Math. J. Okayama Univ. **56** (2014), 27–33

INTERSECTIVE POLYNOMIALS WITH GALOIS GROUP D_5

Melisa J. Lavallee, Blair K. Spearman and Qiduan Yang

Abstract. We give an infinite family of intersective polynomials with Galois group D_5, the dihedral group of order 10.

1. Introduction

A monic polynomial $f(x)$ with integer coefficients is called intersective if it has a root modulo m for all positive integers m. Equivalently $f(x)$ has a root in the field of p-adic numbers $\mathbb{Q}_p$ for all primes p. We call $f(x)$ nontrivially intersective if it is intersective but has no rational root. Henceforth in this paper our polynomials are nontrivially intersective. It is known that $f(x)$ cannot be irreducible over $\mathbb{Q}$. In fact if $f(x)$ is irreducible over $\mathbb{Q}$, then there exist prime numbers p for which the congruence $f(x) \equiv 0 (\text{mod } p)$ cannot be solved in $\mathbb{Z}$ as shown by Brandl, Bubboloni and Hupp [3, Propostion 1.2]. The existence of intersective polynomials depends on properties of the Galois group. Let L denote the splitting field of $f(x)$ and $Gal(f)$ denote the Galois group of $f(x)$. Behrend and Bilu [2] gave a simple condition to decide whether or not a polynomial is intersective. Sonn [11] gave a condition for $f(x)$ to be intersective as well as a method for constructing such polynomials. To apply this method it suffices to check that $Gal(f)$ is n-coverable for some $n > 0$, that is $Gal(f)$ is the union of conjugates of n proper subgroups, the intersection of all the conjugates is trivial, and every decomposition group $G(\mathfrak{p})$ for $\mathfrak{p}$ a prime ideal in L is contained in a conjugate of one of these proper subgroups. We recall that the decomposition group $G(\mathfrak{p})$ is the set of elements $\sigma \in Gal(f)$ such that $\sigma(\mathfrak{p}) = \mathfrak{p}$. This condition clearly holds if $Gal(f)$ is n-coverable and every decomposition group is cyclic. Having checked this condition, it remains to determine a set of n monic polynomials with integer coefficients, defining those subfields of L corresponding to the n chosen proper subgroups. The product of these polynomials will be intersective. Examples of intersective polynomials in general seem to be scarce. A single example of an intersective polynomial with Galois group D_5 the dihedral group of order 10 is given in Sonn [12]. The notation D_{10} is also used for this group. The Galois group D_5 has the added interest that it is 2-coverable so that the constructed intersective polynomial has

Mathematics Subject Classification. Primary 11R32; Secondary 11R09, 11Y40.

Key words and phrases. Intersective polynomial, Galois group, dihedal group, monogenic.

two irreducible factors. In this paper we give an infinite parametric family of intersective polynomials with Galois group D_5. We make use of a family of polynomials studied by Lavallee, Spearman Williams and Yang in [7]. In that paper it was shown that they define monogenic quintic fields, that is algebraic number fields whose rings of integers have a power basis. While the property of monogeneity is not necessary when constructing intersective polynomials, it is helpful when dealing with parametric families. This is due to the fact that we can employ a well known theorem of Dedekind on ideal factorization to assist with the study of the decomposition groups. In Section 2, we recall some known properties of the polynomials we study and some facts about ideal factorization in number fields, including the theorem of Dedekind. In Section 3, we prove our theorem, give an estimate for density of the values of b for which d_b is squarefree and finish with some examples of intersective polynomials using our theorem. In Section 4 we consider some related examples. We state our main theorem next.

Theorem 1.1. *There exist infinitely many integers b such that*

$$d_b := -4b^3 - 28b^2 - 24b - 47 \tag{1}$$

is squarefree. Let b be such an integer. If we set

$$f_b(x) = x^5 - 2x^4 + (b+2)x^3 - (2b+1)x^2 + bx + 1$$

then the polynomial

$$g_b(x) = f_b(x)(x^2 - d_b)$$

is intersective and has Galois group D_5. Moreover for infinitely many of the integers b for which d_b is squarefree, the splitting fields of $g_b(x)$ are distinct.

