Iterated Quadratic Extensions Over $\mathbb{Q}$
(Version 1.2)

Po-Shen Loh

7 May 2001

Problem 1 *Let $\{c_1, c_2, \ldots, c_n\}$ be a set of distinct positive integers such that no product of distinct elements is a square, and let $a_i = \sqrt{c_i}$ for each i. Prove that $[\mathbb{Q}(a_1, a_2, \ldots, a_n) : \mathbb{Q}] = 2^n$ and the extension is Galois over $\mathbb{Q}$ with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$ (n times).*

Solution:

We use strong induction. Our base case is $n = 2$, which follows immediately since it is a biquadratic extension.

Suppose that our problem is true for all $n \leq N$. We show that it is true for an $(N+1)$-set of a_i. Let $\mathcal{S} = \{a_1, a_2, \ldots, a_{N+1}\}$, let K be the extension of $\mathbb{Q}$ by $\mathcal{S}$ and consider a subset $\mathcal{T} \subset \mathcal{S}$ with N elements. By inductive hypothesis, we know that the degree of the extension of $\mathbb{Q}$ with elements of $\mathcal{T}$ is 2^N.

Proceed by contradiction; suppose that $[\mathbb{Q}(a_1, a_2, \ldots, a_{N+1}) : \mathbb{Q}] \neq 2^{N+1}$. It contains $\mathcal{T}$, so the extension must have degree 2^N, so it is exactly the extension field generated by the elements of $\mathcal{T}$. By inductive hypothesis, it is Galois over $\mathbb{Q}$ and has elementary Abelian Galois group G.

Since each subgroup $H \leq G$ is a subgroup of the elementary Abelian group of order 2^N, by the theorem of Finitely Generated Abelian Groups, it is a direct product of cyclic groups, and since all elements have order dividing 2, H must also be elementary Abelian.

We can determine what the corresponding subfields look like. H is of the form $\langle \sigma_1 \rangle \times \langle \sigma_2 \rangle \times \cdots \times \langle \sigma_k \rangle$ where σ_i conjugates its associated (quadratic) root d_i. Then, its fixed field will be an extension of $\mathbb{Q}$ by quadratics d_i which are products of the a_i. Since H is elementary Abelian, it is generated by N elements only if it is G.

Let m be the number of intermediate subfields of the extension generated over $\mathbb{Q}$ by $\mathcal{T}$. Since we have a Galois extension, there are exactly m intermediate subfields under K. Let $\{b\} = \mathcal{S} - \mathcal{T}$. Clearly, $\mathbb{Q}(b)$ is a subfield of the full extension K, so it must be one of the m subfields, say $\mathbb{Q}(d_1, d_2, \ldots, d_k)$. If $k = N$, then from the previous paragraph, this corresponds the full group; this is impossible because $[\mathbb{Q}(b) : \mathbb{Q}] = 2 \neq 2^N = [\mathbb{Q}(\mathcal{T}) : \mathbb{Q}]$.

So $k \neq N$. If we could form a product of distinct generators d_i that was in $\mathbb{Q}$, then we could simply discard one of them and have the same field. Therefore, we can assume that $k < N$ and no product of distinct generators is rational. Furthermore, by the construction above for the subfields, no product of distinct generators and b can be rational, because each $b_i^2 \in \mathbb{Q}$ so any product of distinct generators can be reduced to a product of distinct b_i. We can then apply the inductive hypothesis on $\mathbb{Q}(d_1, \ldots, d_k, b)$, and conclude that $\mathbb{Q}(d_i, \ldots, d_k) \neq \mathbb{Q}(b)$. We have a contradiction.

Thus, $[K : \mathbb{Q}] = 2^{N+1}$. Since it is Galois, it must have exactly 2^{N+1} automorphisms. All automorphisms permute the roots within each irreducible factor, and since there are exactly $N+1$ such factors with two ways to make an map out of each, we find 2^{N+1} maps. Since there are no other kinds of maps and the roots are generators, each map must be an automorphism, and the Galois group is indeed $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$ (n times).

And we are done.