View metadata, citation and similar papers at core.ac.uk brought to you by CORE

provided by Elsevier - Publisher Connector

JOURNAL OF NUMBER THEORY 34, 153–173 (1990)

Odd Degree Polynomials with Dihedral Galois Groups

CLIFTON J. WILLIAMSON*

Department of Mathematics, University of California, Berkeley, California 94720

Communicated by D. Zagier

Received November 15, 1987; revised April 2, 1989

1. INTRODUCTION

In a recent paper Jensen and Yui [2] give a procedure to determine if an irreducible polynomial $\varphi(x) \in \mathbf{Q}[x]$ of odd prime degree p has Galois group isomorphic to D_p, the dihedral group of order $2p$. In this paper we give a generalized notion of dihedral group, then present an algorithm to determine if the Galois group $\mathrm{Gal}(\varphi)$ of an irreducible polynomial $\varphi(x) \in \mathbf{Q}[x]$ of arbitrary odd degree n is a dihedral group of order $2n$. This algorithm relies on the construction of linear resolvent polynomials, the factorization of these polynomials over $\mathbf{Q}$ and over a quadratic number field, and the factorization of the polynomial $\varphi(x)$ modulo a prime p. We will indicate how such computations can be performed by a computer algebra system such as MACSYMA, which we used for the computations in this paper, and then give examples of polynomials with dihedral Galois groups of order $2n$ for $n = 9$, 15, 21, and 25.

In Section 2 we define a generalized dihedral group and note a few elementary properties of such groups. We then state some facts from class field theory, including Jensen's result [1] on dihedral Galois groups and ring class fields.

In Section 3 we define resolvent polynomials and note ways in which linear resolvent polynomials can be used to compute Galois groups. Following Soicher [8], we show how the linear resolvents that interest us may be computed using the resultant functions provided by MACSYMA.

In Section 4 we give a characterization of dihedal Galois groups, which provides an algorithm to determine if $\mathrm{Gal}(\varphi)$ is dihedral. Section 5 contains

* Author's current address: IBM T. J. Watson Research Center, P. O. Box 218, Yorktown Heights, NY 10598.

0022-314X/90 $3.00

Copyright © 1990 by Academic Press, Inc.
All rights of reproduction in any form reserved.

techniques for constructing large dihedral extensions out of smaller ones and we give numerical examples of polynomials with dihedral Galois groups of order $2n$ for the first 4 odd, non-prime values of n.

2. Dihedral Galois Groups

Let D_n be the group of symmetries of a regular n-sided polygon. D_n is a group of order $2n$ and is generated by two elements: σ, a rotation through an angle of $2\pi/n$, and τ, a reflection about an axis. These generators satisfy the relations

$$\sigma^n = \tau^2 = 1, \qquad \tau\sigma\tau = \sigma^{-1}.$$

We generalize the notion of a dihedral group as follows: Let H be a finite abelian group, and let $G = \{1, \tau\}$ be a group of order 2 acting on H via $\sigma^\tau = \sigma^{-1}$. (We say that "$G$ acts by -1"). Let Γ be the semi-direct product of G and H. As a set $\Gamma = H \cup \{\tau\sigma : \sigma \in H\}$ and the group law on Γ is described by

1. elements of H are multiplied as usual,
2. $\tau^2 = 1$, and
3. $\sigma\tau = \tau\sigma^{-1}$, for all $\sigma \in H$.

Thus, if $H = Z_n$, the cyclic group of order n, then Γ is the group D_n. If $H = Z_{n_1} \times \cdots \times Z_{n_k}$, we will write $D_{n_1 \times \cdots \times n_k}$ to denote the semi-direct product of H and a group of order 2 acting by -1. We note that any element of Γ not in H is of order 2 and that the product of any 2 elements of Γ not in H is an element of H.

Let K be a quadratic field. The *ring class extension* of K with conductor f is the class field $K(f)$ corresponding to the ideal group $P_{\mathbf{Z}}(f)$ defined mod f:

$$I(f) \supseteq P_{\mathbf{Z}}(f) \supseteq P_1(f).$$

Here $I(f)$ denotes the group of (fractional) ideals of K prime to f, $P_{\mathbf{Z}}(f)$ denotes the group of principal ideals congruent to some (rational) integer (mod f), and $P_1(f)$ denotes the group of principal ideals congruent to 1 (mod f). The Galois group $\mathrm{Gal}(K(f)/K)$ is isomorphic to $\mathrm{Cl}(\mathcal{O}_f)$, the class group of $\mathcal{O}_f$, the order of K with conductor f, and the Galois group $\mathrm{Gal}(K(f)/\mathbf{Q})$ is isomorphic to the semi-direct product of $\mathrm{Gal}(K(f)/K)$ with $\mathrm{Gal}(K/\mathbf{Q})$, where the non-trivial element of $\mathrm{Gal}(K/\mathbf{Q})$ acts by sending elements of $\mathrm{Gal}(K(f)/K)$ to their inverses. Thus, $\mathrm{Gal}(K(f)/\mathbf{Q})$ is dihedral. Moreover, Jensen [1] noted that if L is a dihedral extension of $\mathbf{Q}$ of degree

