Math 210B. Radical towers and roots of unity

1. Motivation

Let \( f \in \mathbb{Q}[T] \) be a monic irreducible cubic that splits over \( \mathbb{R} \) (that is, has three real roots); explicitly, this splitting condition says that the discriminant of \( f \) is positive (and so is a square in \( \mathbb{R} \)). It was noticed by Cardano and his contemporaries that the use of radicals (the cubic formula) to describe such real roots always seemed to require the use of non-real complex numbers in the middle of the formula.

Put another way, the cubic formula did not seem to ever provide a radical tower contained in \( \mathbb{R} \) for describing cubic real irrationalities \( \alpha \) when all conjugates of \( \alpha \) in \( \mathbb{C} \) lie in \( \mathbb{R} \) (of course, for cases such as \( 2^{1/3} \) we have a “radical formula” but the other two conjugates over \( \mathbb{Q} \) do not lie in \( \mathbb{R} \))! 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).

2. A general theorem on radical towers

Rather more generally, if \( f \in \mathbb{Q}[T] \) is irreducible with odd degree > 1 and \( f \) splits over \( \mathbb{R} \) with splitting field \( K \subseteq \mathbb{R} \) having \( \text{Gal}(K/\mathbb{Q}) \) solvable, then any abstract radical tower \( F/\mathbb{Q} \) containing \( K \) must contain a root of unity of order > 2 and hence \( F \) cannot be embedded into \( \mathbb{R} \). The crucial hypothesis here is not that the ground field is \( \mathbb{Q} \), 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; i.e., it is the oddness hypothesis that is the essential one. Here is a general theorem which we shall prove:

**Theorem 2.1.** Let \( E \) be a field, and let \( K/E \) be a finite Galois extension. Assume that \([K:E]\) has order divisible by a prime \( p \). If \( F \) is a radical tower over \( E \) into which \( K \) admits an \( E \)-embedding, then either \( F \) contains a root of unity of order \( p \) (so the characteristic is distinct from \( p \)) or \( F \) contains a primitive root of unity of odd prime order.

In particular, if \( E \) is a subfield of \( \mathbb{R} \) and \([K:E]\) is odd and > 1, then \( F \) admits no \( E \)-embedding into \( \mathbb{R} \).

**Remark 2.2.** We understand a radical tower to be a finite tower whose successive stages \( E_{i+1}/E_i \) satisfy \( E_{i+1} = E_i(\alpha_i) \) where \( \alpha_i^{n_i} = a_i \in E_i \) for some \( n_i \geq 1 \); that is, we allow \( n_i \) to be divisible by the characteristic (so we do not require a radical tower to be separable) and we do not consider extension of Artin-Schreier form (adjoining solutions to \( X^p - X - a \) in characteristic \( p > 0 \)). In characteristic 0, perhaps the case of most interest, our convention agrees with standard terminology (whereas in positive characteristic our convention differs from that in some books, such as Lang’s *Algebra*).

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 $\text{Gal}(K/E)$ being solvable. The significance of the theorem is that when $E \subseteq \mathbb{R}$, such a radical tower $F/E$ must contain a root of unity of odd prime order and hence $F$ cannot be found inside of $\mathbb{R}$, even if we drop any desire for the radical tower to be Galois over $E$.

Proof. Since $\text{Gal}(K/E) = [K : E]$ has order divisible by $p$, there must be a subgroup of order $p$. Thus, there is an intermediate field $E'$ between $K$ and $E$ with $K/E'$ Galois of degree $p$. If we $E$-embed $K$ and $F$ into a common algebraic closure of $E$, we may form the compositum $F'$ of $F$ and $E'$ over $E$ to make a radical tower $F'/E'$ which contains $K$. Thus, by renaming $E'$ as $E$ and $F'$ as $F$, we are reduced to the case $[K : E] = p$.

Since any radical extension generated by a $d$th 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 $a_i^p \in E_i$, with $p_i$ prime. We may certainly assume $[E_{i+1} : E_i] > 1$ for all $i$ without loss of generality. Fix an $E$-embedding of $K$ into $F$. Consider the intersection $K \cap E_{n-1}$, a field between $K$ and $E$. Since $[K : E]$ is prime, either $K \cap E_{n-1} = K$ or $K \cap E_{n-1} = E$. If the former, then $K \subseteq E_{n-1}$ so we can rename $E_{n-1}$ as $F$ and induct on $n$ (once we handle the case $n = 1$). On the other hand, if $K \cap E_{n-1} = E$ then consider the composite field $KE_{n-1}$ inside of $F$. This is finite Galois over $E_{n-1}$ of degree $> 1$. The following lemma (using $k = E$, $F_0 = E_{n-1}$) ensures that $[KE_{n-1} : E_{n-1}] = [K : E] = p$.

Lemma 2.3. 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 $\text{Gal}(KF_0/F_0) \hookrightarrow \text{Gal}(K/k)$ 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 $\mathbb{Z}$-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 $F$ lie in $K$. Hence, $g$ and $h$ as elements in $F[T]$ lie 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.

