[7] G. L. Mullen, *Equivalence classes of functions over a finite field*, Acta Arith. 29 (1976), pp. 353–358.
[8] — *Equivalence classes of polynomials over finite fields*, ibid. 31 (1976), pp. 113–123.
[9] — *Permutation polynomials in several variables over finite fields*, ibid. 31 (1976), pp. 107–111.
[10] H. Niederreiter, *Permutation polynomials in several variables over finite fields*, Proc. Japan Acad. 46 (1970), pp. 1001–1005.
[11] — *Permutation polynomials in several variables*, Acta Sci. Math. (Szeged), 33 (1972), pp. 53–58.
[12] W. Nöbauer, *Zur theorie der polynomtransformationen und permutationspolynome*, Math. Ann. 157 (1964), pp. 332–342.

Received on 24. 8. 1976 (871)

ACTA ARITHMETICA
XXXV (1979)

On normal radical extensions of real fields

by

DAVID GAY* (Geneva)

In 1926 Darbi [1] and Bessel-Hagen (see [8], p. 302) found all normal binomials $x^m - a$ over the rationals Q. Here is their list:

L_1: $x^2 - c$ $(c \neq c_1^2)$; $x^4 + c^2$ $(c \neq 2c_1^2)$; $x^{2^k} + c^{2^{k-1}}$ $(k \geqslant 3)$; $x^{2^k} + 2^{2^{k-2}} c^{2^{k-1}}$ $(k \geqslant 4)$; $x^6 + 3c^2$ $(c \neq 3c_1^3)$; $x^{12} + 36c^4$ $(c \neq 6c_1^3)$

(In all cases above, it is understood that $c, c_1 \in Q$.) In 1975 Mann and Vélez [5] considered the problem of determining all binomials $x^m - a$ over Q with the property that $Q(\alpha)$ is the splitting field for all roots α of $x^m - a$. We call such binomials *weakly normal*. They obtained a complete list of weakly normal binomials over Q which, of course, includes the irreducible binomials above as well as the following reducible ones:

L_2: $x^2 - c^2$; $x^4 + 4c^4$; $x^6 + 27c^6$; $x^{12} + (36c^4)^3$.

More recently, Norris and Vélez [6] have shown that the normal binomials over a field K play a central rôle in the general structure theory of all radical extensions of K.

The purpose of this paper is to determine all weakly normal (including normal) binomials over an arbitrary real field. Our main results are contained in Section 4 (in particular, Theorems 4.1 and 4.4) where we obtain binomials as explicit as those on the lists above. In Section 1 we present some general results about weakly normal binomials forming a point of departure for our study. Section 2 is devoted to finding explicit (and convenient for our purposes) generators for, and Galois groups of, certain cyclotomic fields. In Section 3, we use these technical results to obtain a precise framework for weakly normal binomials enabling us to complete

* The author was jointly supported by Fonds National Suisse de la Recherche Scientifique and Battelle Institute Grant No. 333-205.

our investigations in Section 4. We conclude the paper in Section 5 with detailed examples and applications.

I am indebted to Henry Mann for suggesting that the lists L_1 and L_2 above might be generalized nicely to real fields.

1. Weakly normal binomials. We begin with some definitions and notation. A polynomial $p(x)$ over a field K is *normal* over K if $p(x)$ is irreducible and $K(a)$ is the splitting field for every root a of $p(x)$. A binomial $q(x)$ is *weakly normal* (w.n.) over K if $K(a)$ is the splitting field of $q(x)$ for every root a of $q(x)$.

If K is a field extension of F, then we denote by $[K:F]$ the degree of the extension and by $G(K/F)$ the Galois group if K happens to be normal and separable over F. We denote by ζ_n a primitive nth root of unity. We assume all fields are of characteristic 0.

It is clear that a binomial x^n+a over a field K is weakly normal iff $\zeta_n \in K(a)$ for every root a of x^n+a. If x^n+a is weakly normal with root a, let $s = [K(a):K(\zeta_n)]$ and call s the *parameter* of x^n+a. The significance of s is found in the following

PROPOSITION 1.1. *If x^n+a is weakly normal over K with parameter s, then for any root a*

(1) *s is the smallest integer such that $a^s \in K(\zeta_n)$,*

(2) *$K(a^s) = K(\zeta_n)$.*

Furthermore, $s\cdot[K(\zeta_n):K] | n$; in particular $s|n$.

Proof. Statements (1) and (2) are essentially Proposition 2.1 of [2]. The final statement is Lemma 2 of [5]. ∎

From now on, we consider binomials x^n+a over a real field R by which we mean a subfield of the real algebraic numbers. If $a \in R$ and $a > 0$, then $\sqrt[n]{a}$ will always mean a real nth root. The following eliminates some special cases.

PROPOSITION 1.2. *Suppose x^n+a weakly normal over R. If $a < 0$, then $n = 1$ or 2. If n is odd, then $n = 1$. Furthermore, x^2+a is weakly normal for any $a \in R$.*

Proof. If $a < 0$, then $\sqrt[n]{-a}$ generates the splitting field of x^n+a. But the splitting field, containing ζ_n, can be real iff $n = 1$ or 2.

Similarly, if n is odd and $a > 0$, then $-\sqrt[n]{a}$ is a root that generates the splitting field. This can happen iff $n = 1$. ∎

In view of this proposition, we shall limit ourselves in what follows to x^n+a with $a > 0$, n even, $n > 2$.

LEMMA 1.3. *If $a > 0$ and $\sqrt[n]{a}$ (real) $\in R(\zeta_m)$ for positive integers n, m $(m > 2)$, then $\sqrt[n]{a} = \sqrt{b}$ for some $b \in R$, $b > 0$.*

Proof. This is Lemma 1 of [5]. ∎

PROPOSITION 1.4. *Let x^n+a be weakly normal over R with $n = 2^{k+j}m$ $(m$ odd$)$ and parameter $s = 2^j m_0$ $(m_0|m)$. Then*

(a) *there is a root β of x^n+a such that $\beta^s = \zeta_{2^{k+1}}\sqrt{b}$ for some $b \in R$, $b > 0$;*

(b) *$[R(\zeta_n):R(\zeta_{2^k})] \leqslant 2$ and $[R(\zeta_n):R] = 2^q$ for some $q \geqslant 1$;*

(c) *$k \geqslant 1$.*

Proof. Suppose x^n+a is weakly normal with parameter s. Then $\beta = \zeta_{2^{k+j+1}}\sqrt[n]{a}$ is a root and $\beta^s = \zeta_{2^{k+1}}(\sqrt[n]{a})^s$. By 1.1, $R(\beta^s) = R(\zeta_n)$ and consequently $(\sqrt[n]{a})^s \in R(\zeta_{2^n})$. By the lemma, $(\sqrt[n]{a})^s = \sqrt{b}$. This proves (a).

To prove (b), note that $\beta^{2s} = b\zeta_{2^k}$ and thus $R(\beta^{2s}) = R(\zeta_{2^k})$. Hence $[R(\zeta_n):R(\zeta_{2^k})] \leqslant 2$. Since $[R(\zeta_{2^k}):R]$ is a power of 2, so is $[R(\zeta_n):R]$.