$2n$ with n odd and K is the unique quadratic subextension of $L/\mathbf{Q}$, then L is contained in some ring class extension of K. Indeed, Jensen's proof shows that L is a subsextension of any ring class extension whose conductor is admissible for L/K. Finally, we note that if the prime p remains inert in K and p is prime to f, then $p\mathcal{O}_K$ splits completely in $K(f)$ and, hence, in any subextension of $K(f)/K$.

3. Resolvent Polynomials

3.1. *Resolvents*

Let $\varphi(x) \in \mathbf{Q}[x]$ be irreducible of degree $n \geqslant 1$ and let $\alpha_1, ..., \alpha_n$ be the roots of $\varphi(x)$ in some algebraic closure of $\mathbf{Q}$. We let S_n, the symmetric group of degree n, act on $\mathbf{Q}[x_1, ..., x_n]$ by permuting the indeterminates x_i. Now take $P \in \mathbf{Q}[x_1, ..., x_n]$ and let $P^{S_n} = \{P_1, ..., P_k\}$ be the orbit of P under the action of S_n. We define the *resolvent polynomial* $R(P, \varphi) = R(P, \varphi)(x)$ to be

$$\prod_{i=1}^{k} (x - P_i(\alpha_1, ..., \alpha_n)).$$

Since the coefficients of $R(P, \varphi)(x)$ are symmetric functions of the roots α_i, we have $R(P, \varphi)(x) \in \mathbf{Q}[x]$. When the polynomial P is a linear form, we call $R(P, \varphi)(x)$ a *linear resolvent polynomial*. For instance, if $P = x_1 + x_2$, then $R(P, \varphi)(x) = \prod_{i<j} (x - (\alpha_i + \alpha_j))$ and if $P = e_1 x_1 + e_2 x_2$ with $e_1 \neq e_2$, then $R(P, \varphi)(x) = \prod_{i \neq j} (x - (e_1\alpha_i + e_2\alpha_j))$.

The factorization of linear resolvents over $\mathbf{Q}$ yields information about the action of $\mathrm{Gal}(\varphi)$ on ordered and unordered sets of roots of $\varphi(x)$. This in turn yields information about the structure of $\mathrm{Gal}(\varphi)$, as is discussed in the paper by McKay and Soicher [5]. As an example, we note the following proposition, which will be used later in the paper.

Proposition 1. *Suppose that $\varphi(x) \in \mathbf{Q}[x]$ is irreducible of arbitrary degree $n \geqslant 2$ and suppose that e_1 and e_2 are distinct non-zero integers such that the resolvent $R(e_1x_1 + e_2x_2, \varphi)(x)$ has distinct roots. Then the splitting field of $\varphi(x)$ has degree n over $\mathbf{Q}$ (i.e.,* $\mathrm{Gal}(\varphi)$ *is a regular permutation group) if and only if $R(e_1x_1 + e_2x_2, \varphi)(x)$ factors into irreducibles of degree n over $\mathbf{Q}$.*

Proof. [5]. ▮

Remark. Jensen and Yui [2] showed that if $\varphi(x) \in \mathbf{Z}[x]$ is monic, irreducible, and of odd prime degree p then

1. the resolvent $R(x_1+x_2, \varphi)(x)$ always has distinct roots, and

2. $R(x_1+x_2, \varphi)(x)$ factors into irreducibles of degree p if and only if $\mathrm{Gal}(\varphi)$ is D_p or Z_p, the cyclic group of order p.

Jensen and Yui note that it is often easy to distinguish between the Galois groups D_p and Z_p. For example, if $p \equiv 3 \pmod 4$, then $\mathrm{Gal}(\varphi)=Z_p$ (resp. $\mathrm{Gal}(\varphi)=D_p$) if $\mathrm{disc}(\varphi)$ is a rational square (resp. non-square), or if it can be shown that $\varphi(x)$ has complex roots, then $\mathrm{Gal}(\varphi)$ must be D_p, because complex conjugation gives an element of $\mathrm{Gal}(\varphi)$ of order 2. However, neither of these methods works for $\varphi(x)=x^5-68590x^3+5212840x^2+120135385x+580051912$, whose splitting field is a totally real D_5-extension of $\mathbf{Q}$. Nevertheless, we may always distinguish between D_p and Z_p by factoring the resolvent $R(x_1-x_2, \varphi)(x)$. We note that condition (1) implies that $R(x_1-x_2, \varphi)(x)$ also has distinct roots and from Proposition 1 we see that $R(x_1-x_2, \varphi)(x)$ factors into irreducibles of degree p if $\mathrm{Gal}(\varphi)=Z_p$ and into irreducibles of degree $2p$ if $\mathrm{Gal}(\varphi)=D_p$. We will see later that if $\mathrm{Gal}(\varphi)=D_p$, then the (unique) quadratic subfield of the splitting field of $\varphi(x)$ is $\mathbf{Q}(\sqrt{-d})$, where d is the constant coefficient of any irreducible factor of $R(x_1-x_2, \varphi)(x)$.