2. The Parametric Family

The parametric family of polynomials

$$f_b(x) = x^5 - 2x^4 + (b+2)x^3 - (2b+1)x^2 + bx + 1$$

for b an integer was studied in [7]. We record some of the properties of these polynomials and their related number fields, referring the reader to [7] for details. The polynomial $f_b(x)$ is irreducible over $\mathbb{Q}$ for all integers b, and if d_b, given by (1) is squarefree, then the Galois group of $f_b(x)$ is isomorphic to D_5. Now assume that d_b is squarefree. The quadratic subfield of the splitting field of $f_b(x)$ is $\mathbb{Q}\left(\sqrt{d_b}\right)$ with discriminant d_b, and if θ is a root of $f_b(x)$ then $\mathbb{Q}(\theta)$ has field discriminant d_b^2, and is monogenic with ring of integers $\mathbb{Z}[\theta]$. Moreover infinitely many of the fields $\mathbb{Q}(\theta)$ are distinct.

The proof of our theorem requires the following propositions concerning ideal factorization in algebraic number fields. For the first proposition, F

and K denote algebraic number fields and $\mathfrak{O}_K$ denotes the ring of integers of K. We only state that part of this proposition which we will use.

Proposition 1. [8, Cor. 4.100] Let K/F be a Galois extension of number fields with $\mathfrak{p}$ a prime $\mathfrak{O}_K$-ideal. If $\mathfrak{p}$ is unramified in K/F then the decomposition group of $\mathfrak{p}$ is cyclic.

The next proposition concerns the factorization of primes in a composite of two extensions of the same field. For notation, K, K_1 and K_2 denote algebraic number fields and R denotes the ring of integers of K.

Proposition 2. [9, p. 159] If $\mathfrak{p}$ is a prime ideal of R unramified in both K_1/K and K_2/K then it is also unramified in the composite extension K_1K_2/K.

For the next proposition we use the notation $\operatorname{irr}_{\mathbb{Q}}(\theta)$ to denote the monic minimal polynomial in $\mathbb{Z}[x]$ of the algebraic integer θ. In addition we use the notation $\operatorname{ind}(\theta)$ to denote the index of θ, as defined by the equation

$$\operatorname{ind}(\theta) = \sqrt{\frac{D(\theta)}{d(K)}}$$

where $D(\theta)$ is the polynomial discriminant of $\operatorname{irr}(\theta)$ and $d(K)$ is the field discriminant of $K = \mathbb{Q}(\theta)$.

Proposition 3. [1, Cor. 10.5.1] Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with $\theta \in O_K$ the ring of integers of K. Let p be a rational prime. Let

$$f(x) = \operatorname{irr}_{\mathbb{Q}}(\theta) \in \mathbb{Z}[x].$$

Let $^-$ denote the natural map $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$, where $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Let

$$\overline{f}(x) = g_1(x)^{e_1} \cdots g_r(x)^{e_r},$$

where $g_1(x), \ldots g_r(x)$ are distinct monic irreducible polynomials in $\mathbb{Z}_p[x]$, and $e_1, \ldots, e_r$ are positive integers. For $i = 1, 2, \ldots, r$, let $f_i(x)$ be any monic polynomial of $\mathbb{Z}[x]$ such that $\overline{f}_i = g_i$ and $\deg(f_i) = \deg(g_i)$. Set

$$P_i = \langle p, f_i(\theta) \rangle, \ i = 1, 2, \ldots, r.$$

If $\operatorname{ind}(\theta) \not\equiv 0 (\operatorname{mod} p)$, then $P_1, \ldots, P_r$ are distinct prime ideals of O_K with

