ACTA ARITHMETICA
XXXVIII (1980)

Structure theorems for radical extensions of fields*

by

MICHAEL J. NORRIS and WILLIAMS YSLAS VÉLEZ** (Albuquerque, New M.)

Let m be a positive integer, F a field, and $a \in F$.

DEFINITION 1. We say that the polynomial, $x^m - a$, is *partially normal* if there exists a root α of $x^m - a$ such that $F(\alpha)$ is the splitting field of $x^m - a$.

DEFINITION 2. We say that the polynomial, $x^m - a$, is *irreducible normal* if $x^m - a$ is partially normal and $x^m - a$ is irreducible.

Of course, if $x^m - a$ is irreducible normal then every root of $x^m - a$ generates its splitting field.

Darbi and Bessel-Hagen, [6], and Mann and Vélez, [5], characterized all irreducible normal binomials over Q, the field of rational numbers. Gay, [3], characterized all irreducible normal binomials over real fields, and Gay, et al., [2], characterized all partially normal binomials over Q.

In this paper we shall study the structure of radical extensions and describe an interesting relationship between radical extensions and irreducible and partially normal binomials.

LEMMA 1. *Let $\gamma \neq 0$, $\gamma^r \in F$, and $x^r - \gamma^r$ be irreducible over F. Then $\gamma^t \in F$ iff $r|t$.*

Proof. For any field K, let K^* denote the multiplicative group of non-zero elements and consider the quotient group $F(\gamma)^*/F^*$. If $x^r - \gamma^r$ is irreducible over F, then the order of γ in $F(\gamma)^*/F^*$ is r. Hence $\gamma^t \in F^*$ iff $r|t$. ■

Throughout this paper α shall denote a root of $x^m - a$. Let m be the smallest power of α such that $\alpha^m \in F$, that is, m is the order of α in K^*/F^*, where K is any field such that $K \supset F$ and $\alpha \in K$. We shall denote this by $o(\alpha) = m$ over F^*, or simply $o(\alpha)$, if F^* is understood.

---

* This work was supported by the U.S. Energy Research and Development Administration (ERDA), Contract No. AT(29-1)-789. By acceptance of this article, the publisher and/or recipient acknowledges the U.S. Government's right to retain a nonexclusive, royalty-free license in and to any copyright covering this paper.

** This author is currently at the Department of Mathematics, University of Arizona, Tucson, Arizona 85721.

Further, we shall assume, throughout this paper, that $\operatorname{char} F \nmid m$. We make this assumption more for convenience than for necessity. All the theorems remain valid without this assumption.

For a, with $o(a) = m$, define

(1) $n = \max\{k\colon k|m,\ \zeta_k \in F(\alpha)$, where ζ_k denotes a primitive kth-root of unity$\}$.

Set $s = [F(\alpha)\colon F(\zeta_n)]$.

THEOREM 1. *Let $o(a) = m$ over F^* and n, s defined as in* (1). *If $F(\alpha) \supset K \supset F(\zeta_n)$, with $l = [F(\alpha)\colon K]$, then $K = F(\alpha^l)$ and $x^l - \alpha^l$ is irreducible over K.*

Furthermore, $s|m$.

Proof. Let $f(x)$ denote the irreducible polynomial that α satisfies over K. Since $\alpha^m = a \in F \subset K$, we have that $f(x)|x^m - a$. Thus, every root of $f(x)$ is of the form, $\zeta_m^i \alpha$, for some i. Hence, $f(x) = \prod_{j=1}^{l} (x - \zeta_m^{i_j}\alpha)$. The constant term of $\pm f(x)$, $(\prod_{j=1}^{l} \zeta_m^{i_j}\alpha) = \zeta_m^e \alpha^l$, $e = \sum_{j=1}^{l} i_j$, is an element of $K \subset F(\alpha)$. Also $\alpha^l \in F(\alpha)$, thus $\zeta_m^e \in F(\alpha)$, and by the definition of n, $\zeta_m^e \in F(\zeta_n) \subset K$, thus $\alpha^l \in K$. Now $l = [F(\alpha)\colon K]$ and $[F(\alpha)\colon F(\alpha^l)] \leqslant l$, since α satisfies the binomial $x^l - \alpha^l$ over $F(\alpha^l)$. Hence we must have that $F(\alpha^l) = K$ and $x^l - \alpha^l$ is irreducible over K.