Of course, the Proposition 1 remains true if $\mathbf{Q}$ is replaced by any number field K, for instance, a quadratic field. Thus, if we have an algorithm to factor univariate polynomials over K, then we have an algorithm to determine if the order of $\mathrm{Gal}(\varphi)$ equals the degree of $\varphi(x)$, provided that we can find e_1, e_2 such that $R(e_1x_1+e_2x_2, \varphi)(x)$ has distinct roots. This can always be done, as is shown by the following proposition.

PROPOSITION 2. *Let K be a number field and let $\varphi(x) \in K[x]$ be irreducible over K and of degree $n \geqslant 4$. Then there are only finitely many ratios e_2/e_1 such that the resolvent $R(e_1x_1+e_2x_2, \varphi)(x)$ has multiple roots.*

Proof. If $R(e_1x_1+e_2x_2, \varphi)(x)$ has multiple roots, then there exist indices $i_1, ..., i_4$, with $i_1 \neq i_3, i_2 \neq i_4$, and such that $e_1\alpha_{i_1}+e_2\alpha_{i_2}=e_1\alpha_{i_3}+e_2\alpha_{i_4}$. Now suppose that there are infinitely many pairs of integers (e_1, e_2), none of which is a rational multiple of another, such that $R(e_1x_1+e_2x_2, \varphi)(x)$ has multiple roots. Then there exist two distinct pairs (e_1, e_2) and (f_1, f_2) such that $e_1\alpha_{i_1}+e_2\alpha_{i_2}=e_1\alpha_{i_3}+e_2\alpha_{i_4}$, for indices $i_1, ..., i_4$, with $i_1 \neq i_3$ and $i_2 \neq i_4$, and $f_1\alpha_{i_1}+f_2\alpha_{i_2}=f_1\alpha_{i_3}+f_2\alpha_{i_4}$, for the *same* indices $i_1, ..., i_4$. Thus, we have

$$e_1(\alpha_{i_1}-\alpha_{i_3})+e_2(\alpha_{i_2}-\alpha_{i_4})=0$$

$$f_1(\alpha_{i_1}-\alpha_{i_3})+f_2(\alpha_{i_2}-\alpha_{i_4})=0.$$

Since $e_1 f_2 - e_2 f_1 \neq 0$, we must have $\alpha_{i_1} - \alpha_{i_3} = \alpha_{i_2} - \alpha_{i_4} = 0$. This contradiction establishes the proposition. ▌

3.2. *Resultants*

As we noted above, the coefficients of a resolvent polynomial $R(P, \varphi)(x)$ are symmetric functions of the roots α_i of $\varphi(x)$, and, hence, can be expressed in terms of the elementary symmetric functions of the α_i, that is, the coefficients of the polynomial $\varphi(x)$. In theory, we could expand $\prod_{i=1}^{k} (x - P_i(\alpha_1, ..., \alpha_n))$ and express the coefficients of this polynomial in terms of the elementary symmetric functions of the α_i. However, this procedure is difficult to carry out in practice except for polynomials of small degree.

Instead, we will follow Soicher [8], who showed how resultants may be used to calculate linear resolvents. Thus, we may use MACSYMA's resultant functions to compute the resolvents that we will need in this paper, namely, those of the form $R(e_1 x_1 + e_2 x_2, \varphi)(x)$ with $e_1 \neq e_2$.

The definition of resultants can be found in any basic text on algebra, such as Lang [3] or van der Waerden [9].

Definition 1. *Suppose $\varphi(x), \psi(x) \in K[x]$, where K is any field, and suppose that φ and ψ factor as follows over an algebraic closure of K:*

$$\varphi(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$$

$$\psi(x) = b(x - \beta_1) \cdots (x - \beta_m).$$

Then $\mathrm{res}(\varphi, \psi) = \mathrm{res}(\varphi(x), \psi(x), x)$, *the* resultant *of φ and ψ, is*

$$\mathrm{res}(\varphi, \psi) = a^m b^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

We see that $\mathrm{res}(\varphi, \psi) \in K$, since it is a symmetric function of the roots of φ and ψ.

