MATH 594. RADICAL TOWERS AND ROOTS OF UNITY

Some time ago, there was a proposed quals problem which asked the students to prove that if $f \in \mathbf{Q}[T]$ is irreducible with odd degree > 1 and f splits over $\mathbf{R}$ with splitting field $K \subseteq \mathbf{R}$ having $\mathrm{Gal}(K/\mathbf{Q})$ solvable, then any radical tower $F/\mathbf{Q}$ containing K must contain a root of unity of order > 2 and hence F *cannot* be embedded into $\mathbf{R}$. This turned out to be a bit too hard to be a quals problem. The crucial aspect of this problem is not that it takes place with ground field $\mathbf{Q}$, or even that the fields have characteristic zero. Both of these conditions can be eliminated. What really matters is that 2 is a very small prime number (as the proof will explain); i.e., it is the oddness hypothesis that is the essential one. Here is a general theorem which we shall prove (after explaining how it relates back to the above proposed quals problem).

Theorem 0.1. *Let E be a field, and let K/E be a finite Galois extension. Assume that $[K:E]$ is not a power of 2 (in particular, $[K:E] > 1$). If F is a radical tower over E into which K admits an E-embedding, then F contains a root of unity of odd prime order. In particular, if E is a subfield of $\mathbf{R}$, then F admits no E-embedding into $\mathbf{R}$.*

An important special case is to consider a separable irreducible polynomial $f \in E[T]$ of odd degree > 1 and to take K/E to be a splitting field of f. Note that $[K:E]$ is divisible by the odd integer $\deg f > 1$ since f is irreducible, so $[K:E]$ is not a power of 2. The hypothesis that K admits an E-embedding into a radical tower says that "f can be solved in radicals" over E, and in characteristic zero the existence of such a radical tower is equivalent to $\mathrm{Gal}(K/E)$ being solvable. The significance of the theorem is that when $E \subseteq \mathbf{R}$, such a radical tower F/E must contain a root of unity of odd prime order and hence F *cannot* be found inside of $\mathbf{R}$, even if we *drop* any desire for the radical tower to be Galois over E.

The case $E = \mathbf{Q}$ and cubic f is the classical "casus irreducibilis", where an irreducible cubic over $\mathbf{Q}$ has 3 real roots but any attempt to describe them in terms of radicals seems (by experience, and in fact by necessity due to the above theorem!) to force the use of non-real complex numbers. This was most disturbing to the mathematicians who first worked with the cubic formula, at a time when complex numbers were still regarded with great suspicion (and so to seem to "need" the use of complex numbers to describe solutions to a cubic with three *real* roots was quite alarming).

Proof. Since any radical extension generated by a dth root (with $d > 1$) can be expressed as a successive extension of adjoining prime roots (as we run over a prime factorization of d), we can chop up the radical tower F/E into steps

$$E = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = F$$

where $E_{i+1} = E_i(a_i)$ with $a_i^{p_i} \in E_i$, with p_i prime. We may certainly assume $[E_{i+1} : E_i] > 1$ for all i without loss of generality. For each i, I claim that either $[E_{i+1} : E_i] = p_i$ or else E_{i+1} contains a non-trivial p_ith root of unity. For this claim, it suffices to show more generally that if p is prime and K'/K is an extension of fields with $[K' : K] > 1$ and $K' = K(a)$ where $a^p = b$ lies in K, then either $[K' : K] = p$ or else K' contains a non-trivial pth root of unity. Consider the polynomial $T^p - b$ in $K[T]$. If this is irreducible, then clearly K' is K-isomorphic to $K[T]/(T^p - b)$ and hence $[K' : K] = p$. Thus, we may suppose $T^p - b$ is reducible. In this case, $[K' : K] < p$, so $\gcd([K' : K], p) = 1$, and applying the multiplicative norm map $\mathrm{N}_{K'/K} : K' \to K$ to the equation $b = a^p$ gives $b^{[K':K]} = \mathrm{N}_{K'/K}(a)^p$. But $[K' : K]$ is relatively prime to p, so $up + v[K' : K] = 1$ with $u, v \in \mathbf{Z}$, and hence $b = b^{up+v[K':K]} = c^p$ with $c = b^u \cdot \mathrm{N}_{K'/K}(a)^v \in K$. In this case, we have $a^p = b = c^p$, so $\zeta = a/c$ is a pth root of unity. But a is not in K since $K' = K(a)$ with $[K' : K] > 1$, so $\zeta \neq 1$ and hence ζ is a non-trivial pth root of unity in K' (in particular, the characteristic is not equal to p).

Of course, when $p_i = 2$ then $1 < [E_{i+1} : E_i] \leq 2$ forces $[E_{i+1} : E_i] = 2 = p_i$. However, for odd p_i we have $1 < [E_{i+1} : E_i] \leq p_i$ and the possibility $1 < [E_{i+1} : E_i] < p_i$ may happen. But in such cases, the preceding shows that E_{i+1} contains a root of unity of odd prime order p_i, so F contains such a root of unity too. This would provide what we want to prove, so we may assume that $[E_{i+1} : E_i] = p_i$ for all i. Note that this step makes crucial use of a special property of the prime 2: there are no integers strictly between 1 and 2. This is the source of the special role of 2 in the proof.

Fix an E-embedding of K into F. Let $K_i = K \cap E_i$ for each i, so K/K_i is a Galois extension and $[K_i : E]$ divides $[E_i : E]$ (since $E \subseteq K_i \subseteq E_i$). Since K/K_i is finite Galois, the compositum $L_i \stackrel{\text{def}}{=} KE_i$ inside of F is not only finite Galois over E_i but the following lemma ensures that $[L_i : E_i] = [K : K_i]$.

