Hindawi Publishing Corporation
International Journal of Mathematics and Mathematical Sciences
Volume 2007, Article ID 89713, 8 pages
doi:10.1155/2007/89713

Research Article

On the Common Index Divisors of a Dihedral Field of Prime Degree

Blair K. Spearman, Kenneth S. Williams, and Qiduan Yang

Received 11 September 2006; Revised 6 January 2007; Accepted 6 January 2007

Recommended by Dihua Jiang

A criterion for a prime to be a common index divisor of a dihedral field of prime degree is given. This criterion is used to determine the index of families of dihedral fields of degrees 5 and 7.

1. Introduction

Let L be an algebraic number field of degree n. Let O_L denote the ring of integers of L. The element $\alpha \in O_L$ is called a generator of L if $L = \mathbb{Q}(\alpha)$. The index of α is the positive integer $\operatorname{ind}\alpha$ given by

$$D(\alpha) = (\operatorname{ind}\alpha)^2 d(L), \tag{1.1}$$

where $d(L)$ is the discriminant of L and $D(\alpha)$ is the discriminant of the minimial polynomial of α. The index of L is

$$i(L) = \gcd\{\operatorname{ind}\alpha \mid \alpha \text{ is a generator of } L\}. \tag{1.2}$$

A positive integer > 1 dividing $i(L)$ is called a common index divisor of L. If O_L possesses an element β such that $\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$ is an integral basis for L, then L is said to be monogenic. If L is monogenic, then $i(L) = 1$. Thus a field possessing a common index divisor is nonmonogenic.

Let $f(x)$ be an irreducible polynomial in $\mathbb{Z}[x]$ of odd prime degree q and suppose that $\operatorname{Gal}(f(x)) \simeq D_q$ (the dihedral group of order $2q$). We note that $D_q = \langle \sigma, \tau \rangle$ with $\sigma^q = \tau^2 = (\sigma\tau)^2 = 1$. Let M be the splitting field of $f(x)$. Let θ be a root of $f(x)$ and set

$L = \mathbb{Q}(\theta)$ so that the degree of L over $\mathbb{Q}$ is equal to q. We denote the unique quadratic subfield of M by K.

We prove in Section 2 the following theorem which gives a criterion for a prime p to be a common index divisor of L.

Theorem 1.1. *Let $f(x) \in \mathbb{Z}[x]$ be irreducible, $\deg(f(x)) = q$ (an odd prime), and $\mathrm{Gal}(f(x)) \simeq D_q$. Let M be the splitting field of $f(x)$. Let $\theta \in \mathbb{C}$ be a root of $f(x)$. Set $L = \mathbb{Q}(\theta)$ so that $[L:\mathbb{Q}] = q$. Let K be the unique quadratic subfield of M. If p is a prime satisfying*

$$p < \frac{1}{2}(q+1), \quad p \mid d(K), \tag{1.3}$$

then

$$p = R_1 R_2^2 \cdots R_{(q+1)/2}^2 \tag{1.4}$$

for distinct prime ideals $R_1, R_2, \ldots, R_{(q+1)/2}$ of O_L, and p is a common index divisor of L.

As an application of Theorem 1.1, we determine in Section 3 the index of a field defined by a dihedral quintic trinomial of the form $x^5 + ax + b$, $a, b \in \mathbb{Z}$.

In Section 4, we determine the index of an infinite family of fields defined by dihedral polynomials of degree 7.

Finally in Section 5, we consider a dihedral field of degree 11 and use Theorem 1.1 to show that it is nonmonogenic.

We note that a method for calculating a generator of K, and hence $d(K)$, directly from $f(x)$ is given in [1].