Soicher [8] notes the following lemma.

Lemma 1. *Let $\varphi(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ and $\psi(x) = (x - \beta_1) \cdots (x - \beta_m)$. Then $p(x)$, the polynomial of degree mn whose roots are*

$$\alpha_i + \beta_j, \qquad 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m,$$

is given by

$$p(x) = \mathrm{res}(\varphi(X), \psi(x - X), X),$$

where $\varphi(X)$ and $\psi(x - X)$ are viewed as polynomials in a new indeterminate X.

We call the polynomial $p(x)$ the *root sum polynomial* for $\varphi(x)$ and $\psi(x)$ and denote this polynomial by $S(\varphi, \psi) = S(\varphi, \psi)(x)$.

Now fix a polynomial $\varphi(x) = (x-\alpha_1)\cdots(x-\alpha_n)$. We let $\varphi_1(x) = e_1^n \cdot \varphi(x/e_1)$, whose roots are $e_1\alpha_1, ..., e_1\alpha_n$, let $\varphi_2(x) = e_2^n \cdot \varphi(x/e_2)$, whose roots are $e_2\alpha_1, ..., e_2\alpha_n$, and let $L = e_ix_1 + e_2x_2$ with $e_1 \neq e_2$. Here $R(L, \varphi)(x) = \prod_{i \neq j} (x - (e_1\alpha_i + e_2\alpha_j))$. By the lemma,

$$\begin{aligned}
\operatorname{res}(\varphi_1(X), \varphi_2(x-X), X) &= \prod_{i=1}^{n} \prod_{j=1}^{n} (x - (e_1\alpha_i + e_2\alpha_j)) \\
&= \prod_{i \neq j} (x - (e_1\alpha_i + e_2\alpha_j)) \cdot \prod_{i=j} (x - (e_1\alpha_i + e_2\alpha_j)) \\
&= \prod_{i \neq j} (x - (e_1\alpha_i + e_2\alpha_j)) \cdot \prod_{i=1}^{n} (x - (e_1 + e_2)\alpha_i).
\end{aligned}$$

Therefore, if $e_1 + e_2 = 0$, then

$$R(L, \varphi)(x) = \frac{\operatorname{res}(\varphi_1(X), \varphi_2(x-X), X)}{x^n},$$

and if $e_1 + e_2 \neq 0$, then

$$R(L, \varphi)(x) = \frac{\operatorname{res}(\varphi_1(X), \varphi_2(x-X), X)}{\varphi_3(x)},$$

where $\varphi_3(x) = (e_1 + e_2)^n \cdot \varphi(x/(e_1 + e_2))$.

4. Dihedral Galois Groups of Order $2n$, n Odd

PROPOSITION 3. *Let* $\varphi(x) = \prod (x - \alpha_i) \in \mathbf{Z}[x]$ *be irreducible of odd degree n and let L be the splitting field of* $\varphi(x)$.

First supose that $\operatorname{Gal}(\varphi) = \operatorname{Gal}(L/\mathbf{Q})$ *is a dihedral group of order 2n, and let K be the unique quadratic subfield of L. Then*

1. $\varphi(x)$ *is irreducible over K (i.e.,* $\operatorname{Gal}(L/K)$ *permutes the roots* α_i *transitively) and the splitting field of* $\varphi(x)$ *has degree n over K.*

2. $K = \mathbf{Q}(\sqrt{-d})$, *where d is the constant coefficient of any monic, irreducible factor* $p(x)$ *of the resolvent* $R(x_1 - x_2, \varphi)(x)$. *Further* $p(x)$ *is an* even *polynomial (i.e.,* $p(x)$ *is of the form* $q(x^2)$ *for some polynomial* $q(x)$*).*

3. *If* $p \nmid \operatorname{disc}(\varphi)$ *remains inert in K, then* $p\mathcal{O}_K$ *splits completely in L:* $p\mathcal{O}_L = \mathcal{P}_1 \cdots \mathcal{P}_n$. *The decomposition fields for the primes* $\mathcal{P}_i$ *in* $L/\mathbf{Q}$ *are distinct. The polynomial* $\varphi(x)$ *factors into a linear polynomial times a product of* $(n-1)/2$ *irreducible quadratic polynomials* $(\operatorname{mod} p)$.

Conversely, suppose that

1. *The monic, irreducible factors of* $R(x_1-x_2,\varphi)(x)$ *are even polynomials and the field* $K=\mathbf{Q}(\sqrt{-d})$, *where* d *is the constant coefficient of some monic, irreducible factor of* $R(x_1-x_2,\varphi)(x)$, *is quadratic over* $\mathbf{Q}$ *and is independent of the choice of irreducible factor.*

2. *The polynomial* $\varphi(x)$ *is irreducible over* K *and the splitting field of* $\varphi(x)$ *over* K *has degree* n.