Finally, if $k = 0$, then β^s is real and generates $R(\zeta_n)$. This is impossible if $n > 2$. Thus $k \geqslant 1$. ∎

COROLLARY 1.5. *If x^n+a is weakly normal over R and K is the maximal extension of the rationals Q such that $K \subseteq Q(\zeta_n)$ and $[K:Q]$ is odd, then $K \subseteq R$.*

COROLLARY 1.6. *Let x^n+a be weakly normal with parameter s and k, j, m, m_0 as in 1.4. Then x^n+a is irreducible iff $m_0 = m$ and $[R(\zeta_n):R] = 2^k$.*

Proof. The binomial x^n+a is irreducible iff for every root $[R(a):R] = n$. But $[R(a):R] = s\cdot[R(\zeta_n):R] = 2^j m_0 \cdot 2^q$ (by 1.4). Thus $m_0 = m$ and $q = k$. ∎

2. Generators of cyclotomic fields and square roots. In this section we will develop some rather explicit information about certain subfields of $R(\zeta_n)$. In some instances we determine formulas for generators of these subfields; in other instances we pin-point exactly where $\sqrt{b}$ $(b > 0, b \in R)$ can lie. Many of the items in this section are well-known; others may be new. We have made no attempt to separate the two.

As before, we denote by ζ_n a primitive nth root of unity. Let $\eta_n = \zeta_n + \zeta_n^{-1}$ and $\xi_n = 4-\eta_n^2$. Thus ζ_n is a root of $x^2-\eta_n x+1 = 0$ and we have

LEMMA 2.1. (a) *η_n is real and, if $n > 2$, $|\eta_n| < 2$ and $\xi_n > 0$.*

(b) $\zeta_n = (\eta_n \pm i\sqrt{\xi_n})/2$.

(c) *$R(\eta_n)$ is the maximal real subfield of $R(\zeta_n)$.*

(d) *$R(\zeta_{nm}) = R(\zeta_n, \zeta_m)$ if $(n, m) = 1$.*

(e) *$R(\zeta_n) = R(i\sqrt{\xi_n})$, n odd.*

(f) *$R(\zeta_{2^k}) = R(i, \eta_{2^k})$, $k \geqslant 2$.*

(g) *$R(\zeta_{2^k m}) = R(i, \eta_{2^k}, \sqrt{\xi_m})$, $k \geqslant 2$, m odd.*

Proof. Parts (a), (b), (d) and (f) are easy. Part (c) follows from the facts that $R(\eta_n)$ is real and ζ_n satisfies a quadratic over $R(\eta_n)$.

To prove part (e), note that $R(\zeta_n) = R(\eta_n, i\sqrt{\xi_n})$ from (b) and (c). We will have finished if we can show $\eta_n \in R(i\sqrt{\xi_n})$. However, $\xi_n \in R(i\sqrt{\xi_n})$ and $\xi_n = 4-\eta_n^2 = 4-(\zeta_n+\zeta_n^{-1})^2 = 2-(\zeta_n^2+\zeta_n^{-2})$. But n odd implies that ζ_n, ζ_n^2 are conjugate and, therefore, η_n and $\zeta_n^2+\zeta_n^{-2}$ are conjugate. Thus $\eta_n \in R(i\sqrt{\xi_n})$.

Part (g) follows from (d), (e) and (f):

$$R(\zeta_{2^k m}) = R(\zeta_{2^k}, \zeta_m) = R(i, \eta_{2^k}, i\sqrt{\xi_m}). \blacksquare$$

LEMMA 2.2. *With respect to the particular choices*

$$\zeta_{2^k} = \exp(2\pi i/2^k), \quad \text{for all } k \geqslant 1,$$

we have

$$\zeta_{2^{k+1}}^2 = \zeta_{2^k} \quad (k \geqslant 1)$$

and

(a) $\eta_{2^{k+1}} = \sqrt{\eta_{2^k}+2}$ *for all* $k \geqslant 1$; $\eta_2 = -2$;

(b) $\xi_{2^{k+1}} = 4-\eta_{2^{k+1}}^2 = 2-\eta_{2^k} = (\eta_{2^k}+2)\xi_{2^{k+1}}^2\xi_{2^k}^{-1}$ $(k \geqslant 2)$; *in particular,* $\xi_{2^{k+1}} = (\eta_{2^k}+2)r^2$ *where* $r \in Q(\eta_{2^k})$;

(c) $\zeta_{2^{k+1}} = \eta_{2^{k+1}}(1+ri)/2$ *where* $r \in Q(\eta_{2^k})$.

Proof. (a) We have $\eta_{2^{k+1}}^2 = \zeta_{2^{k+1}}^2+\zeta_{2^{k+1}}^{-2}+2 = \zeta_{2^k}+\zeta_{2^k}^{-1}+2 = \eta_{2^k}+2$. Thus $\eta_{2^{k+1}} = \sqrt{\eta_{2^k}+2}$.

(b) By (a), $\xi_{2^{k+1}} = 2-\eta_{2^k}$. Furthermore,

$$\xi_{2^{k+1}}/\eta_{2^{k+1}}^2 = (2-\eta_{2^k})/(2+\eta_{2^k}) = (2-\eta_{2^k})^2/(4-\eta_{2^k}^2) = \xi_{2^{k+1}}^2/\eta_{2^k}.$$

To prove the second part of (b), it is sufficient to show that ξ_{2^k} is a square in $Q(\eta_{2^k})$. We do this by induction on k. If $k = 2$, then $\xi_4 = 4$. Assume true for n so that $\xi_{2^n} = s^2$, $s \in Q(\eta_{2^n})$ and $\xi_{2^{n+1}} = \eta_{2^{n+1}}^2\xi_{2^{n+1}}^2 s^{-2}$ = square in $Q(\eta_{2^{n+1}})$, since $\eta_{2^{n+1}}, \xi_{2^{n+1}} \in Q(\eta_{2^{n+1}})$.

(c) Finally, $\zeta_{2^{k+1}} = (\eta_{2^{k+1}} \pm i\sqrt{\xi_{2^{k+1}}})/2$ (by 2.1 (b)) $= \eta_{2^{k+1}}(1+ri)/2$ (by (a) and (b) above). $\blacksquare$

COROLLARY 2.3. *If* $c, b, r \in R(\eta_{2^k})$ *and* $(\eta_{2^k}+2)b = r^2c$, *then there exists* $s \in R(\eta_{2^k})$ *such that* $b = s^2(\eta_{2^k}+2)c$.

Proof. Let $s = r\xi_{2^{k+1}}\xi_{2^k}^{-1}$ and use 2.2 (b). $\blacksquare$

LEMMA 2.4. *Let* K *be a field with* $a, b \in K$. *If* $K(\sqrt{a}) = K(\sqrt{b})$, *then* $a = k^2b$ *for some* $k \in K$.

Proof. Well-known and easy. $\blacksquare$

LEMMA 2.5. *Let* R *be a real field such that* $\eta_{2^A} \in R$ *but* $\eta_{2^{A+1}} \notin R$. *Then*

(a) $R(\eta_{2^{A+q}})$ *is cyclic of degree* 2^q *over* R;

(b) *if* $R(\eta_{2^p}) = R(\eta_{2^q})$, *then either* $p = q$ *or* $p, q \leqslant A$;

(c) *if* $b \in R$, $b > 0$, $\sqrt{b} \in R(\eta_{2^{q+1}})$ *and* $\sqrt{b} \notin R(\eta_{2^q})$, *then* $q = A$ *and* $b = r^2(\eta_{2^A}+2)$ *for some* $r \in R$.

Proof. (a) $Q(\eta_{2^{A+q}})$ is cyclic of degree 2^q over $Q(\eta_{2^A})$. Furthermore, if $S = R \cap Q(\eta_{2^{A+q}})$, then $S = Q(\eta_{2^A})$. For certainly $Q(\eta_{2^A}) \subseteq S$ and, if $S \neq Q(\eta_{2^A})$, then $S = Q(\eta_{2^{A+l}})$ (for some l with $q \geqslant l \geqslant 1$) since $Q(\eta_{2^{A+q}})$ is cyclic over $Q(\eta_{2^A})$. But this implies $\eta_{2^{A+l}} \in R$, a contradiction. Thus $S = Q(\eta_{2^A})$ and (a) follows by a translation argument ([4], p. 19).

