Canad. Math. Bull. Vol. **47** (2), 2004 pp. 229–236

Solvability by Real Radicals and Fermat Primes

C. U. Jensen

Abstract. We give a survey of old and new results concerning the expressibility of the real roots of a solvable polynomial over a real number field by real radicals. A characterization of Fermat primes is obtained in terms of solvability by real radicals for certain ploynomials.

1 Introduction

In recent years there has been growing interest in the old question about explicit solutions of solvable equations. It is a famous result from classical Galois theory that the roots of a polynomial can be expressed by radicals if and only if the Galois group of the polynomial is solvable. However, if the base field is real and the polynomial has real roots it may happen that these roots can be expressed by radicals of complex numbers, but not by radicals inside the field of real numbers. For instance, if K is a real field and $f(x)$ a cubic irreducible polynomial in $K[x]$ with three real roots, none of these can be expressed in terms of real radicals. Lately, a detailed treatment of these questions has been given in [1], [2], [5] and [6].

In this paper we shall give a survey of classical and recent results in this area as well as some new results for polynomials of prime degree. To make the paper self-contained we also present proofs of some of the known results.

2 Terminology and Preliminary Results

All fields in this paper are number fields.

A field extension L/K is called a *simple radical extension* if $L = K(\alpha)$, where α is an element in $L \setminus K$ for which $\alpha^p \in K$ for some prime number p. If L is a real number field L/K is called a *real simple radical extension*. If in this case $\alpha^p = a$ we write $\alpha = \sqrt[p]{a}$. (If p is odd and a is real $\sqrt[p]{a}$ thus means the unique real p-th root of a and if $p = 2$ the element a should be real and positive and $\sqrt{a}$ should be the positive element α with $\alpha^2 = a$.)

A field extension L/K is called a *radical extension* if there is chain of fields between L and K such that each field in the chain is a simple radical extension of the preceding field. If L is a real number field and a radical extension of K, we call L/K a *real radical extension*. A real number is said to be *expressible by real radicals over* K if it is contained in a real radical extension of K.

The first result goes back to Loewy [8].

Received by the editors August 2, 2002.
AMS subject classification: 12E05, 12F10.

Theorem 1 *If K is a real field and $f(x)$ an irreducible polynomial in $K[x]$ of odd degree n, then $f(x)$ has at most one real root expressible by real radicals; in that case all other roots of $f(x)$ are non-real.*

For the proof we need a classical lemma, which, for instance, can be found in [7] or [9]:

Lemma 1 **(Abel)** *Let K be a field and p a prime number. Then for a in K the polynomial $x^p - a$ is either irreducible in $K[x]$ or has a root in K.*

We are now able to prove Loewy's theorem.

Writing the degree n of $f(x)$ as a product $p_1 \cdots p_t$ of (not necessarily distinct) odd prime numbers we proceed by induction on t.

We first consider the case $t = 1$. Let $f(x)$ be an irreducible polynomial in $K[x]$ of odd prime degree p having a root α in some real radical extension L of K. We have to prove that α is the only real root of $f(x)$.

Let $M(\sqrt[q]{a})/M$, M a real field, $a \in M$, q a prime number, be the first simple radical subextension of L for which $f(x)$ is irreducible in $M[x]$ but reducible in $M(\sqrt[q]{a})[x]$. If $\sqrt[q]{a}$ were not in $M(\alpha)$, Abel's lemma implies that $x^q - a$ would be irreducible in $M(\alpha)$ and then the degree $[M(\alpha, \sqrt[q]{a}) : M]$ would be pq, which is impossible, $f(x)$ being reducible in $M(\sqrt[q]{a})[x]$. Since the degree of α with respect to M is p and p is a prime number, the inclusion $M \subset M(\sqrt[q]{a}) \subseteq M(\alpha)$ implies $p = q$ and $M(\alpha) = M(\sqrt[p]{a})$.