3. *For some prime* $p \nmid disc(\varphi)$ *which remains inert in* K, $\varphi(x)$ *factors into a linear polynomial times a product of* $(n-1)/2$ *irreducible quadratic polynomials* (mod p).

Then Gal(φ) *is dihedral of order* $2n$ *and* K *is the unique quadratic subfield of the splitting field of* $\varphi(x)$.

If condition (1) *in the second part of the proposition fails, then the Galois group is not dihedral of order* $2n$. *If* (1) *is satisfied and* (2) *fails or* (3) *fails for any prime* $p \nmid$ disc(φ) *which remains inert if* K, *then the Galois group is not dihedral of order* $2n$.

Remark. Conditions (1)–(3) in the second part of the proposition may be verified using a computer algebra system. One only needs to construct linear resolvents and factor polynomials with integer coefficients over $\mathbf{Q}$, a quadratic extension of $\mathbf{Q}$, and modulo a prime number p.

Proof. First assume that Gal(φ) is dihedral of order $2n$.

Part (1): Let α_i and α_j be two distinct roots of $\varphi(x)$ and let σ be any element of Gal(φ) such that $\alpha_i^\sigma=\alpha_j$. Let τ generate Gal$(L/\mathbf{Q}(\alpha_i))$, so that $\alpha_i^\tau=\alpha_i$ and $\tau^2=1$. Then σ and $\tau\sigma$ both take α_i to α_j and, since $\tau\notin$ Gal(L/K), if σ is not an element of Gal(L/K), then $\tau\sigma$ is. This establishes the first part of (1); the second part is trivial.

Note that σ and $\tau\sigma$ are the only elements of Gal(φ) which take α_i to α_j, so given any $\alpha_i\neq\alpha_j$, there is a unique element (of order 2) of Gal(φ) which interchanges α_i and α_j. Further, the non-trivial elements of Gal(L/K) do not leave any α_i fixed, since Gal(L/K) is a group of order n acting transitively on a set of n elements, and any element of Gal$(L/\mathbf{Q})$ of order 2 leaves exactly one α_i fixed, because the fields $\mathbf{Q}(\alpha_i)$ are distinct: let α_i and α_j be distinct roots of $\varphi(x)$ and let $\sigma\in$ Gal(L/K) be such that $\alpha_i^\sigma=\alpha_j$. If Gal$(L/\mathbf{Q}(\alpha_i))=\{1,\tau\}$, then

$$\mathrm{Gal}(L/\mathbf{Q}(\alpha_j))=\sigma^{-1}\{1,\tau\}\,\sigma=\{1,\tau\sigma^2\}.$$

Since $\sigma\neq 1$ has odd order, $\tau\neq\tau\sigma^2$, and $\mathbf{Q}(\alpha_i)\neq\mathbf{Q}(\alpha_j)$.

Part (2): Let $p(x)$ be a monic, irreducible factor of $R(x_1-x_2,\varphi)(x)$. Then $p(x)$ is the minimal polynomial of $\alpha_i-\alpha_j$ for some choice of roots

$\alpha_i \neq \alpha_j$ of $\varphi(x)$. Let $\beta = N_{L/K}(\alpha_i - \alpha_j)$ and let $\tau \in \mathrm{Gal}(\varphi)$ be any element of order 2, so that $\tau \mid K$ generates $\mathrm{Gal}(K/\mathbf{Q})$.

Claim. $\beta^\tau = -\beta$.

Let $\alpha = \alpha_i$ and take $\sigma_0 \in \mathrm{Gal}(L/K)$ such that $\alpha_i^{\sigma_0} = \alpha_j$. Since any two elements of order 2 induce the same action on K, we may take τ to be the generator of $\mathrm{Gal}(L/\mathbf{Q}(\alpha))$.

Then $\beta = N_{L/K}(\alpha - \alpha^{\sigma_0}) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (\alpha - \alpha^{\sigma_0})^\sigma$, so

$$\begin{aligned}
\beta^\tau &= \prod_\sigma (\alpha - \alpha^{\sigma_0})^{\sigma\tau} \\
&= \prod_\sigma (\alpha - \alpha^{\sigma_0})^{\tau\sigma^{-1}} \\
&= \prod_\sigma (\alpha^{\tau\sigma^{-1}} - \alpha^{\sigma_0\tau\sigma^{-1}}) \\
&= \prod_\sigma (\alpha^{\tau\sigma^{-1}} - \alpha^{\tau\sigma_0^{-1}\sigma^{-1}}) \\
&= \prod_\sigma (\alpha^{\sigma^{-1}} - \alpha^{\sigma_0^{-1}\sigma^{-1}}).
\end{aligned}$$

