in k. That is, the hypothesis is that the one-dimensional representations of $\mathrm{Gal}(K/k)$ on the lines $k \cdot \alpha_j$ are pairwise non-isomorphic, although the discussion need not be carried out in such terms.

[0.0.1] Claim: The α_j's are *linearly independent* over k.

Proof: Suppose $\sum_j c_j \cdot \alpha_j = 0$ is a shortest non-trivial linear relation with $c_j \in k$. For indices $i \neq j$ appearing in this relation, take $\sigma \in \mathrm{Gal}(K/k)$ such that $\sigma(\alpha_i)/\alpha_i \neq \sigma(\alpha_j)/\alpha_j$. Then

$$0 \;=\; \frac{\sigma(\alpha_i)}{\alpha_i} \cdot 0 - \sigma(0) \;=\; \frac{\sigma(\alpha_i)}{\alpha_i} \sum_t c_t \cdot \alpha_t - \sigma\Big(\sum_t c_t \cdot \alpha_t\Big) \;=\; \sum_t c_t \cdot \alpha_t \cdot \big(\frac{\sigma(\alpha_i)}{\alpha_i} - \frac{\sigma(\alpha_t)}{\alpha_t}\big)$$

The coefficient of α_i is 0, while the coefficient of α_j is non-zero, by arrangement. This would contradict the assumption that the relation is shortest. Thus, there is no non-trivial relation. ///

[0.0.2] Remark: The argument reproves the impossibility of mapping a sum of mutually non-isomorphic irreducibles of $\mathrm{Gal}(K/k)$ non-trivially to the trivial representation. The argument resembles the argument for *linear independence of characters*.

[0.0.3] Corollary: For *relatively prime* integers $a_1, \ldots, a_n$, the 2^n algebraic numbers $\sqrt{a_{i_1} \ldots a_{i_k}}$ with $i_1 < \ldots < i_k$ and $0 \le k \le n$ are linearly independent over $\mathbb{Q}$, so are a $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$. In particular, the degree of that field over $\mathbb{Q}$ is the maximum possible, 2^n. ///

Bibliographic notes: Specific bibliographic pointers were gleaned from [Dubuque 2011], in which [Bergstrom 1953] is quoted refering to the text [Hasse 1933].

[Bergstrom 1953] H. Bergstrom, review of [Mordell 1953], Math. Reviews MR0058649.

[Besicovitch 1940] A.S. Besicovitch, *On the linear independence of fractional powers of integers*, J. London Math. Soc. **15** (1940), 3-6.

[Dubuque 2011] W. Dubuque's answer to math.stackexchange.com/questions/30687, retrieved 22 Dec 2011.

[Hasse 1933] H. Hasse, *Klassenkorpertheorie*, Marburg, 1933, 187-195.

[Mordell 1953] L.J. Mordell, *On the linear independence of algebraic numbers*, Pacific J. Math. **3** (1953), 625-630.

[Robinson 2011] G. Robinson's answer to math.stackexchange.com/questions/93453, retrieved 22 Dec 2011.