(b) If $p > q$ and $p > A$, then by (a) $R(\eta_{2^p})$ is cyclic of degree 2^{p-A} and $R(\eta_{2^q})$ is cyclic of lower degree.

(c) If $\sqrt{b} \in R(\eta_{2^{q+1}})$, $\notin R(\eta_{2^q})$, then $q \geqslant A$. However, since $R(\eta_{2^{q+1}})$ is cyclic over R of degree 2^{q+1-A}, $R(\eta_{2^{A+1}})$ is the unique quadratic extension of R contained in $R(\eta_{2^{q+1}})$. Since $R(\sqrt{b})$ is also a quadratic extension of R contained in $R(\eta_{2^{q+1}})$, $R(\sqrt{b}) = R(\eta_{2^{A+1}})$. Thus $q = A$ and $b = r^2(\eta_{2^A}+2)$ for some $r \in R$ by Lemmas 2.2 (a) and 2.4. $\blacksquare$

LEMMA 2.6. *If* $r, b \in R$, $r \neq 0$, $b > 0$, *then* $R\big((1+ri)\sqrt{b}\big) = R(i, \sqrt{b})$.

Proof. First, $[(1+ri)\sqrt{b}]^2 = b(1-r^2+2ri)$. Then $i \in R\big((1+ri)\sqrt{b}\big)$ and thus $R\big((1+ri)\sqrt{b}\big) = R\big(i, (1+ri)\sqrt{b}\big) = R(i, \sqrt{b})$. $\blacksquare$

LEMMA 2.7. *Let* m *be an odd integer,* $b \in R$ $(b > 0)$ *and* $F = R(\zeta_{2^l m}\sqrt{b})$. *Then* F *is an abelian extension of* R *and*

$$F = R(\zeta_m, \zeta_{2^l}\sqrt{b}) = \begin{cases} R(i, \eta_{2^l}\sqrt{b}, \sqrt{\xi_m}) & l > 2, \\ R(i\sqrt{b}, i\sqrt{\xi_m}), & l = 2, \\ R(\zeta_m, \sqrt{b}), & l = 0 \text{ or } 1. \end{cases}$$

Proof. Since $R(\zeta_{2^l m})$ and $R(\sqrt{b})$ are abelian extensions, so is $R(\zeta_{2^l m}, \sqrt{b})$. Thus F, a subfield of the latter, is also abelian.

To complete the proof, let $\beta = \zeta_{2^l m}\sqrt{b}$. Then $R(\beta^{2^l}) = R(\zeta_m)$ if $l \geqslant 1$ and $R(\beta^2) = R(\zeta_m)$ if $l = 0$. In any case $\zeta_m \in F$ so that $F = R(\zeta_m, \zeta_{2^l}\zeta_m\sqrt{b})$ $= R(\zeta_m, \zeta_{2^l}\sqrt{b})$. The rest is obvious by Lemma 2.1 (e) in case $l \leqslant 2$. If $l > 2$, then $\zeta_{2^{l-1}} \in F$ and $F = R(\zeta_m, \zeta_{2^l}\sqrt{b}) = R\big(i\sqrt{\xi_m}, i, \eta_{2^l}(1+ri)\sqrt{b}, \eta_{2^{l-1}}\big)$ for some $r \in R(\eta_{2^{l-1}})$ by 2.1 (g) and 2.2 (c). Thus $F = R(i, \sqrt{\xi_m}, \eta_{2^l}\sqrt{b})$ by Lemma 2.6. $\blacksquare$

Remark. In case $\zeta_n = \exp(2\pi i/n)$, $\eta_n = 2\cos(2\pi/n)$ and $\sqrt{\xi_n}$ $= 2\sin(2\pi/n)$.

3. Necessary and sufficient conditions on weak normality; associated binomials. In this section we will offer applications of some of the lemmas of §2 to the study of weakly normal binomials. Recall that in Proposition 1.4 we showed if $x^{2^{k+j}m}+a$ is weakly normal over R with parameter $s=2^j m_0$, then the binomial has a root β with $\beta^s=\zeta_{2^{k+1}}\sqrt{b}$ for some positive $b\in R$. Furthermore, by Proposition 1.1, $R(\beta^s)=R(\zeta_{2^{k+j_m}})$. Thus $R(\zeta_{2^{k+1}}\sqrt{b})=R(\zeta_{2^{k+j_m}})$. The following gives necessary and sufficient conditions for when this latter equation can hold.

PROPOSITION 3.1. *Let $b\in R$, $b>0$, $k,j,m\in\mathbf{Z}$ with $k\geqslant 1$, $j\geqslant 0$ and m odd. Then $R(\zeta_{2^{k+1}}\sqrt{b})=R(\zeta_{2^{k+j_m}})$ iff one of the following holds:*

(a) *$k\geqslant 2$ and $R(\eta_{2^{k+1}}\sqrt{b})=R(\eta_{2^{k+j}},\sqrt{\xi_m})$;*

(b) *$k=1$, $j=0$ and $R(\sqrt{b})=R(\sqrt{\xi_m})$, $m>1$;*

(c) *$k=1$, $j\geqslant 1$ and $\sqrt{\xi_m},\sqrt{b}\in R$.*

Proof. On the one hand, by Lemma 2.1 (e) and (g),

$$R(\zeta_{2^{k+j_m}})=\begin{cases}R(i,\eta_{2^{k+j}},\sqrt{\xi_m}), & k+j\geqslant 2,\\ R(i\sqrt{\xi_m}), & k+j=1,\ m>1.\end{cases}$$

On the other hand, by Lemma 2.7,

$$R(\zeta_{2^{k+1}}\sqrt{b})=\begin{cases}R(i,\eta_{2^{k+1}}\sqrt{b}), & k\geqslant 2,\\ R(i\sqrt{b}), & k=1.\end{cases}$$

The proposition follows by comparing maximal real subfields in case $k\geqslant 2$, using Lemma 2.4 in case $k=1$, $j=0$, and doing both in case $k=1$, $j\geqslant 1$. ∎

The following is an analogue to Capelli's Theorem (for irreducible binomials) for weakly normal binomials with parameter s. It and the Corollary which follows will enable us to reduce, in part, questions of weak normality and irreducibility for $x^{2^l m}+a$ to those for $x^{2^l}+a$.

PROPOSITION 3.2. *The binomial $p(x)=x^{2^{k+j}m}+a$ is weakly normal with parameter $s=2^j m_0$ and with $\varepsilon=[R(\zeta_{2^{k+j_m}}):R(\zeta_{2^{k+j}})]$ (Proposition 1.4 says $\varepsilon=1$ or 2) iff $a=b^{2^{k-1}m/m_0}$ ($b\in R$, $b>0$) b is not a q-th power for any $q|m_0$ ($q>1$) and $q(x)=x^{2^{k-1}}+b^{2^{k-1}}$ is weakly normal with parameter $s_1=\varepsilon 2^j$ such that for any root β of $q(x)$, $R(\beta^{2^j})=R(\zeta_{2^{k+j_m}})$.* (We call $p(x)$, $q(x)$ *associated* binomials.)