Replacing σ by $\sigma^{-1}\sigma_0^{-1}$, we have

$$\begin{aligned}
\beta^\tau &= \prod_\sigma (\alpha^{\sigma_0\sigma} - \alpha^\sigma) \\
&= \prod_\sigma (\alpha^{\sigma_0} - \alpha)^\sigma \\
&= (-1)^n \beta \\
&= -\beta.
\end{aligned}$$

Now $\beta^\tau = -\beta$ implies that $\beta^2 \in \mathbf{Q}$ and $K = \mathbf{Q}(\beta)$. Thus,

$$K = \mathbf{Q}(\sqrt{-\beta\beta^\tau}) = \mathbf{Q}(\sqrt{-N_{L/\mathbf{Q}}(\alpha_i - \alpha_j)}).$$

Since there is an element of $\mathrm{Gal}(\varphi)$ which interchanges α_i and α_j, we have $p(-x) = p(x)$ and $p(x)$ is of the form $q(x^2)$. In particular, $p(x)$ has even degree. Thus, $N_{L/\mathbf{Q}}(\alpha_i - \alpha_j)$ is an *odd* power of d, the constant coefficient of $p(x)$. Therefore,

$$\mathbf{Q}(\sqrt{-d}) = \mathbf{Q}(\sqrt{-N_{L/\mathbf{Q}}(\alpha_i - \alpha_j)}) = K.$$

Remark. In the case where $R(x_1 - x_2, \varphi)(x)$ has distinct roots, each $\alpha_i - \alpha_j$ has $2n$ distinct conjugates, since no non-trivial element of $\mathrm{Gal}(\varphi)$ leaves both α_i and α_j fixed, and the irreducible factors of $R(x_1 - x_2, \varphi)(x)$

all have degree $2n$. However, it is possible for the resolvent $R(x_1 - x_2, \varphi)(x)$ to have multiple roots when the degree n of $\varphi(x)$ is not prime. A typical case occurs when $\varphi(x)$ is a root sum polynomial: suppose that $\varphi_1(x) = \prod_{i=1}^{m} (x - u_i)$ and $\varphi_2(x) = \prod_{j=1}^{k} (x - v_j)$ are polynomials of degrees m and k such that $mk = n$ and $\varphi(x) = \prod_{i=1}^{m} \prod_{j=1}^{k} (x - (u_i + v_j))$. Then for any $i_1 \neq i_2$ and any $j_1 \neq j_2$, $u_{i_1} - u_{i_2}$ is a root of $R(x_1 - x_2, \varphi)(x)$ of multiplicity k and $v_{j_1} - v_{j_2}$ is a root of $R(x_1 - x_2, \varphi)(x)$ of multiplicity m, that is, $R(x_1 - x_2, \varphi)(x)$ is divisible by $R(x_1 - x_2, \varphi_1)(x)^k$ and by $R(x_1 - x_2, \varphi_2)(x)^m$.

Part (3): If $p \nmid \operatorname{disc}(\varphi)$ and p remains inert in K, then p does not divide the conductor $\mathfrak{f}(L/K)$, nor does p divide f, the smallest rational integer divisible by $\mathfrak{f}(L/K)$. Thus, $p\mathcal{O}_K \in P_{\mathbf{Z}}(f)$, so $p\mathcal{O}_K$ splits completely in the ring class field $K(f)$. Since $L \subseteq K(f)$, $p\mathcal{O}_K$ splits completely in L: $p\mathcal{O}_K = \mathscr{P}_1 \cdots \mathscr{P}_n$. Since $\mathscr{P}_i$ has residue degree 2, its decomposition group in $L/\mathbf{Q}$ has order 2: $G_{\mathrm{P}_i} = \{1, \tau\}$ for some $\tau \in \operatorname{Gal}(L/\mathbf{Q})$ of order 2. If $\mathscr{P}_j$ is another such prime, then $\mathscr{P}_j = \mathscr{P}_i^{\sigma}$ for some $\sigma \in \operatorname{Gal}(L/K)$ and $G_{\mathscr{P}_j} = \sigma^{-1} G_{\mathscr{P}_i} \sigma = \{1, \tau\sigma^2\} \neq G_{\mathscr{P}_i}$. Since the decomposition groups are distinct, any $\tau \in \operatorname{Gal}(\varphi)$ generates the decomposition group for some $\mathscr{P}_i$. It follows that each field $\mathbf{Q}(\alpha_i)$ is the decomposition field for exactly one prime $\mathscr{P}_i$. Hence, if $F = \mathbf{Q}(\alpha_i)$, then $p\mathcal{O}_F$ factors into a degree 1 prime times a product of $(n-1)/2$ degree 2 primes. Equivalently, $\varphi(x)$ factors into a linear polynomial times a product of $(n-1)/2$ irreducible quadratic polynomials (mod p), which proves (3).

