

Pacific Journal of Mathematics

ON THE DEGREE OF THE SPLITTING FIELD OF AN IRREDUCIBLE BINOMIAL

DAVID ANDREW GAY AND WILLIAM YSLAS VÉLEZ

ON THE DEGREE OF THE SPLITTING FIELD OF AN IRREDUCIBLE BINOMIAL

DAVID GAY AND WILLIAM YSLAS VÉLEZ

Let $x^m - a$ be irreducible over a field F . We give a new proof of Darbi's formula for the degree of the splitting field of $x^m - a$ and investigate some of its properties. We give a more explicit formula in case the only roots of unity in F are ± 1 .

A formula for the degree of the splitting field of an irreducible binomial over a field F of characteristic 0 was given in 1926 in the following:

THEOREM (Darbi [1]). *Let ζ_m denote a primitive m th-root of unity and let $x^m - a \in F[x]$ be irreducible with root α . Define an integer k as follows:*

$$(1) \quad k = \max \{l : l \mid m \text{ and } \alpha^{m/l} \in F(\zeta_m)\}.$$

Then the degree of the splitting field of $x^m - a$ is $m\phi_F(m)/k$, where $\phi_F(m) = [F(\zeta_m) : F]$.

In §1 of this paper we give a new proof of this theorem which, with an appropriate interpretation of the symbols above, will also be valid when $\text{char } F > 0$. In §2, with the aid of a theorem of Schinzel, we obtain some properties of the number k , defined as in (1). Finally in §3, we will express k explicitly as a function of a and m for a field F of characteristic 0 such that the only roots of unity in F are ± 1 .

1. Proof of Darbi's theorem for arbitrary characteristic. Let $\text{char } F = p > 0$ and let m be a positive integer. Set $m = m_0 p^f$, with $(m_0, p) = 1$ and set $\zeta_m = \zeta_{m_0}$. Thus $\phi_F(m) = \phi_F(m_0)$.

Our first step is to reduce the proof of the general theorem to a proof of the separable case, that is, to the case where $\text{char } F \nmid m$. Indeed, let $\text{char } F = p > 0$ and $x^m - a$ be irreducible over F with root α . The splitting field of $x^m - a$ is $F(\alpha, \zeta_m) = F(\alpha^{p^f}, \alpha^{m_0}, \zeta_{m_0})$, which in turn is the compositum, over F , of $F(\alpha^{p^f}, \zeta_{m_0})$, a separable extension of F , and $F(\alpha^{m_0})$, a purely-inseparable extension. Thus, if Theorem 1 were true for the separable case, $x^{m_0} - a$ (with splitting field $F(\alpha^{p^f}, \zeta_{m_0})$), then we would have:

$$[F(\alpha, \zeta_{m_0}) : F] = p^f (m_0 \phi_F(m_0) / k) = m \phi_F(m) / k.$$

We therefore assume, for the rest of this paper, that $\text{char } F \nmid m$. To complete the proof we will use the following:

LEMMA (Norris and Vélez, [5]). *Let $x^m - a$ be irreducible over F with root α . Let $n = \max \{l : l \mid m \text{ and } \zeta_l \in F(\alpha)\}$ and suppose K is a field such that $F(\zeta_n) \subseteq K \subseteq F(\alpha)$. If $l = [F(\alpha) : K]$, then $K = F(\alpha')$.*

Proof. Let $f(x)$ denote the irreducible polynomial that α satisfies over K . Since $\alpha^m = a \in F \subset K$, we have that $f(x) \mid x^m - a$. 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 $f(x)$, $\prod_{j=1}^l \zeta_m^{i_j} \alpha = \zeta_m^e \alpha^l$, $e = \sum_{j=1}^l i_j$, 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 $l = [F(\alpha) : K]$ and $[F(\alpha) : F(\alpha')] \leq l$, since α satisfies the binomial $x^l - \alpha^l$ over $F(\alpha')$. Hence we must have that $F(\alpha') = K$ and $x^l - \alpha^l$ is irreducible over K .

