ACTA ARITHMETICA
115.3 (2004)

# On the number of real roots of a solvable polynomial

by

C. U. Jensen (Copenhagen)

**1. Introduction and Loewy's theorem.** By a classical theorem the number of real roots of an irreducible polynomial $f(X)$ of odd prime degree $p$ over a real number field $K$ is either 1 or $p$ if the Galois group of $f(X)$ over $K$ is solvable. This result was generalized by A. Loewy in the following way:

For a polynomial $f(X)$ we let $r(f)$ denote the number of real roots of $f(X)$.

Loewy's theorem. *Let $K$ be a real number field and $f(X)$ an irreducible polynomial in $K[X]$ of odd degree $n$. If $p$ is the smallest prime divisor of $n$ and the Galois group of $f(X)$ over $K$ is solvable*, *then* $r(f) = 1$ *or $n$ or satisfies the inequalities $p \le r(f) \le n - p + 1$.*

When the degree of $f(X)$ is a prime number the above theorem is an immediate corollary to the following

Galois' theorem. *Let $f(X)$ be an irreducible separable polynomial over a field $K$ having a solvable Galois group over $K$. If the degree of $f(X)$ is a prime number*, *then any two roots of $f(X)$ generate the splitting field of $f(X)$ over $K$.*

Galois' theorem, which is basically a group-theoretic result, cannot be generalized to yield a proof of Loewy's theorem. Indeed, for any odd prime number $p$ and any $t$, $1 \le t \le p$, there exists an irreducible polynomial $f(X)$ in $\mathbb{Q}[X]$ of degree $p^2$ with solvable Galois group having $t$ roots $\alpha_1, \ldots, \alpha_t$ such that no other root of $f(X)$ lies in the field $\mathbb{Q}(\alpha_1, \ldots, \alpha_t)$.

Loewy's theorem was published in [3], a journal which is not easily available ([1]). Loewy's (rather long) proof does not use Galois theory. It might then be of some interest to give a proof using Galois theory and also yielding a sharpening of Loewy's theorem. We shall do this in Section 2. In Section 3

2000 *Mathematics Subject Classification*: 12E05, 12F10.

[1] The author is grateful to Helmut Koch for providing him a copy of that paper.

we, in particular, prove that Loewy's theorem is in some sense best possible. For these purposes it is convenient to introduce the following notation.

For a real number field $K$ and a positive odd integer $n$ we define

$$C_K(n) = \{r(f) \mid f \text{ is an irreducible polynomial of degree } n \text{ in } K[X] \\ \text{with a solvable Galois group}\}$$

and define $C(n)$ as the union of the $C_K(n)$'s, $K$ running through all real number fields. In other words a positive integer $N$ belongs to $C(n)$ if and only if there exists a real number field $K$ and an irreducible polynomial $f(X)$ in $K[X]$ having degree $n$ and solvable Galois group such that $r(f) = N$.

By induction on the degree Loewy's theorem is an immediate consequence of the following

Theorem 1. *For any positive odd integer $n > 1$ we have the following inclusion*:

$$(\Diamond) \qquad C(n) \subseteq \bigcup C(d')^{\langle d\rangle},$$

*where $d$ and $d'$ run through the divisors of $n$ such that $dd' \mid n$ and $d' \neq n$. Here for a set $A$ of integers $A^{\langle d\rangle}$ denotes the set of numbers that can be written as a sum of $d$ numbers in $A$.*

The inclusion $(\Diamond)$ in Theorem 1 is an equality if the degree $n$ is a power $p^h$ of an odd prime $p$. Indeed—as we shall prove in Section 3—if $K$ is a real number field then there exists an irreducible solvable polynomial in $K[X]$ of degree $p^h$ with $r$ real roots if and only if $r \le p^h$ and $r$ is $\equiv 1 \bmod (p-1)$. In the above terminology this is expressed in

Theorem 2. *For every real number field $K$ and every power $n = p^h$ of an odd prime number $p$, the set $C_K(n)$ consists exactly of the natural numbers $\le p^h$ which are $\equiv 1 \bmod (p-1)$.*

By these results knowledge of the number of real roots of an irreducible polynomial may yield some information about the Galois group of the polynomial. For instance, if the number of real roots of an irreducible polynomial of degree $p^h$ is $\not\equiv 1 \bmod (p-1)$ the Galois group of the polynomial is not solvable.