$$\langle p \rangle = P_1^{e_1} \cdots P_r^{e_r},$$

$$N(P_i) = p^{\deg f_i}, \ i = 1, \ldots, r.$$

3. PROOF OF THEOREM

Proof. The fact that there are infinitely many integers b such that

$$d_b = -4b^3 - 28b^2 - 24b - 47$$

is squarefree follows from a theorem of Erdös [5]. It was noted in [12] that D_5 is 2-coverable with the subgroup of order 5 and a subgroup of order 2. In order to construct intersective polynomials, then as stated in the introduction we first show that the decomposition group $G(\mathfrak{p})$ is cyclic for each prime ideal $\mathfrak{p}$ in the splitting field L of $f_b(x)$. If $\mathfrak{p}$ is unramified in L then $G(\mathfrak{p})$ is cyclic by Proposition 1. Now let $\mathfrak{p}$ be a ramified prime in L lying above the rational prime p. Since $Gal(f_b) \simeq D_5$, $G(\mathfrak{p})$ is cyclic if and only if $G(\mathfrak{p})$ is a proper subgroup of D_5. As $Gal(f_b)$ acts transitively on the set of prime ideals in L lying above p we deduce that $G(\mathfrak{p})$ is a proper subgroup of D_5 if there are at least two prime ideals in L lying above p. If θ denotes a root of $f_b(x)$, then L is the compositum of $\mathbb{Q}(\theta)$ and $\mathbb{Q}\left(\sqrt{d_b}\right)$ so that p must ramify in at least one of these fields by Proposition 2. We recall from Section 2 that these fields have discriminants d_b and d_b^2 which obviously contain the same prime factors. Therefore p must ramify in both of these fields and in particular in $\mathbb{Q}(\theta)$. If only one prime ideal $\mathfrak{p}$ in L lies above p it follows that only one prime ideal of $\mathbb{Q}(\theta)$ lies above p. Since $\mathbb{Q}(\theta)$ is monogenic with ring of integers $\mathbb{Z}[\theta]$ we have $\operatorname{ind}(\theta) \not\equiv 0 (\operatorname{mod} p)$. Therefore we can apply Proposition 3 and conclude that the only possible factorization of $f_b(x)$ modulo p, consistent with the previous statements about the factorization of a ramified ideal $\langle p \rangle$ leads to $r = 1$ and $e = 5$ so that

$$f_b(x) \equiv (x+t)^5 \ (\operatorname{mod} p), \tag{2}$$

where t is an integer. Equating each coefficient of $f_b(x) - (x+t)^5$ to zero modulo p gives us a set of congruences from which we will derive a contradiction. The coefficient of x^4 is

$$-2 - 5t,$$

and the constant term is

$$1 - t^5,$$

each of which is divisible by p. From the identity

$$(625t^4 - 250t^3 + 100t^2 - 40t + 16)(-2-5t) - 5^5(1-t^5) = -7 \cdot 11 \cdot 41,$$

it follows that the prime p must be one of 7, 11 or 41. Suppose that $p = 7$. Since

$$-2 - 5t \equiv 0 \ (\text{mod } 7),$$

we have

$$t \equiv 1 \pmod{7}. \tag{3}$$

Since p is ramified we have

$$d_b \equiv 0 \pmod{7},$$

so that

$$b \equiv 4 \pmod{7}. \tag{4}$$

However the coefficient of x^3 in $f_b(x) - (x+t)^5$ is

$$b - 10t^2 + 2,$$

which is not divisible by 7 if (3) and (4) hold. If $p = 11$ we are led in the same way to the congruence

$$(t, b) \equiv (4, 4) \text{ or } (4, 7) \pmod{11},$$

The pair $(4, 4)$ is omitted because d_b is not squarefree, while the remaining pair $(4, 7)$ yields a contradiction as in the case $p = 7$. For the case $p = 41$ we are led to the congruence

$$(t, b) \equiv (16, 25) \pmod{41}$$

and this possibility leads to the same type of contradiction as in the case $p = 7$. Hence (2) is impossible. Thus, we conclude that more than one prime ideal in L lies over p, so that all of the decomposition groups are proper and hence cyclic. The method of construction for an intersective polynomial when $Gal(f) \simeq D_5$ requires us to form the product of $f_b(x)$ with a defining polynomial for $\mathbb{Q}\left(\sqrt{d_b}\right)$, thus

$$g_b(x) = f_b(x)(x^2 - d_b)$$

is intersective and has Galois group D_5. Finally, since infinitely many of the algebraic number fields $\mathbb{Q}(\theta)$ are distinct as noted in the introduction to Section 2, we have that infinitely many of the splitting fields $\mathbb{Q}\left(\theta, \sqrt{d_b}\right)$ of $g_b(x)$ are distinct. □

Remark. The frequency with which the quantity d_b is squarefree is clarified by a theorem of Hooley on the squarefree values of cubic polynomials given in [6]. This theorem implies that for a positive constant C we have

$$S(b, x) \sim Cx$$

where

$$S(b, x) = \# \{b : |b| \leq x \text{ and } d_b \text{ is squarefree}\}.$$

Thus the set of integers b for which d_b is squarefree has positive density.

We close this section with some examples of intersective polynomials obtained from our theorem.