Thus there is a polynomial $\psi(x) \in M[x]$ for which $\alpha = \psi(\sqrt[p]{a})$. If ζ_p denotes a primitive p-th root of unity the polynomial

$$P(x) = \prod_{j=0}^{p-1} [x - \psi(\sqrt[p]{a}\zeta_p^j)]$$

has coefficients in M. Since $P(x)$ and $f(x)$ have the same degree and α is a root of both of them it follows that $P(x) = f(x)$. (Here we have tacitly assumed that $f(x)$ is monic.) None of the roots $\psi(\sqrt[p]{a}\zeta_p^j)$, $1 \leq j \leq p-1$ are real. Indeed, if $\psi(\sqrt[p]{a}\zeta_p^j)$ were real for some j, $1 \leq j \leq p-1$, it would be equal to its complex conjugate $\psi(\sqrt[p]{a}\zeta_p^{p-j})$ and consequently $f(x)$ would have a multiple root.

Thus α is the only real root of $f(x)$.

Next, let $f(x)$ be an irreducible polynomial in $K[x]$ of odd degree $n = p_1 \cdots p_t$, $t > 1$, having a root α expressible by real radicals over K. By the induction hypothesis we assume the theorem has been proved for polynomials whose degree contains less than t prime divisors.

Let L/K be a real radical extension of K containing α and let $M(\sqrt[q]{a})/M$ be the first simple radical subextension of L for which $f(x)$ is irreducible in $M[x]$ but reducible in $M(\sqrt[q]{a})[x]$. As before we conclude that $M \subset M(\sqrt[q]{a}) \subseteq M(\alpha)$. Hence q divides n and the degree of the minimal polynomial $g(x)$ of α with respect to $M(\sqrt[q]{a})$ is n/q. Here q must be one of the primes p_i, $1 \leqq i \leqq t$, and the degree n/q thus a product of $t-1$ prime numbers. For a suitable polynomial $G(x, y) \in M[x, y]$ of degree n/q with respect to x, we can write $g(x) = G(x, \sqrt[p]{a})$.

https://doi.org/10.4153/CMB-2004-022-9 Published online by Cambridge University Press

For a primitive p-th root of unity ζ_p, the product

$$P(x) = g(x) \prod_{j=1}^{q-1} G(x, \sqrt[q]{a}\zeta_p^j) = \prod_{j=0}^{q-1} G(x, \sqrt[q]{a}\zeta_p^j)$$

has coefficients in M and degree $q \cdot n/q = n$. As before we get $P(x) = f(x)$. Moreover, by passage to complex conjugates, it follows that the product $\prod_{j=1}^{q-1} G(x, \sqrt[q]{a}\zeta_p^j)$ has no real roots.

Now, α is expressible by real radicals over M and is a root of the irreducible polynomial $g(x) \in M[x]$, whose degree contains $t-1$ prime factors. By the induction assumption, α is the only real root of $g(x)$, and in view of the above observation also the only real root of $f(x)$. ∎

3 Polynomials of Prime Degree

3.1 Sufficient Conditions for Solvability by Real Radicals

Let $f(x)$ be an irreducible polynomial over a real field K of degree an odd prime number p. If the Galois group over K is solvable, by a classical theorem of Galois $f(x)$ has either one real root or p real roots. If $f(x)$ has any real root expressible by real radicals Loewy's theorem implies that the remaining $p-1$ roots are non-real. The following theorem says that in certain cases the above necessary condition for the existence of a root expressible by real radicals is sufficient.

Theorem 2 *Let $f(x)$ be an irreducible polynomial with solvable Galois group over a real field K of degree p, p being an odd prime number and let M be the splitting field of $f(x)$ over K. If the degree $[M(\zeta_p):K]$ is $p \cdot$ (a power of 2), ζ_p being a primitive p-th root of unity, and $f(x)$ has exactly one real root, then this root is expressible by real radicals.*

Proof Let α be the unique real root of $f(x)$. The Galois group of M/K is a Frobenius group $F_{p\ell}$, where ℓ is a divisor of $p-1$ and a power of 2. Since $f(x)$ has just one real root, $\mathrm{Gal}(M/K)$ cannot be cyclic, so ℓ is at least 2. The maximal 2-subextension N of $M(\zeta_p)/K$ has an abelian Galois group over K, and clearly $M(\zeta_p) = N(\alpha)$ and $[N(\alpha):N] = p$. We now consider the maximal real subfields of these two fields: $M(\zeta_p) \cap \mathbb{R}$ and $N \cap \mathbb{R}$.