2. Proof of Theorem 1.1

As $p \mid d(K)$, we have $p = \wp^2$ for some prime ideal $\wp$ of O_K. Suppose that $\wp$ is inert in M/K. Then $p = \wp^2$ in $M/\mathbb{Q}$. This contradicts [2, Theorem 10.1.26, part (6)]. Hence $\wp$ is not inert in M/K. Suppose $\wp$ totally ramifies in M/K. Then $\wp = Q^q$ for some prime ideal Q of M. Thus $p = \wp^2 = Q^{2q}$ in M. Hence, by [2, Theorem 10.1.26, part (9)], we have $p \mid q$. But p and q are primes so $p = q$. This contradicts the assumption $p < (1/2)(q+1)$. Hence $\wp$ does not totally ramify in M. Then, as M is normal over K of prime degree q, we have

$$\wp = Q_1 Q_2 \cdots Q_q \tag{2.1}$$

for distinct prime ideals $Q_1, Q_2, \ldots, Q_q$ of M. Thus

$$p = \wp^2 = Q_1^2 Q_2^2 \cdots Q_q^2. \tag{2.2}$$

Hence, by [2, Theorem 10.1.26, part (6)], we have

$$p = R_1 R_2^2 \cdots R_{(q+1)/2}^2 \tag{2.3}$$

for distinct prime ideals $R_1, R_2, \ldots, R_{(q+1)/2}$ of L, which is (1.4). We note that the decomposition of p in L can be checked directly by studying the $\mathrm{Gal}(M/L)$ action on the coset space D_q/D, where D is a decomposition subgroup at p.

Let $g(x)$ be any defining polynomial for L, so that $\deg(g(x)) = q$. Let ϕ be a root of $g(x)$ such that $\mathbb{Q}(\phi) = L$. Suppose $p \nmid \operatorname{ind}(\phi)$. The inertial degree $f = 1$ in the extension $M/\mathbb{Q}$ (using the tower $M/K/\mathbb{Q}$), hence in $L/\mathbb{Q}$, so that all the irreducible factors of $g(x)$ modulo p are linear. Thus $g(x)$ has at most p irreducible factors modulo p. Hence, by Dedekind's theorem, p factors into at most p prime ideals in L. Thus by (1.4) we have $(1/2)(q+1) \leq p$. This contradicts $p < (1/2)(q+1)$. Hence $p \mid \operatorname{ind}(\phi)$ for all defining polynomials g. Thus p is a common index divisor of L.

3. Dihedral quintic trinomials

Let $f(x) = x^5 + ax + b \in \mathbb{Z}[x]$ have Galois group D_5. Then there exist coprime integers m and n and $i, j \in \{0,1\}$ such that

$$\begin{aligned} a &= 2^{2-4i}5^{1-4j}d_2(m^2 - mn - n^2)E^2F, \\ b &= 2^{4-5i}5^{-5j}d_1(2m-n)(m+2n)E^3F, \end{aligned} \tag{3.1}$$

where d_1^2 is the largest square dividing m^2+n^2, d_2^5 is the largest fifth power dividing $m^2 + mn - n^2$, and

$$E = \frac{m^2+n^2}{d_1^2}, \qquad F = \frac{m^2+mn-n^2}{d_2^5}. \tag{3.2}$$

This result is due to Roland et al. [3, page 138], see also [4, page 139]. The discriminant of x^5+ax+b is

$$D(f) = 2^{16-20i}5^{6-20j}\left(2m^6+4m^5n+5m^4n^2-5m^2n^4+4mn^5-2n^6\right)^2E^{10}F^4, \tag{3.3}$$

see [3, equation (3), page 139]. As $\gcd(m,n) = 1$, we have $3 \nmid m^2+n^2$ and $3 \nmid m^2+mn-n^2$ so $3 \nmid E$ and $3 \nmid F$. If $3 \mid n$, then $3 \nmid m$, and so $3 \nmid 2m^6+4m^5n+5m^4n^2-5m^2n^4+4mn^5-2n^6$. If $3 \nmid n$, then as the polynomial $2x^6+4x^5+5x^4-5x^2+4x-2$ is irreducible $(\bmod 3)$, we deduce that $3 \nmid 2m^6+4m^5n+5m^4n^2-5m^2n^4+4mn^5-2n^6$. Hence $3 \nmid D(f)$. Thus $3 \nmid \operatorname{ind}(\theta)$, where $L = \mathbb{Q}(\theta)$, $f(\theta) = 0$. Hence $3 \nmid i(L)$. By Engstrom [5, page 234] as $[L:\mathbb{Q}] = 5$, the only primes that can divide $i(L)$ are 2 and 3. We use our theorem to show that $2 \mid i(L)$. From Spearman and Williams [4, pages 149, 150], the discriminant $d(K)$ of the unique quadratic subfield of the splitting field of $f(x)$ satisfies

$$\begin{aligned} &2^2 \,\|\, d(K) \quad \text{if } m \equiv n+1 \pmod 2, \\ &2^3 \,\|\, d(K) \quad \text{if } m \equiv n \equiv 1 \pmod 2. \end{aligned} \tag{3.4}$$