## 2. Proof of Theorem 1.

The proof of Theorem 1 is based on four lemmas. We omit the proofs of Lemmas 1 and 2 since they are just easy exercises in standard Galois theory.

Lemma 1. *Let $L/K$ be a finite Galois extension with Galois group $G$ and let $f(X)$ be a monic irreducible polynomial in $K[X]$ of degree $n$. All irreducible polynomials in $L[X]$ that divide $f(X)$ have the same degree. If $g(X)$ is a monic divisor of $f(X)$ and irreducible in $L[X]$ then $f(X)$ is the* *product of the distinct automorphic images of $g(X)$ under $G$. The number of irreducible factors of $f(X)$ in $L[X]$ is a divisor of $n$ and of $[L:K]$.*

LEMMA 2. *Let $K$ be a real number field and $L/K$ a finite abelian extension. If $\beta$ is a real number in $L$, then $\sigma\beta$ is also a real number in $L$ for all $\sigma\in\mathrm{Gal}(L/K)$. If $f(X)$ is an irreducible polynomial in $K[X]$ with at least one real root, then every irreducible monic polynomial in $L[X]$ dividing $f(X)$ has real coefficients.*

LEMMA 3. *Let $K$ be a number field which is invariant under complex conjugation and $c$ a real number in $K$. Assume $K$ contains a primitive pth root of unity $\zeta_p$, where $p$ is an odd prime. Let $L=K(\sqrt[p]{c})$, $\sqrt[p]{c}$ being the real root of $x^p-c$. If $\beta$ is a real number in $L\setminus K$, then $\sigma\beta$ is non-real for $\sigma\in\mathrm{Gal}(L/K)\setminus\mathrm{id}_L$.*

*Proof.* We may assume that $\sqrt[p]{c}\notin K$. The number $\beta$ can be uniquely written as $\beta=\sum_{i=0}^{p-1}a_i(\sqrt[p]{c})^i$, where $a_i\in K$ and $a_i\neq 0$ for at least one $i$, $1\le i\le p-1$.

In the following $\overline{x}$ denotes the complex conjugate of a number $x$. Since $\bar{\beta}=\sum_{i=0}^{p-1}\overline{a}_i(\sqrt[p]{c})^i$ and $\overline{a}_i\in K$ and $\beta$ is real, we conclude that $a_i$ is real for all $i$'s.

For the non-trivial automorphism $\sigma$ in $\mathrm{Gal}(L/K)$ we may assume that $\sigma(\sqrt[p]{c})=(\sqrt[p]{c})\zeta_p$. Now,

$$\sigma\beta=\sum_{i=0}^{p-1}a_i(\sqrt[p]{c}\,\zeta_p)^i,\qquad \overline{\sigma\beta}=\sum_{i=0}^{p-1}\overline{a}_i(\sqrt[p]{c}\,\overline{\zeta}_p)^i.$$

If $\sigma\beta$ were real, then $\sigma\beta=\overline{\sigma\beta}$ and thus $a_i\zeta_p^i=a_i\zeta_p^{-i}$ for all $i$'s. But there exists an $i$, $1\le i\le p-1$, such that $a_i\neq 0$. But since $p$ is odd, $\zeta_p^i\neq\zeta_p^{-i}$. This gives the desired contradiction. ■

LEMMA 4. *Let $K$ be a number field which is invariant under complex conjugation and contains a primitive pth root of unity $\zeta_p$, $p$ being an odd prime number. Let $\alpha$ be a number in $K$ such that the real value of $\sqrt[p]{c}$ lies in $K$, where $c=|\alpha|^2=\alpha\overline{\alpha}$. Then if $\beta$ is a real number in the field extension $L=K(\sqrt[p]{\alpha})$, all automorphic images $\sigma\beta$, $\sigma\in\mathrm{Gal}(L/K)$, are real.*