We have the following diagram:

$$\begin{array}{ccc} M(\zeta_p) \cap \mathbb{R} & \overset{2}{\text{———}} & M(\zeta_p) = N(\alpha) \\ \Big| p & & \Big| p \\ N \cap \mathbb{R} & \overset{2}{\text{———}} & N \end{array}$$

Here $[M(\zeta_p):N] = \big[(M(\zeta_p) \cap \mathbb{R}):(N \cap \mathbb{R})\big] = p$ and since the unique real root α of $f(x)$ lies in $M(\zeta_p) \cap \mathbb{R}$, the extension $(M(\zeta_p) \cap \mathbb{R})/(N \cap \mathbb{R})$ is not Galois. Hence

https://doi.org/10.4153/CMB-2004-022-9 Published online by Cambridge University Press

the Galois group of $M(\zeta_p)/(N \cap \mathbb{R})$, which has order $2p$, must be the dihedral group D_p.

Since $\mathrm{Gal}(M(\zeta_p)/N)$ is cyclic of order p and N contains the p-th roots of unity, $M(\zeta_p)/N$ is a Kummer extension, so that $M(\zeta_p) = N(\sqrt[p]{\beta})$ for some $\beta \in N$. Let σ, defined by $\sigma(\sqrt[p]{\beta}) = (\sqrt[p]{\beta})\zeta_p$, be a generating automorphism of $\mathrm{Gal}(M(\zeta_p)/N)$.

Now $\mathrm{Gal}\big(M(\zeta_p)/(N \cap \mathbb{R})\big)$ is generated by σ and complex conjugation τ, subject to the relations $\sigma^p = \tau^2 = (\sigma\tau)^2 = e$. Since $N(\sqrt[p]{\beta})$ is a Galois extension of $N \cap \mathbb{R}$, it follows that $\tau\beta = \beta^t\gamma^p$ for some $t, 1 \leqq t \leqq p-1$, and some $\gamma \in N$. Thus $(\tau\sqrt[p]{\beta}) = (\sqrt[p]{\beta})^t\tilde{\gamma}$, where $\tilde{\gamma}^p = \gamma^p$. Moreover, $\tau^2(\sqrt[p]{\beta}) = (\sqrt[p]{\beta})^{t^2}\tilde{\gamma}\tau\tilde{\gamma}$. Since τ^2 is the identity, we conclude that $t^2 \equiv 1 \bmod p$ and hence $t \equiv 1$ or $\equiv -1 \bmod p$.

If $t \equiv -1 \bmod p$, then σ and τ would commute:

$$\sigma\tau\sqrt[p]{\beta} = \sigma(\sqrt[p]{\beta})^t\tilde{\gamma} = (\sqrt[p]{\beta})^t\zeta_p^t\tilde{\gamma}$$
$$\tau\sigma\sqrt[p]{\beta} = \tau(\sqrt[p]{\beta}\zeta_p) = (\sqrt[p]{\beta})^t\zeta_p^{-1}\tilde{\gamma}$$

Hence $t \equiv 1 \bmod p$ and w.l.o.g. we may assume $t = 1$ so that $\tau\beta = \beta\gamma^p$. Then $\beta\tau\beta = \beta^2\gamma^p$ is a real number in N, hence in $N \cap \mathbb{R}$, and is not in $(N \cap \mathbb{R})^p$, since p is odd.

Any root of $x^p - \beta\tau\beta$ lies in $M(\zeta_p)$; in particular, the real value of $\sqrt[p]{\beta\tau\beta}$ lies in $M \cap \mathbb{R}$. By Abel's lemma we see that for this real value we have $M(\zeta_p) \cap \mathbb{R} = (N \cap \mathbb{R})(\sqrt[p]{\beta\tau\beta})$. Now $N \cap \mathbb{R}$ is a real Galois extension of K of degree a power of 2 and therefore a real radical extension. Since the real root α of $f(x)$ lies in $M(\zeta_p) \cap \mathbb{R}$ it follows that α is expressible by real radicals over K. ■

Corollary 1 *Let p be an odd prime number and $f(x)$ an irreducible polynomial over a real field K with the dihedral group D_p as Galois group. If $f(x)$ has exactly one real root and if the degree $[K(\zeta_p) : K]$ is a power of 2, this real root is expressible by real radicals over K.*

