ACTA ARITHMETICA
XXXVI (1980)

On normal binomials*

by

WILLIAM YSLAS VÉLEZ (Albuquerque, N. Mex.)

1. Introduction. Throughout this paper small latin letters shall denote either elements from a field F or rational integers, the context should make it clear which is meant. Greek letters shall denote elements which are algebraic over F. By ζ_m we shall mean a primitive mth root of unity. If p is a prime then $p^e \| m$ shall mean that $p^e | m$, $p^{e+1} \nmid m$.

(1.1) Let K be a field extension of F and let K^* denote the multiplicative group of non-zero elements in K. For $\alpha \in K$, let $o(\alpha)$ denote the *order of* α in the quotient group, K^*/F^*.

We say that $x^m - a$ is *weakly normal* if $F(\alpha)$ is the splitting field of $x^m - a$, for every root α of $x^m - a$. We say that $x^m - a$ is *irreducible normal* if $x^m - a$ is irreducible and normal.

Weakly and irreducible normal binomials have been characterized over Q (Darbi [1], Bessel-Hagen [9], p. 302, and Mann and Vélez [5]), and also over real fields (Gay [3]).

(1.2) Given F, set $U(F) = \{m\colon \operatorname{char} F \nmid m$ and there exists an $a \in F^*$ such that $x^m - a$ is weakly normal$\}$, $C(F) = \{m\colon \operatorname{char} F \nmid m,\ F(\zeta_m) = F(b^{1/r})$, where $x^r - b$ is irreducible over F and $r | m\}$, $I(F) = \{m\colon \operatorname{char} F \nmid m$ and there exists an $a \in F$ such that $x^m - a$ is irreducible normal$\}$.

In Section 2 we give a new proof of a theorem of Schinzel. The proof is broken up into a series of lemmas, lemmas which we shall use again in Section 3. In Section 3 we study weakly and irreducible normal binomials over arbitrary fields. We characterize those fields, whose characteristic is not 2, which have the property that $U(F) = C(F)$. We then specialize to algebraic number fields and show that $C(F) = I(F)$, for F a finite extension of Q.

Finally, in Section 4 we apply these results to answer a question

* This work was supported by the U.S. Energy Research and Development Administration (ERDA) under Contract No. AT (29-1)-789.

raised by Henry B. Mann, namely, if $F = Q(\zeta_4)$, then what are all of the weakly and irreducible normal binomials over $Q(\zeta_4)$.

For convenience, we shall state a theorem which will be used often in our investigations.

(1.3) Let $o(\alpha) = m$ and set $n = \max\{l : l|m \text{ and } \zeta_l \in F(\alpha)\}$, $s = [F(\alpha):F(\zeta_n)]$.

THEOREM 1.1. *With $o(\alpha) = m$ and n, s defined as in* (1.3), *we have that $F(\alpha^s) = F(\zeta_n)$ and $s|m$. Further, if $F(\alpha) \supset K \supset F(\zeta_n)$, $l = [F(\alpha):K]$, then $K = F(\alpha^l)$.*

Proof. See Theorem 1 of [6]. ■

The author would like to thank Henry B. Mann and David Gay for many conversations concerning the subject matter of this paper.

2. Proof of Schinzel's theorem

LEMMA 2.1. *Let F be a field, m, n integers so that $(m, n) = 1$. If $a = b_1^m = b_2^n$, with $b_1, b_2 \in F$, then there exists an element $b \in F$ such that $a = b^{mn}$.*

Proof. Set $m+n = k$, then $(mn, k) = 1$. Thus there are integers x, y such that $xk - ymn = 1$. Set $b = (b_1 b_2)^x / a^y$, then $b^{mn} = a$. ■

LEMMA 2.2. *Let $4|m$, $a^{1/2} \notin F$ yet $x^4 - a$ reducible over F. If α is any root of $x^m - a$, then $F(\alpha^{m/4}) = F(\alpha^{m/2}) = F(\zeta_4)$.*

Proof. Clearly $\alpha^{m/4}$ is a root of $x^4 - a$. Further, since $a^{1/2} \notin F$ and $\alpha^{m/2}$ is a root of $x^2 - a$, we have that $[F(\alpha^{m/2}):F] = 2$.

We shall now show that $F(\alpha^{m/2})$ is the splitting field of $x^4 - a$. This fact implies that $F(\alpha^{m/4}) = F(\alpha^{m/2}) = F(\zeta_4)$.

Since $x^4 - a$ is reducible and $x^2 - a$ is irreducible, we have that $\zeta_4 \notin F$ and $-4a = c^4$, $c \in F$. Thus $-a = (c^2/2)^2$, so $(-a)^{1/2} \in F$. But $F(\alpha^{m/2}) = F(a^{1/2})$, thus, since $(-a)^{1/2}$, $a^{1/2} \in F(a^{1/2})$, we have that $\zeta_4 \in F(a^{1/2})$. So $F(\alpha^{m/2}) = F(\zeta_4)$.

To show that $F(\alpha^{m/2})$ is the splitting field of $x^4 - a$, all we have to show is that $F(\alpha^{m/2})$ contains one root of $x^4 - a$. Now, since $-4a = c^4$, we have that $(-4a)^{1/4} \in F$. But $(-4a)^{1/4} = \zeta_8 2^{1/2} a^{1/4}$ and $\zeta_8 2^{1/2} = 1 + \zeta_4 \in F(\zeta_4)$, thus $a^{1/4} \in F(\zeta_4)$. Hence, $F(\zeta_4)$ contains all of the roots of $x^4 - a$, yet $\alpha^{m/4}$ is a root of $x^4 - a$, so $F(\alpha^{m/4}) = F(\alpha^{m/2}) = F(\zeta_4)$. ■

Let $K \supset F$, we say that K has the *unique subfield property* if for every divisor l of $[K:F]$, there exists exactly one subfield, $K \supset F_1 \supset F$, with $[F_1:F] = l$.

LEMMA 2.3. *Let $\operatorname{char} F \nmid m$, $x^m - a$ irreducible over F, and $F(a^{1/m}) = F(b^{1/m})$. If $F(a^{1/m})$ has the unique subfield property, then $b^{1/m} = c(a^{1/m})^t$, $(t, m) = 1$, $c \in F$.*

Proof. We first prove this for the case $m = p^k$, p a prime. For $k = 1$, see Theorem 59 of [4]. Thus, assume the lemma is true for k and let $m = p^{k+1}$. So $F(a^{1/p^{k+1}}) = F(b^{1/p^{k+1}})$. Since $F(a^{1/p^{k+1}})$ has the unique subfield property, we have that $b^{1/p^k} = c(a^{1/p^k})^t$, $(t, p) = 1$. Thus, $b^{1/p^{k+1}} = c^{1/p}(a^{1/p^{k+1}})^t$. If $c^{1/p} \in F$, then the theorem is proven. If not, then $F(c^{1/p}) = F(a^{1/p})$, so $c^{1/p} = c_1(a^{1/p})^{t_1}$, $(t_1, p) = 1$. Thus

$$c^{1/p} = c_1(a^{1/p^{k+1}})^{t_1 p^k}, \quad \text{so} \quad b^{1/p^{k+1}} = c_1(a^{1/p^{k+1}})^{t+t_1p^k} \quad \text{and} \quad (t+t_1p^k, p) = 1.$$

So the lemma is proven if m is a prime power.

