ACTA ARITHMETICA
107.4 (2003)

A remark on real radical extensions

by

C. U. Jensen (Copenhagen)

1. Introduction and statement of the results. One of the most famous results in classical Galois theory is the fact that the roots of a polynomial can be expressed by radicals if and only if the Galois group of the polynomial is solvable. If the base field is real (i.e. a subfield of $\mathbb{R}$) and the polynomial has real roots it may happen that these roots can be expressed by radicals of complex numbers, but not by real radicals (i.e. the roots are contained in a radical extension of the base field, but not in a *real* radical extension of the base field, cf. Section 2). The best known case is the "*casus irreducibilis*" for a cubic polynomial: 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. In this direction there are two more general results, due to Hölder and Loewy.

Theorem A (Hölder (cf. [7], p. 346). *Let $f(x)$ be an irreducible polynomial over a real field K. If all the roots of $f(x)$ are real and expressible by real radicals, then the Galois group of $f(x)$ over K is a 2-group.*

Theorem B (Loewy [5]). *Let $f(x)$ be an irreducible polynomial over a real field K for which the degree is $n = 2^\mu u$, u an odd number. If $f(x)$ has r real roots expressible by real radicals, then there are at least $r(u-1)$ non-real roots. In particular, if the degree of $f(x)$ is odd there is at most one real root expressible by real radicals; in this case all other roots are non-real.*

If $f(x)$ is an irreducible polynomial over a real field K, and the degree of $f(x)$ is an odd prime p, it follows that a necessary condition for $f(x)$ to have a real root expressible by real radicals is that the Galois group of $f(x)$ over K is solvable and $f(x)$ has just one real root. It has been proved in [4] that this condition is sufficient if p is a Fermat prime (i.e. of the form $1 +$ a power of 2). In [4] the question was raised whether this property actually characterizes the Fermat primes. In [1] an example is given of an

2000 *Mathematics Subject Classification*: Primary 11R32, 11R37; Secondary 12F10.

irreducible polynomial in $\mathbb{Q}$ of degree 7 and the Frobenius group of order 42 as Galois group having 6 non-real roots and one real root which is not expressible by real radicals.

We shall show that the above question in [4] can be answered in the affirmative by proving

THEOREM C. *Let n be an integer > 2 and $f(x)$ an irreducible polynomial in $\mathbb{Q}[X]$ of degree n such that the Galois group of $f(x)$ over $\mathbb{Q}$ is the dihedral group D_n of order $2n$. Assume further that $f(x)$ has at least one real root.*

(1) *If n is odd, then $f(x)$ has a root α expressible by real radicals if and only if α is the only real root and every prime divisor of n is a Fermat prime.*

(2) *If n is even, but not a power of 2, then $f(x)$ has a root expressible by real radicals if and only if $f(x)$ has exactly 2 real roots and every odd prime divisor of n is a Fermat prime.*

(3) *If n is a power of 2 the real roots of $f(x)$ are expressible by real radicals.*

REMARK. Since for every $n > 2$ every imaginary quadratic number field is contained in a Galois extension of $\mathbb{Q}$ with Galois group D_n, the Fermat primes are characterized by the property described above.

Finally, we give an application concerning class fields over an imaginary quadratic number field $\mathbb{Q}(\sqrt{-D}), D$ a square-free natural number. If $\mathcal{O}$ is an order in $\mathbb{Q}(\sqrt{-D})$ and A the corresponding (ring) class group, the ring class field is an abelian extension of $\mathbb{Q}(\sqrt{-D})$ which is Galois over $\mathbb{Q}$ and the Galois group over $\mathbb{Q}$ is the semi-direct product of A with respect to the cyclic group of order 2 consisting of the identity and the complex multiplication τ, the latter operating on A by inversion.

The ring class field can be obtained as $\mathbb{Q}(\alpha, \sqrt{-D})$, where α is a real algebraic number whose degree with respect to $\mathbb{Q}$ is the order $h_{\mathcal{O}}$ of the ring class group. (If $\mathcal{O}$ is the ring of all integers in $\mathbb{Q}(\sqrt{-D})$, the ring class field is, of course, just the absolute class field of $\mathbb{Q}(\sqrt{-D})$ and $h_{\mathcal{O}}$ is the usual absolute class number of $\mathbb{Q}(\sqrt{-D})$.)