Proof. ($\Rightarrow$) By Proposition 1.4, there is a root a of $p(x)$ such that $a^s=\zeta_{2^{k+1}}\sqrt{b}$ for some positive $b\in R$. Thus $a=b^{2^{k-1}m/m_0}$. It is clear that b cannot be a qth power for any $q|m_0$ otherwise the odd part of s would be smaller, contradicting Proposition 1.1 (1). Now if β is a root of $q(x)$, then $\beta=\zeta_{2^{k+j+1}}^h\sqrt[2^{j+1}]{b}$, for some odd h. Also, $\beta^{2^j}=\zeta_{2^{k+1}}^h\sqrt{b}$ generates $R(\zeta_{2^{k+j_m}})$ over R. Thus β^{2^j} or $\beta^{\varepsilon 2^j}$ generates $R(\zeta_{2^{k+j}})$ and hence $q(x)$ is weakly normal. Consider a special root γ of $q(x)$ with $\gamma^{2^j}=\zeta_{2^{k+1}}\sqrt{b}$. If $\varepsilon=2$, then clearly $R(\zeta_{2^k})=R(\zeta_{2^{k+j}})=R(\gamma^{2^{j+1}})$ and thus $s_1=2^{j+1}$. If $\varepsilon=1$, then $s_1=2^g$ for some $g\leqslant j$ and $\gamma^{2^g}=\alpha^{2^g m_0}$. Also $R(\gamma^{2^g})=R(\zeta_{2^{k+j}})=R(\zeta_{2^{k+j_m}})$. Thus $g=j$.

($\Leftarrow$) Let δ be a root of $p(x)$. Then $\delta^{2^j m_0}=\zeta_{2^{k+1}}^{h_1}\zeta_{m/m_0}^{h_2}\sqrt{b}$ for h_1 odd. Furthermore, by Lemma 2.7,

$$\begin{aligned}R(\delta^{2^j m_0}) &= R(\zeta_{m/m_0}^{h_2},\zeta_{2^{k+1}}^{h_1}\sqrt{b})\\ &= R(\zeta_{m/m_0}^{h_2},\beta^{2^j}), \quad \text{for some root } \beta \text{ of } q(x)\\ &= R(\zeta_{2^{k+j_m}}).\end{aligned}$$

Thus $p(x)$ is weakly normal with parameter s_2, say. It is clear that $s_2=2^h m_0$ for some $h\leqslant j$ since b is not a qth power for any $q|m_0$, $q>1$. For ease, let α be a root of $p(x)$ such that $\alpha^{2^j m_0}=\zeta_{2^{k+1}}\sqrt{b}=\gamma^{2^j}$ for some root γ of $q(x)$. Then it is easy to see that $\alpha^{2^h m_0}=\gamma^{2^h}$ and thus $R(\gamma^{2^h})=R(\zeta_{2^{k+j_m}})$. It follows that $h=j$. ∎

COROLLARY 3.3. *Let $p(x)=x^{2^{k+j}m}+a$ be weakly normal and $q(x)=x^{2^{k+j}}+c$ the associated weakly normal binomial of Proposition 3.2. Then $p(x)$ is irreducible iff $m_0=m$ and $q(x)$ is irreducible.*

Proof. This follows from Capelli's Theorem ([3], p. 60f) and the proposition. ∎

In view of Propositions 3.1 and 3.2 and Corollary 3.3, our future program should be clear:

Determine which binomials $x^{2^l}+c$ are weakly normal over R and which are normal over R.

Find necessary and sufficient conditions on R and b so that, in case $k\geqslant 2$, $R(\eta_{2^{k+1}}\sqrt{b})=R(\eta_{2^{k+j}},\sqrt{\xi_m})$.

In the next section we will carry out this program.

4. Classification of weakly normal binomials. Let A be a positive integer such that $\eta_{2^A}\in R$ but $\eta_{2^{A+1}}\notin R$, if such exists; otherwise let $A=\infty$.

THEOREM 4.1. *A binomial $x^{2^h}+a$ is weakly normal over R iff for some $r\in R$ it is one of the following:*

1. x^2-r;
2. $x^{2^h}+r^{2^h}$, $h\leqslant A$;
3. $x^{2^{A+1}}+r^{2^g}(\eta_{2^A}+2)^{2^{g-1}}$, $2\leqslant g<A$;
4. $x^{2^h}+r^{2^{h-1}}$, $h\geqslant A+1$;
5. $x^{2^h}+r^{2^{h-1}}(\eta_{2^A}+2)^{2^{h-2}}$, $h>A+1$.

Those weakly normal binomials are also irreducible.

(a) *For all* A:
x^2-r, $\sqrt{r} \notin R$.

(b) *For* $A=2$:
x^4+r^2, $|r| \neq 2r_1^2$,
$x^{2^h}+r^{2^{h-1}}$, $h \geqslant 3$,
$x^{2^h}+r^{2^{h-1}}2^{2^{h-2}}$, $h \geqslant 4$.

(c) *For* $A \geqslant 3$:
$x^{2^h}+r^2$, $\sqrt{|r|} \notin R$, $A \geqslant h > 1$,
$x^{2^{A+1}}+r^4(\eta_{2^A}+2)^2$.

Proof. We use a theorem of Schinzel ([7], Theorem 1) concerning binomials which are products of normal factors. It follows directly from that theorem that a binomial $x^{2^h}+a$ over a real field R is a product of normal factors iff it satisfies one of the following for suitable integer q and $r \in R$:

(i) $a^2 = r^{2^h}$,
(ii) $a = r^2$, $h \leqslant A$,
(iii) $a = (\eta_{2^A}+2)^{2^{2q-1}} r^{2q}$, $h = A+1$, $2 \leqslant q < A$,
(iv) $a = (\eta_{2^A}+2)^{2^{h-2}} r^{2^{h-1}}$, $h > A+1$.

A weakly normal binomial must correspond to one of the binomials on this list. It is not difficult to see that (ii), (iii), (iv) correspond to 2, 3, 5 (respectively) of our theorem and to show that these are indeed weakly normal. (See also remark preceding Lemma 5 in [7].)

It remains to consider a binomial satisfying (i). If $h = 1$, then we obtain our case 1 which is clearly weakly normal. Now suppose $h > 1$ and $a^2 = r^{2^h}$. Then $a = \pm r^{2^{h-1}}$. In order that $x^{2^h}+a$ be weakly normal, $a = +r^{2^{h-1}}$ (by 1.2). If a is a root of $x^{2^h}+r^{2^{h-1}}$, then $a = \zeta_{2^h} \sqrt{|r|}$ and $R(a^2) = R(\zeta_{2^h})$. Thus this binomial is weakly normal and corresponds to our cases 2 and 4.

The list of normal binomials follows from Capelli's theorem ([3], p. 60) and the list of weakly normal binomials above. ∎

Remark. Notice that the list of normal binomials for $A = 2$ is exactly the same as L_1. Note also that the list of normal binomials for $A \geqslant 3$ is quite small compared with that for $A = 2$.

As we promised at the end of §3, we next determine necessary and sufficient conditions on b and R so that in case $k \geqslant 2$, $j \geqslant 0$ $R(\eta_{2^{k+1}}\sqrt{b}) = R(\eta_{2^{k+j}}, \sqrt{\xi_m})$ (m odd, $m > 1$). Part of this is accomplished in the next two propositions; the rest is done in the proof of the classification theorem that follows.