Thus $2 \mid d(K)$. Hence, by Theorem 1.1, 2 is a common index divisor of L. From Engstrom [5, Table, page 234], as $2 = R_1R_2^2R_3^2$ by Theorem 1.1, we deduce, $i(L) = 2$. As $i(L) \neq 1$, this gives an infinite family of nonmonogenic dihedral quintic fields. In [6], an infinite family of monogenic dihedral quintic fields was exhibited.

4. A class of dihedral polynomials of degree 7

We recall a family of polynomials of degree 7 due to Smith [7, page 790]. This family is $f_t(x)$ $(t \in \mathbb{Z})$, where $f_t(x)$ is given by

$$\begin{aligned} f_t(x) = x^7 - (7t^3+35t^2+21t+1)\big[&21x^5+(98t+70)x^4 \\ &-(1029t^3+4557t^2+343t-105)x^3 \\ &-28(7t+1)(49t^3+147t^2+63t-3)x^2 \\ &+7(7t^2+42t-1)(7t^2+14t-5)(7t+1)^2x \\ &+235298t^7+1236858t^6+1138074t^5 \\ &+562226t^4+11270t^3-4914t^2-322t+6\big]. \end{aligned} \tag{4.1}$$

Smith showed that the Galois group of $f_t(x)$ over $\mathbb{Q}(t)$ is D_7. We are interested in determining integers t for which the Galois group of $f_t(x)$ (considered as a polynomial in $\mathbb{Z}[x]$) over $\mathbb{Q}$ is D_7. MAPLE gives the discriminant of $f_t(x)$ as

$$\begin{aligned} D(f_t) &= 2^{46}7^{12}t^{15}(7t^2-14t-9)^6(7t^3+35t^2+21t+1)^6 \\ &\quad\times(63t^2+266t-25)^2(49t^4-196t^3-1694t^2-140t-3)^2. \end{aligned} \tag{4.2}$$

Lemma 4.1. (i) *If* $t \equiv 1 \pmod 3$, *then* $3 \nmid D(f_t)$.
(ii) *If* $t \equiv 1, 2$ *or* $4 \pmod 5$, *then* $5 \nmid D(f_t)$.

The proof follows from (4.2).

Lemma 4.2. *If* $t \in \mathbb{Z}$ *is such that*

$$2 \mid t, \quad 7t^3+35t^2+21t+1 \text{ is square-free } > 1, \tag{4.3}$$

then $f_t(x)$ *is irreducible over* $\mathbb{Q}$.

Proof. Set $a(t) = 7t^3+35t^2+21t+1$ and $b(t) = -235298t^7 - 1236858t^6 - 1138074t^5 - 562226t^4 - 11270t^3 + 4914t^2 + 322t - 6$. Then, from (4.1), we see that

$$f_t(x) \equiv x^7 \pmod{a(t)}, \tag{4.4}$$

$$f_t(0) = a(t)b(t). \tag{4.5}$$

The resultant of $a(t)$ and $b(t)$ as polynomials in t is (by MAPLE) $2^{45}7^7$. Clearly $7 \nmid a(t)$ and (as $2 \mid t$) $2 \nmid a(t)$. Thus $\gcd_{\mathbb{Z}}(a(t), b(t)) = 1$. Let q be any prime dividing $a(t)$ (so $q \neq 2, 7$). Then $q \| a(t)$ and $q \nmid b(t)$. Thus, by (4.1) and (4.4), q divides the coefficients of x^i $(i = 0,1,2,3,4,5,6)$ in $f_t(x)$ and by (4.5) $q \| f_t(0)$. Hence, by Eisenstein's criterion, $f_t(x)$ is irreducible over $\mathbb{Q}$. □

Let θ denote one of the roots of $f_t(x)$. Let $\alpha_1 = \theta, \alpha_2, \ldots, \alpha_7$ be all the roots of $f_t(x)$. Set $L = \mathbb{Q}(\theta)$. Under condition (4.3), we have $[L:\mathbb{Q}] = 7$.

