SAMI'S QUESTION

EYAL GOREN

Sami Douba had asked me the following question. We have proven in the tutorial session that there is a real number α such that $[\mathbb{Q}(\alpha):\mathbb{Q}]=4$ and such that there is no field M with $\mathbb{Q}(\alpha)\supsetneq M\supsetneq\mathbb{Q}$. This allows us to conclude that we cannot construct α by adjoining a square root to $\mathbb{Q}$, getting a field M and then adjoining a square root of an element of M to get $\mathbb{Q}(\alpha)$, but

why does that prove that α is not constructible??

That is, maybe there is another sequence of real fields

$$\mathbb{Q}=K_0\subseteq K_1\subseteq\cdots\subseteq K_n, \tag{1}$$

such that $K_i=K_{i-1}(\sqrt{\alpha_i})$, $i=1,\dots,n$, where α_i is a positive element of K_{i-1}, and such that $\alpha\in K_n$? We will show that this is not the case.

We introduce a convenient terminology. We say that a finite extension $K/\mathbb{Q}$ is **weakly constructible** if there is a sequence of fields as in (1), with $K=K_n$, but where we do not require the α_i to necessarily be positive.

Lemma 0.0.1. *If $K/\mathbb{Q}$ is weakly constructible then there is a weakly constructible Galois extension $L/\mathbb{Q}$ that contains K.*

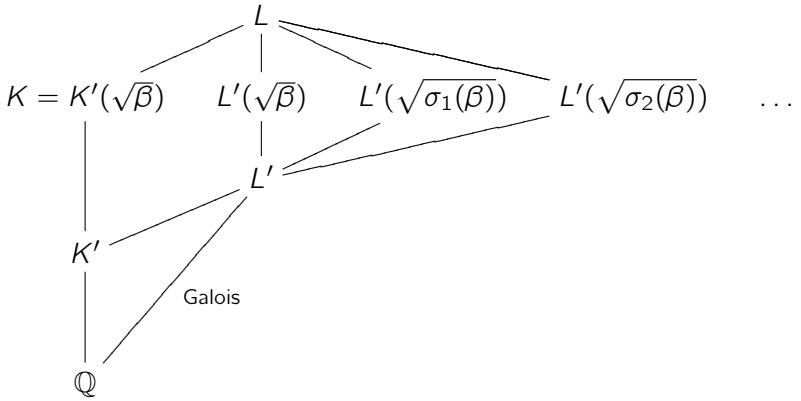
Proof. We prove that by induction on the degree $[K:\mathbb{Q}]$, which is a power of 2. The case of $[K:\mathbb{Q}]=1$, or 2, are clear. In that case $K/\mathbb{Q}$ *is* Galois.

In the general case, by assumption K contains a subfield $K':=K_{n-1}$ such that $[K:K']=2$ and K' is constructible. In addition $K=K'(\beta)$, for some element $\beta\in K'$. Applying the induction hypothesis to K' we find a Galois extension L' containing K' that is weakly constructible over $\mathbb{Q}$.

Consider now the extension

$$L:=L'(\{\sqrt{\sigma(\beta)}:\sigma\in\mathrm{Gal}(L'/\mathbb{Q})\}).$$

We organize the information in the following diagram:



We note the following. First $L \supseteq K$ and since L/L' is obtained from L' by successively adding a root from the set $\{\sqrt{\sigma(\beta)} : \sigma \in \mathrm{Gal}(L'/\mathbb{Q})\}$, its degree is power of 2 and, in fact, it is a weakly constructible extension of $\mathbb{Q}$. Furthermore, L is Galois over $\mathbb{Q}$. To show that, take an element θ such that $L' = \mathbb{Q}(\theta)$ and let f be its minimal polynomial over $\mathbb{Q}$ (such θ exists by the Primitive Element Theorem). Then, clearly L is the splitting field over $\mathbb{Q}$ of

$$f \cdot \prod_{\sigma \in \mathrm{Gal}(L'/\mathbb{Q})} (x^2 - \sigma(\beta)),$$

which is a polynomial with rational coefficients.

An alternative proof. Start with $\tilde{K}$ a finite Galois extension of $\mathbb{Q}$ containing K. Argue that for every $\sigma \in \mathrm{Gal}(\tilde{K}/\mathbb{Q})$ also $\sigma(K)$ is also weakly-constructible. Then, $\prod_{\sigma \in \mathrm{Gal}(\tilde{K}/\mathbb{Q})} \sigma(K)$ is a Galois extension of $\mathbb{Q}$ that contains K and is weakly-constructible. To fill in the details in this argument, in particular the very last claim, see the proof of Proposition 13.2.1. □

Now let us consider the situation of an extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ with no quadratic subfield. If α is constructible then α belongs to some finite extension $K/\mathbb{Q}$ such that K is weakly constructible over $\mathbb{Q}$ (in fact, by definition, there is such real field K and then K is constructible; there is a sequence as in (1) with each α_i positive real number). Thus, by the Lemma, α belongs to some weakly constructible Galois extension $L/\mathbb{Q}$. Since $L/\mathbb{Q}$ is weakly constructible the Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$ is a 2-group. Let H be its subgroup such that

$$\mathbb{Q}(\alpha) = L^H.$$

Since G is a 2-group, we can find a subgroup H_1 of G such that $H \subsetneqq H_1 \subsetneq G$ (Proposition 21.0.11 in my notes for MATH370). But that gives a subfield

$$\mathbb{Q}(\alpha) = L^H \supsetneqq L^{H_1} \supsetneqq \mathbb{Q},$$

and that is a contradiction.

◇ ◇ ◇

There is something more that we can learn from our discussion. If we examine our arguments we will see that they imply the following. Suppose that we know that α is constructible and that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^r$, then, by taking successively r roots we can construct the field $\mathbb{Q}(\alpha)$. If you wish, heuristically, to construct α we need to draw no more than r circles.