*Proof.* Clearly, we may assume that $\alpha\notin K^p$. If $\beta$ is an arbitrary number in $L$, we may write

$$\beta=\sum_{i=0}^{p-1}a_i(\sqrt[p]{\alpha})^i,\qquad a_i\in K.$$

If we as before let $\overline{x}$ denote the complex conjugate of $x$ we get:

$$\sqrt[p]{\alpha}\,\overline{\sqrt[p]{\alpha}}=\sqrt[p]{c},\qquad \overline{(\sqrt[p]{\alpha})^i}=\frac{(\sqrt[p]{c})^i}{\alpha}\,(\sqrt[p]{\alpha})^{p-i}$$

hence

$$\bar{\beta} = \sum_{i=0}^{p-1} \overline{a}_i \, \overline{(\sqrt[p]{\alpha})^i} = \sum_{i=0}^{p-1} \overline{a}_i \, \frac{(\sqrt[p]{c})^i}{\alpha} \, (\sqrt[p]{\alpha})^{p-i}.$$

Since $K$ is invariant under complex conjugation we have:

$$\beta \text{ real} \Leftrightarrow \beta = \bar{\beta} \Leftrightarrow a_0 = \overline{a}_0 \text{ and } a_{p-i} = \overline{a}_i \, \frac{(\sqrt[p]{c})^i}{\alpha}, \ 1 \le i \le p-1.$$

Now let $\beta$ be a real number in $L$. If $\sigma$ is a non-trivial automorphism in $\mathrm{Gal}(L/K)$ then $\sigma\beta = \sum_{i=0}^{p-1} a_i \zeta^i (\sqrt[p]{\alpha})^i$, $\zeta$ being some primitive $p$th root of unity. Since $\beta$ is real we conclude that $a_0 = \overline{a}_0$ and $a_{p-i} = \overline{a}_i (\sqrt[p]{c})^i/\alpha$, $0 \le i \le p-1$, which in turn implies

$$a_{p-i}\zeta^{p-i} = \overline{a_i \zeta^i} \, \frac{(\sqrt[p]{c})^i}{\alpha}, \qquad 1 \le i \le p-1.$$

Consequently $\sigma\beta = \overline{\sigma\beta}$, i.e. $\sigma\beta$ is real. ∎

We are now in a position to prove Theorem 1. Let $f(X)$ be an irreducible polynomial in $K[X]$ of odd degree $n$, where $K$ is a real number field and the Galois group of $f(X)$ over $K$ is solvable. $f(X)$ has at least one real root.

Let $\zeta$ be an arbitrary root of unity. If $f(X)$ is reducible in $K(\zeta)$ by Lemma 1 all irreducible factors of $f(X)$ in $K(\zeta)$ have the same degree, which must be a proper divisor $d'$ of $n$. Since the number of factors $d = n/d'$ is odd and possible factors with non-real coefficients must appear in pairs of complex conjugates there must be at least one factor with real coefficients. Hence $f(X)$ becomes reducible in $(K(\zeta) \cap \mathbb{R})[X]$.

Since $K(\zeta)/K$ is abelian the extension $(K(\zeta) \cap \mathbb{R})/K$ is Galois; therefore by Lemma 1 all irreducible factors of $f(X)$ in $K(\zeta)[X]$ lie in $(K(\zeta) \cap \mathbb{R})[X]$. Hence $r(f) \in C(d')^{\langle d \rangle}$, where $d' \neq n$. Thus $(\Diamond)$ in Theorem 1 is verified in this case.

We may therefore assume that $f(X)$ is irreducible in $K(\zeta)[X]$ for every root of unity $\zeta$. Let $\gamma$ be a real root of $f(X)$ and consider a radical extension of $K$ containing $\gamma$. Clearly we may assume that the radical extension is built up by simple radical extensions of prime degrees. We let $t$ be the product of all the prime numbers appearing in the degrees of the simple radical extensions. $\zeta_t$ denotes a primitive $t$th root of unity.

Now, let

$$(\star) \quad K_0 = K(\zeta_t), \quad K_1 = K_0(\sqrt[p_1]{\alpha_1}), \quad \alpha_1 \in K_0, \quad \ldots, \\ K_s = K_{s-1}(\sqrt[p_s]{\alpha_s}), \quad \alpha_s \in K_{s-1},$$

be a radical extension of $K$ containing $\gamma$, the degrees $p_1, \ldots, p_s$ being prime numbers.

