HW 6
due May 25

In class we discussed the cubic $x^3 + x^2 - 2x - 1$, which has three real roots (and Galois group $\mathbb{Z}/3$). One can express these real roots in terms of a radical expression as follows:

$$x_1 = -\frac{1}{3} + z_1 + z_2$$

$$x_2 = -\frac{1}{3} + \omega z_1 + \omega^2 z_2$$

$$x_1 = -\frac{1}{3} + \omega^2 z_1 + \omega z_2,$$

where z_1 is a cube root of $\frac{7}{2}(1 + i3\sqrt{3})$ and $z_2 = 7/3z_1^{-1}$. These expressions heavily involve complex numbers to describe real numbers.

The goal of this homework is to show that, in this and most examples, one is *forced* to use complex numbers to express real roots in terms of radicals.

1. Suppose $\alpha \in \mathbb{C}$ is algebraic and let L be the Galois closure of the finite extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$. Show that for any prime p dividing the order of $\mathrm{Gal}(L/\mathbb{Q})$, there is a subfield of L with $[L : F] = p$ and $L = F(\alpha)$.

2. Let F be a subfield of the real numbers $\mathbb{R}$. Let a be an element of F and $K = F(\sqrt[m]{a})$, where m is a prime and $\sqrt[m]{a}$ denotes a real mth root of a. Prove that if L is any Galois extension of F contained in K then $[L : F] \leq 2$.

3. Let $f \in \mathbb{Q}[x]$ is an irreducible polynomial all of whose roots are real. Suppose that one of the roots α of f can be expressed in terms of *real* radicals, meaning: There is a 'radical' tower of extensions
$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n \subset \mathbb{R},$$
such that $\alpha \in K_n$ and for each i, $K_{i+1} = K_i(\sqrt[m_i]{a_i})$ for some prime number m_i and some $a_i \in K_i$.

   We will show that the Galois group of f is a 2-group!

   Let $L \subset \mathbb{R}$ be the splitting field of f over $\mathbb{Q}$. For the sake of contradiction, let p be an odd prime that divides $[L : \mathbb{Q}]$.

(a) Apply Problem 1 to get a subfield F of L with $[L : F] = p$ and $L = F(\alpha)$. Consider the tower of extensions $K_i' = FK_i$ obtained from the one above by taking the compositum with F. Show that the new tower is again a 'radical' tower and each $[K_{i+1}' : K_i']$ is either the prime m_i or 1.

(b) Show that there exists an integer s such $\alpha \notin K_{s-1}'$, but $\alpha \in K_s'$.

(c) Show that $K_s' = K_{s-1}'(\alpha)$.

(d) Note that $F \subset L$ is Galois of degree p and use this to show that $K_{s-1}' \subset K_s'$ is Galois and of degree p.

(e) Use Problem 2 applied to $K_{s-1}' \subset K_s' = K_{s-1}'(\sqrt[p]{a_{s-1}})$ to obtain our desired contradiction.