We now induct on the number of distinct prime factors in m. Write $m = rs$, $(r, s) = 1$, $r > 1$, $s > 1$. Since $a^{1/m}$ has the unique subfield property, we have that $F(a^{1/r}) = F(b^{1/r})$, $F(a^{1/s}) = F(b^{1/s})$. Hence, by induction, we have that $b^{1/r} = c_1(a^{1/r})^{t_1}$, $(t_1, r) = 1$, $b^{1/s} = c_2(a^{1/s})^{t_2}$, $(t_2, s) = 1$. There are integers x, y so that $xr + sy = 1$; so $(x/s) + (y/r) = 1/rs = 1/m$. Thus $b^{y/r} = c_1^y(a^{1/rs})^{yt_1s}$, $b^{x/s} = c_2^x(a^{1/rs})^{xt_2r}$, so $b^{1/m} = c_1^y c_2^x (a^{1/m})^{yt_1s+xt_2r}$, and $(yt_1s + xt_2r, m) = 1$. ■

Let $\operatorname{char} F \nmid m$ and let w_m be the number of mth roots of unity contained in F.

LEMMA 2.4. *Let p be a prime and $x^{p^e} - a$ have abelian Galois group, then $a^{w_{p^e}} = b^{p^e}$, for some $b \in F$.*

Proof. First of all, assume that $p = 2$ and $\zeta_4 \notin F$.

If $e = 1$, the assertion is obvious. Thus assume that the assertion is true for all $k < e$. Clearly, $x^{2^{e-1}} - a$ has abelian Galois group, so by the induction hypothesis, we have that $a^2 = b_1^{2^{e-1}}$ (since $\zeta_4 \notin F$, $w_{2^k} = 2$, $k \geqslant 1$). If $b_1 = b^2$, the induction is complete. Hence, assume that $b_1 \neq b^2$, for all $b \in F$. Now, if α is a root of $x^{2^e} - a$, then $\alpha = \zeta_{2^{e+1}}^i b_1^{1/4}$, for some i, and $F(\alpha, \zeta_{2^e}) \subset F(\alpha, \zeta_{2^{e+1}})$. Thus $F(b_1^{1/4})$ is an abelian extension. If $x^4 - b_1$ is irreducible, then $\zeta_4 \in F(b_1^{1/4})$. If not, then by Lemma 2.2, $\zeta_4 \in F(b_1^{1/4})$. Hence, in either case, $F(\zeta_4) = F(b_1^{1/2})$, so $b_1^{1/2} = b\zeta_4$, $b \in F$, by Lemma 2.3. Thus $b_1 = -b^2$, so $a^2 = (-b^2)^{2^{e-1}} = b^{2^e}$. Thus the theorem is true for $p = 2$ and $\zeta_4 \notin F$.

Now assume that either p is odd or if $p = 2$ then $\zeta_4 \in F$.

Let $e = 1$. If $\zeta_p \in F$, then $w_p = p$ and $a^{w_p} = a^p$. If $\zeta_p \notin F$, then a must be a pth power, so $a^{w_p} = a^1 = b^p$.

Thus, we may assume that the assertion is true for all $k < e$. Assume that $a = b_1^{p^f}$, where $1 < f \leqslant e$. Then $x^{p^{e-f}} - b_1$ has abelian Galois group and by the induction hypothesis, we have that $b_1^{w_q} = c^{p^{e-f}}$, where $q = p^{e-f}$. Thus $(b_1^{w_q})^{p^f} = (b_1^{p^f})^{w_q} = a^{w_q} = c^{p^e}$. However $w_q | w_{p^e}$, thus $a^{w_{p^e}} = (c^l)^{p^e}$ where $l = (w_{p^e})/(w_q)$.

Thus, we may assume that a is not a pth power, hence $x^{p^e} - a$ is irreducible. (This can be obtained by a slight modification of Theorem 51 of [4].) Let α be any root of $x^{p^e} - a$, then since $x^{p^e} - a$ is normal and abelian, we have that $\zeta_{p^e} \in F(\alpha)$ and $F(\alpha^s) = F(\zeta_{p^e})$, by Theorem 1.1. However, $F(\zeta_{p^e})$ has the unique subfield property (since its Galois group is cyclic), ζ_{p^e} satisfies the irreducible binomial $x^{p^e} - \zeta_{w_{p^e}}$, and $s = w_{p^e}$.

Thus, by Lemma 2.3, $\alpha^s = b\zeta_{p^e}$, so $(\alpha^s)^{p^e/w_{p^e}} = \alpha^{p^e} = a = b^{p^e/w_{p^e}}\zeta_{w_{p^e}}$, thus $a^{w_{p^e}} = b^{p^e}$. ∎

THEOREM 2.1 (Schinzel [8]). *The binomial $x^m - a$ has abelian Galois group iff $a^{w_m} = b^m$.*

Proof. Assume that $a^{w_m} = b^m$, then $a = \zeta_{w_m}^i b^{m/w_m}$. Let $K = F(b^{1/w_m}, \zeta_{mw_m})$, then K is an abelian extension of F since $F(b^{1/w_m})$ and $F(\zeta_{mw_m})$ are both abelian. Since $a = \zeta_{w_m}^i b^{m/w_m} = (\zeta_{mw_m}^i b^{1/w_m})^m$, we have that K contains a root of $x^m - a$. Also $\zeta_m \in K$, thus the splitting field of $x^m - a$ is contained in K, so the Galois group is abelian.

Assume that $x^m - a$ has abelian Galois group and write $m = \prod_i p_i^{e_i}$. Then $x^{p_i^{e_i}} - a$ has abelian Galois group, so, by Lemma 2.4, $a^{w_{p_i^{e_i}}} = b_i^{p_i^{e_i}}$. However, $w_m = l_i w_{p_i^{e_i}}$, so $a^{w_m} = (b_i^{l_i})^{p_i^{e_i}}$, for each i. Thus by Lemma 2.1, $a^{w_m} = b^m$. ∎

LEMMA 2.5. *Let $x^m - a$ be irreducible normal with cyclic Galois group. If $4|m$ then $\zeta_4 \in F$.*

Proof. Let α be a root of $x^m - a$, then $\alpha^{m/4}$ is a root of $x^4 - a$. Further, $x^4 - a$ is irreducible normal with cyclic Galois group, thus $\zeta_4 \in F(\alpha^{m/4}) = F(a^{1/4})$.