To complete the proof of Darbi's theorem, let $k' = [F(\zeta_m) \cap F(\alpha) : F]$. It is clear that the order of the splitting field $x^m - a$ is $m\phi_r(m)/k'$. We must show that $k = k'$. Now, by the definition of n in the above lemma, $F(\zeta_n) \subseteq F(\zeta_m) \cap F(\alpha) = K \subseteq F(\alpha)$, and thus, by the lemma, we have that there is an integer l such that $K = F(\alpha')$. Clearly, since $x^m - a$ is irreducible, $[K : F] = m/l = k'$. This proves the theorem since $\alpha^l \in F(\zeta_m)$ and $l = m/k'$.

2. Some properties of the denominator k and $x^k - a$. For irreducible $x^m - a \in F[x]$, let k be defined as in formula (1). Set

$$(2) \quad h = \max \{l : l \mid m \text{ and } x^l - a \text{ has abelian Galois group}\}.$$

Then it is easy to see from the proof of Darbi's theorem that there exist positive integers t_1, t_2 such that

$$(3) \quad h = \phi_r(h)t_1 = kt_2, \text{ where } t_2 \mid t_1.$$

We would like to derive some properties of h, t_1 , and t_2 . For an integer q , let w_q be the number of the q th-roots of unity in F and $\mathcal{P}(q)$ be the set of primes dividing q . Then we have:

THEOREM (Schinzel). *A binomial $x^m - a \in F[x]$ has abelian Galois group iff $a^{w_m} = c^m$, for some $c \in F$.*

Proof. See [6] or [7] for a proof.

From this we obtain

PROPOSITION 1. (A) *Let $x^m - a$ be irreducible with abelian*

Galois group. Then $x^m - a$ is normal and, if p is a prime and $p|m$, then $\zeta_p \in F$, that is, $p(m) \subseteq p(w_m)$. Moreover $\phi_F(m) | m$.

(B) *Let $x^m - a$ be irreducible and h, t_1 defined as in (2) and (3). Then $p(h) \subseteq p(w_h)$ and $t_1 | w_h$.*

Proof. (A) Suppose p prime, $p|m$ and $\zeta_p \notin F$. Then $p \nmid w_m$. However, by Schinzel's theorem, $a^{w_m} = b^m$ for some $b \in F$. Thus $a = c^p$ for some $c \in F$. Consequently $x^m - a$ is reducible. This contradiction implies $\zeta_p \in F$.

To complete the proof, since $x^m - a$ is irreducible and normal, $F(\alpha)$ is the splitting field of $x^m - a$, for any root α of $x^m - a$. Thus $\zeta_m \in F(\alpha)$, so $F(\zeta_m) \subset F(\alpha)$ and $\phi_F(m) | m$.

(B) In view of (A), all we need to show is that $t_1 | w_h$. To do this, let β be a root of $x^h - a$. Then $t_1 = [F(\beta) : F(\zeta_h)]$. Thus, $F(\beta^{t_1}) = F(\zeta_h)$ by the lemma. Since $x^{t_1} - \beta^{t_1}$ is irreducible over $F(\zeta_h)$, we have that $\beta^{t_1} \in F(\zeta_h)$ iff $t_1 | l$. However, by Schinzel's theorem we have $a^{w_h} = c^h$ (for some $c \in F$), so that $\beta = \zeta_h^i \zeta_{hw_h}^j c^{1/h}$, for some i, j . Thus $\beta^{w_h} = \zeta_h^{i w_h} \zeta_h^j c \in F(\zeta_h)$, and consequently $t_1 | w_h$.

3. Applications. In this section let F denote a field with the following two properties: (a) $\text{char } F = 0$, and (b) if $\zeta_m \in F$, then $\zeta_m = \pm 1$. Clearly real fields satisfy properties (a) and (b). Furthermore, $w_m = 1$ if m is odd and $w_m = 2$ if m is even.