We replace $(\star)$ by the following radical extension:

$$(\star\star)\quad K_1' = K_0(\sqrt[p_1]{\alpha_1\overline{\alpha}_1}),\quad K_1'' = K_1'(\sqrt[p_1]{\alpha_1}),\quad \ldots,\quad K_s' = K_{s-1}''(\sqrt[p_s]{\alpha_s\overline{\alpha}_s}),\quad K_s'' = K_s'(\sqrt[p_s]{\alpha_s}),$$

which will also contain $\gamma$.

We note that all the fields in $(\star\star)$ are invariant under complex conjugation.

We consider the first field in the series $(\star\star)$ in which $f(X)$ is reducible. We distinguish between two cases:

(1) The first such field is $K_i' = K_{i-1}''(\sqrt[p_i]{\alpha_i\overline{\alpha}_i})$ for some $i$, $1 \le i \le s$ (where we set $K_0'' = K_0$).

(2) The first such field is $K_i'' = K_i'(\sqrt[p_i]{\alpha_i})$ for some $i$, $1 \le i \le s$.

(1) Here $f(X)$ is irreducible in $K_{i-1}''[X]$, but reducible in $K_i'[X] = K_{i-1}''(\sqrt[p_i]{\alpha_i\overline{\alpha}_i})[X]$. Because of Lemma 1, $p_i$ must be odd. The minimal polynomial $g(X)$ of $\gamma$ over $K_i'$ is a divisor of $f(X)$ in $K_i'[X]$ and the degree of $g(X)$ is $n/p_i$, since $K_i'/K_{i-1}''$ is a Kummer extension of degree $p_i$.

$g(X)$ has real coefficients; otherwise $\gamma$ would also be a root of the complex conjugate polynomial $\overline{g}(X)$. Since $f(X)$ has real coefficients and $g(X)$ divides $f(X)$ so would $\overline{g}(X)$. Clearly $g(X)$ and $\overline{g}(X)$ are relatively prime. Consequently $g(X)\overline{g}(X)$ would divide $f(X)$ and thus $\gamma$ would be a multiple root of $f(X)$.

Since $f(X)$ is irreducible in $K_{i-1}''[X]$ at least one coefficient in $g(X)$ is not in $K_{i-1}''$. Since this coefficient is real Lemma 3 implies that $\sigma g(X)$ has at least one non-real coefficient for every $\sigma \in \mathrm{Gal}(K_i'/K_{i-1}'')$, $\sigma \neq \mathrm{id}_{K_i'}$. By Lemma 1 every monic irreducible polynomial in $K_i'[X]$ which is $\neq g(X)$ and divides $f(X)$ has at least one non-real coefficient. Since $K_i'$ is invariant under complex conjugation each of these non-real factors must occur in pairs of complex conjugates. As before we see that none of these factors has a real root. Hence all real roots of $f(X)$ are roots of $g(X)$.

Therefore $r(f) = r(g)$ and hence $r(f) \in C(n/p_i)$ $(= C(n/p_i)^{\langle 1\rangle})$, where the degree $n/p_i$ of $g(x)$ is a proper divisor of $n$. Thus the inclusion $(\Diamond)$ is verified in this case.

(2) Here $f(X)$ is irreducible in $K_i'[X]$ but reducible in

$$K_i''[X] = K_i'(\sqrt[p_i]{\alpha_i})[X].$$

By the construction of $(\star\star)$ the field $K_i'$ contains $\sqrt[p_i]{\alpha_i\overline{\alpha}_i}$.

The minimal polynomial $g(X)$ of $\gamma$ over $K_i''$ divides $f(X)$ and has degree $n/p_i$. Just as in case (1) it follows that $g(X)$ has real coefficients. By Lemma 1 the monic irreducible polynomials in $K_i''[X]$ that divide $f(X)$ are automorphic images of $g(X)$ under the action of $\mathrm{Gal}(K_i''/K_i')$. By Lemma 4 each of these polynomials has real coefficients. There are $p_i$ such factors of

$f(X)$ in $K_i''[X]$. Each of these factors has coefficients in the real number field $K_i'' \cap \mathbb{R}$ and is irreducible over this field. Hence $r(f)$ is a number in $C(n/p_i)^{\langle p_i \rangle}$ and the inclusion ($\Diamond$) is also verified in this case. The proof of Theorem 1 is now complete. ∎

**3. Proof of Theorem 2 and construction of solvable polynomials with prescribed number of real roots.** In this section we first show that the bounds given in the original formulation of Loewy's theorem are best possible, and next in the case where the degree of the polynomial is an odd prime power we give the precise numbers of real roots that can occur.