Corollary 2 (*cf.* [5]) *Let $f(x)$ be an irreducible polynomial over a real field K of degree p having exactly one real root. If the Galois group of $f(x)$ over K is solvable and p is a Fermat prime, then the unique real root is expressible by real radicals over K.*

3.2 Necessary Conditions for Solvability by Real Radicals

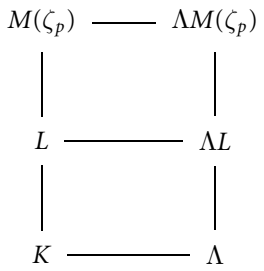
In this section we show that the results in 3.1 are in some sense best possible. For this we need the following:

Descent Theorem (*cf.* [2]) *Let L/K be an extension of degree p with M the Galois closure of L/K and let ζ_p denote a primitive p-th root of unity.*

Assume there exists an extension Λ/K for which $M(\zeta_p) \cap \Lambda = K$ and $L\Lambda/\Lambda$ is a simple radical extension of degree p, then L/K is a simple radical extension of degree p.

https://doi.org/10.4153/CMB-2004-022-9 Published online by Cambridge University Press

Proof The position of the fields is described in the following diagram:



By assumption $\Lambda L = \Lambda(\sqrt[p]{a})$ for a suitable a in Λ. Any automorphism ρ in $\mathrm{Gal}(M(\zeta_p)/K)$ extends uniquely to an automorphism $\bar{\rho}$ in $\mathrm{Gal}(\Lambda M(\zeta_p)/\Lambda)$.

We define a crossed homomorphism ν from $\mathrm{Gal}(M(\zeta_p)/K)$ to the multiplicative group $M(\zeta_p)^\star$ of the non-zero elements in $M(\zeta_p)$ by $\nu(\rho) = \bar{\rho}(\sqrt[p]{a})/\sqrt[p]{a}$.

The crossed homorphism ν is principal, since the cohomology group $H^1\big(\mathrm{Gal}(M(\zeta_p)/K), M(\zeta_p)^\star\big)$ is trivial. Thus $\nu(\rho) = \rho(\alpha)/\alpha$ for a suitable α in $M(\zeta_p)$. Since the values of ν are p-th roots of unity we have $\rho(\alpha^p) = \alpha^p$ for every ρ. Thus α^p lies in K. Because ν is a non-trivial crossed homomorphism α is not in K. Consequently $L = K(\alpha)$ and hence is a simple radical extension of K. ∎

We shall also need the following lemmas which are well known and just easy exercises in Galois theory. (A proof of Lemma 3 may be found in [3].)

Lemma 2 *If L/K is a simple radical extension of prime degree p such that L/K is Galois, then $\mathrm{Gal}(L/K)$ is cyclic and the base field K contains the p-th roots of unity.*

Lemma 3 *Let K be a field containing the p-th roots of unity. Two simple radical extensions $K(\sqrt[p]{a_1})$ and $K(\sqrt[p]{a_2})$, $a_1, a_2 \in K$, coincide if and only if there exists an integer r, not divisible by p, such that $a_1^r = a_2\gamma^p$ for some $\gamma \in K$.*

We are now able to prove

Theorem 3 *Let p be an odd prime and $f(x)$ be an irreducible polynomial of degree p over a real field K having exactly one real root α. If the Galois group of $f(x)$ over K is the dihedral group D_p and the unique real root α is expressible by real radicals over K, then the degree $[K(\zeta_p) : K]$ is a power of 2.*

Proof We write $[K(\zeta_p) : K]$ as $2^s u$ where u is an odd number dividing $p-1$. We shall show that $u = 1$. Assume $u > 1$. Let M be the splitting field of $f(x)$ over K and N the maximal 2-extension of K inside $M(\zeta_p)$. The assumption $u > 1$ implies that N does not contain ζ_p.

M is cyclic of degree p over a quadratic extension of K, hence $MN = N(\alpha)$ is cyclic of degree p over N.