Proposition 4.2. *Suppose* $k \geqslant 2$ *and* $k+j \leqslant A$. *Then*

$$R(\eta_{2^{k+1}}\sqrt{b}) = R(\eta_{2^{k+j}}, \sqrt{\xi_m}) \tag{1}$$

iff $R(\sqrt{\xi_m}) = R(\sqrt{c})$ *for some positive* $c \in R$ *and*

$$b = \begin{cases} r^2 c, & k < A, \\ r^2 c(\eta_{2^A}+2), & k = A. \end{cases}$$

Proof. Since $k+j \leqslant A$, $\eta_{2^{k+j}} \in R$ and $R(\eta_{2^{k+j}}, \sqrt{\xi_m}) = R(\sqrt{\xi_m})$. If $k < A$, then $\eta_{2^{k+1}} \in R$ and $R(\eta_{2^{k+1}}\sqrt{b}) = R(\sqrt{b})$. Thus (1) holds iff $R(\sqrt{b}) = R(\sqrt{\xi_m})$. The result then follows by Lemma 2.4. If $k = A$, then (1) holds iff $R(\eta_{2^{A+1}}\sqrt{b}) = R(\sqrt{\xi_m})$ iff $R(\sqrt{\xi_m}) = R(\sqrt{c})$ for some $c \in R$ and $b = r^2 c(\eta_{2^A}+2)$, some $r \neq 0 \in R$, by 2.3 and 2.4. ∎

Proposition 4.3. *Suppose* $j = 0$ *and* $k > A$. *Let* B *be largest such that* $\eta_{2^B} \in R(\sqrt{\xi_m})$. *Then* $R(\eta_{2^{k+1}}\sqrt{b}) = R(\eta_{2^k}, \sqrt{\xi_m})$ *iff one of the following holds*:

(a) $k = B-1$, $R(\sqrt{\xi_m}) = R(\eta_{2^B})$ *and* $b = \begin{cases} r^2, \\ r^2(\eta_{2^A}+2); \end{cases}$

(b) $k = B$, $[R(\sqrt{\xi_m}) : R(\eta_{2^B})] = 2$, $R(\sqrt{\xi_m})$ *cyclic over* R (*of degree* 2^{B+1-A}), $\sqrt{b} \notin R$ *and* $\sqrt{b}$ *lies in one of two quadratic extensions* K *of* R *with* $K \subseteq R(\sqrt{\xi_m}, \eta_{2^{B+1}})$ *but* $K \neq R(\eta_{2^A+1})$.

Proof. ($\Rightarrow$) Suppose $R(\eta_{2^{k+1}}\sqrt{b}) = R(\eta_{2^k}, \sqrt{\xi_m})$. Thus $\sqrt{b} \in R(\eta_{2^{k+1}}, \sqrt{\xi_m})$ and either (a) $\sqrt{b} \in R(\eta_{2^k}, \sqrt{\xi_m})$ or (b) $\sqrt{b} \notin R(\eta_{2^k}, \sqrt{\xi_m})$.

In case (a),

$$\eta_{2^{k+1}} \in R(\eta_{2^k}, \sqrt{\xi_m}). \tag{2}$$

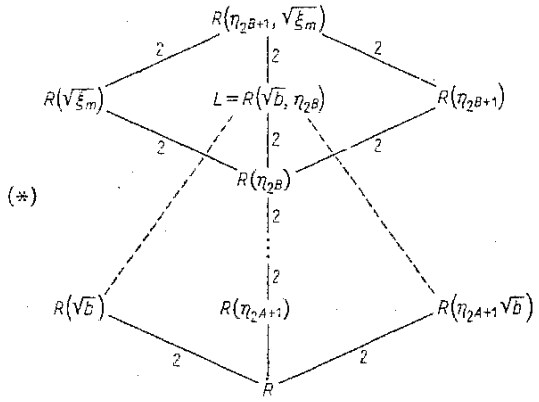
Thus $k < B$ and

$$[R(\eta_{2^k}, \sqrt{\xi_m}) : R(\eta_{2^k})] = 2. \tag{3}$$

The relations (2) and (3) then imply $R(\eta_{2^k}, \sqrt{\xi_m}) = R(\eta_{2^{k+1}})$ or, which is the same, $R(\sqrt{\xi_m}) = R(\eta_{2^{k+1}})$. Thus also $k+1 = B$ and b is either a square in R or is equal to $r^2(\eta_{2^A}+2)$.

In case (b), let $R' = R(\sqrt{\xi_m})$. Then $\sqrt{b} \in R'(\eta_{2^{k+1}})$ and $\sqrt{b} \notin R'(\eta_{2^k})$ implies $k = B$ by Lemma 2.5 (c). Thus $R(\eta_{2^k}, \sqrt{\xi_m}) = R(\sqrt{\xi_m})$. Furthermore, $[R(\sqrt{\xi_m}) : R(\eta_{2^B})] = 2$ since, if the two fields were equal, we would have $\sqrt{b} \in R(\eta_{2^{B+1}})$, $\sqrt{b} \notin R(\eta_{2^B})$ contradicting the fact that $B = k > A$ and Lemma 2.5 (c). By similar reasoning we also have $\sqrt{b} \notin R(\eta_{2^{B+1}})$. Of course we also have $\sqrt{b} \notin R(\sqrt{\xi_m})$. We are thence led to the following

diagram of fields:



We have that $G(R(\sqrt{\xi_m}, \eta_{2B+1})/R(\eta_{2B})) \simeq \mathbf{Z}_2 \times \mathbf{Z}_2$. Thus there is a unique field L as in the diagram and $\sqrt{b} \in L$. Furthermore $R(\eta_{2B+1})$ is cyclic of degree 2^{B+1-A} over R and thus $G(R(\sqrt{\xi_m}, \eta_{2B+1})/R) \simeq \mathbf{Z}_2 \times \mathbf{Z}_{2^{B+1-A}}$. Consequently, exactly one of $R(\sqrt{\xi_m})$ and L is cyclic over R. But if L were cyclic (of degree 2^{B+1-A}), then $\sqrt{b} \in L$ implies $\sqrt{b} \in R(\eta_{2A+1})$ contradicting the fact that $\sqrt{b} \notin R(\eta_{2B+1})$. Hence $R(\sqrt{\xi_m})$ is cyclic and $G(L/R) \simeq \mathbf{Z}_2 \times \mathbf{Z}_{2^{B-A}}$. Therefore L contains exactly three quadratic extensions of R: one is $R(\eta_{2A+1})$, the others must be $R(\sqrt{b})$ and $R(\sqrt{b}\eta_{2A+1})$.

($\Leftarrow$) If the conditions as given in (a) in the statement of the proposition hold, then

$$R(\eta_{2^k+1}\sqrt{b}) = R(\eta_{2^B}\sqrt{b}) = R(\eta_{2^B}) = R(\sqrt{\xi_m}) = R(\eta_{2^B-1}, \sqrt{\xi_m}) = R(\eta_{2^k}, \sqrt{\xi_m}).$$

If the conditions in (b) hold, then diagram (*) holds and

$$R(\eta_{2^k+1}\sqrt{b}) = R(\eta_{2B+1}\sqrt{b}) = R(\sqrt{\xi_m}) = R(\sqrt{\xi_m}, \eta_{2B}) = R(\eta_{2^k}, \sqrt{\xi_m}). \blacksquare$$

Remark. The conditions $j = 0$, $k > A$ and $R(\eta_{2^k+1}\sqrt{b}) = R(\eta_{2^k}, \sqrt{\xi_m})$ of this proposition arise from the weak normality of $x^{2^k m} + b^{2^{k-1} m/m_0}$ with parameter m_0. The ε of Proposition 3.2 is 2 and the associated weakly normal binomial is $x^{2^k} + b^{2^{k-1}}$ with parameter 2. This is case 4 of Theorem 4.1.