For this we need the following well known slight sharpening of Hilbert's irreducibility theorem:

Theorem 3. *Let $K$ be an algebraic number field and $F(X, T_1, \ldots, T_u)$ an irreducible polynomial in $K[X, T_1, \ldots, T_u]$. The rational $u$-tuples $(q_1, \ldots$ $\ldots, q_u)$ for which $F(X, q_1, \ldots, q_u)$ is irreducible in $K[X]$ are everywhere dense in the Euclidean space $\mathbb{R}^u$.*

*Proof (sketch).* By [2, Prop. 3.3, p. 236] the assertion is reduced to the case where $K = \mathbb{Q}$. By iterative use of Kronecker specializations (cf. [2, Prop. 3.1, p. 234]) it is reduced to the case where $u = 1$. The theorem then follows from [2, Cor. 2.5, p. 231]. ∎

We first prove that for any odd natural number $n$ and any prime divisor $p$ of $n$ there exist—over an arbitrarily prescribed real number field $K$—irreducible polynomials $f_1(X)$ and $f_2(X)$ having degree $n$ and solvable Galois groups such that $r(f_1) = p$ and $r(f_2) = n - p + 1$.

Since there exist cyclic extensions of any degree over any number field the existence of $f_1(X)$ is just a special case of the following

Theorem 4. *Let $n$ be an odd natural number and $d$ a divisor of $n$. Then for any real number field $K$ we have the inclusion*

$$C_K(d) \subseteq C_K(n).$$

*Proof.* Let $f(X)$ be a monic irreducible polynomial in $K[X]$ of degree $d$ having a solvable Galois group over $K$. We have to construct an irreducible polynomial $g(X)$ in $K[X]$ of degree $n$ having a solvable Galois group over $K$ and the same number of real roots as $f(X)$ has. The polynomial $f(X^{n/d}+T)$ is irreducible in $K[X, T]$. Indeed, $f(T)$ is irreducible in $K[X, T]$, hence so is $f(X^{n/d}+T)$. Clearly, $f(X^{n/d})$ and $f(X)$ have the same number of real roots (which are simple). Hence $f(X^{n/d} + q)$ and $f(X)$ have the same number of real roots for every sufficiently small (in absolute value) rational number $q$. By Theorem 3 we can choose such a $q$ so that $f(X^{n/d} + q)$ is irreducible in $K[X]$. Clearly, $f(X^{n/d} + q)$ has solvable Galois group and thus has the desired properties. ∎

The existence of $f_2(X)$ is a consequence of the following

Theorem 5. *For any two odd natural numbers $m$ and $d$ and any real number field $K$ we have*

$$\begin{aligned} C_K(md) &\supseteq \{d, d+(m-1), d+2(m-1), \dots, d+d(m-1)\} \\ &= \{d+t(m-1) \mid 0 \le t \le d\}. \end{aligned}$$

For the proof we use the existence of a $D_m$-generic polynomial, where $D_m$ is the dihedral group of order $2m$, $m$ being an odd integer $> 1$ (cf. [1, Chap. 5] or [4, Section 3]). This means that there is a polynomial $f(X, T_1, \dots, T_\nu) \in \mathbb{Q}[X, T_1, \dots, T_\nu]$ of degree $m$ with respect to $X$ with the following properties:

(i) The Galois group of $f(X, T_1, \dots, T_\nu)$, viewed as a polynomial in $X$ over the function field $\mathbb{Q}(T_1, \dots, T_\nu)$, is $D_m$.

(ii) For every field $K$ of characteristic 0 and every Galois extension $M$ of $K$ with $D_m$ as Galois group there exist elements $k_1, \dots, k_\nu$ in $K$ such that $M$ is the splitting field over $K$ for the specialized polynomial $f(X, k_1, \dots, k_\nu)$.