Assume that $\zeta_4 \notin F$, then $F(\zeta_4) = F(a^{1/2})$; by Theorem 1.1, hence $a^{1/2} = b\zeta_4$ and $a^{1/4} = b^{1/2}\zeta_8$. Now $F(\zeta_8 b^{1/2}) \subset F(\zeta_8, b^{1/2})$. Thus $[F(\zeta_8, b^{1/2}): F] = 4$ or 8. If the degree is 8, then this field has Galois group $Z_2 + Z_2 + Z_2$ and this contradicts the assumption that a subfield has cyclic group Z_4. Thus $[F(\zeta_8, b^{1/2}): F] = 4$, and it must have Galois group $Z_2 + Z_2$. However, $F(\zeta_8, b^{1/2}) = F(a^{1/4})$, and this has cyclic Galois group, a contradiction. Thus $\zeta_4 \in F$. ∎

LEMMA 2.6. *Let p be prime, $x^{p^e} - a$ irreducible normal with abelian Galois group. If p is odd or if $p = 2$ and $\zeta_4 \in F$, then the Galois group is cyclic.*

Proof. Since $x^{p^e} - a$ is irreducible and has cyclic Galois group we have that $x^p - a$ is irreducible and normal. Thus if β is any root of $x^p - a$, we have that $\zeta_p \in F(\beta)$, yet $[F(\beta): F] = p$, so $\zeta_p \in F$. Further, if α is any root of $x^{p^e} - a$, then $\zeta_{p^e} \in F(\alpha)$. Set $w_{p^e} = p^f$, where $f > 0$. Then $x^{p^k} - \zeta_{p^f}$ is irreducible over F (recall that if $p = 2$, then $\zeta_4 \in F$). Thus $[F(\zeta_{p^e}): F] = p^{e-f}$ and $[F(\alpha): F(\zeta_{p^e})] = p^f$.

If $e = f$ then the assertion is obvious. Thus we may assume that $f < e$. Consider $F(\zeta_{p^{e+f}})$. This has degree p^e over F and has cyclic Galois group. Let σ denote the generator of this Galois group. Then $\sigma(\zeta_{p^{e+f}}) = \zeta_{p^e}^i \zeta_{p^{e+f}}$, for some i, and $\sigma(\zeta_{p^e}) = \zeta_{p^e}^{ip^f}\zeta_{p^e}$.

By Theorem 2.1, we have that $a^{p^f} = b^{p^e}$, thus $a = \zeta_{p^f} b^{p^{e-f}}$, and $\alpha = \zeta_{p^{e+f}} b^{1/p^f}$. Define $\tau(\alpha) = \zeta_{p^e}^i \alpha = \zeta_{p^e}^i \zeta_{p^{e+f}} b^{1/p^f}$, thus $\tau(\alpha)$ is a conjugate of α. By Theorem 1.1, we have that $F(\alpha^{p^f}) = F(\zeta_{p^e})$, and $F(\zeta_{p^e})$ has the unique subfield property, so $\zeta_{p^e} = c\alpha^{p^f}$, $c \in F$, by Lemma 2.3.

Thus $\tau(\zeta_{p^e}) = \tau(c\alpha^{p^f}) = c(\zeta_{p^e}^i \alpha)^{p^f} = c\zeta_{p^e}^{ip^f}\alpha^{p^f} = \zeta_{p^e}^{ip^f}\zeta_{p^e}$. Note that $\tau(\zeta_{p^e}) = \sigma(\zeta_{p^e})$. Thus τ is an automorphism and it has the same order as σ, thus the Galois group of $x^{p^e} - a$ is cyclic. ∎

THEOREM 2.2 (Schinzel). *Let $x^m - a$ be irreducible with abelian Galois group. If $4|m$ and $\zeta_4 \notin F$, then the Galois group is $Z_2 + Z_{m/2}$, otherwise the Galois group is cyclic.*

Proof. Let $m = \prod_i p_i^{e_i}$. Then $x^{p_i^{e_i}} - a$ is irreducible normal with abelian Galois group. If G_{p_i} is the Galois group of $x^{p_i^{e_i}} - a$, then the Galois group, G, of $x^m - a$ is isomorphic to the direct sum of the G_i. If p_i is odd, then G_i is cyclic, by Lemma 2.6. Thus G is cyclic iff G_2 is cyclic. If $\zeta_4 \in F$ and $4|m$, then by Lemma 2.6, G_2 is cyclic, thus G is cyclic.

Assume that $4|m$ and $\zeta_4 \notin F$. Then G is not cyclic by Lemma 2.5. If α is any root of $x^m - a$, then $\alpha^{m/4}$ is a root of $x^4 - a$, and $x^4 - a$ is irreducible normal. Thus, by Theorem 1.1, we have that $F(\alpha^{m/2}) = F(\zeta_4)$. Thus $x^{m/2} - \alpha^{m/2}$ is irreducible over $F(\alpha^{m/2})$, $\zeta_4 \in F(\alpha^{m/2})$ and the Galois group of $F(\alpha)$ over $F(\alpha^{m/2})$ is cyclic. Call this Galois group G', then we have that $G/G' \approx Z_2$. Thus G is either Z_m or $Z_2 + Z_{m/2}$ (Section 52 of [2]). However, $G \neq Z_m$ since $\zeta_4 \notin F$, thus G is isomorphic to $Z_2 + Z_{m/2}$. ∎

3. Weakly and irreducible normal binomials

THEOREM 3.1. *Let $\operatorname{char} F \nmid m$ and $x^m - a$ weakly normal, p a prime, $p|m$ and $\zeta_p \notin F$, then $(\varphi_F(m), p) = 1$, where $\varphi_F(m) = [F(\zeta_m): F]$.*

Proof. Since $x^m - a$ is weakly normal, we have that $m = kl\varphi_F(m)$, where $l\varphi_F(m) = [F(\alpha): F]$ and α is any root of $x^m - a$. Let $p^e \| m$ and let $a = b^{p^f}$, where if $f < e$ then $a \neq b_1^{p^{f+1}}$, for all $b_1 \in F$. With $m' = m/p^f$, we have that $x^{m'} - b | x^m - a$ and $x^{m'} - b$ is weakly normal. So $m' = k'l\varphi_F(m)$. If $e = f$, then $(m', p) = 1$, so $(\varphi_F(m), p) = 1$. Thus, we may assume that $e > f$. Then $x^p - b$ is irreducible and if β is any root of $x^{m'} - b$, then $\beta^{m'/p}$ is a root of $x^p - b$. If $p | \varphi_F(m)$, then $p^{e-f} \nmid l$ so $l | (m'/p)$. Thus $F(\beta^l) \supset F(\beta^{m'/p})$. However, $F(\beta^l) = F(\zeta_m)$, by Theorem 1.1, thus $F(\beta^{m'/p})$ is normal, so $x^p - b$ is irreducible normal and this implies $\zeta_p \in F$, a contradiction. Thus $p \nmid \varphi_F(m)$. ∎