Lemma 0.2. *Let F/k be an extension of fields and let K/k be a subextension which is finite Galois. Let F_0/k be another intermediate extension with $K \cap F_0 = k$. Then the finite Galois extension KF_0/F_0 has degree $[KF_0 : F_0]$ equal to $[K : k]$, and the natural injection $\mathrm{Gal}(KF_0/F_0) \hookrightarrow \mathrm{Gal}(K/k)$ is an isomorphism.*

The Galois group aspect is not relevant for our purposes.

Proof. Once the degree result is proven, the isomorphism on Galois groups is immediate by counting. To compute the degrees, let y be a primitive element for K/k, say with minimal polynomial $f \in k[T]$. Note that K/k is a splitting field of f over k. Since KF_0/F_0 is generated by a root of f, it is necessary and sufficient to prove that $f \in F_0[T]$ is irreducible. Suppose $f = gh$ is a monic factorization of f over F_0; it suffices to show that this factorization is trivial. Since f splits over K and hence over F, when we consider the factorization $f = gh$ in $F[T]$ we see that g and h split over F and hence their coefficients may be expressed as $\mathbf{Z}$-polynomials in the roots of f (recall that g and h were chosen to be monic). But the roots of f in F lie in K, so the coefficients of g and h in F lies in K. Hence, g and h as elements in $F[T]$ lies in $(K \cap F_0)[T] = k[T]$, so our factorization of f takes place in $k[T]$. But f is irreducible in $k[T]$, so our factorization is indeed trivial. ∎

Now consider the intersection $L_i \cap E_{i+1}$ inside of F for some $0 \leq i < n$. This is an intermediate field between E_{i+1} and E_i (since $E_i \subseteq KE_i = L_i$), so since $[E_{i+1} : E_i] = p_i$ is prime we conclude that $L_i \cap E_{i+1}$ is equal to either E_{i+1} or E_i. In the first case, the finite Galois extension L_i/E_i contains E_{i+1}, so E_{i+1}/E_i is separable and L_i contains a Galois closure of E_{i+1} over E_i. But E_{i+1} is generated over E_i by a root of an irreducible polynomial $T^{p_i} - b_i$ for some b_i in E_i, and hence the Galois closure contains a non-trivial p_ith root of unity. Thus, L_i would contain a non-trivial p_ith root of unity, so F would too. If p_i is odd, we'd be done. Thus, *for the purposes of what we are trying to prove*, there is no loss of generality in assuming that $p_i = 2$ whenever $L_i \cap E_{i+1} = E_{i+1}$. In particular, when p_i is odd then $L_i \cap E_{i+1} = E_i$. We will now proceed to deduce a contradiction from this situation.

When p_i is odd, since $L_i \cap E_{i+1} = E_i$ and $L_i/E_i = KE_i/E_i$ is finite Galois, by Lemma 0.2 we conclude that L_iE_{i+1} is finite Galois over E_{i+1} with degree equal to $[L_i : E_i]$. But $L_iE_{i+1} = KE_iE_{i+1} = KE_{i+1} = L_{i+1}$, so we see that when p_i is odd then $[L_{i+1} : E_{i+1}] = [L_i : E_i]$. On the other hand, if $p_i = 2$ then either $L_i \cap E_{i+1} = E_i$, in which case the same application of Lemma 0.2 shows $[L_{i+1} : E_{i+1}] = [L_i : E_i]$, or else $L_i \cap E_{i+1} = E_{i+1}$. But in this latter case we have $E_{i+1} \subseteq L_i$ and $[E_{i+1} : E_i] = p_i = 2$, so in fact $[L_i : E_{i+1}] = [L_i : E_i]/2$. But such situations also must have $L_{i+1} = L_i$ since $L_{i+1} = L_iE_{i+1}$ and $E_{i+1} \subseteq L_{i+1}$, so in fact $[L_{i+1} : E_{i+1}] = [L_i : E_i]/2$. To summarize, for every $i < n$ we see that $[L_{i+1} : E_{i+1}]$ is equal to either $[L_i : E_i]$ or $[L_i : E_i]/2$. In particular, the odd parts of $[L_i : E_i]$ and $[L_{i+1} : E_{i+1}]$ are *the same* for all $i < n$. But $[L_n : E_n] = 1$ since $E_n = F$, so it follows that $[L_i : E_i]$ is a power of 2 for all i. We will now show that there is actually an i for which $[L_i : E_i]$ has a non-trivial odd factor, and this contradiction will complete the proof.

Since $[K : E]$ has a non-trivial odd factor by hypothesis and $[K : E] | [F : E]$, we conclude that $[F : E] = \prod p_i$ has a non-trivial odd factor. Thus, *some* p_i must be odd! Hence, we may choose a least i_0 (possibly $i_0 = 0$) for which p_{i_0} is odd. We then have $p_i = 2$ for all $i < i_0$, so $[E_{i_0} : E] = \prod_{i<i_0} p_i$ is a (possibly trivial) power of 2. Since $[K_{i_0} : E] | [E_{i_0} : E]$, as $K_i \subseteq E_i$ for any i, we conclude that $[K_{i_0} : E]$ is also a power of 2. But $[K : E]$ has an odd factor > 1 by hypothesis, so the quotient $[K : K_{i_0}] = [K : E]/[K_{i_0} : E]$ by a power of 2 also has (the same) odd factor > 1. Since $K_{i_0} = K \cap E_{i_0}$, by Lemma 0.2 we have $[K : K_{i_0}] = [KE_{i_0} : E_{i_0}] = [L_{i_0} : E_{i_0}]$. It follows that $[L_{i_0} : E_{i_0}]$ has a non-trivial odd factor, and we saw above that this yields a contradiction. ∎