Now let $L$ be a cyclic extension of degree $d$ over $K$. Any quadratic extension of $L$ can be embedded into a $D_m$-extension of $L$. Let $\pi$ be a number in $L$ such that $\pi \notin \gamma L^2$ for every $\gamma$ in every proper subfield of $L$. (For instance, let $\pi$ be the generator of a principal prime ideal in the ring $\mathcal{O}_L$ of integers in $L$, such that the prime ideal $\mathbb{Z}p$ in $\mathbb{Z}$ determined by $\mathbb{Z}p = \mathcal{O}_L\pi \cap \mathbb{Z}$ splits completely in $[L : \mathbb{Q}]$ distinct prime ideals in $\mathcal{O}_L$.)

Let $\beta_1, \dots, \beta_\nu$ be numbers in $L$ such that the splitting field over $L$ for the specialized generic $D_m$-polynomial $f(X, \beta_1, \dots, \beta_\nu)$ is a Galois extension of $L$ containing $\sqrt{\pi}$ and having $D_m$ as Galois group. Then $f(X, \beta_1, \dots, \beta_\nu)$ is necessarily irreducible in $L[X]$ and—by the construction of $\pi$—no proper subfield of $L$ contains all its coefficients. This implies that the product $F(X, \beta_1, \dots, \beta_\nu)$ of the polynomials $\sigma f(X, \beta_1, \dots, \beta_\nu)$, $\sigma$ running through the automorphisms in the Galois group of $L/K$, is an irreducible polynomial in $K[X]$.

Let $\alpha$ be a primitive element for $L/K$, i.e. $L = K(\alpha)$. We write

$$\beta_1 = \sum_{\mu=0}^{d-1} k_{1\mu}\alpha^\mu, \quad \dots, \quad \beta_\nu = \sum_{\mu=0}^{d-1} k_{\nu\mu}\alpha^\mu$$

where the $k$'s are numbers in $K$.

If $\alpha = \alpha_1, \alpha_2, \dots, \alpha_d$ are the conjugates of $\alpha$ with respect to $K$, the above polynomial $F(X, \beta_1, \dots, \beta_\nu)$ can be written

$$\prod_{i=1}^{d} f\Big(X, \sum_{\mu=0}^{d-1} k_{1\mu}\alpha_i^\mu, \dots, \sum_{\mu=0}^{d-1} k_{\nu\mu}\alpha_i^\mu\Big).$$

The polynomial obtained by replacing the $k$'s by variables, i.e.

$$F(X, U_{10}, \dots, U_{\nu,d-1}) := \prod_{i=1}^{d} f\Big(X, \sum_{\mu=0}^{d-1} U_{1\mu}\alpha_i^{\mu}, \dots, \sum_{\mu=0}^{d-1} U_{\nu\mu}\alpha_i^{\mu}\Big),$$

is an irreducible polynomial in $K[X, U_{10}, \dots, U_{\nu,d-1}]$.

Since there exist $D_m$-extensions of $\mathbb{Q}$ whose unique quadratic subfield is imaginary quadratic, and $D_m$-extensions of $\mathbb{Q}$ whose unique quadratic subfield is real quadratic, there are rational numbers $a_1, \dots, a_\nu$ such that $f(X, a_1, \dots, a_\nu)$ has exactly $m$ real roots and rational numbers $b_1, \dots, b_\nu$ such that $f(X, b_1, \dots, b_\nu)$ has exactly one real root. Moreover, the roots of these polynomials are simple.

For an integer $t$, $1 \le t \le d$, we consider the following $\nu$ systems of linear equations:

$$a_j = \sum_{\mu=0}^{d-1} x_{j\mu}\alpha_i^{\mu}, \qquad 1 \le j \le \nu,\ 1 \le i \le t,$$

$$b_j = \sum_{\mu=0}^{d-1} x_{j\mu}\alpha_i^{\mu}, \qquad 1 \le j \le \nu,\ t+1 \le i \le d.$$

Since the determinant of the matrix $\{\alpha_i^{\mu}\}$ $(1 \le i \le d,\ 0 \le \mu \le d-1)$ is $\ne 0$, the above systems have a solution $x_{j\mu}$ inside $L$.

