proof of casus irreducibilis for real fields

Canonical name	ProofOfCasusIrreducibilisForRealFields
Date of creation	2013-03-22 17:43:08
Last modified on	2013-03-22 17:43:08
Owner	rm50 (10146)
Last modified by	rm50 (10146)
Numerical id	8
Author	rm50 (10146)
Entry type	Theorem
Classification	msc 12F10

The classical statement of the *casus irreducibilis* is that if $f(x)$ is an irreducible cubic polynomial with rational coefficients and three real roots, then the roots of $f(x)$ are not expressible using real radicals. One example of such a polynomial is x^3-3x+1, whose roots are $2\cos(2\pi/9), 2\cos(8\pi/9), 2\cos(14\pi/9)$.

This article generalizes the classical case to include all polynomials whose degree is not a power of 2, and also generalizes the base field to be any real extension of $\mathbb{Q}$:

Theorem 1. *Let $F \subset \mathbb{R}$ be a field, and assume $f(x) \in F[x]$ is an irreducible polynomial whose splitting field L is real with $F \subset L \subset \mathbb{R}$. Then the following are equivalent:*

1. *Some root of $f(x)$ is expressible by real radicals over F;*
2. *All roots of $f(x)$ are expressible by real radicals over F using only square roots;*
3. *$F \subset L$ is a radical extension;*
4. *$[L : F]$ is a power of 2.*

Proof. That (2) $\Rightarrow$ (1) is obvious, and (3) $\Rightarrow$ (1) since $F \subset L$ is radical, and is real since $L \subset \mathbb{R}$. (4) implies that $G = \mathrm{Gal}(L/F)$ has order a power of 2. Since G is a 2-group, it has a nontrivial center (this follows directly from the class equation, or look `http://planetmath.org/ANontrivialNormalSubgroupOfAFinitePGro`
and thus has a normal subgroup H of order 2, which corresponds to a subfield M of L Galois over F with $[L : M] = 2$. But then $\mathrm{Gal}(M/F)$ is also a 2-group, so inductively we see that we can write

$$F = K_0 \subset K_1 \subset \ldots \subset K_{m-1} = M \subset K_m = L$$

where $[K_i : K_{i-1}] = 2$. Thus each K_i is obtained from K_{i-1} by adjoining a square root; it must be a real square root since $L \subset \mathbb{R}$. This shows that (4) $\Rightarrow$ (2) and (3).

The meat of the proof is in showing that (1) $\Rightarrow$ (4). Let the roots of $f(x)$ be $\alpha_1, \ldots, \alpha_m$, and assume, by renumbering if necessary, that $\alpha = \alpha_1$ lies in a real radical extension K of F but that $[L : F]$ is not a power of 2. Choose an odd prime p dividing $[L : F] = |G|$, and choose an element $\tau \in G$ of order p. Then τ is not the identity, so for some i, $\tau(\alpha_i) \neq \alpha_i$. Also, since $f(x)$

is irreducible, G acts transitively on the roots of $f(x)$, so for some $\nu \in G$, $\nu(\alpha) = \alpha_i$. Then $\sigma = \nu^{-1}\tau\nu$ does not fix α, since

$$\nu^{-1}\tau\nu(\alpha) = \nu^{-1}\tau(\alpha_i) \neq \nu^{-1}(\alpha_i) = \alpha$$

Let $N = L^\sigma$ be the fixed field of σ. Then L is Galois over N, and clearly $[L : N] = p$. But Galois subfields of real radical extensions are at most quadratic, so L cannot lie in a real radical extension of N.

However, $\alpha \notin N, \alpha \in L$, and $[L : N]$ is prime. Thus $L = N(\alpha) \subset NK$ (since $\alpha \in K$). Additionally, since $F \subset F(\alpha) \subset K$ is a real radical extension of F, we have also that NK is a real radical extension of $NF = N$. So L lies in the real radical extension NK of N. But this is a contradiction and thus $[L : F]$ must be a power of 2.

One consequence of this theorem is the fact that if $f(x) \in F[x]$ has degree not a power of 2, then if $f(x)$ has all real roots, those roots are not expressible in terms of real radicals. If $\deg f = 3$, we recover the original *casus irreducibilis.*

References

[1] D.A. Cox, *Galois Theory*, Wiley-Interscience, 2004.