Now assume that $\varphi(x) = \prod (x - \alpha_i) \in \mathbf{Z}[x]$ is irreducible of odd degree n and satisfies conditions (1)–(3) in the second part of the proposition. Let L be the splitting field of $\varphi(x)$ over $\mathbf{Q}$. The irreducible factors of $R(x_1 - x_2, \varphi)(x)$ are the minimal polynomials of the integers $\alpha_i - \alpha_j$ for the various choices of i and j. Thus, every $\alpha_i - \alpha_j$ has even degree over $\mathbf{Q}$ and $(L:\mathbf{Q})$ is even. Since $\varphi(x)$ is irreducible over $\mathbf{Q}$, its degree n divides $(L:\mathbf{Q})$. Hence, we know that $2n$ divides $(L:\mathbf{Q})$.

Next we know that E, the splitting field of $\varphi(x)$ over K, has degree n over K. Since $L \subseteq E$, we see that $(L:\mathbf{Q})$ divides $2n = (E:\mathbf{Q})$. Therefore, $(L:\mathbf{Q}) = 2n$ and $L = E$. We have shown that the splitting field of $\varphi(x)$ over $\mathbf{Q}$ has degree $2n$ over $\mathbf{Q}$ and has K as its unique quadratic subfield.

Now take a prime $p \nmid \operatorname{disc}(\varphi)$ which remains inert in K and such that $\varphi(x)$ factors into a linear polynomial times a product of $(n-1)/2$ irreducible quadratic polynomials (mod p). We see that $\varphi(x)$ factors completely over $\mathbf{F}_{p^2} = \mathcal{O}_K/p\mathcal{O}_K$, so $p\mathcal{O}_K$ splits completely in L. Thus, $p\mathcal{O}_L = \mathscr{P}_1 \cdots \mathscr{P}_n$, where each $\mathscr{P}_i$ has residue degree 2 over p. Therefore, the decomposition group of $\mathscr{P}_i$ in $L/\mathbf{Q}$ has order 2. Let $F = \mathbf{Q}(\alpha_i)$, for some root α_i of $\varphi(x)$. From the factorization of $\varphi(x)$ (mod p), we know that $p\mathcal{O}_L$ is the product of a degree 1 prime times a product of $(n-1)/2$ degree 2 primes. Therefore, F is the decomposition field for the prime of L lying over the degree 1 prime and is not the decomposition field for any other prime of L lying over p. Hence, the decomposition fields of the various $\mathscr{P}_i$ are distinct and $\mathrm{Gal}(L/\mathbf{Q})$ has n distinct elements of order 2.

We now know that $\mathrm{Gal}(L/\mathbf{Q})$ consists of the elements of $\mathrm{Gal}(L/K)$ and n elements of order 2. Hence, any element of $\mathrm{Gal}(L/\mathbf{Q})$ not in $\mathrm{Gal}(L/K)$ must have order 2. In particular, if $\sigma \in \mathrm{Gal}(L/K)$ and $\tau \in \mathrm{Gal}(L/\mathbf{Q})$ has order 2, then $\tau\sigma \notin \mathrm{Gal}(L/K)$, so $(\tau\sigma)(\tau\sigma) = 1$, i.e., $\tau\sigma\tau = \sigma^{-1}$. It follows that $\sigma \mapsto \sigma^{-1}$ is an automorphism of $\mathrm{Gal}(L/K)$, so $\mathrm{Gal}(L/K)$ must be abelian. It is clear now that $\mathrm{Gal}(L/\mathbf{Q})$ is the semi-direct product of $\mathrm{Gal}(L/K)$ and a group of order 2 which acts by -1.

Finally, we note that if any of the conditions (1)–(3) in the second part of the proposition fail to hold, then the Galois group cannot be dihedral by what we proved in the first part of the proposition. ▮

5. Numerical Examples

5.1. *Introduction*

For small, odd values of n, there are known ways to construct families of polynomials with Galois group D_n. For $n = 3$, one only needs an irreducible cubic polynomial whose discriminant is not a rational square. We will use a parametric family of D_3-polynomials, constructed so that it is easy to produce a polynomial in the family whose splitting field contains a given quadratic field K. Roland, Yui, and Zagier [7] give a family of D_5-polynomials, each of the form $x^5 + ax + b$. A polynomial in this family must have complex roots, so the quadratic subfield of its splitting field is imaginary. Mestre [6] uses elliptic curves to construct families of polynomials with Galois groups D_5 and D_7. We will use his method to construct a family of polynomials with Galois group D_9.