LEMMA 3.1. *With $U(F), C(F), I(F)$ defined as in (1.2), we have that $U(F) \supset C(F) \supset I(F)$.*

Proof. Let $m \in I(F)$, then there exists $a \in F$ such that $x^m - a$ is irreducible normal. If α is any root of $x^m - a$, then $F(\zeta_m) \subset F(\alpha)$, thus $\varphi_F(m) | m$. Let $s = [F(\alpha): F(\zeta_m)]$, then by Theorem 1.1, we have that $F(\alpha^s) = F(a^{1/r}) = F(\zeta_m)$, where $r = \varphi_F(m)$, and $x^r - a$ is irreducible, thus $m \in C(F)$.

Let $m \in C(F)$, thus $F(\zeta_m) = F(b^{1/r})$, where $r | m$ and $x^r - b$ is irreducible normal. Let $a = bc^r$, and let α be any root of $x^m - a$. Then $\alpha = \zeta_m^i b^{1/m} c^{1/k}$, where $k = m/\varphi_F(m)$. Then $\alpha^k = \zeta_{m/k}^i b^{1/r} c$, thus $F(\alpha) \supset F(\alpha^k) = F(\zeta_r^i b^{1/r})$.

However, $\zeta_r^i b^{1/r}$ is a root of x^r-b, and x^r-b is irreducible normal, thus $F(\zeta_r^i b^{1/r}) = F(\zeta_m)$ and $\zeta_m\in F(a)$, so x^m-a is weakly normal, and $m\in U(F)$. ■

(3.1) Let char $F\nmid m$ and write $m=\prod_i p_i^{e_i}$. Define f_i by: $a = b_i^{p_i^{f_i}}$, where $f_i\leqslant e_i$, and if $f_i<e_i$, then $a\neq b^{p_i^{f_i+1}}$, for all $b\in F$. Set $P=\prod_i p_i^{f_i}$ and $m'=m/P$. By Lemma 2.1, we have that there exists $b\in F$ for which $a=b^P$, furthermore $x^{m'}-b\,|\,x^m-a$.

LEMMA 3.2. *If $\zeta_4\in F$, then $x^{m'}-b$ is irreducible. Furthermore, $U(F)=C(F)$.*

Proof. By Theorem 51 of [4], we have that $x^{m'}-b$ is irreducible. If x^m-a is weakly normal, then $x^{m'}-b$ is also weakly normal and $m'|m$. Then if β is any root of $x^{m'}-b$, we have $F\subset F(\zeta_{m'})\subset F(\zeta_m)\subset F(\beta)$, since β is also a root of x^m-a. By Theorem 1.1, we have that $F(\beta^l) = F(b^{1/(m'/l)}) = F(\zeta_m)$, where $l=[F(\beta):F(\zeta_m)]$ and $x^{m'/l}-b$ is irreducible. Thus $\varphi_F(m)|m'$, so $\varphi_F(m)|m$, and $U(F)=C(F)$. ■

(3.2) Set $\eta_{2^l}=\zeta_{2^l}+\zeta_{2^l}^{-1}$. If $\zeta_4\notin F$, set $A=\infty$ if $\eta_{2^l}\in F$, for all l, otherwise set $A=\max\{l:\ \eta_{2^l}\in F\}$. Note that $(\eta_{2^l})^2=\eta_{2^{l-1}}+2$ and $\varphi_F(2^f)=2$ for $f\geqslant 2$ if $A=\infty$.

LEMMA 3.3. *If $m\in U(F)$, $2^f\|m$ and $f\leqslant A$, then $m\in C(F)$.*

Proof. If $\zeta_4\in F$, then the lemma follows by Lemma 3.2. So we may assume that $\zeta_4\notin F$. Let $m\in U(F)$ and let x^m-a be weakly normal. Then $x^{m'}-b$ is weakly normal, where $x^{m'}-b$ is defined as in (3.1). Furthermore, if β is any root of $x^{m'}-b$, then $F(\zeta_m)\subset F(\beta)$. If $4\nmid m$, then $x^{m'}-b$ is irreducible and the argument of Lemma 3.2 applies. Thus we may assume that $4|m$. Let $m=2^k m_0$, $m'=2^{k_1}m_1$, $l=2^{k_2}m_2=[F(\beta):F(\zeta_m)]$, where $(2,m_i)=1$. Then, $F(\beta^l)=F(\zeta_m)$, by Theorem 1.1. Now, $\varphi_F(m)=2m_1/m_2$ since $x^{m_1}-b$ is irreducible and $f\leqslant A$. Furthermore, by applying Theorem 3.1, we have that if $p|m_1$, then $\zeta_p\in F$, so the Galois group of $F(\zeta_m)$ over F is cyclic. The element $\beta^{2^{k_1}m_2}$ is a root of $x^{m_1/m_2}-b$ and $[F(\beta^{2^{k_1}m_2}):F]=m_1/m_2$. Moreover, $l=2^{k_2}m_2|2^{k_1}m_2$, so $F(\beta^l)=F(\zeta_m)\supset F(\beta^{2^{k_1}m_2})$. However $F(\zeta_m)\supset F(\zeta_{m_0})$ and $[F(\zeta_{m_0}):F]=m_1/m_2$. Since $F(\zeta_m)$ has cyclic Galois group, we have that $F(\zeta_{m_0})=F(\beta^{2^{k_1}m_2})=F(b^{1/(m_1/m_2)})$.

Also, if x^4-b is irreducible, then $F(\zeta_4)=F(b^{1/2})$. If x^4-b is reducible, then $F(\zeta_4)=F(b^{1/2})$, by Lemma 2.2. Thus $F(\zeta_{2^f})=F(\zeta_4)=F(b^{1/2})$, since $f\leqslant A$. Hence $F(\zeta_m)=F(\zeta_{2^f},\zeta_{m_0})=F(b^{1/2}, b^{1/(m_1/m_2)})=F(b^{1/(2m_1/m_2)})$, $x^{2m_1/m_2}-b$ is irreducible and $(2m_1/m_2)|m$. Thus $m\in C(F)$. ■

LEMMA 3.4 (Schinzel [8]). *Let F be such that $\varphi_F(2^f)=2^{f-1}$. If $x^{2^f}-a$ is weakly normal with abelian Galois group and $x^{2^f}-a$ is reducible, then $f\leqslant 2$.*

Proof. Assume that $x^{2^f}-a$ is weakly normal with abelian Galois group but not irreducible normal, and $f\geqslant 3$. Then $a^2=b^{2^f}$, so $a=\pm b^{2^{f-1}}$.