PROPOSITION 2. (A) *The irreducible, normal binomials in $F[x]$ with abelian Galois groups are:*

(i) $x - c$

(ii) $x^2 - c, \sqrt{c} \notin F$

(iii) $x^4 + c^2, c^2 \neq 4d^4, d \in F$

(iv) $x^{2^h} + c^{2^{h-1}}, h \geq 3, \sqrt{2} \notin F, c \neq 0$.

(B) *Relative to the irreducible binomial $x^m - a \in F[x]$,*

(i) $h = \max \{2^q : 2^q | m \text{ and } -a = c^{2^{q-1}}, c \in F\}$.

(ii) $t_1 = \begin{cases} 1, & \text{if } h = 1. \\ 2, & \text{if } h > 1. \end{cases}$

(iii) $k = \begin{cases} h, & \text{if } h = 1 \text{ or } h = 2^q, -a = c^{2^{q-1}} \text{ and } \zeta_{2^{q+1}} \sqrt{c} \in F(\zeta_m). \\ h/2, & \text{otherwise.} \end{cases}$

In particular, k is a power of 2. If $\sqrt{2} \notin F$, then any power of 2 is possible. If $\sqrt{2} \in F$, then $k = 1, 2$, or 4.

Proof. (A) If $x^m - a$ is irreducible, normal, and abelian, then by Proposition 2, we have that $m = 2^q$, for some $q \geq 0$. Schinzel's theorem then implies $a^2 = c^{2^q}$, for some $c \in F$. Thus, if $q \geq 1$, $a = \pm c^{2^{q-1}}$. The rest follows by Cappelli's theorem for irreducible

binomials ([4], p. 62).

Conversely, it is easy to check that the binomials (i)—(iv) are irreducible, normal, with abelian Galois group.

(B) Statement (i) follows from (A).

To prove (ii), note first that by Proposition 2, $t_1 | w_{2^q}$. Thus $t_1 = 1$ or 2 . If $h = 1$, then clearly $t_1 = 1$. Assume that $h > 1$. Recall that $t_1 = [F(\beta) : F(\zeta_{2^q})]$, where β is a root of $x^{2^q} + c^{2^{q-1}}$. If $h = 2$, then since $[F(\zeta_4) : F] = 2$, we must have that $t_1 = 2$. If $q > 2$, then by (A) we have that $\sqrt{2} \notin F$. Hence $[F(\zeta_{2^q}) : F] = 2^{q-1}$, and thus $t_1 = 2$.

Finally, to prove (iii), we note that $t_2 | t_1$ and by (ii), $t_1 = 1$ or 2 , so $t_2 = 1$ or 2 . Furthermore, if $h = 2^q (q \geq 1)$ then $t_2 = 1$ iff the splitting field of $x^{2^q} + c^{2^{q-1}}$ is contained in $F(\zeta_m)$ iff $\zeta_{2^{q+1}} \sqrt{c} \in F(\zeta_m)$.

Thus, if the h of formula (2) has been determined, then

$$k = \begin{cases} h, & \text{if } h = 1 \text{ or } \sqrt{c} \in F(\zeta_{2m}) \\ h/2, & \text{otherwise.} \end{cases}$$

If $m = 2^l \cdot p_1^{a_1} \cdots p_q^{a_q}$, with $l \geq 1$ and p_1, \dots, p_q distinct odd primes, then the condition $\sqrt{c} \in F(\zeta_{2m})$ is equivalent to the condition $\sqrt{c} \in F(\zeta_{2^{l+1}P})$, where $P = p_1 \cdots p_q$. For $F = \mathbb{Q}$, the latter is equivalent to $\sqrt{c} \in \mathbb{Q}(\zeta_{2^a P})$, where $a = \min\{3, l+1\}$. For an arbitrary real field however, we cannot do as well. Indeed, given any integer $q \geq 3$, there exists an integer m with $2^q || m$, a real field F and $c \in F$ such that $\sqrt{c} \notin F(\zeta_{2m})$, yet $\sqrt{c} \in F(\zeta_m)$. (See [2], 5.4.)