$M(\zeta_p)$ is a Galois extension of the maximal real subextension $N \cap \mathbb{R}$ of N, and $\mathrm{Gal}\big(M(\zeta_p)/(N \cap \mathbb{R})\big)$ is isomorphic to $D_p \times C_u$, where C_u is the cyclic group of order u. The fixed field of complex conjugation is the compositum of $(N \cap \mathbb{R})(\alpha)$

https://doi.org/10.4153/CMB-2004-022-9 Published online by Cambridge University Press

(which has degree p over $N \cap \mathbb{R}$) and $N(\zeta_p) \cap \mathbb{R}$ (which has degree u over $N \cap \mathbb{R}$). We shall need the following observation: Any real extension of $N \cap \mathbb{R}$ inside $M(\zeta_p)$, which does not contain α must be contained in $N(\zeta_p) \cap \mathbb{R}$.

If the root α were expressible by real radicals over K it would *a fortiori* be expressible by real radicals over $N \cap \mathbb{R}$.

Let $\Lambda_0 \subsetneqq \Lambda_1 \subsetneqq \cdots \subsetneqq \Lambda_n$ be a tower of simple real radical extensions of $N \cap \mathbb{R}$ such that α lies in Λ_n but not in Λ_{n-1}.

In view of the above observation $\Lambda_{n-1} \cap M(\zeta_p)$ is contained in $N(\zeta_p) \cap \mathbb{R}$. The latter is an abelian extension of $N \cap \mathbb{R}$ of a degree dividing the odd number u. By Theorem 1, this degree must be 1. We can therefore use the Descent Theorem with $\Lambda = \Lambda_{n-1}, K = N \cap \mathbb{R}, L = (N \cap \mathbb{R})(\alpha)$, showing that $(N \cap \mathbb{R})(\alpha)$ would be a simple radical extension of $N \cap \mathbb{R}$. Then $N(\alpha) = MN$ would be a simple radical extension of N. However, MN/N is cyclic, in particular, Galois. In view of Lemma 2 this gives the desired contradiction since N does not contain the p-th roots of unity. ∎

Theorem 4 *An odd prime number p is a Fermat prime if the following holds. Every real algebraic number α which is the only real root in an irreducible polynomial $f(x)$ in $\mathbb{Q}[X]$ of degree p having the Frobenius group $F_{p(p-1)}$ as Galois group is expressible by real radicals.*

Proof Assume that p is not a Fermat prime, *i.e.* $p-1 = 2^s u$, where u is an odd number > 1. We have to construct an irreducible polynomial $f(x)$ in $\mathbb{Q}[x]$ of degree p whose Galois group is $F_{p(p-1)}$, such that $f(x)$ has exactly one real root and this root is not expressible by real radicals.

If g is a primitive root modulo p the automorphism ρ of $\mathbb{Q}(\zeta_p)$ defined by $\rho(\zeta_p) = \zeta_p^g$ generates the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. The proof goes in three steps.

(I) For any integer t not divisible by p there exists a number $\beta \in \mathbb{Q}(\zeta_p)$ such that β is not the p-th power of a number in $\mathbb{Q}(\zeta_p)$ and $\rho(\beta) = \beta^t \gamma^p$ for a suitable $\gamma \in \mathbb{Q}(\zeta_p)$.

(II) For the β constructed in (I) the field $M = \mathbb{Q}(\zeta_p)(\sqrt[p]{\beta})$ is Galois over $\mathbb{Q}$. If $t = g^2$ the Galois group is the Frobenius group $F_{p(p-1)}$.

(III) M (*i.e.* the above field with $t = g^2$ in (II)) is the splitting field of an irreducible polynomial $f(x)$ in $\mathbb{Q}[x]$ of degree p having exactly one real root and this root is not expressible by real radicals.

Ad (I): For any $\eta \in \mathbb{Q}(\zeta_p)$ the number

$$\beta = \prod_{i=0}^{p-2} \rho^i \eta^{t^{p-i-2}}$$

satisfies $\rho\beta = \beta\gamma^t$ for some $\gamma \in \mathbb{Q}(\zeta_p)$. To see that we can choose η such that β is not the p-th power of a number in $\mathbb{Q}(\zeta_p)$ we may use Hilbert's irreducibility theorem. We consider the polynomial

$$h(x, y) = x^p - \prod_{i=0}^{p-2} (y + \rho^i \zeta_p)^{t^{p-i-2}}$$

https://doi.org/10.4153/CMB-2004-022-9 Published online by Cambridge University Press

which is irreducible in $\mathbb{Q}(\zeta_p)[x, y]$. By (the generalized version of) Hilbert's irreducibility theorem (*cf.* [4, Corollary 11.7]) there exists a rational number q (actually infinitely many) such that $h(x, q)$ is irreducible in $\mathbb{Q}(\zeta_p)[x]$. Thus

$$\beta = \prod_{i=0}^{p-2} (q + \rho^i \zeta_p)^{t^{p-i-2}}$$

has the desired property.