In particular, if $l = s$, then since $\alpha^m = a \in F \subset F(\zeta_n)$, we have that $s|m$, by Lemma 1. ■

Theorem 1 generalizes Proposition 2.1 in [2].

Remark 1. Before continuing we want to make a remark about the notation $a^{1/m}$. The symbol $a^{1/m}$ can denote any of the m roots of $x^m - a$. However, assume that $k|m$. Then $F(\alpha^{m/k}) \subset F(\alpha)$ and $(\alpha^{m/k})^k = a$, so $\alpha^{m/k}$ is a root of $x^k - a$ in $F(\alpha)$, so by $a^{1/k} \in F(\alpha)$ we shall mean one of the solutions of $x^k - a$ which is contained in $F(\alpha)$.

Remark 2. Let $x^m - a$ be irreducible over F and $\zeta_m \in F$, where $\operatorname{char} F \nmid m$. Then, by a well-known theorem, $F(\alpha)$ has cyclic Galois group over F. This theorem gives very precise information as to the subfields of $F(\alpha)$, namely, if $l|m$, then $F(\alpha^l)$ is the unique subfield of $F(\alpha)$ of degree m/l over F and for $l_i|m$, $i = 1, 2$, $F(\alpha^{l_1}) \supset F(\alpha^{l_2})$ iff $l_1|l_2$. Theorem 1 is a generalization of this result to the non-normal case. That is, if F contains every mth-root of unity that is contained in $F(\alpha)$, then if $l|s$, where $s = [F(\alpha)\colon F]$, $F(\alpha^l)$ is the unique subfield of $F(\alpha)$ of degree s/l over F, and if $l_i|s$, $i = 1, 2$, then $F(\alpha^{l_1}) \supset F(\alpha^{l_2})$ iff $l_1|l_2$.

In the case where F contains every mth-root of unity that is contained in $F(\alpha)$, Theorem 1 gives very precise information as to the lattice of subfields of $F(\alpha)$ as pointed out in Remark 2. In general, there are more subfields than just those of the form $F(\alpha^l)$.

However, let us consider the following: Let $F(\alpha) \supset K \supset F$, $K \cap F(\zeta_n) = F(\theta)$, and $t = \min\{i : i|m \text{ and } \alpha^i \in K\}$. Under what conditions is $K = F(\theta, \alpha^t)$?

THEOREM 2. *Let $F(\alpha) \supset K \supset F$, $K \cap F(\zeta_n) = F(\theta)$, $t = \min\{i\colon i|m$ and $\alpha^i \in K\}$, $r = \max\{i\colon i|m$ and $F(\alpha^r) \supset K\}$. Then $K = F(\theta, \alpha^t)$ iff $(s, t) = (s, r)$.*

Proof. Let us first recall the following elementary result: Let $L \supset M$ a field extension and let $L \supset M_i \supset M$, for $i = 1, 2$, such that $M_1 M_2 = L$, $M_1 \cap M_2 = M$. Then $N \to M_2 N$ defines an injection from the lattice of intermediate fields of M_1 over M to the lattice of intermediate fields of L over M_2, which preserves inclusions, intersections and composita.

Set $M = F(\theta)$, $M_1 = K$, $M_2 = F(\zeta_n)$. Note that $KF(\zeta_n) \supset F(\zeta_n)$, so, by Theorem 1, $KF(\zeta_n) = F(\alpha^l)$, where $l|s$. Further, $F(\alpha^r) \supset K$, $F(\alpha^l) \supset K$, thus $F(\alpha^{[l,r]}) \supset K$, where $[l, r]$ denotes the l.c.m. of l and r. However, r was maximal with this property, thus $[r, l] = r$, so $l|r$. Further, $F(\alpha^r)F(\zeta_n) = F(\alpha^{(r,s)}) \supset KF(\zeta_n)$, thus $l = (s, r)$, and $KF(\zeta_n) = F(\alpha^r)F(\zeta_n) = F(\alpha^{(s,r)})$. So we have that $L = F(\alpha^{(s,r)})$.