Assume that $a=b^{2^{f-1}}$. Then $a^{1/2^f}=\zeta_{2^f}b^{1/2}$ and $F(a^{1/2^f})=F(\zeta_{2^f}b^{1/2}) = F(\zeta_{2^f})$. Thus $b^{1/2}\in F(\zeta_{2^f})$, hence $b^{1/2}=c\zeta_4$ or $b^{1/2}=c(\pm 2)^{1/2}$. If $b^{1/2}=c\zeta_4$, then $b=-c^2$, so $a=b^{2^f}$, and $x^{2^f}-a=x^{2^f}-b^{2^f}$ is irreducible, a contradiction. If $b^{1/2}=c(\pm 2)^{1/2}$, then $b=\pm 2c^2$, and $a=2^{2^{f-2}}c^{2^f}$, so $2^{1/4}\in F(\zeta_{2^f})$, yet $F(2^{1/4})$ is non-abelian. Thus $a\neq b^{2^{f-1}}$. Hence $a=-b^{2^{f-1}}$. Then $a^{1/2^f}=\zeta_{2^{f+1}}b^{1/2}$ and $F(a^{1/2^f})=F(\zeta_{2^f})$, implies that $\zeta_{2^{f+1}}b^{1/2}\in F(\zeta_{2^f})\subset F(\zeta_{2^{f+1}})$, thus $b^{1/2}\in F(\zeta_{2^{f+1}})$, however, since $f\geqslant 3$, we have that $b^{1/2}\in F(\zeta_{2^f})$, thus $\zeta_{2^{f+1}}\in F(\zeta_{2^f})$, a contradiction. Hence $x^{2^f}-a$ is irreducible. ■

Remark. If char $F>0$, then $\varphi_F(2^f)<2^{f-1}$, for all $f>2$.

LEMMA 3.5. *If F is a field such that $\varphi_F(2^f)=2^{f-1}$, then $U(F)=C(F)$. Let x^m-a be weakly normal and $x^{m'}-b$ defined as in (3.1). Then, $F(\beta)=F(\alpha)$, where $\beta^{m'}=b$, $\alpha^m=a$. Further, if $8|m'$, $x^{m'}-b$ is irreducible normal.*

Proof. Let $m=2^k m_0$, $m'=2^{k_1}m_1$, $(2,m_i)=1$. If $k_1\leqslant 2$, then apply Lemma 3.3. Thus we assume that $k_1\geqslant 3$. Since $x^{m_1}-b$ is irreducible, we have that $m_1|[F(\beta):F]$. Recall that $\varphi_F(2^f)=2^{f-1}$. Thus $2^{k_1-1}|[F(\beta):F]$. Hence, the degree of the splitting field is either $2^{k_1}m_1$ or $2^{k_1-1}m_1$. Assume that $x^{m'}-b$ is reducible, then the degree of the splitting field is $2^{k_1-1}m_1$. Now, β^{m_1} satisfies $x^{2^{k_1}}-b$ and this is reducible, thus $F(\beta^{m_1})=F(\zeta_{2^{k_1}})$. So $x^{2^{k_1}}-b$ has at least one root that yields the splitting field. The other roots of $x^{2^{k_1}}-b$ are $(\zeta^i_{2^{k_1}m_1}\beta)^{m_1}$, since $(m_1,2)=1$. Thus every root of $x^{2^{k_1}}-b$ yields the splitting field since $\zeta^i_{2^{k_1}m_1}\beta$ is a root of $x^{m'}-b$, so $x^{2^{k_1}}-b$ is weakly normal and reducible, and this contradicts Lemma 3.4. Thus $x^{m'}-b$ is irreducible and if β is any root of $x^{m'}-b$, then $F(\beta)=F(\alpha)\supset F(\zeta_m)$. Thus $F(\zeta_m)=F(\beta^l)$, where $l=[F(\beta):F(\zeta_m)]$. Thus $F(\zeta_m)=F(b^{1/(m'/l)})$, $x^{m'/l}-b$ is irreducible and $(m'/l)|m$. Thus $m\in C(F)$ and $U(F)=C(F)$. ■

LEMMA 3.6. *Let* char $F=p$, $p>0$, $p\neq 2$, *and* $\zeta_4\notin F$. *Then there exists an f such that $[F(\zeta_{2^f}):F]=4$ and $F(\zeta_{2^f})\neq F(b^{1/4})$, for all $b\in F$.*

Proof. Let K be a finite field such that $\zeta_4\notin K$ and char $K\neq 2$. We first prove that if $a\in K$, then x^4-a is reducible over K. If $a^{1/2}\in K$, x^4-a is reducible. Thus we may assume that $a^{1/2}\notin K$, and $[K(a^{1/2}):K]=2$. Since $\zeta_4\notin K$, we have that $|K|\not\equiv 1\ (\mathrm{mod}\ 4)$, but then $|K|^2\equiv 1\ (\mathrm{mod}\ 8)$. Thus if b generates the cyclic group $K(a^{1/2})^*$, then 8 divides the order of b. However, the order of $a^{1/2}$ is not divisible by 8, so there exists $c\in K(a^{1/2})$ such that $a^{1/2}=c^2$. Thus c is a root of x^4-a. Hence the splitting field of x^4-a is $K(a^{1/2})$, thus x^4-a is reducible.

Given F, let F' denote the compositum of all the finite fields contained in F. Since $\zeta_4\notin F$, we have that if char $F=p$, then $p\not\equiv 1\ (\mathrm{mod}\ 4)$. Furthermore, if $\mathrm{GF}(p^e)\subset F$, then e must be odd. Let $2^{f-1}\|(p^2-1)$, where $f-1\geqslant 3$. Then $2^{f-1}\|(p^{2e}-1)$, where e is odd. Thus $F(\zeta_4)=F(\zeta_{2^{f-1}})$ and $[F(\zeta_{2^f}):F]=4$.