From the results of this section together with Propositions 3.1 and 3.2, we are able to obtain a complete list of weakly normal binomials of type $x^{2^h m} + a$. This is given in the following

THEOREM 4.4. *Let $m \in \mathbf{Z}$, $m > 1$, m odd. Then a binomial $q(x) = x^{2^h m} + a$*

is weakly normal over R iff $q(x)$ is one of the following for suitable $m_0 | m$ and $r, c \in R$ (a binomial in number n or n_i below has its associated binomial — according to Proposition 3.2 — in number n of Theorem 4.1; the asterisk (*) denotes the cases where $c \in R$, $c > 0$, $R(\sqrt{c}) = R(\sqrt{\xi_m})$ and $\sqrt{c} \notin R$).

1_1. $x^{2m} + r^{2m/m_0}$, $\sqrt{\xi_m} \in R$.

1_2. $x^{2m} + (r^2 c)^{m/m_0}$(*).

2_1. $x^{2^h m} + r^{2^{h-g} m/m_0}$, $\sqrt{\xi_m} \in R$, $h \leqslant A$.

2_2. $x^{2^h m} + (r^2 c)^{2^{h-g} m/m_0}$, $A \geqslant h > g \geqslant 2$ *or* $A > h > 1 = g$(*).

2_3. $x^{2^A m} + [r^2 c(\eta_{2^A} + 2)]^{2^{A-1} m/m_0}$(*).

3. $x^{2^A+1 m} + [r^2(\eta_{2^A} + 2)]^{2^{g-1} m/m_0}$, $\sqrt{\xi_m} \in R(\eta_{2^A+1})$, $2 \leqslant g < A$.

4_1. $x^{2^h m} + r^{2^{h-1} m/m_0}$, $\sqrt{\xi_m} \in R(\eta_{2^h})$, $h \geqslant A+1$.

4_2. $x^{2^h m} + r^{2^h m/m_0}$, $R(\sqrt{\xi_m}) = R(\eta_{2^h+1})$, $h \geqslant A+1$.

4_3. $x^{2^h m} + [r^2(\eta_{2^A} + 2)]^{2^{h-1} m/m_0}$, $R(\sqrt{\xi_m}) = R(\eta_{2^h+1})$, $h \geqslant A+1$.

4_4. $x^{2^h m} + b^{2^{h-1} m/m_0}$, *where R and b satisfy condition* (b) *of Proposition* 4.3 *with* $h = k$; $h \geqslant A+1$.

5. $x^{2^h m} + [r^2(\eta_{2^A} + 2)]^{2^{h-2} m/m_0}$, $\sqrt{\xi_m} \in R(\eta_{2^h})$, $h > A+1$.

Moreover, the irreducible normal binomials of the given type are

(a) *For all A:*
$x^{2m} + r^2$, $\sqrt{\xi_m} \in R$;
$x^{2m} + r^2 c$(*).

(b) *For $A = 2$:*
$x^{4m} + r^4 c^2 2^2$(*);
all weakly normal binomials of types 4 *and* 5 *above.*

(c) *For $A \geqslant 3$:*
$x^{2^h m} + r^2$, $\sqrt{\xi_m} \in R$, $|r| \neq r_1^2$, $A \geqslant h > 1$;
$x^{2^A m} + r^4 c^2$(*);
$x^{2^A+1 m} + r^4(\eta_{2^A} + 2)^2$, $\sqrt{\xi_m} \in R(\eta_{2^A+1})$.

In all cases of irreducible binomials, it is understood that the coefficient is not a q-th power for any $q | m$, $q > 1$.

Proof. We divide the proof into four cases: (i) $h = 1$, (ii) $A \geqslant h > 1$, (iii) $h > A$ and even parameter, (iv) $h > A$ and odd parameter.

(i) The binomial $x^{2m} + a$ is weakly normal with parameter $m_0 | m$ iff, by 3.2, $a = b^{m/m_0}$ and $R(\zeta_4\sqrt{b}) = R(\zeta_{2m})$. The latter is true iff, by 3.1 (b), $R(\sqrt{b}) = R(\sqrt{\xi_m})$. This gives us cases 1_1 and 1_2.

(ii) Now suppose $A \geqslant k+j > 1$. Then binomial $x^{2^{k+j} m} + a$ is weakly normal with parameter $2^j m_0$ ($m_0 | m$) iff, by 3.2, $a = b^{2^{k-1} m/m_0}$, $x^{2^{k+j}} + b^{2^{k-1}}$ is weakly normal with parameter $\varepsilon 2^j$ and $R(\zeta_{2^k+1}\sqrt{b}) = R(\zeta_{2^k+j m})$. By 3.1

(a, c) and 4.2, the latter implies either (a) $\sqrt{\xi_m} \in R$ or (b) $[R(\sqrt{\xi_m}):R] = 2$. In case (a) we have $\varepsilon = 1$ and case 2 of 4.1 leads us to the present 2_1. In case (b), we have $\varepsilon = 2$ which, together with case 2 of 4.1 and 4.2, yields our present 2_2 ($k < A$) and 2_3 ($k = A$).

(iii) If $k+j > A$ and $x^{2^{k+j}m}+a$ is weakly normal with parameter $2^j m_0$ ($m_0 | m$, $j \geqslant 1$), then by 3.2 $a = b^{2^{k-1}m/m_0}$, $x^{2^k}+b^{2^{k-1}}$ is weakly normal with parameter $\varepsilon 2^j$ and $R(\zeta_{2^{k+1}}\sqrt{b}) = R(\zeta_{2^{k+j}}, \sqrt{\xi_m})$. This latter implies

$$[R(\eta_{2^{k+j}}):R(\eta_{2^k})] = 2, \quad \sqrt{\xi_m} \in R(\eta_{2^{k+j}}) \quad \text{and} \quad \varepsilon = 1.$$

Furthermore, $x^{2^k}+b^{2^{k-1}}$ must be one of cases 3, 4 or 5 of Theorem 4.1. This gives us our present cases 3, 4_1 and 5. Conversely, it is easy to show that these cases are weakly normal.

(iv) Finally suppose $h > A$ and that $x^{2^h m}+a$ is weakly normal with parameter $m_0|m$. By 3.1, this is so iff $a = b^{2^{h-1}m/m_0}$, $x^{2^h}+b^{2^{h-1}}$ is weakly normal and $R(\zeta_{2^{h+1}}\sqrt{b}) = R(\zeta_{2^h}, \sqrt{\xi_m})$. Thus our present cases 4_2, 4_3, and 4_4 follow from Proposition 4.3 and the fact that $x^{2^h}+b^{2^{h-1}}$ must be case 4 of 4.1. ∎

5. Examples and applications. In this final section, we would like to accomplish two things. First, we would like to apply our results to a class of real fields for which the results of Darbi, Mann and Vélez generalize more naturally than for the class of all real fields (see 5.1 below). Secondly, we would like to construct a real field for which the conditions of 4_2 and 4_3 (of Theorem 4.4) hold and a real field for which the conditions of 4_4 hold.

We realize our first aim in

PROPOSITION 5.1. *Let Q_a be the maximal abelian extension of Q and suppose R is a real field such that $R \cap Q_a \subseteq Q(\eta_t)$ for some odd integer t. Then $q(x) = x^n + a$ ($a > 0$, $a \in R$) is weakly normal over R iff $q(x)$ is one of the following*

(a) x^2+r^2; x^2+r, $\sqrt{r} \notin R$ (*); x^4+4r^4; x^4+r^2, $r \neq 2r_1^2$ (*); $x^{2^h}+r^{2^{h-1}}$, $h \geqslant 3$ (*); $x^{2^h}+2^{2^h-2}r^{2^{h-1}}$, $h \geqslant 4$ (*). (*In all cases $r \in R$, $r > 0$.*)

(b) $x^{2m}+(r^2\xi_m)^{m/m_0}$, $x^{4m}+(2r^2\xi_m)^{2m/m_0}$, m *odd*, $m_0|m$, $\eta_m \in R$, $r \in R$.