Lemma 4.3. *For $t \in \mathbb{Z}$, set*

$$P_{f_t}(x) = \prod_{1\le i<j\le 7} (x - (\alpha_i + \alpha_j)). \tag{4.6}$$

Then $P_{f_t}(x) \in \mathbb{Z}[x]$ and

$$P_{f_t}(x) = F_t(x)G_t(x)H_t(x), \tag{4.7}$$

where $F_t(x)$, $G_t(x)$, and $H_t(x)$ are distinct polynomials of degree 7 in $\mathbb{Z}[x]$, which satisfy

$$\begin{gathered} F_t(x) \equiv G_t(x) \equiv H_t(x) \equiv x^7 \,(\bmod\, a(t)), \\ F_t(0) = -32a(t)c(t), \\ G_t(0) = -32a(t)d(t), \\ H_t(0) = 32a(t)e(t), \end{gathered} \tag{4.8}$$

where

$$\begin{aligned} c(t) &= 27783t^6 + 43218t^5 - 300615t^4 + 131516t^3 + 17241t^2 - 14t - 25, \\ d(t) &= 8575t^6 - 52822t^5 + 34153t^4 + 27244t^3 + 2737t^2 - 406t - 25, \\ e(t) &= 1029t^6 - 4802t^5 - 9457t^4 - 5292t^3 - 973t^2 + 14t + 25. \end{aligned} \tag{4.9}$$

Proof. The assertion $P_{f_t}(x) \in \mathbb{Z}[x]$ follows from [8, Lemma 11.1.3, page 359] and the fact that $\alpha_1, \alpha_2, \ldots, \alpha_7$ are algebraic integers. The remaining assertions of the lemma can be verified using MAPLE. □

Lemma 4.4. *If $t \in \mathbb{Z}$ is such that*

$$2 \mid t, \quad 7t^3 + 35t^2 + 21t + 1 \text{ is square-free} > 1 \tag{4.10}$$

then the polynomials $F_t(x)$, $G_t(x)$, and $H_t(x)$ are irreducible over $\mathbb{Q}$.

Proof. The resultants of $a(t)$ and $c(t)$ (resp., $a(t)$ and $d(t)$, $a(t)$ and $e(t)$) regarded as polynomials in t are by MAPLE $-2^{30}7^6$ (resp., $-2^{30}7^6$, $2^{30}7^6$). Exactly as in the proof of Lemma 4.2, making use of Lemma 4.3, we find by Eisenstein's criterion that the polynomials $F_t(x)$, $G_t(x)$, and $H_t(x)$ are irreducible over $\mathbb{Q}$. □

Lemma 4.5. *If $t \in \mathbb{Z}$ is such that*

$$2 \mid t, \quad 7t^3+35t^2+21t+1 \text{ is square-free } > 1, \\ t \text{ is not a perfect square,} \tag{4.11}$$

then

$$\operatorname{Gal}\left(f_t(x)\right) \simeq D_7. \tag{4.12}$$

Proof. Jensen and Yui [8, Theorem II.1.2, page 359] have shown that a monic polynomial $f(x) \in \mathbb{Q}[x]$ of degree p, where p is a prime $\equiv 3 \pmod 4$, has $\operatorname{Gal}(f) \simeq D_p$ if and only if

(i) $f(x)$ is irreducible over $\mathbb{Q}$,

(ii) $D(f)$ is not a perfect square,

(iii) $P_f(x)$ factors as a product of $(p-1)/2$ distinct irreducible polynomials of degree p over $\mathbb{Q}$.