Thus, by renaming $E_{n-1}$ as $E$ and $KE_{n-1}$ as $K$, we get to the special case $n = 1$, which is to say that $F = E(a)$ with $a^{p'} = b \in F^\times$ for some prime $p'$ and $K/E$ is an intermediate Galois extension of prime degree $p$. I claim that either $[F : E] = p'$ or else $F = E(\zeta)$ with $\zeta$ a primitive $p'$th root of unity (and the characteristic is distinct from $p'$). Consider the polynomial $T^{p'} - b$ in $E[T]$. If this is irreducible, then clearly $F$ is $E$-isomorphic to $E[T]/(T^{p'} - b)$ and hence $[F : E] = p'$. On the other hand, if $T^{p'} - b$ is reducible over
3. An amazing application

Let \( n > 2 \) be an integer and let \( L/Q \) be a splitting field for the \( n \)th cyclotomic polynomial, so \( L = Q(ζ_n) \) with \( ζ_n \in L \) any primitive \( n \)th root of unity. This is an abelian extension of \( Q \) with degree \( φ(n) \) and Galois group \((Z/nZ)^{×}\). The element \(-1 \in (Z/nZ)^{×}\) with order \( 2 \) induces \( ζ \mapsto 1/ζ \) on all primitive \( n \)th roots of unity in \( L \), so under any embedding of \( L \) into \( C \) this automorphism of \( L \) is induced by complex conjugation on \( C \). Let \( L^+ \) be the fixed field of this involution of \( L \), so \( L^+ = Q(ζ_n + ζ_n^{-1}) \) is a “totally real” field (i.e., its embeddings into \( C \) always land in \( R \); of course, the image under any embedding is the same subfield of \( C \) since \( L^+/Q \) is Galois). This subfield \( L^+ \) is classically denoted \( Q(\cos(2π/n)) \) since 
\[
2 \cos(2π/n) = e^{2πi/n} + e^{-2πi/n}
\]
with \( i \in C \) denoting either solution to \( z^2 + 1 = 0 \). Note that \( L^+ \) was intrinsically defined in the extension \( L/Q \), so it does not depend upon the choice of \( ζ_n \) used to describe it concretely. Also, \( L^+/Q \) must be abelian of degree \( φ(n)/2 \), and so since it is Galois with a real embedding it follows that the minimal polynomial of \( \cos(2π/n) \) over \( Q \) splits completely in \( R \). That is, all \( Q \)-conjugates of \( \cos(2π/n) \) can be found inside of \( R \).

By the algebraic theory of solvability, since \( L^+/Q \) is a solvable extension it follows that \( \cos(2π/n) \) admits a “radical formula” once we adjoin enough roots of unity to \( L^+ \), such as a primitive root of unity of order \( φ(n)/2 \). However, for \( n > 6 \) such a root of unity cannot be found inside of \( R \) and so it is very natural to ask the following question: can we find a “radical formula” for \( \cos(2π/n) \) inside of \( R \)? That is, is \( \cos(2π/n) \) “solvable in real radicals”? For \( n = 2^k \prod p_i \) with \( k \geq 0 \) and a finite (perhaps empty) set of pairwise distinct odd Fermat primes \( p_i \) (exactly the cases when \( φ(n)/2 \) is a power of 2) it is obvious that this can be done because \( L^+/Q \) is then a solvable extension with degree \( φ(n)/2 \) that is a power of 2 and hence it is a tower of quadratic extensions (that may be taken inside of \( R \) upon embedding \( L^+ \) into \( R \)). This is the reason Fermat primes intervene in the construction of regular polygons by straightedge and compass. The impossibility of construction problems for non-Fermat
primes merely reflects the elementary fact that when $\phi(n)/2$ is not a power of 2 then for degree reasons alone (not requiring any Galois theory!) $L^+/\mathbb{Q}$ cannot be embedded in a tower of quadratic extensions.

One might think that it should be possible to express $\cos(2\pi/n)$ in terms of real radicals for some $n$ with $\phi(n)/2$ not a power of 2, since now there is no “quadratic” restriction being imposed as in the classical Greek construction problems. Incredibly, this question always has a negative answer:

**Theorem 3.1.** If $n > 2$ has an odd prime factor with multiplicity $> 1$ or if $n$ is divisible by an odd non-Fermat prime (i.e., if $\phi(n)/2$ is not a power of 2) then the solvable algebraic number $\cos(2\pi/n) \in \mathbb{R}$ does not lie inside of a radical tower within $\mathbb{R}$. That is, the field $L^+/\mathbb{Q}$ cannot be embedded in a radical tower inside of $\mathbb{R}$.

This is a lot stronger than the classical theorem of Gauss on exactly which regular $n$-gons can be constructed by straightedge and compass!

**Proof.** By the assumption on $n$, $\phi(n)/2$ has an odd prime factor $\ell$. Since $L^+/\mathbb{Q}$ is an abelian extension with degree divisible by $\ell$, it contains a subfield $K/\mathbb{Q}$ with degree $\ell$ and this subfield is Galois over $E = \mathbb{Q}$. If $\cos(2\pi/n)$ lies in a radical tower within $\mathbb{R}$, then $K \subseteq L^+$ lies in such a tower. But $[K : E]$ has odd degree $> 1$, so this contradicts the final part of Theorem 2.1. □