Now, $K \supset F(\theta, \alpha^t) \supset F(\theta)$ and the subfield, between $F(\alpha^{(s,r)})$ and $F(\zeta_n) = F(\alpha^s)$, that corresponds to $F(\theta, \alpha^t)$ is, $F(\zeta_n, \alpha^t) = F(\alpha^{(t,r)})$. Thus $F(\theta, \alpha^t) = K$ iff $(t, s) = (r, s)$. ■

We point out that Theorem 2 still does not account for all subfields K, where $F(\alpha) \supset K \supset F$. In fact, already in $Q(\alpha)$, where $\alpha^{12} + 36 = 0$, one can find an example of a field which is not covered by Theorem 2.

Recall that $x^{12} + 36$ is irreducible normal and $Q(\alpha^3) = Q(\zeta_{12})$. Further $Q(\alpha)$ contains the splitting field of $x^3 + 36$ and this field is $Q(\alpha^4, \zeta_3) \supset Q(\alpha^4)$, and $[Q(\alpha^4)\colon Q] = 3$, $[Q(\alpha^4, \zeta_3)\colon Q(\alpha^4)] = 2$. Now $Q(\zeta_3\alpha^4)$ is a conjugate of $Q(\alpha^4)$. Further $\min\{i\colon i|12$ and $\alpha^i \in Q(\zeta_3\alpha^4)\} = 12$ and $\max\{i\colon i|12$ and $Q(\alpha^i) \supset Q(\zeta_3\alpha^4)\} = 4$, so $(s, r) = (3, 4) \neq (3, 12) = (s, t)$.

THEOREM 3. *Let $o(a) = m$ over F^*. If $F(\alpha)$ is normal over F, then $\zeta_m \in F(\alpha)$ and $x^m - a$ is partially normal.*

Proof. Factor

$$x^m - a = \prod_{j=1}^{k_1} f_j(x) \cdot \prod_{j=k_1+1}^{k} f_j(x),$$

where each $f_j(x)$ is irreducible over F and for $1 \leqslant j \leqslant k_1$, $f_j(x)$ has a root in $F(\alpha)$, while for $k_1 < j \leqslant k$, $f_j(x)$ does not have a root in $F(\alpha)$. If $f_j(x)$ has a root in $F(\alpha)$, then it is of the form $\zeta_m^{i_1}\alpha$. However $\alpha \in F(\alpha)$, hence $\zeta_m^{i_1}\alpha/\alpha = \zeta_m^{i_1} \in F(\alpha)$. Let n be defined as in (1), then $\zeta_m^{i_1} = \zeta_n^i$. So every root of $f_j(x)$ in $F(\alpha)$ must be of the form $\zeta_n^i \alpha$. Hence $\prod_{j=1}^{k_1} f_j(x) = \prod_{j=0}^{n-1} (x - \zeta_n^j \alpha) = x^n - \alpha^n$. But $\prod_{j=1}^{k_1} f_j(x) \in F[x]$, hence $x^n - \alpha^n \in F[x]$, so $\alpha^n \in F$. But m was minimal and $n|m$, hence $n = m$, so $\zeta_m \in F(\alpha)$. ■

THEOREM 4. *Let $o(a) = m$ over F^*, then $F(a^{m/n})$ is the splitting field of $x^n - a$, that is, $x^n - a$ is partially normal. If $x^m - a$ is irreducible, then $x^n - a$ is irreducible normal. Furthermore, $(m/n)|s$.*

Proof. $F(a^{m/n})$ is the splitting field of $x^n - a$ iff $\zeta_n \in F(a^{m/n})$, that is, iff $F(a^{m/n}) \supset F(\zeta_n) = F(a^s)$, and this certainly occurs if $(m/n)|s$. Consider $F(a^{m/n}, \zeta_n)$. This is the splitting field of $x^n - a$. Since $F(a^{m/n}, \zeta_n) \supset F(\zeta_n)$, we have, by Theorem 1, that $F(a^{m/n}, \zeta_n) = F(a^l)$, where $l|s$.

Since $F(a^l)$ is a normal extension and $o(a^l) = m/l$, we have that $\zeta_{m/l} \in F(a^l) \subset F(a)$, thus $(m/l)|n$, hence $(m/n)|l$. However, $l|s$, so $(m/n)|s$. So $F(a^{m/n}) \supset F(a^s) = F(\zeta_n)$.