The polynomials $f(X, \sum_{\mu=0}^{d-1} x_{1\mu}\alpha_i^{\mu}, \dots, \sum_{\mu=0}^{d-1} x_{\nu\mu}\alpha_i^{\mu})$ have exactly $m$ real roots for $1 \le i \le t$, and exactly one real root for $t+1 \le i \le d$.

If the above numbers $x_{j\mu}$ are replaced by rational numbers $q_{j\mu}$ sufficiently close to $x_{j\mu}$ the new polynomials will have the same number of real roots as the original polynomials. The product

$$\prod_{i=1}^{d} f\Big(X, \sum_{\mu=0}^{d-1} q_{1\mu}\alpha_i^{\mu}, \dots, \sum_{\mu=0}^{d-1} q_{\nu\mu}\alpha_i^{\mu}\Big)$$

will then have $tm + (d-t) = d + t(m-1)$ real roots.

Since $F(X, U_{10}, \dots, U_{\nu,d-1})$ is irreducible in $K[X, U_{10}, \dots, U_{\nu,d-1}]$ it follows from Theorem 3 that the $q_{j\mu}$'s can be chosen so that moreover the specialized polynomial $F(X, q_{10}, \dots, q_{\nu,d-1})$ is irreducible in $K[X]$. Obviously $F(X, q_{10}, \dots, q_{\nu,d-1})$ has solvable Galois group. ■

We are now able to prove Theorem 2: If $n$ is a power $p^h$ of an odd prime number $p$, it is immediate to check that every number in the set $\bigcup C_K(d')^{\langle d\rangle}$ appearing in Theorem 1 is $\equiv 1 \bmod (p-1)$. Conversely, by application of Theorems 4 and 5 setting $m = p$ and successively $d = p, d = p^2, \dots, d = p^{h-1}$, we see that every natural number $\le p^h$ which is $\equiv 1 \bmod (p-1)$ lies in $C_K(p^h)$. ■

**4. Concluding remarks.** It would be natural to ask for a description of the set $C_K(n)$ when $n$ is an odd positive integer not necessarily a prime power. The main obstacle to give a complete answer is that it is unknown (to the author) whether the inclusion ($\Diamond$) in Theorem 1 is actually an equality. Even if this were true a precise description would be rather complicated.

So far we only have fragmentary results. For certain numbers $n$ (for every $K$) the set $C_K(n)$ is just the set of odd numbers from 1 to $n$. This holds if $n = 3^t \cdot u$, where $3 \nmid u$ and $3^t \geq u - 2$. For instance if $n = 15$, $C_K(15)$ consists of all odd numbers from 1 to 15, while for $n = 21$, $C_K(21)$ consists of all odd numbers from 1 to 21 except 5. [Hence an irreducible polynomial of degree 21 with exactly 5 real roots cannot have a solvable Galois group.]

As the referee has kindly pointed out, Theorems 1, 4 and 5 easily imply that (for every $K$) $C_K(pq) = \{1 + a(p-1) + b(q-1) \mid 0 \leq a \leq q,\ 0 \leq b \leq p,\ \min(a,b) \leq 1\}$ for any two distinct odd primes $p$ and $q$. However, if $n$ is divisible by more than two distinct primes, the methods in this paper probably do not allow a precise description of $C_K(n)$.

Finally we remark that the results in Section 2 will be valid for an arbitrary ordered field $K$ if $\mathbb{R}$ is replaced by the corresponding real closure of $K$. As for the results from Section 3 it is likely that they may be carried over to any ordered field $K$ if one moreover assumes that $K$ is a Hilbertian field.

## References

[1] C. U. Jensen, A. Ledet and N. Yui, *Generic Polynomials*, Cambridge Univ. Press, 2002.

[2] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.

[3] A. Loewy, *Über algebraisch auflösbare Gleichungen*, Scripta Univ. Hierosolymitanarum 1 (1923), no. 5, 1–12.

[4] D. J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. 43 (1982), 250–283.

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

*Received on 1.12.2003*
*and in revised form on 1.3.2004* (4671)