By Lemma 4.2, $f_t(x)$ is irreducible over $\mathbb{Q}$. As t is not a perfect square, we see by (4.2) that $D(f_t)$ is not a perfect square. Finally, by Lemmas 4.3 and 4.4, $P_{f_t}(x)$ factors as a product of 3 distinct irreducible polynomials of degree 7 over $\mathbb{Q}$. Hence, by the Jensen-Yui criterion, $\operatorname{Gal}(f_t(x)) \simeq D_7$. □

Theorem 4.6. (i) *There exist infinitely many integers t satisfying*

$$2 \| t, \quad t \equiv 1 \pmod 3, \quad t \equiv 1, 2 \text{ or } 4 \pmod 5, \\ 7t^3+35t^2+21t+1 \text{ is square-free} > 1, \tag{4.13}$$

and for these values of t,

$$i(L) = 2^4. \tag{4.14}$$

(ii) *There exist infinitely many integers t satisfying*

$$2 \| t,\ 3 \| t, \quad t \equiv 1, 2 \text{ or } 4 \pmod 5, \\ 7t^3+35t^2+21t+1 \text{ is square-free} > 1. \tag{4.15}$$

and for these values of t,

$$i(L) = 2^4 3. \tag{4.16}$$

Proof. The infinitude of integers of the required forms follows from a result of Erdös [9].

Under conditions (4.13) and (4.15), L is a dihedral field of degree 7, by Lemma 4.5. With the notation of Theorem 1.1, we see from (4.2) that $K = \mathbb{Q}(\sqrt{t})$. Clearly $2 \mid d(K)$. By Theorem 1.1, 2 is a common index divisor of L. Also from Theorem 1.1, we see that $2 = R_1 R_2^2 R_3^2 R_4^2$ for distinct prime ideals R_1, R_2, R_3, R_4 of L. Hence, by Engstrom [5, Table, page 235], we see that $2^4 \| i(L)$. For both (4.13) and (4.15) we have by Lemma 4.1(ii) $5 \nmid D(f_t)$

so $5 \nmid i(L)$. For (4.13) by Lemma 4.1(i) we have $3 \nmid D(f_t)$, so $3 \nmid i(L)$. As $[L : \mathbb{Q}] = 7$, by [5, page 224], the only possible prime divisors of $i(L)$ are 2, 3, and 5. Hence $i(L) = 2^4$ in case (i). For case (ii), by Theorem 1.1, 3 is a common index divisor of L. Also, by Theorem 1.1, we see that $3 = R_1 R_2^2 R_3^2 R_4^2$ for distinct prime ideals R_1, R_2, R_3, R_4 of L. Hence, by Engstrom [5, Table, page 235], we see that $3 \| i(L)$. Finally, as the only possible prime divisors of $i(L)$ are 2, 3, and 5, we deduce that $i(L) = 2^4 3$ in case (ii). □

5. A dihedral field of degree 11

Let

$$\begin{aligned} f(x) = x^{11} - 2x^{10} - 51x^9 - x^8 + 536x^7 \\ + 3x^6 - 1999x^5 + 281x^4 + 2571x^3 \\ - 485x^2 - 680x + 69. \end{aligned} \tag{5.1}$$

By MAPLE, $f(x)$ is irreducible over $\mathbb{Q}$. Let θ be a root of $f(x)$ and set $L = \mathbb{Q}(\theta)$, so that $[L : \mathbb{Q}] = 11$. Let M be the splitting field of $f(x)$. It is known that M is the Hilbert class field of $K = \mathbb{Q}(\sqrt{10401})$ [10] so that L is a dihedral extension of $\mathbb{Q}$. By Theorem 1.1, 3 is a common index divisor of L, hence L is not monogenic.

Acknowledgments

The research of the first and second authors was supported by grants from the Natural Sciences and Engineering Research Council of Canada.

References

[1] B. K. Spearman, K. S. Williams, and Q. Yang, "The 2-power degree subfields of the splitting fields of polynomials with Frobenius Galois groups," *Communications in Algebra*, vol. 31, no. 10, pp. 4745–4763, 2003.

[2] H. Cohen, *Advanced Topics in Computational Number Theory*, vol. 193 of *Graduate Texts in Mathematics*, Springer, New York, NY, USA, 2000.

[3] G. Roland, N. Yui, and D. Zagier, "A parametric family of quintic polynomials with Galois group D_5," *Journal of Number Theory*, vol. 15, no. 1, pp. 137–142, 1982.