Ad (II): $M = \mathbb{Q}(\zeta_p)(\sqrt[p]{\beta})$ is the splitting field over $\mathbb{Q}$ of the polynomial

$$\prod_{i=0}^{p-2} (x^p - \rho^i \beta),$$

which has rational coefficients. Hence M is Galois over $\mathbb{Q}$. Clearly the order of $\mathrm{Gal}(M/\mathbb{Q})$ is $p(p-1)$.

The automorphism $\rho \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ can be prolonged to an automorphism in $\mathrm{Gal}(M/\mathbb{Q})$ of order $p-1$. By abuse of language we also denote this prolongation by ρ.

Let σ be the automorphism in $\mathrm{Gal}(M/\mathbb{Q}(\zeta_p)) \subset \mathrm{Gal}(M/\mathbb{Q})$ defined by $\sigma(\sqrt[p]{\beta}) = \sqrt[p]{\beta}\zeta_p$. (Here $\sqrt[p]{\beta}$ denotes some fixed root of $x^p - \beta$.) σ has order p.

Now let $t = g^2$ and let c be the integer defined by $cg^2 \equiv g \pmod{p}$. Then c is also a primitive root modulo p and a straightforward calculation shows that

$$(*) \qquad \rho\sigma\rho^{-1} = \sigma^c$$

Now $(*)$ together with the relations $\rho^{p-1} = \sigma^p = e$ are defining relations for the Frobenius group $F_{p(p-1)}$ since c is a primitive root modulo p.

Ad (III): $\mathrm{Gal}(M/\mathbb{Q})$ has p subgroups of index p, which are mutually conjugate. Every subgroup of index divisible by p is contained in one of the subgroups of index p. Hence M has exactly p subfields of degree p over $\mathbb{Q}$ and every subfield of M whose degree over $\mathbb{Q}$ is divisible by p contains one of these p fields. The compositum of these is M. Since $M \not\subseteq \mathbb{R}$ exactly one of these fields is real, say $L = \mathbb{Q}(\alpha)$. Here α is root of an irreducible polynomial $f(x)$ in $\mathbb{Q}[X]$. We claim that this α and $f(x)$ have the desired properties.

M is the splitting field of $f(x)$ over $\mathbb{Q}$. If N is the maximal 2-subextension of $\mathbb{Q}(\zeta_p)$, the degree $[N:\mathbb{Q}]$ is 2^s and $[N \cap \mathbb{R}:\mathbb{Q}] = 2^{s-1}$. $M \cap \mathbb{R}$ is the compositum of $N(\alpha)$, which has degree p over $N \cap \mathbb{R}$, and of $\mathbb{Q}(\zeta_p) \cap \mathbb{R}$, which has degree u over $N \cap \mathbb{R}$. The latter extension is cyclic over $N \cap \mathbb{R}$. We shall need the following: If F is a field such that $N \cap \mathbb{R} \subseteq F \subseteq M \cap \mathbb{R}$ and $\alpha \notin F$, then $F \subseteq \mathbb{Q}(\zeta_p) \cap \mathbb{R}$.

We now proceed as in Theorem 3. If α were expressible by real radicals over $\mathbb{Q}$ it would *a fortiori* be expressible by real radicals over $N \cap \mathbb{R}$.