Assume that $F(\zeta_{2^f}) = F(b^{1/4})$, where x^4-b is irreducible. Then $b \notin F'$. Also $F(\zeta_4) = F(b^{1/2})$, so $b^{1/2} = c\zeta_4$, $c \in F$. Thus $F(b^{1/4}) = F(\zeta_8 c^{1/2}) = F(\zeta_4, c^{1/2})$, since $\zeta_8 \in F(\zeta_4)$. If $F(c^{1/2}) = F(\zeta_4)$, we have a contradiction. Thus $F(c^{1/2}) \neq F(\zeta_4)$, and $\zeta_4 \notin F(c^{1/2})$. Consider $F(c^{1/2})'$. Clearly, $[F(c^{1/2})': F'] \leqslant 2$. If the degree were 2, then $\zeta_4 \in F(c^{1/2})' \subset F(c^{1/2})$, a contradiction. Thus $F(c^{1/2})' = F'$. But then, $[F(c^{1/2}, \zeta_{2^f}): F(c^{1/2})] = 4$, and this contradicts the fact that $F(\zeta_{2^f}) = F(\zeta_4, c^{1/2})$, thus x^4-b is reducible. ∎

THEOREM 3.2. *Let* $\operatorname{char} F \neq 2$. *Then* $U(F) = C(F)$ *iff* (a) $\zeta_4 \in F$ *or* (b) $\zeta_4 \notin F$, $\operatorname{char} F = 0$ *and either* $\varphi_F(2^f) = 2$, *for all* $f \geqslant 2$, *or* $\varphi_F(2^f) = 2^{f-1}$, *for all* $f \geqslant 1$.

Proof. If $\zeta_4 \in F$, then $U(F) = C(F)$, by Lemma 3.2. If $\zeta_4 \notin F$ and $\varphi_F(2^f) = 2$, for $f \geqslant 2$, then Lemma 3.3 applies. If $\varphi_F(2^f) = 2^{f-1}$, for all $f \geqslant 1$, then Lemma 3.5 applies.

Assume that $U(F) = C(F)$ and $\zeta_4 \notin F$. Now, $x^{2^f}+1$ is weakly normal for all $f \geqslant 1$, thus $2^f \in U(F) = C(F)$. Assume that $\operatorname{char} F = p > 0$, $p \neq 2$. Since $\zeta_4 \notin F$, we have that $p \not\equiv 1 \pmod 4$ and if $GF(p^e) \subset F$, then $p^e \not\equiv 1 \pmod 4$, thus e must be odd. So if $2^{f-1} \| (p^2-1)$, then $2^{f-1} \| (p^{2e}-1)$. Thus $[F(\zeta_{2^f}): F] = 4$. Since $2^f \in C(F)$, we have that $F(\zeta_{2^f}) = F(b^{1/4})$, where x^4-b is irreducible, and this contradicts Lemma 3.6. Hence, $\operatorname{char} F = 0$.

If $\varphi_F(2^f) = 2$, for all $f > 1$, then the theorem is proven. Thus we have that $\varphi_F(2^f) = 2$ for $f \leqslant L$ and $\varphi_F(2^{L+i}) = 2^{i+1}$. If $L = 2$, then the theorem is proven. Thus, assume that $L > 2$. Since $2^{L+2} \in C(F)$, we have that $F(\zeta_{2^{L+2}}) = F(b^{1/8})$, x^8-b is irreducible, and the Galois group is Z_2+Z_4. By Theorem 1.1, we have that $F(b^{1/2}) = F(\zeta_4)$. Also $F((\zeta_{2^{L+2}})^4) = F(\zeta_{2^L}) = F(\zeta_4)$. Thus $\zeta_{2^{L+2}}$ and $b^{1/8}$ satisfy irreducible binomials over $F(\zeta_4)$ and $F(b^{1/8})$ over $F(\zeta_4)$ has the unique subfield property, hence, by Lemma 2.3, we have that $\zeta_{2^{L+2}} = \gamma b^{1/8}$, $\gamma \in F(\zeta_4)$. With $o(\alpha)$ defined as in Section 1, we have that $o(\zeta_{2^{L+2}}) = 2^{L+1}$, $o(b^{1/8}) = 8$, thus $o(\gamma) = 2^{L+1}$, thus $\gamma \notin F$. However $\gamma \in F(\zeta_4)$, thus $F(\gamma) = F(\zeta_4)$. So we have that $o(\gamma) = 2^{L+1}$, $F(\gamma)$ is a normal extension of F, hence by Theorem 3 of [6], we have that $\zeta_{2^{L+1}} \in F(\gamma) = F(\zeta_4)$, and this contradicts the fact that $[F(\zeta_{2^{L+1}}): F] = 4$. Thus $L = 2$ and $\varphi_F(2^f) = 2^{f-1}$, and the theorem is proven. ∎

Throughout the rest of this section we shall assume that F is a finite extension of the rationals, that is, an algebraic number field. We shall show that $C(F) = I(F)$ for all algebraic number fields. First we prove a technical lemma.

LEMMA 3.7. *Let F be an algebraic number field, x^r-b irreducible over F and $r|m$. Then there exist infinitely many $c \in F$ such that x^m-bc^r is irreducible over F.*

Proof. Let $\mathscr{P}$ denote the set of all rational, positive primes in Q. We shall show that if $p|m$, then if $B = \{c \in \mathscr{P}: x^p-bc^r \text{ is reducible}\}$, then $|B| < \infty$, and if $4|m$ then $C = \{c \in \mathscr{P}: x^4-bc^r \text{ is reducible}\}$, then $|C| < \infty$. This result clearly implies the lemma.

We first show that $|B| < \infty$. If $p|r$, then $b \neq d^p$, for $d \in F$, since x^p-b is irreducible. Also c^r is a pth power, hence $bc^r \neq d^p$, for all $d \in F$, thus $B = \emptyset$. Assume that $p \nmid r$, then $bc^r = d^p$, for all $c \in B$. Thus $c^{1/p} \in F(b^{1/p})$, since $(r, p) = 1$. Let $L = Q(c^{1/p}: c \in B)$, then $[L:Q] = p^{|B|}$. Since $L \subset F(b^{1/p})$, and $[F(b^{1/p}):Q] < \infty$, we have that $|B| < \infty$.

If $4|r$, then $C = \emptyset$, as above. Let $2|r$, $4 \nmid r$. If $c \in C$, then $-4bc^r = d^4$. Thus $(c^r)^{1/4} \in F((-4b)^{1/4})$, so $c^{1/2} \in F((-4b)^{1/4})$. Hence $|C| < \infty$. If $2 \nmid r$, then the same technique applies. ∎

THEOREM 3.3. *If F is an algebraic number field, then $C(F) = I(F)$.*

Proof. By Lemma 3.1, we have that $C(F) \supset I(F)$.