[4] B. K. Spearman and K. S. Williams, "The discriminant of a dihedral quintic field defined by a trinomial $X^5 + aX + b$," *Canadian Mathematical Bulletin*, vol. 45, no. 1, pp. 138–153, 2002.

[5] H. T. Engstrom, "On the common index divisors of an algebraic field," *Transactions of the American Mathematical Society*, vol. 32, no. 2, pp. 223–237, 1930.

[6] M. J. Lavallee, B. K. Spearman, K. S. Williams, and Q. Yang, "Dihedral quintic fields with a power basis," *Mathematical Journal of Okayama University*, vol. 47, pp. 75–79, 2005.

[7] G. W. Smith, "Some polynomials over $\mathbb{Q}(t)$ and their Galois groups," *Mathematics of Computation*, vol. 69, no. 230, pp. 775–796, 2000.

[8] C. U. Jensen and N. Yui, "Polynomials with D_p as Galois group," *Journal of Number Theory*, vol. 15, no. 3, pp. 347–375, 1982.

[9] P. Erdös, "Arithmetical properties of polynomials," *Journal of the London Mathematical Society. Second Series*, vol. 28, pp. 416–425, 1953.

[10] http://math.univ-lyon1.fr/~roblot/resources/hilb.gp.

Blair K. Spearman: Department of Mathematics and Statistics, University of British Columbia Okanagan, Kelowna, BC, Canada V1V 1V7
Email address: blair.spearman@ubc.ca

Kenneth S. Williams: School of Mathematics and Statistics, Carleton University, Ottawa, ON, Canada K1S 5B6
Email address: kwilliam@connect.carleton.ca

Qiduan Yang: Department of Mathematics and Statistics, University of British Columbia Okanagan, Kelowna, BC, Canada V1V 1V7
Email address: qiduan.yang@ubc.ca

Special Issue on
Modeling Experimental Nonlinear Dynamics and Chaotic Scenarios

Call for Papers

Thinking about nonlinearity in engineering areas, up to the 70s, was focused on intentionally built nonlinear parts in order to improve the operational characteristics of a device or system. Keying, saturation, hysteretic phenomena, and dead zones were added to existing devices increasing their behavior diversity and precision. In this context, an intrinsic nonlinearity was treated just as a linear approximation, around equilibrium points.

Inspired on the rediscovering of the richness of nonlinear and chaotic phenomena, engineers started using analytical tools from "Qualitative Theory of Differential Equations," allowing more precise analysis and synthesis, in order to produce new vital products and services. Bifurcation theory, dynamical systems and chaos started to be part of the mandatory set of tools for design engineers.

This proposed special edition of the *Mathematical Problems in Engineering* aims to provide a picture of the importance of the bifurcation theory, relating it with nonlinear and chaotic dynamics for natural and engineered systems. Ideas of how this dynamics can be captured through precisely tailored real and numerical experiments and understanding by the combination of specific tools that associate dynamical system theory and geometric tools in a very clever, sophisticated, and at the same time simple and unique analytical environment are the subject of this issue, allowing new methods to design high-precision devices and equipment.

Authors should follow the Mathematical Problems in Engineering manuscript format described at http://www.hindawi.com/journals/mpe/. Prospective authors should submit an electronic copy of their complete manuscript through the journal Manuscript Tracking System at http://mts.hindawi.com/ according to the following timetable:

Manuscript Due	December 1, 2008
First Round of Reviews	March 1, 2009
Publication Date	June 1, 2009

Guest Editors

José Roberto Castilho Piqueira, Telecommunication and Control Engineering Department, Polytechnic School, The University of São Paulo, 05508-970 São Paulo, Brazil; piqueira@lac.usp.br

Elbert E. Neher Macau, Laboratório Associado de Matemática Aplicada e Computação (LAC), Instituto Nacional de Pesquisas Espaciais (INPE), São Josè dos Campos, 12227-010 São Paulo, Brazil ; elbert@lac.inpe.br

Celso Grebogi, Center for Applied Dynamics Research, King's College, University of Aberdeen, Aberdeen AB24 3UE, UK; grebogi@abdn.ac.uk