Proposition 2 generalizes a theorem of Hooley ([3], pp. 212-214).

REFERENCES

1. G. Darbi, *Sulla riducibilità delle equazioni algebriche*, Annali di Mat. pur e Appl., Ser. 4, **4** (1926), 185-208.
2. D. Gay, *On normal radical extensions of real field*, to appear, Acta Arithmetica, **35** (1978).
3. C. Hooley, *On Artin's conjecture*, J. für Mathematik, Band **225**, (1967), 209-220.
4. I. Kaplansky, *Fields and Rings*, Univ. of Chicago Press, 1969.
5. M. J. Norris and W. Y. Vélez, *Structure theorems for radical extensions of fields*, to appear, Acta Arithmetica.
6. A. Schinzel, *Abelian binomials, power residues, and exponential congruences*, Acta Arithmetica, **32** (1976/1977), 245-274.
7. W. Y. Vélez, *On Normal Binomials*, to appear, Acta Arithmetica.

Received September 16, 1977 and in revised form March 10, 1978. Supported in part by Battelle Institute and Fonds National Suisse.

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

RICHARD ARENS (Managing Editor)

University of California
Los Angeles, California 90024

C. W. CURTIS

University of Oregon
Eugene, OR 97403

C. C. MOORE

University of California
Berkeley, CA 94720

J. DUGUNDJI

Department of Mathematics
University of Southern California
Los Angeles, California 90007

R. FINN AND J. MILGRAM

Stanford University
Stanford, California 94305

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA, RENO
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON

UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF HAWAII
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON

Simeon M. Berman, <i>A class of isotropic distributions in \mathbf{R}^n and their characteristic functions</i>	1
Ezra Brown and Charles John Parry, <i>The 2-class group of biquadratic fields. II</i>	11
Thomas E. Cecil and Patrick J. Ryan, <i>Focal sets of submanifolds</i>	27
Joseph A. Cima and James Warren Roberts, <i>Denting points in B^p</i>	41
Thomas W. Cusick, <i>Integer multiples of periodic continued fractions</i>	47
Robert D. Davis, <i>The factors of the ramification sequence of a class of wildly ramified v-rings</i>	61
Robert Martin Ephraim, <i>Multiplicative linear functionals of Stein algebras</i>	89
Philip Joel Feinsilver, <i>Operator calculus</i>	95
David Andrew Gay and William Yslas Vélez, <i>On the degree of the splitting field of an irreducible binomial</i>	117
Robert William Gilmer, Jr. and William James Heinzer, <i>On the divisors of monic polynomials over a commutative ring</i>	121
Robert E. Hartwig, <i>Schur's theorem and the Drazin inverse</i>	133
Hugh M. Hilden, <i>Embeddings and branched covering spaces for three and four dimensional manifolds</i>	139
Carlos Moreno, <i>The Petersson inner product and the residue of an Euler product</i>	149
Christopher Lloyd Morgan, <i>On relations for representations of finite groups</i>	157
Ira J. Papick, <i>Finite type extensions and coherence</i>	161
R. Michael Range, <i>The Carathéodory metric and holomorphic maps on a class of weakly pseudoconvex domains</i>	173
Donald Michael Redmond, <i>Mean value theorems for a class of Dirichlet series</i>	191
Daniel Reich, <i>Partitioning integers using a finitely generated semigroup</i>	233
Georg Johann Rieger, <i>Remark on a paper of Stux concerning squarefree numbers in non-linear sequences</i>	241
Gerhard Rosenberger, <i>Alternierende Produkte in freien Gruppen</i>	243
Ryōtarō Satō, <i>Contraction semigroups in Lebesgue space</i>	251
Tord Sjödin, <i>Capacities of compact sets in linear subspaces of \mathbf{R}^n</i>	261
Robert Jeffrey Zimmer, <i>Uniform subgroups and ergodic actions of exponential Lie groups</i>	267