Let $m \in C(F)$, then $F(\zeta_m) = F(b^{1/r})$, x^r-b is irreducible and $r|m$. By Lemma 3.7, there is a c such that x^m-bc^r is irreducible. Let α be any root of x^m-bc^r, then $\alpha = \zeta_m^i b^{1/m} c^{1/(m/r)}$, hence $\alpha^{m/r} = \zeta_r^i b^{1/r} c$, so $F(\alpha^{m/r}) = F(\zeta_r^i b^{1/r}) = F(\zeta_m)$, since $\zeta_r^i b^{1/r}$ is a root of x^r-b, thus $\zeta_m \in F(\alpha)$, so x^m-bc^r is irreducible normal, hence $m \in I(F)$ and $C(F) = I(F)$. ∎

COROLLARY 3.1. *Let F be an algebraic number field. Then $U(F) = I(F)$ iff* (a) *$\zeta_4 \in F$ or* (b) *if $\zeta_4 \notin F$, then $\varphi_F(2^f) = 2^{f-1}$, for $f \geqslant 1$.*

Proof. This is an immediate consequence of Theorems 3.1 and 3.2. Furthermore, since F is an algebraic number field, then $\varphi_F(2^f) \neq 2$, for some f. ∎

THEOREM 3.4. *Let F be an algebraic number field and x^m-a irreducible over F. Then x^m-a is irreducible normal iff $a = bc^r$, where $F(\zeta_m) = F(b^{1/r})$, and $r|m$.*

Proof. Let x^m-a be irreducible normal, α a root and $r = [F(\zeta_m):F]$, then by Theorem 1.1, we have that $F(\alpha^{m/r}) = F(\zeta_m)$. Let $F(\zeta_m) = F(b^{1/r})$, then by the Corollary to Theorem 3 of [7], we have that $\alpha^{m/r} = c(b^x)^{1/r}$ or $\alpha^{m/r} = c\eta_{2^{A+1}}(b^x)^{1/r}$, where A and η_{2^f} are defined as in (3.2), and $(x, r) = 1$. However, $\eta_{2^{A+1}}(b^x)^{1/r} = ((\eta_{2^A}+2)^{r/2} b^x)^{1/r} = b_1^{1/r}$ and $F(b_1^{1/r}) = F(b^{1/r})$, thus $a = (\alpha^{m/r})^r = c^r b^x$ or $a = c^r b_1^x$. ∎

4. Applications. In this section we shall apply the results of Sections 2 and 3 to determine the weakly and irreducible normal binomials over $F = Q(\zeta_4)$. Of course, if x^m-a is weakly normal, then $\varphi_F(m)|m$. The following lemma is easy to prove:

LEMMA 4.1. *Let $F = Q(\zeta_4)$, then $\varphi_F(m)|m$ iff $m \in \{2^k, 2^{k_1}3^i, 2^{k_2}5^j: k_1 > 0, k_2 > 1, i > 0, j > 0\}$.* ∎

LEMMA 4.2. *If $m \in U(Q(\zeta_4))$, $p|m$, p an odd prime, then $p^2 \nmid m$.*

Proof. By Theorem 3.1, we have that if $p|m$, $\zeta_p \notin F$, then $(\varphi_F(m), p) = 1$. ∎

LEMMA 4.3. *Let $m \in U(Q(\zeta_4))$. If $p|m$, p an odd prime, then $8 \nmid m$.*

Proof. By Theorem 3.2, we have that $U(Q(\zeta_4)) = C(Q(\zeta_4))$. Then, for $m \in C(Q(\zeta_4))$, we have that $Q(\zeta_4, \zeta_m) = Q(\zeta_4, b^{1/r})$, and this has cyclic Galois group, by Theorem 2.2. However, $Q(\zeta_{2^i 3})$, $Q(\zeta_{2^i 5})$ do not have cyclic Galois groups for $i > 2$. ■

Thus, the candidates for $U(Q(\zeta_4))$ are $2^k, 6, 12$, and 20, and in fact $U(Q(\zeta_4)) = \{2^k, 6, 12, 20\colon k \geq 0\}$. We first determine the irreducible binomials which define $Q(\zeta_4, \zeta_m)$, for $m \in C(Q(\zeta_4))$.

THEOREM 4.1. *We have that $C(Q(\zeta_4)) = \{2^k, 6, 12, 20\colon k \geq 0\}$ and,*

(a) *$Q(\zeta_4, \zeta_{2^f})$ is defined by $x^{2^{f-2}} - \zeta_4$,*
(b) *$Q(\zeta_4, \zeta_6) = Q(\zeta_4, \zeta_{12})$ is defined by $x^2 - 3$,*
(c) *$Q(\zeta_4, \zeta_{20})$ is defined by $x^4 - 5(1+2\zeta_4)^2$.*

Furthermore, these binomials are irreducible and essentially unique.

Proof. By essentially unique we mean that if $x^m - a$ is one of (a)–(c), and $x^m - b$ defines the same field as $x^m - a$, then $b = c^m a^x$, $(m, x) = 1$.

(a), (b) are obvious. We now consider (c). Since $Q(\zeta_4, \zeta_5)$ has cyclic Galois group of order 4 over $Q(\zeta_4)$, we have that $Q(\zeta_4, \zeta_5)$ is defined by an irreducible binomial. Thus, if we compute the Lagrange resolvent (see p. 169, [10]), we have that $(\zeta_4, \zeta_5) = \zeta_5 + \zeta_4\zeta_5^2 - \zeta_5^4 - \zeta_4\zeta_5^3$ and $(\zeta_4, \zeta_5)^4 = 5(1+2\zeta_4)^2$. ■

COROLLARY 4.1. *We have that $U(Q(\zeta_4)) = C(Q(\zeta_4)) = I(Q(\zeta_4)) = \{2^k, 6, 12, 20\colon k \geq 0\}$.* ■

THEOREM 4.2. *The irreducible normal binomials over $Q(\zeta_4)$ are:*

(a) $x^2 - c$, $c \neq c_1^2$,
(b) $x^4 - c$, $c \neq c_1^2$,
(c) $x^{2^f} - \zeta_4 c^{2^{f-2}}$, $f \geq 3$, *all* $c \neq 0$,
(d) $x^6 - 3c^2$, $c \neq 3c_1^3$,
(e) $x^{12} - 3c^2$, $c \neq 3c_1^3$,
(f) $x^{20} - 5(1+2\zeta_4)^2 c^4$, $c \neq 5(1+2\zeta_4)^2 c_1^5$.

In (a)–(f) we have suppressed mth powers, that is, if $x^m - a$ is irreducible normal, then $x^m - ab^m$ is also irreducible normal. Furthermore, the Galois groups are cyclic for (a), (b), (c), and non-abelian for (d), (e), (f).

Proof. This follows from Theorems 3.4 and 4.2. It is also important to point out that ζ_4 denotes any primitive 4th root of unity. ■

In order to determine those weakly normal binomials which are not irreducible normal, we shall need the following lemma.

LEMMA 4.4. *Let $F = Q(\zeta_4)$ and let $x^m - a$ be reducible and weakly normal. Then there exist m', b such that $m'|m$, $b^{m/m'} = a$, $x^{m'} - b$ is irreducible normal and $x^{m'} - b | x^m - a$. Further, if $\beta^{m'} = b$, $\alpha^m = a$, then $F(\alpha) = F(\beta)$.*

Proof. We define m' and b as in (3.1), thus $x^{m'} - b$ is weakly normal. By Lemma 3.2, $x^{m'} - b$ is irreducible, thus $x^{m'} - b$ is irreducible normal. ■

Thus, if $x^m - a$ is reducible and weakly normal, then $x^m - a$ has a binomial factor which is irreducible normal.

