Structure theorems for radical extensions of fields*

by

MICHAEL J. NORMIS 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 \( \gamma \) of \( x^m - a \) such that \( F(\gamma) \) 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 \( \gamma \neq 0, \gamma' \in F \), and \( x^r - \gamma' \) be irreducible over \( F \). Then \( \gamma' \in F \) iff \( r | r' \).

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

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

---

* This work was supported by the U.S. Energy Research and Development Administration (ERDA), Contract No. AT(39-1)-738. 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 \( \text{char} F = m \).

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) \quad n = \max \{ k: k|m, \zeta_k \in F(a) \}, \text{ where } \zeta_k \text{ denotes a primitive } k\text{-th root of unity} \}.

Set \( s = [F(a): F(\zeta_n)] \).

**Theorem 1.** Let \( o(a) = m \) over \( F \) and \( n, s \) defined as in (1). If \( F(a) \supset K \supset F(\zeta_n) \), with \( l = [F(a):K] \), then \( K = F(a') \) and \( a' - a \) is irreducible over \( K \).

Furthermore, \( s|m \).

**Proof.** Let \( f(x) \) denote the irreducible polynomial that \( a \) satisfies over \( K \). Since \( a^m = a \in F \subset K \), we have that \( f(x)|x^m - a \). Thus, every root of \( f(x) \) is of the form \( \zeta_k^s a \), for some \( s \). Hence, \( f(x) = \prod_{s=1}^{[F(a):K]} (x - \zeta_k^s a) \).
The constant term of \( \zeta_k^s f(x) \) equals \( \zeta_k^s a' \), so \( s = \sum_{s=1}^{[F(a):K]} \zeta_k^s a' \), is an element of \( K \subset F(a) \).

Also \( a' \in F(a) \), thus \( \zeta_k^s a' \in F(a) \), and by the definition of \( n, \zeta_k^s a' \in F(\zeta_n) \subset K \), thus \( a' \in K \).

**Theorem 2.** Let \( F(a) \supset K \supset F(\zeta_n) \), \( t = \min \{ i: i|m \text{ and } a' \in K \} \), \( r = \max \{ i: i|m \text{ and } F(a') \supset K \} \), then \( K = F(\theta, a') \) iff \( s = (s,t) \).

**Proof.** Let us first recall the following elementary result: Let \( L \supset K \) be a field extension and let \( L \supset M_i \supset M_j \) for \( i = 1, 2 \), such that \( M_i M_j = L \) and \( M_i \cap M_j = M \). Then \( N \supset M_i \cap M_j \) defines an injection from the lattice of intermediate fields of \( M_i \) over \( M \) to the lattice of intermediate fields between \( L \) and \( M_i M_j \), which preserves inclusions, intersections and composites.

Set \( M = F(\theta), M_i = K, M_j = F(\zeta_n) \).

Note that \( K \supset F(\zeta_n) \supset M \), so, by Theorem 1, \( [F(\theta):K] = [F(\zeta_n):F(\theta)] \), thus \( F(\theta) \supset K \).

Further, \( F(\zeta_n) \supset K \) and \( F(a') \supset K \), thus \( F(\zeta_n) \supset K \) and \( [F(\zeta_n):F(a')] \), where \( [r,t] \) denotes the lcm of \( r \) and \( t \).

However, \( r \) was maximal with this property, thus \( [r,t] = r \).

Further, \( F(\zeta_n) \supset K \) and \( F(\zeta_n) \supset K \), thus \( F(\zeta_n) \supset K \), and \( K \supset F(\zeta_n) \).

Thus \( F(\theta, a') = K \) iff \( (s,t) = (s,r) \).

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

Recall that \( a^m + 36 \) is irreducible normal and \( Q(a^m) = Q(a) \).

However, \( Q(a^m) \) contains the splitting field of \( a^m + 36 \) and this field is \( Q(a', \zeta_m) = Q(a') \), and \( Q(a') = Q(\zeta_m) = Q(a') \). Now \( Q(a') = Q(a') \) is a conjugate of \( Q(a') \).

Further, \( \max \{ i: i|m \text{ and } a' \in Q(a') \} = 12 \) and \( \max \{ i: i|m \text{ and } Q(a') \} = 4 \), so \( (s,t) = (3,4) \).

**Theorem 3.** Let \( o(a) = m \) over \( F \). If \( F(a) \) is normal over \( F \), then \( \zeta_n \in F(a) \) and \( a^m - a \) is partially normal.

**Proof.**

\[ x^m - a = \prod_{j=1}^{k_1} f_j(x) \times \prod_{j=1}^{k_2} f_j(x), \]

where each \( f_j(x) \) is irreducible over \( F \) and for \( 1 \leq j \leq k_1 \), \( f_j(x) \) has a root in \( F(a) \), while for \( k_1 < j \leq k_2 \), \( f_j(x) \) does not have a root in \( F(a) \). If \( f_j(x) \) has a root in \( F(a) \), then it is of the form \( \zeta_k^s a \).

However, \( a \in F(a) \), hence \( \zeta_k^s a \in F(a) \).

Set \( n = m \).

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

Recall that \( a^m + 36 \) is irreducible normal and \( Q(a^m) = Q(a) \).

However, \( Q(a^m) \) contains the splitting field of \( a^m + 36 \) and this field is \( Q(a', \zeta_m) = Q(a') \), and \( Q(a') = Q(\zeta_m) = Q(a') \). Now \( Q(a') = Q(a') \) is a conjugate of \( Q(a') \).