Moreover, the irreducible binomials consist of the binomials in (a) *followed by* (*) *plus those binomials in* (b) *with $m = m_0$ and the coefficient not a q-th power for any $q|m$, $q > 1$.*

Proof. Since $A = 2$, by Theorem 4.1 the binomials in (a) are all the weakly normal binomials with degree n = power of 2.

Let m be an odd integer with $m > 1$. We now consider binomials over R with degree $2^k m$ for some $k \geqslant 1$. We first note that $4m$ is the smallest

integer q such that $\sqrt{\xi_m} \in Q(\eta_q)$. Thus, since $R \cap Q_a \subset Q(\eta_t)$ for some odd t, we must have $\sqrt{\xi_m} \notin R$. Furthermore, we claim $R(\sqrt{\xi_m}) \cap R(\eta_{2^h}) = R$ for all $h \geqslant 3$. For, if not, then by 2.5 $\sqrt{2} \in R(\sqrt{\xi_m})$. Thus also $\sqrt{2} \in R(\sqrt{\xi_m}) \cap Q_a$ which, by the above comments, is a subfield of $Q(\zeta_{4q})$ for some odd q. But $\sqrt{2} \in Q(\zeta_{4q})$ contradicts the fact that $Q(\eta_{2^h}) \cap Q(\zeta_{4q}) = Q$ (any h, any odd q). Thus if $x^{2^h m}+a$ is weakly normal over R, a glance at the list in Theorem 4.4 shows that $[R(\sqrt{\xi_m}):R] = 2$, $h \leqslant A = 2$, and that therefore only cases 1_2 and 2_3 are admissible. We must only determine the coefficients in order to complete the proof of the proposition.

Now $[R(\sqrt{\xi_m}):R] = 2$ implies $[R(\zeta_{4m}):R] = 4$ so that, since $R \cap Q_a \subseteq Q(\eta_t)$, we have $[R(\zeta_{4m}):R] = [R(\zeta_4):R]\cdot[R(\zeta_m):R]$. Thus $[R(\zeta_m):R] = 2$. Consequently, by Lemma 2.1 (c), $\eta_m \in R$ and hence $\xi_m \in R$. Hence we can choose c in 1_2 and 2_3 to be ξ_m. Since $\eta_{2^A}+2 = 2$, we are done. ∎

Remark. One obtains the lists L_1 and L_2 ($R = Q$) immediately since $\eta_m \in Q$ (m odd, $m > 1$) iff $m = 3$. Furthermore, $\eta_3 = -1$ and $\xi_3 = 4 - \eta_3^2 = 3$.

The fact that $R(\sqrt{\xi_m}) \cap R(\eta_{2^k}) = R$ for all k in the above proof, shows that the situation considered in Proposition 5.1 is an extreme case of the following immediate corollary to Theorem 4.4 (and Lemma 2.5).

PROPOSITION 5.2. *If m is odd, $m > 1$ and $x^{2^h m}+a$ weakly normal over R, then either $R(\sqrt{\xi_m}) = R(\eta_{2^g})$ for some $g \leqslant h$ or $[R(\sqrt{\xi_m}):R(\eta_{2^h})] = 2$. In all cases $R(\sqrt{\xi_m})$ is cyclic over R of degree a power of 2.*

We would like to construct examples of real fields satisfying the conclusions of 5.2 for some choice of m and $h > A$. In particular we want

(A) an odd integer $m > 1$ and a field R such that $R(\sqrt{\xi_m}) = R(\eta_{2^h})$ with $h > A$; and

(B) an odd integer $m > 1$ and a field R such that

$$[R(\sqrt{\xi_m}):R(\eta_{2^{h-1}})] = 2, \quad R(\sqrt{\xi_m}) \neq R(\eta_{2^h}),$$

$R(\sqrt{\xi_m})$ cyclic over R with $h > A+1$.

(Compare Proposition 4.3.)

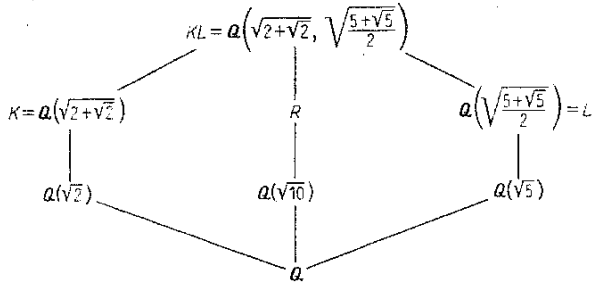
As an aid, we have

LEMMA 5.3. *If $R(\sqrt{\xi_m})$ is cyclic over R of degree 2^k, then there exists a prime p such that $p|m$ and $2^k|p-1$.*

Proof. $G(R(\sqrt{\xi_m})/R)$ must be a subgroup of $G(Q(\sqrt{\xi_m})/Q)$. ∎

We first seek to satisfy (A) with R a subfield of Q_a, $A = 2$, $h = 4$, $m = 5$. Lemma 5.3 is not contradicted. Consider the following diagram

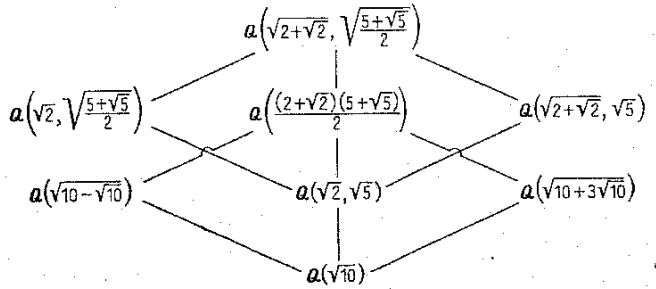
of fields:



where $\eta_{2^3} = \sqrt{2}$, $\eta_{2^4} = \sqrt{2+\sqrt{2}}$, $\eta_5 = \dfrac{-1+\sqrt{5}}{2}$, $\xi_5 = \dfrac{5+\sqrt{5}}{2}$ (the field R to be described later). Now $G(K/Q) = Z_4$ and $G(L/Q) \simeq Z_4$. Let the two groups be generated by ϱ, σ respectively. Then $G(KL/Q) = \langle\sigma\rangle \times \langle\varrho\rangle$ with $\varrho(\sqrt{\xi_5}) = \sqrt{\xi_5}$ and $\sigma(\eta_{2^4}) = \eta_{2^4}$. Let H be the subgroup of $\langle\sigma\rangle \times \langle\varrho\rangle$ generated by the element (σ, ϱ). (H is thus a so-called "diagonal" subgroup) and let R be the fixed-field of H. We claim that R satisfies (A) with $A = 2$, $h = 4$, $m = 5$. To show this, note that $\langle\varrho\rangle \times \langle\sigma\rangle = H \times \langle\varrho\rangle = H \times \langle\sigma\rangle$. Thus $KL = Q(\sqrt{\xi_5}, \eta_{2^4})$ is, on the one hand, the composition of R and $Q(\sqrt{\xi_5})$ and, on the other, the compositum of R and $Q(\eta_{2^4})$. Thus $R(\sqrt{\xi_5}) = Q(\sqrt{\xi_5}, \eta_{2^4}) = R(\eta_{2^4})$. Also, $[R(\sqrt{\xi_5}):R] = 4$ since H has order 4. By a straightforward computation, we arrive at $R = Q(\sqrt{10-\sqrt{10}})$ or $R = Q(\sqrt{10+3\sqrt{10}})$, depending on the choices of σ, ϱ as generators of their respective groups. (The two possibilities for R are not the same fields!)