THEOREM D. *With the above notation α can be expressed by real radicals if and only if every odd prime divisor of $h_{\mathcal{O}}$ is a Fermat prime.*

Theorem D can also be expressed in terms of the class fields of complex multiplication. Indeed, let $j(\omega)$, for a complex number ω with positive imaginary part, denote the absolute invariant of the modular group, known from the theory of elliptic modular functions, usually defined by

$$j(\omega) = 1728\,\frac{g_2(\omega)^3}{\Delta(\omega)}$$

where $\Delta(\omega)$ stands for the discriminant of the complex lattice generated by 1 and ω, and $g_2(\omega)$ is the Weierstrass invariant of this lattice.

If 1 and ω, $\mathrm{Im}(\omega) > 0$, form a $\mathbb{Z}$-basis for the order $\mathcal{O}$ in $\mathbb{Q}(\sqrt{-D})$ then $j(\omega)$ is a real algebraic number and the ring class field is $\mathbb{Q}(\sqrt{-D}, j(\omega))$. (More details on the theory of ring class fields and complex multiplication can be found in [3] or [6].) Therefore Theorem D implies

THEOREM E. *If* 1 *and* ω $(\mathrm{Im}(\omega) > 0)$ *form a* $\mathbb{Z}$*-basis for an order* $\mathcal{O}$ *in an imaginary quadratic field* $\mathbb{Q}(\sqrt{-D})$, *then* $j(\omega)$ *is expressible by real radicals if and only if every odd prime divisor of the order of the class group of* $\mathcal{O}$ *is a Fermat prime.*

In particular, if 1 *and* ω, $\mathrm{Im}(\omega) > 0$, *form an integral basis for* $\mathbb{Q}(\sqrt{-D})$, *then* $j(\omega)$ *is expressible by real radicals if and only if every odd prime divisor of the class number of* $\mathbb{Q}(\sqrt{-D})$ *is a Fermat prime.*

2. Proofs of Theorems C and D. Firstly we fix some terminology. 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.*

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, L/K is called a *real radical extension.*

A real number is then expressible by real radicals over K if it is contained in a real radical extension of K.

A basic result for the following is due to F. Barrera-Mora and W. Y. Vélez [2, Theorem 2.3], which we here only formulate for number fields and simple radical extensions.

DESCENT THEOREM. *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 a finite 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.

For the proof of Theorems C and D we need two lemmas.

LEMMA 1. *Let* K *be a real number field and* p^t *a power of a Fermat prime* p. *If* $f(x)$ *is an irreducible polynomial in* $K[X]$ *of degree* p^t *such that* $f(x)$ *has exactly one real root* α *and the Galois group of* $f(x)$ *over* K *is the dihedral group* D_{p^t} *of order* $2p^t$, *then* α *is contained in a real radical extension of* K.

Proof. We proceed by induction on t. For $t = 1$ the statement follows from [4, Theorem 9.2]. Assume the lemma is proved for polynomials of degree p^{t-1} and consider a polynomial of the described type of degree p^t.

Let N be the splitting field of $f(x)$ over K. The degree over K of the unique real root α of $f(x)$ is p^t and there exists a number $\beta \in K(\alpha)$ whose degree over K is p. The Galois group of the Galois closure over K of $K(\beta)$ is the dihedral group D_p of order $2p$. Hence by the above result $K(\beta)$ is contained in a real radical extension of K. The degree of the minimal polynomial $g(x)$ of α with respect to $K(\beta)$ is p^{t-1}. The polynomial $g(x)$ has α as its only real root and the Galois group of $g(x)$ over $K(\beta)$ is the dihedral group $D_{p^{t-1}}$. By the induction hypothesis α is contained in a real radical extension of $K(\beta)$ and hence also in a real radical extension of K. ∎

LEMMA 2. *Let A be an abelian p-group, where p is a Fermat prime, and let G be the semi-direct product of A by the cyclic group $\{e, \tau\}$ of order 2, where τ operates on A by inversion of elements. If $f(x)$ is an irreducible polynomial of degree $|A|$ over a real number field K such that $f(x)$ has exactly one real root α and G is the Galois group of $f(x)$ over K, then α lies in a real radical extension of K.*