**Remark 1.** Before continuing we want to make a remark about the notation \( a^{m/k} \).

The symbol \( a^{m/k} \) can denote any of the \( m \) roots of \( a^m - a \).

However, assume that \( k|m \). Then \( F(a^{m/k}) = F(a) \) and \( F(a^{m/k}) = a^{m/k} \).

**Remark 2.** Let \( a^m - a \) be irreducible over \( F \) and \( \zeta_n \in F(a) \), where \( \text{char} F = m \).

Then, \( F(a) \) has cyclic Galois group over \( F \). This theorem gives very precise information as to the subfields of \( F(a) \), namely, if \( n|m \), then \( F(a') \) is the unique subfield of \( F(a) \) of degree \( m \) over \( F \) and for \( s|m, i = 1, 2 \), \( F(a^i) = F(a') \) iff \( l_i | n \).

This is a generalization of this result to the non-normal case. That is, if \( F(a) \)

contains every \( m\text{-th root of unity} \) that is contained in \( F(a) \), then if \( l_i | s \), where \( s = [F(a):F], F(a') \) is the unique subfield of \( F(a) \) of degree \( s \) over \( F \), and if \( l_i | s, i = 1, 2 \), then \( F(a^i) = F(a') \) iff \( l_i | n \).

In the case where \( F(a) \) contains every \( m\text{-th root of unity} \) that is contained in \( F(a) \), Theorem 1 gives very precise information as to the lattice of subfields of \( F(a) \) as pointed out in Remark 2. In general, there are more subfields than just those of the form \( F(a') \).
Theorem 4. Let \( o(a) = m \) over \( F^g \), then \( F(a^{m/n}) \) is the splitting field of \( x^n - a \), that is, \( x^n - a \) is partially normal. If \( x^n - a \) is irreducible, then \( x^n - a \) is irreducible normal. Furthermore, \( (m/n)/a \) is.

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

Since \( F(a^g) \) is a normal extension and \( o(a^g) = m/l \), we have that \( \zeta_m \in F(a^g) \supseteq F(a^g) \), thus \( (m/l)/a \), hence \( (m/n)/a \). However, \( l/a \), so \( (m/n)/a \).

So \( F(a^{m/n}) = F(a^g) = F(\zeta) \).

If \( x^n - a \) is irreducible, then since \( n/m \), we have that \( x^n - a \) is irreducible normal.

Corollary 1. Let \( o(a) = m \) over \( F^g \), \( F(a) = K = F^g \), 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 \( K(\zeta) \) is a normal extension of \( F \) and \( F(a) = K(\zeta) = F(\zeta) \), thus by Theorem 1, we have that \( K(\zeta) = F(a^g) \), where \( l/m \). Since \( F(a^g) \) is normal over \( F \) and \( o(a^g) = m/l \), over \( F^g \) we have that \( \zeta_m \in F(a) \). Hence \( (m/l)/a \), so \( (m/n)/a \). Hence \( F(a^{m/n}) = F(a^g) = K(\zeta) = K \).

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

Theorem 5. Let \( x^n - a \) be irreducible over \( Q \) and \( a^{m/n} = a \). Let \( l = \max \{ j \in Q(a) \} \), then \( l = 6, 12, \) or \( 2^k, k \geq 1 \).

Proof. Let \( n \) be defined as in (1), above, then \( Q(\zeta) = Q(\zeta^k) = Q(a) \), thus, by Theorem 1, \( Q(\zeta) = Q(a^g) \), for some \( r \), and hence, we may assume that \( Q(\zeta) = Q(a) \). Hence, every subfield of \( Q(a) \) is abelian. Let \( p/m \), \( p \) a prime. Then \( o(a^{m/p}) = p \), \( [Q(a^{m/p}): Q^a] = p \) and \( Q(a^{m/p}) \) is abelian. From this we can 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 \( \zeta_{2k} \in Q(a) \). If \( \zeta_{2k+1} \in Q(a) \), then \( Q(a) = Q(\zeta_{2k+1}) \), so \( l = 2^{k+1} \), thus we may assume that \( \zeta_{2k+1} \notin Q(a) \). Hence \( [Q(\zeta): Q(\zeta_{2k+1})] = 2 \), thus \( l = 3 \cdot 2^k \). The binomials \( x^2 + 3 \), \( x^4 + 36 \), show that \( l = 8 \) and \( l = 12 \) can occur, and it remains to show that \( k \geq 3 \) is impossible.

We have that \( Q(\zeta) = Q(a) \), where \( l = 3 \cdot 2^k \), \( a \) satisfies the irreducible binomial \( x^2 - a \) and \( x^2 - a \) has abelian Galois group. From \([5]\), we have that \( a = -\sigma^2 - 1 \) thus \( \sigma = \zeta_{2k+1} \zeta_{2^{k+1}}^2 \). Hence \( Q(\zeta_{2k+1}, \zeta_{2^{k+1}}^2) = Q(\zeta) \) \( = Q(\zeta_{2k+1}, \zeta_{2^{k+1}}) = Q(\zeta) \) \( = Q(\zeta_{2k+1}, \zeta_{2^{k+1}}) = Q(\zeta) \). Since \( k \geq 3 \), this implies that \( \sigma^2 \in Q(\zeta_{2k+1}, \zeta_{2^{k+1}}) = Q(\zeta) \) (see \([1]\)). However this implies that \( \zeta_{2k+1} \notin Q(\zeta) \), a contradiction. Thus \( k \leq 2 \).