Therefore, by Theorem 4.4, in addition to the binomials on the lists L_1 and L_2 (with the obvious modifications), the only weakly normal binomials over R are $x^{80} + r^{16 \cdot 5/m_0}$ and $x^{80} + [2^8 r^{16}]^{5/m_0}$ ($m_0 = 1$ or 5, $r \in R$).

We now turn to the problem of finding an example satisfying (B). Fortunately for us, we are able to use the example for (A) given above. (This is not a coincidence; see 5.4 below.) Indeed, consider the following diagram of fields:



Let $R = Q(\sqrt{10})$. Then

$$R(\sqrt{\xi_5}) = Q\left(\sqrt{2}, \sqrt{\frac{5+\sqrt{5}}{2}}\right) \quad \text{and} \quad R(\eta_{2^4}) = Q(\sqrt{2+\sqrt{2}}, \sqrt{5})$$

are both cyclic of degree 4 over R. Moreover, $R(\eta_{2^4}) \neq R(\sqrt{\xi_5})$. Thus the conditions of (B) are satisfied with $R = Q(\sqrt{10})$, $A = 2$, $h = 4$, and $m = 5$.

On the other hand, the diagram above is exactly diagram (*) in the proof of Proposition 4.3 with $m = 5$, $A = 2$, $B = 3$, $R = Q(\sqrt{10})$, $b = 10 - \sqrt{10}$ or $10 + 3\sqrt{10}$. (It is easy to check that $R(\sqrt{10+3\sqrt{10}}) = R(\sqrt{2}\sqrt{10-\sqrt{10}})$ by noting that $10 + 3\sqrt{10} = 2(4+\sqrt{10})^2(10-\sqrt{10})/36$.) Thus by Theorem 4.4, the weakly normal binomials over R are

$$x^{40} + [(10-\sqrt{10})^4 r^8]^{5/m_0} \quad \text{and} \quad x^{40} + [2^4 \cdot (10-\sqrt{10})^4 r^8]^{5/m_0}$$

($m_0 = 1$ or 5, $r \in R$) plus those on the lists L_1 and L_2.

The construction of the above examples illustrates the following general procedure for constructing fields satisfying (A) or (B).

5.4. Given $A \geqslant 2$, $k \geqslant A+1$

(1) Choose m such that there exists prime p with $p|m$ and $2^{k-A}|p-1$. (Thus $G(Q(\sqrt{\xi_m})/Q)$ has a cyclic factor Z_{2^l} for some $l \geqslant k-A$.)

(2) Pick subfield $K \subseteq Q(\sqrt{\xi_m})$ with $G(Q(\sqrt{\xi_m})/K) = \langle\sigma\rangle \simeq Z_{2^{k-A}}$. Note that $G(K(\eta_{2^k})/K) = \langle\varrho\rangle \simeq Z_{2^{k-A}}$ and that $G(K(\eta_{2^k}, \sqrt{\xi_m})/K) = \langle\varrho\rangle \times \langle\sigma\rangle$.

(3) Let $R_{(A)}$ = fixed-field of subgroup $\langle(\varrho, \sigma)\rangle$ of $\langle\varrho\rangle \times \langle\sigma\rangle$.

(4) If $k > A+1$, let $R_{(B)}$ = fixed-field of subgroup $\langle(\varrho, \sigma), (\varrho^{2^{k-A-1}}, 1)\rangle$.

Then $R_{(A)}$, m, A, k satisfy (A) with $h = k$; $R_{(B)}$, m, A, $h = k$ ($k > A+1$) satisfy (B).

Remark. If R, m, h, A satisfy (A) ((B)), then a translation argument ([4], p. 196) shows that $R \cap Q(\eta_{2^{h+1}}, \sqrt{\xi_m})$ must be a field constructed in the above manner.

The number of choices in the procedure 5.4 seems to indicate that finding an explicit expression for the "b" in binomial 4_4 of Theorem 4.4 would be quite difficult. Nevertheless, we have been explicit in all other cases; it would be nice if we could be so in this case.

References

[1] Giulio Darbi, *Sulla riducibilità delle equazioni algebriche*, Ann. Mat. Pura Appl., Ser. 4, 4 (1926), pp. 185–208.

[2] David Gay, Andrew McDaniel and William Yslas Vélez, *Partially normal radical extensions of the rationals*, Pacific J. Math. 72(1977), pp. 403–417.

[3] Irving Kaplansky, *Fields and rings*, University of Chicago Press, 1969.

[4] Serge Lang, *Algebra*, Addison-Wesley, Reading 1965.
[5] Henry B. Mann and William Yslas Vélez, *On normal radical extensions of the rationals*, J. Lin. Multilin. Alg. 3 (1975), pp. 73–80.
[6] Michael J. Norris and William Yslas Vélez, *Structure theorems for radical extensions of fields*, Acta Arith., to appear.
[7] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. 32 (1976), pp. 245–274.
[8] N. G. Tschebotarów and H. Schwerdtfeger, *Grundzüge der Galois'schen Theorie*, Groningen–Djakarta 1950.

Received on 8. 9. 1976
and in revised form on 25. 1. 1977 (892)

ACTA ARITHMETICA
XXXV (1979)

Über die simultane Darstellung zweier ganzer Zahlen durch quadratische und lineare Formen

von

A. A. Walfisz (Tbilissi)

1. Einleitung. In der vorliegenden Arbeit wird eine asymptotische Formel für die Anzahl der ganzzahligen Lösungen $r(q, n; l, m)$ des diophantischen Gleichungssystems

$$\begin{aligned} q(x_1, \ldots, x_s) &= n, \\ l(x_1, \ldots, x_s) &= m, \end{aligned} \tag{1.1}$$

bei $s \geqslant 5$ aufgestellt und untersucht. Hier ist

$$q = q(X) = q(x_1, \ldots, x_s) = \sum_{i,k=1}^{s} q_{ik} x_i x_k = X^T Q X$$

eine positiv definite ganzzahlige quadratische Form mit der symmetrischen Matrix $Q = (q_{ik})$ und der Determinate $D = \det q$; $X^T = (x_1, \ldots, x_s)$, und

$$l = l(X) = l(x_1, \ldots, x_s) = \sum_{i=1}^{s} c_i x_i = C^T X \tag{1.2}$$

ist eine ganzzahlige lineare Form; $C^T = (c_1, \ldots, c_s)$.

Ohne Beschränkung der Allgemeinheit kann man annehmen, daß die Elemente der Matrix $Q = (q_{ik})$ ganze Zahlen (1) und q, l primitive Formen sind, d.h. $\mathrm{ggT}(q_{ik}) = 1$, $\mathrm{ggT}(c_1, \ldots, c_s) = 1$.

Die Hauptergebnisse dieser Arbeit sind in dem Bericht [10] mitgeteilt.

I. M. Winogradow [13] war der erste, der die Kreismethode auf Probleme diophantischer Gleichungssysteme (sogar allgemeinere als (1.1)) angewendet hat. Er hat eine Methode für die Aufstellung und Untersuchung der asymptotischen Formeln für die Lösungszahl solcher Systeme ausge-

(1) Es ist nicht schwer unsere Ergebnisse auch auf beliebige ganze Formen q zu übertragen, d.h. auf homogene Polynome des zweiten Grades mit ganzen Koeffizienten.