THEOREM 4.3. *Let $x^m - a$ be reducible and weakly normal and let $D = [F(\alpha)\colon F]$, where $F = Q(\zeta_4)$, $\alpha^m = a$. Then $x^m - a$ must be one of the following:*

(1) $x^2 - c^2$, $D = 1$.
(2) $x^4 - c^{D/4}$, $D = 1$ *or* 2, $c \neq c_1^2$ *if* $D = 2$.
(3) $x^{2^k} + c^{2^{k-1}}$, $D = 2^{k-1}$.
(4) $x^6 - (3c^2)^3$, $D = 2$.
(5) $x^{12} - (3c^2)^{12/D}$, $D = 2, 4$, *or* 6 *and, if* $D = 6$, *then* $c \neq 3c_1^3$.
(6) $x^{20} - (5(1+2\zeta_4)^2 c^4)^5$, $D = 4$.

Proof. The first two are obvious. So let $m = 2^k$, $k > 2$. If α is any root of $x^{2^k} - a$, then $F(\zeta_{2^k}) \subset F(\alpha)$, thus $2^{k-2}|D$, so $D = 2^{k-1}$ or $D = 2^{k-2}$. Assume that $D = 2^{k-2}$. Then $a = b^4$, $a \neq b_1^8$, for all $b_1 \in F$, and $x^{2^{k-2}} - b$ is irreducible normal. Thus $F(b^{1/2^{k-2}}) = F(\zeta_{2^k})$, thus by Lemma 2.3, we have that $b^{1/2^{k-2}} = c\zeta_{2^k}$, so $b = c^{2^{k-2}}\zeta_4$, $a = b^4 = c^{2^k}$ and this contradicts the fact that $a \neq b_1^8$, for all $b_1 \in F$. Thus, we must have $D = 2^{k-1}$. Hence $a = b^2$, $x^{2^{k-1}} - b$ is irreducible. Thus $F(b^{1/2^{k-2}}) = F(\zeta_{2^k})$, so $b^{1/2^{k-2}} = c\zeta_{2^k}$, $b = c^{2^{k-2}}\zeta_4$, $a = b^2 = -c^{2^{k-1}}$.

Let us now consider (4). If $\alpha^6 = a$, then $F(\zeta_6) \subset F(\alpha)$. Thus $2|D$. However, $D < 6$, since $x^6 - a$ is reducible, so $D = 2$. Thus $a = b^3$ and $b^{1/2} \notin F$. Further $F(b^{1/2}) = F(\zeta_6) = F(3^{1/2})$, so $b = 3c^2$.

Let $x^{12} - a$ be reducible and weakly normal, $D = [F(\alpha)\colon F]$, then $D = 2, 4$, or 6. Thus $a = b^{12/D}$, $x^D - b$ is irreducible normal, and $F(b^{1/2}) = F(\zeta_{12}) = F(3^{1/2})$, so $b = 3c^2$, thus $a = (3c^2)^{12/D}$. If $D = 2$ or 4, $x^D - 3c^2$ is irreducible. If $D = 6$, then $x^6 - 3c^2$ is irreducible if $c \neq 3c_1^3$.

Let $x^{20} - a$ be reducible and weakly normal, then $F(\zeta_{20}) \subset F(\alpha)$, so $4|D$. But $D < 20$, so $D = 4$. Thus $a = b^5$, $x^4 - b$ is irreducible and $F(b^{1/4}) = F(\zeta_{20})$, thus $b = 5(1+2\zeta_4)^2 c^4$. ■

References

[1] Giulio Darbi, *Sulla Riducibilità delle Equazioni Algebriche*, Annali di Mat. pura e appl., Ser. 4, 4 (1926), pp. 185–208.

[2] László Fuchs, *Infinite Abelian groups*, Academic Press, New York and London 1970.

[3] David Gay, *On normal radical extensions of real fields*, Acta Arith. 35 (1979), pp. 273–288.

[4] Irving Kaplansky, *Fields and rings*, The University of Chicago Press, Chicago and London 1972.

[5] Henry B. Mann and William Yslas Vélez, *On normal radical extensions of the rationals*, Linear and Multilinear Algebra 3 (1975), pp. 73–80.

[6] Michael J. Norris and William Yslas Vélez, *Structure theorems for radical extensions of fields*, to appear in Acta Arith.

[7] A. Schinzel, *On linear dependence of roots*, Acta Arith. 28 (1975), pp. 161–175.
[8] — *Abelian binomials, power residues, and exponential congruences*, ibid. 32 (1977), pp. 245–274.
[9] N. G. Tschebotarëw, *Grundzüge der Galois'schen Theorie*, Groningen-Djakarta, 1950.
[10] B. L. van der Waerden, *Modern algebra*, Vol. 1, Frederick Ungar Publishing Co., New York 1966.

APPLIED MATHEMATICS GROUP
SANDIA LABORATORIES
Albuquerque, New Mexico, U.S.A.

Received on 1. 3. 1977
and in revised form on 9. 7. 1977 (917)

ACTA ARITHMETICA
XXXVI (1980)

On sums of powers and a related problem

by

K. Thanigasalam (Monaca, Penn.)

1. Introduction. K. F. Roth [6] showed that all sufficiently large integers N are representable in the form

$$N = \sum_{s=1}^{50} x_s^{s+1} \quad (x\text{'s being non-negative integers}). \tag{1}$$

In [7], I improved this to $N = \sum_{s=1}^{35} x_s^{s+1}$.

R. C. Vaughan [10] and [11] improved on this further, showing that

$$N = \sum_{s=1}^{26} x_s^{s+1}. \tag{2}$$

Torleiv Kløve [9] found by computations for $N \leqslant 250\,000$ that $N = \sum_{s=1}^{6} x_s^{s+1}$ (for $N \leqslant 250\,000$), and conjectured that for large N, $N = \sum_{s=1}^{4} x_s^{s+1}$.

In this paper, we improve further on (2), and prove the following:

Theorem 1. *All sufficiently large integers N are representable in the form*

$$N = \sum_{s=1}^{22} x_s^{s+1} \tag{3}$$

where the x's are non-negative integers.

The methods used in [6], [7], [10] or [11] are insufficient to prove (3), and so, we indicate all the necessary changes.

The method in this paper, can also be used to prove

Theorem 2. *All sufficiently large odd integers N_1, and even integers N_2 are representable in the forms*

$$N_1 = \sum_{s=1}^{23} p_s^{s+1}, \quad N_2 = \sum_{s=1}^{24} p_s^{s+1}, \tag{4}$$

where the p's are primes.