Proof. The splitting field of $f(x)$ over K is a compositum of Galois extensions $\{N_i\}$ of K, whose Galois groups are dihedral groups of order $2 \cdot$ (a power p^{t_i} of p). Each N_i is the splitting field of an irreducible polynomial $f_i(x) \in K[X]$ of degree p^{t_i} having exactly one real root α_i. By the preceding lemma each α_i lies in a real radical extension of K. Since $K(\alpha)$ is the compositum of the fields $K(\alpha_i)$ it follows that α lies in a real radical extension of K. ∎

LEMMA 3. *Let M/K be a Galois 2-extension of a real number field K. The maximal real subextension of M is a radical extension of K.*

Proof. If M is real the assertion is obvious. Otherwise let τ denote complex conjugation. The maximal real subextension is the subfield fixed by τ. The statement then follows by choosing a composition series of $\mathrm{Gal}(M/K)$ starting with the subgroup $\{e, \tau\}$ of order 2. ∎

For the sake of completeness we list the next lemma, which is just an elementary exercise in Galois theory.

LEMMA 4. *If L/K is a simple radical extension of prime degree p such that L/K is a Galois extension, then $\mathrm{Gal}(L/K)$ is cyclic and the base field K contains the pth roots of unity.*

We are now in a position to prove Theorem C.

Assertion (3) is an immediate consequence of Lemma 3.

We first prove the "if" part of assertion (1). Let $n = p_1^{t_1} \dots p_r^{t_r}$, where $p_1, \dots, p_r$ are distinct Fermat primes. The splitting field N of $f(x)$ is a compositum of fields $N_i, 1 \le i \le r$, where each N_i is a Galois extension of $\mathbb{Q}$ with the dihedral group D_{p^i} as Galois group, and each N_i is the splitting field of a polynomial $f_i(x) \in \mathbb{Q}[X]$ which has degree p^{t_i} and exactly one real root α_i. By Lemma 1 each α_i lies in a real radical extension of $\mathbb{Q}$. The unique real root α of $f(x)$ is in the compositum of the fields $\mathbb{Q}(\alpha_i)$ and therefore also in the real radical extension of $\mathbb{Q}$.

As for the "if" part of assertion (2) the two real roots of $f(x)$ generate the same number field over $\mathbb{Q}$. This real field is the compositum of subfields each of which has the form $\mathbb{Q}(\alpha)$ where the minimal polynomial of α over $\mathbb{Q}$ is either of the type described in (1) or has degree a power of 2 and a dihedral 2-group as Galois group. The result from the "if" part of (1) combined with Lemma 3 yields the assertion.

Now the "only if" part of assertion (1): By virtue of Theorem B the polynomial $f(x)$ has exactly one real root α. For each prime divisor p of n there exists a number α_p such that α_p lies in $\mathbb{Q}(\alpha)$ and the minimal polynomial of α_p has degree p, has no other real roots and has D_p as Galois group over $\mathbb{Q}$. If α lies in a real radical extension of $\mathbb{Q}$ so does α_p. Hence without loss of generality we may assume that n is a prime number p. We have to show that p is necessarily a Fermat prime. If p were not a Fermat prime, we could write $p - 1 = 2^s u$, where $s \ge 1$ and u is an odd integer > 1.

Since $f(x)$ has only one real root α, the splitting field M of $f(x)$ can be written $\mathbb{Q}(\alpha, \sqrt{-D})$, where D is a square-free natural number. The cyclotomic field $\mathbb{Q}(\zeta_p)$ is a compositum $\Gamma_0\Gamma_1$, where $\mathrm{Gal}(\Gamma_0/\mathbb{Q})$ is the cyclic group C_{2^s} of order 2^s and $\mathrm{Gal}(\Gamma_1/\mathbb{Q})$ is the cyclic group C_u of order u. Now, Γ_1 is a real number field and $\Gamma_0 = \Gamma_0^+(\sqrt{-\delta})$, where Γ_0^+ is the maximal real subfield of Γ_0 and δ is a positive number in Γ_0^+. Consequently, we get $M(\zeta_p) = \mathbb{Q}(\alpha, \sqrt{-D})\Gamma_0^+(\sqrt{-\delta})\Gamma_1$ and the maximal real subfield of $M(\zeta_p)$ is $\Gamma_0^+(\sqrt{D\delta})\Gamma_1(\alpha)$. (Here $D\delta$ may be a square in Γ_0^+, namely if $p \equiv 3 \bmod 4$ and $D = p$, but that does not affect the following argument.)