Example 1. For the following values of b we construct intersective polynomials using our theorem. All of the roots in $\mathbb{C}$ of the first two intersective polynomials are real, while in the last two examples only one root is real. The splitting fields of these polynomials are distinct.

b	d_b	Intersective Polynomial
-9	817	$(x^5 - 2x^4 - 7x^3 + 17x^2 - 9x + 1)(x^2 - 817)$
-8	401	$(x^5 - 2x^4 - 6x^3 + 15x^2 - 8x + 1)(x^2 - 401)$
0	-47	$(x^5 - 2x^4 + 2x^3 - x^2 + 1)(x^2 + 47)$
2	-239	$(x^5 - 2x^4 + 4x^3 - 5x^2 + 2x + 1)(x^2 + 239)$.

4. Related Examples

For the purpose of comparison with the D_5 polynomials that we made use of in this paper we consider dihedral quintic trinomials $x^5 + ax + b$ where a and b denote rational numbers. A parametrization of these polynomials is given by Roland, Yui and Zagier [10]. It was shown in [13] that the quintic fields defined by these polynomials have a common index divisor of 2, so that none of these fields are monogenic. Nevertheless some of them give rise to intersective polynomials.

Example 2. If $f(x) = x^5 + 11x + 44$ then $Gal(f) \simeq D_5$. It can be checked that all of the decomposition groups are cyclic. To deal with the ramified primes and associated decomposition groups, algorithms for factoring ideals are given in Cohen [4]. The quadratic subfield of the splitting field of $f(x)$ is $\mathbb{Q}\left(\sqrt{-2}\right)$ and so the method used in [12] shows that

$$(x^5 + 11x + 44)(x^2 + 2)$$

is intersective.

Example 3. If $f(x) = x^5 - 5x + 12$ then $Gal(f) \simeq D_5$. The quadratic subfield of the splitting field is $\mathbb{Q}\left(\sqrt{-10}\right)$. However there is a single ideal lying above 5 in the splitting field of $f(x)$ and the decomposition group of this ideal is all of D_5. Following the method in [12] yields the polynomial

$$(x^5 - 5x + 12)(x^2 + 10),$$

which is not intersective since it has no root modulo 25.

References

[1] Ş. Alaca and K. S. Williams, *Introductory Algebraic Number Theory,* Cambridge University Press, Cambridge, 2004.

[2] D. Behrend and Y. Bilu*, Polynomials with roots modulo every integer*, Proc. Amer. Math. Soc. **124** (1996), no. 6*,* 1663-1671.

[3] R. Brandl, D. Bubboloni and I. Hupp, *Polynomials with roots mod p for all primes p.* J. Group Theory **4** (2001), 233-239.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory,* Springer-Verlag, (1993).

[5] P. Erdös, *Arithmetic properties of polynomials,* J. London Math. Soc. **28** (1953), 416-425.

[6] C. Hooley, *Applications of sieve methods to the theory of numbers.* Cambridge Tracts in Mathematics, No. 70. Cambridge University Press, Cambridge-New York-Melbourne, 1976.

[7] M. J. Lavallee, B. K. Spearman, K. S. Williams and Q. Yang, *Dihedral Quintic Fields With A Power Basis*, Math. J. Okayama Univ. **47**, (2005), 75-79.

[8] R. A. Mollin, *Algebraic Number Theory,* Chapman and Hall, 1999.

[9] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, third edition, 1990.

[10] G. Roland, N. Yui and D. Zagier, *A parametric family of quintic polynomials with Galois group D5.* J. Number Theory **15**(1982), 137–142.

[11] J. Sonn, *Polynomials with roots in Q_p for all p.* Proc. Amer. Math Soc. **136** (2008), no. 6, 1955-1960.

[12] J. Sonn, *Two Remarks On The Inverse Galois Problem For Intersective Polynomials,* J. Theor. Nombres Bordeaux, **21**, (2009), no. 2, 437-439.

[13] B. K. Spearman, K. S. Williams and Q. Yang, *On the Common Index Divisors of a Dihedral Field of Prime Degree.* Int. J. Math. Math. Sci. (2007), Article ID 89713, 8 pages.

Melisa J. Lavallee
Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, BC, Canada, V1V 1V7.
e-mail address: Melisa_Lavallee@hotmail.com

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

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

(*Received November 15, 2011*)
(*Revised April 10, 2012*)