If $x^m - a$ is irreducible, then since $n|m$, we have that $x^n - a$ is irreducible normal. ∎

COROLLARY 1. *Let $o(a) = m$ over F^*, $F(a) \supset K \supset F$, and K be normal over F, then $K \subset F(a^{m/n}) = F(a^{1/n})$.*

Proof. Since K is normal, we have that $K(\zeta_n)$ is a normal extension of F and $F(a) \supset K(\zeta_n) \supset F(\zeta_n)$, thus by Theorem 1, we have that $K(\zeta_n) = F(a^l)$, where $l|m$. Since $F(a^l)$ is normal over F and $o(a^l) = m/l$, over F^* we have that $\zeta_{m/l} \in F(a)$. Hence $(m/l)|n$, so $(m/n)|l$. Hence $F(a^{m/n}) \supset F(a^l) = K(\zeta_n) \supset K$. ∎

Let us now specialize by setting $F = Q$ and by assuming that $x^m - a$ is irreducible, then we obtain the following interesting result.

THEOREM 5. *Let $x^m - a$ be irreducible over Q and $a^m = a$. Let $l = \max\{i | \zeta_i \in Q(a)\}$, then $l = 6, 12$, or 2^k, $k \geqslant 1$.*

Proof. Let n be defined as in (1), above, then $Q(\zeta_n) \subset Q(\zeta_l) \subset Q(a)$, thus, by Theorem 1, $Q(\zeta_l) = Q(a^r)$, for some r, and hence, we may assume that $Q(\zeta_l) = Q(a)$, thus, every subfield of $Q(a)$ is abelian. Let $p|m$, p a prime. Then $o(a^{m/p}) = p$, $[Q(a^{m/p}):Q] = p$ and $Q(a^{m/p})$ is abelian. From this we obtain that $p = 2$ and thus $m = 2^k$. Further since $Q(a)$ is abelian and $o(a) = 2^k$ we have, by Theorem 3, that $\zeta_{2^k} \in Q(a)$. If $\zeta_{2^{k+1}} \in Q(a)$, then $Q(a) = Q(\zeta_{2^{k+1}})$, so $l = 2^{k+1}$, thus we may assume that $\zeta_{2^{k+1}} \notin Q(a)$. Hence $[Q(\zeta_l) : Q(\zeta_{2^k})] = 2$, so $l = 3 \cdot 2^k$. The binomials, $x^2 + 3$, $x^4 + 36$, show that $l = 6$ and $l = 12$ can occur, and it remains to show that $k \geqslant 3$ is impossible.

We have that $Q(\zeta_l) = Q(a)$, where $l = 3 \cdot 2^k$, a satisfies the irreducible binomial $x^{2^k} - a$ and $x^{2^k} - a$ has abelian Galois group. From [5], we have that $a = -c^{2^{k-1}}$, thus $a = \zeta_{2^{k+1}} c^{1/2}$. Hence $Q(\zeta_{2^{k+1}} c^{1/2}) = Q(\zeta_l) \subset Q(\zeta_{2^{k+1}}, \zeta_3)$, so $c^{1/2} \in Q(\zeta_{2^{k+1}}, \zeta_3)$. Since $k \geqslant 3$, this implies that $c^{1/2} \in Q(\zeta_{2^k}, \zeta_3) = Q(\zeta_l)$ (see [1]). However this implies that $\zeta_{2^{k+1}} \in Q(\zeta_l)$, a contradiction. Thus $k \leqslant 2$. ∎

References

[1] Lisl Gaal, *Classical Galois theory*, Chelsea, New York 1973.

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

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

[4] Serge Lang, *Algebra*, Addison-Wesley Publishing Co., Reading, Mass., 1969.

[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] N. Tschebotaröw, *Grundzüge der Galoisschen Theorie*, P. Noordhoff, Groningen-Djakarta 1950, pp. 301–303.

APPLIED MATHEMATICS DEPARTMENT
SANDIA LABORATORIES
Albuquerque, New Mexico 87115

Received on 16. 9. 1977
and in revised form on 15. 4. 1978 (984)