The maximal 2-subextension of $M(\zeta_p)$ is $\Gamma_0^+(\sqrt{-D}, \sqrt{-\delta})$ and the maximal real subfield F of that field is $\Gamma_0^+(\sqrt{D\delta})$. Here the Galois group $\mathrm{Gal}(M(\zeta_p)/F)$ is $D_p \times C_u$.

We need the following observation: Let L be a real subfield of $M(\zeta_p)$ containing F. If $[L : F]$ is divisible by p, then L contains $F(\alpha)$, which has degree p over F. If $[L : F]$ is not divisible by p, then L is contained in $F\Gamma_1$, which has degree u over F.

If there were a real radical extension of $\mathbb{Q}$ containing α there would also be a real radical extension of F containing α.

Now, let $\Lambda_0 \subsetneq \Lambda_1 \subsetneq \ldots \subsetneq \Lambda_n$ be a tower of simple real radical extensions of F for which Λ_n contains α. We may assume that Λ_{n-1} does not contain α. We now apply the Descent Theorem with $K = F$, $L = F(\alpha)$ and $\Lambda = \Lambda_{n-1}$.

By the above observation we see that the intersection $M(\zeta_p) \cap \Lambda_{n-1}$ must be a field between F and $F\Gamma_1$. Hence $M(\zeta_p) \cap \Lambda_{n-1}$ is an abelian extension of F contained in a real radical extension of the real number field F. Since the degree is an odd number Theorem A implies that the intersection $M(\zeta_p) \cap \Lambda_{n-1}$ is exactly F. Clearly, $\Lambda_{n-1}(\alpha) = \Lambda_n$. Hence by the Descent Theorem $F(\alpha)$ is a simple radical extension of F. Then $F(\alpha, \sqrt{-D})$ would be a simple radical extension of $F(\sqrt{-D})$. But $F(\alpha, \sqrt{-D})$ is a Galois extension of F with D_p as Galois group. In particular, $F(\alpha, \sqrt{-D})$ is a cyclic extension of $F(\sqrt{-D})$ of degree p. However, in a cyclic radical extension of degree p, by Lemma 4 the base field necessarily contains the pth roots of unity. Since $u > 1$ this is not the case in our situation. This yields the desired contradiction.

Finally, we have to show the "only if" part of assertion (2). Since the Galois group of $f(x)$ over $\mathbb{Q}$ is D_n, the number of real roots is 0, 2 or n. In view of Theorem B we see that in this situation there must be exactly 2 real roots. They generate the same field N over $\mathbb{Q}$, namely the maximal real subfield of the splitting field M of $f(x)$. For each odd prime divisor p of n the field N contains a real root of an irreducible polynomial in $\mathbb{Q}[X]$ of degree p with D_p as Galois group. We proceed then as above to conclude that p is necessarily a Fermat prime.

The proof of Theorem C is now complete.

As for Theorem D the ring class field may not be a dihedral extension of $\mathbb{Q}$, but for any odd prime divisor p in the order of the ring class group the maximal real subfield of the ring class field will contain a number α whose minimal polynomial is of the type described above. This shows the "only if" part of Theorem D. The "if" part follows from the fact that the ring class field is a compositum of 2-extensions and extensions of the type considered in Lemma 2.

References

[1] F. Barrera-Mora 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] M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, Enzyklopädie Math. Wiss., Band I_2, Heft 10, Teil II, Teubner, Stuttgart, 1958.

[4] I. M. Isaacs and D. P. Moulton, *Real fields and repeated radical extensions*, J. Algebra 201 (1998), 429–455.

[5] A. Loewy, *Über die Reduktion algebraischer Gleichungen durch Adjunktion insbesondere reeller Radikale*, Math. Z. 15 (1922), 261–273.
[6] J.-P. Serre, *Complex multiplication*, in: Algebraic Number Theory, J. W. S. Cassels and A. Fröhlich (eds.), Academic Press, 1967, 292–296.
[7] N. S. Tschebotarev, *Grundzüge der Galoisschen Theorie*, Noordhoff, Groningen, 1950. [Translated by H. Schwerdtfeger from Russian to German.]

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

Received on 18.2.2002
and in revised form on 15.4.2002 (4227)