Let $\Lambda_0 \subsetneqq \Lambda_1 \subsetneqq \cdots \subsetneqq \Lambda_n$ be a tower of simple real radical extensions of $N \cap \mathbb{R}$ such that α lies in $\Lambda_n \setminus \Lambda_{n-1}$. In view of the above observation $\Lambda_{n-1} \cap M$ is contained in $\mathbb{Q}(\zeta_p) \cap \mathbb{R}$. Since $\mathbb{Q}(\zeta_p) \cap \mathbb{R}$ is an abelian extension of $N \cap \mathbb{R}$ of degree dividing the odd integer u, by Theorem 1 this degree must be 1. As in Theorem 3 the Descent Theorem

https://doi.org/10.4153/CMB-2004-022-9 Published online by Cambridge University Press

implies that $(N \cap \mathbb{R})(\alpha)$ is a simple radical extension of $N \cap \mathbb{R}$ of degree p, *i.e.* of the form $(N \cap \mathbb{R})(\sqrt[p]{a})$ for some $a \in N \cap \mathbb{R}$. This implies that $\mathbb{Q}(\zeta_p)(\sqrt[p]{\beta}) = \mathbb{Q}(\zeta_p)(\sqrt[p]{a})$. By Lemma 3 we conclude that $a^r = \beta\gamma^p$ for some integer r, not divisible by p, and some $\gamma \in \mathbb{Q}(\zeta_p)$. Since a is invariant under the automorphism $\rho^{2^{s-1}}$, the numbers β and $\rho^{2^{s-1}}(\beta)$ are in the same p-power class, *i.e.* coincide up to a factor in $(\mathbb{Q}(\zeta_p)^*)^p$. Because $\rho^{2^{s-1}}(\beta) = \beta^{t^{2^{s-1}}}\tilde{\gamma}^p$ for some $\tilde{\gamma} \in \mathbb{Q}(\zeta_p)$, the numbers β and $\beta^{t^{2^{s-1}}}$ are in the same p-power class, so that $t^{2^{s-1}} \equiv 1 \bmod p$. This gives the desired contradiction since the order of $t(= g^2)$ modulo p is $(p-1)/2 = u2^{s-1}$ modulo p and $u > 1$. ■

Finally, the following theorem summarizes the results from 3.1 and 3.2. (As for (iv) note that any quadratic number field can be embedded into a D_p-extension for every p. (*cf. e.g.* [4, Proposition 24.47].))

Theorem 5 *For an odd prime number p the following conditions are equivalent:*

(i) *p is a Fermat prime.*
(ii) *If $f(x)$ is any irreducible polynomial of degree p over a real field K with solvable Galois group and exactly one real root, then this unique real root is expressible by real radicals over K.*
(iii) *If $f(x)$ is any irreducible polynomial in $\mathbb{Q}[x]$ of degree p with the Frobenius group $F_{p(p-1)}$ as Galois group and exactly one real root, then this unique real root is expressible by real radicals.*
(iv) *There exists an irreducible polynomial in $\mathbb{Q}[x]$ with the dihedral group D_p as Galois group having exactly one real root expressible by real radicals.*

References

[1] F. Barrera-Moro and P. Lam-Estrada, *Radical extensions and crossed homomorphisms*. Bull. Austral. Math. Soc. **64**(2001), 107–119.
[2] F. Barrera-Moro and W. Y. Vélez, *Some results on radical extensions*. J. Algebra **162**(1993), 295–301.
[3] J. B. Birch, *Cyclotomic Fields and Kummer Extensions*. In: Algebraic Number Theory, (eds., W. Cassels and A. Fröhlich), Academic Press, 1967, 85–93.
[4] M. D. Fried and M. Jarden, *Field Arithmetic*. Springer, 1986.
[5] I. M. Isaacs and D.P. Moulton,*Real fields and repeated radical extensions*. J. Algebra **201**(1998), 429–455.
[6] C. U. Jensen, *A Remark on Real Radical Extensions*. Acta Arith. **107**(2003), 373–379.
[7] S. Lang, *Algebra*. Addison-Wesley, 1965.
[8] A. Loewy, *Über die Reduktion algebraischer Gleichungen durch Adjunktion insbesondere reeller Radikale*. Math. Z. **15**(1922), 261–273.
[9] B. L. van der Waerden, *Algebra I*. Springer, 1976.

Department of Mathematics
University of Copenhagen
Universitetsparken 5
DK-2100 Copenhagen
Denmark
e-mail: cujensen@math.ku.dk

https://doi.org/10.4153/CMB-2004-022-9 Published online by Cambridge University Press