To construct larger dihedral extensions, we note the following: suppose that for $i = 1, 2$, L_i is an abelian extension of a quadratic field K contained in the ring class field $K(f_i)$. Then the field $L_1 L_2$ is contained in the ring class field $K(f_1 f_2)$ and, hence, is dihedral over $\mathbf{Q}$. If for $i = 1, 2$, $\varphi_i(x) \in \mathbf{Q}[x]$ is a polynomial whose splitting field is L_i, then we would like the root sum polynomial $S(\varphi_1, \varphi_2)(x)$ to be irreducible over $\mathbf{Q}$ and have splitting field $L_1 L_2$.

First we note the following proposition:

Proposition 4. *Let K be a number field and let $\varphi_1(x), \varphi_2(x) \in K[x]$ be irreducible over K with splitting fields L_1 and L_2 over K. Then if L_1 and L_2 are linearly disjoint over K (i.e., if $L_1 \cap L_2 = K$), then $S(\varphi_1, \varphi_2)(x)$ is irreducible over K and its splitting field over K is $L_1 L_2$.*

Proof. Suppose that $\varphi_1(x) = \prod_{i=1}^{n_1} (x - \alpha_i)$ and $\varphi_2(x) = \prod_{j=1}^{n_2} (x - \beta_j)$

in some algebraic closure of K. Since L_1 and L_2 are linearly disjoint over K, we have $\mathrm{Gal}(L_1 L_2/K) = \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$. Thus, given any two roots α_{i_1} and α_{i_2} of $\varphi_1(x)$, there is an element of $\mathrm{Gal}(L_1 L_2/K)$ which maps α_{i_1} to α_{i_2} and which fixes every root β_j of $\varphi_2(x)$. Similarly, given β_{j_1} and β_{j_2}, there is an automorphism which maps β_{j_1} to β_{j_2} and fixes every α_i. It is clear that any two field elements of the form $\alpha_i + \beta_j$ are conjugate over K. Thus, $S(\varphi_1, \varphi_2)(x) = \prod_{i,j} (x - (\alpha_i + \beta_j))$ is irreducible over K.

Now let α_i be a root of $\varphi_1(x)$ and β_j be a root of $\varphi_2(x)$. It is clear that $K(\alpha_i + \beta_j) \subseteq K(\alpha_i, \beta_j)$ and, since $\alpha_i + \beta_j$ has degree $n_1 n_2$ over K, these fields are equal. Therefore, the extension generated by $\alpha_i + \beta_j$ contains α_i and β_j, so the splitting field of $S(\varphi_1, \varphi_2)(x)$ over K is $L_1 L_2$. ▌

We will use this result in the following situation: suppose that for $i = 1, 2$, $\varphi_i(x) \in \mathbf{Q}[x]$ is irreducible of odd degree n_i with splitting field L_i and dihedral Galois group of order $2n_i$. Suppose further that L_1 and L_2 have the same quadratic subfield K. We have noted that $\varphi_1(x)$ and $\varphi_2(x)$ are irreducible over K, so if L_1 and L_2 are linearly disjoint over K, then $\varphi(x) = S(\varphi_1, \varphi_2)(x) \in \mathbf{Q}[x]$ is irreducible over K and, hence, over $\mathbf{Q}$ and the splitting field of $\varphi(x)$ over K and over $\mathbf{Q}$ is $L_1 L_2$. Thus, $\mathrm{Gal}(\varphi)$ is dihedral of order $2n_1 n_2$. In fact, if $\mathrm{Gal}(\varphi_1) = D_{m_1 \times \cdots \times m_s}$ and $\mathrm{Gal}(\varphi_2) = D_{k_1 \times \cdots \times k_t}$, then $\mathrm{Gal}(\varphi) = D_{m_1 \times \cdots \times m_s \times k_1 \times \cdots \times k_t}$. When n_1 and n_2 are relatively prime, then L_1 and L_2 are automatically linearly disjoint over K, and in many other cases we will be able to show that L_1 and L_2 are linearly disjoint by studying which primes of K ramify in L_1 and which ramify in L_2.

5.2. *The Case* $n = 9$

Clearly the extension $\mathbf{Q}(\mu_3, \sqrt[3]{2}, \sqrt[3]{3})/\mathbf{Q}$ has Galois group $D_{3 \times 3}$ and it is a easy matter to write down a degree 9 polynomial that has this extension as its splitting field: we let $\varphi(x) = x^9 - 15x^6 - 87x^3 - 125$, the minimal polynomial of $\sqrt[3]{2} + \sqrt[3]{3}$. Here $\mathrm{disc}(\varphi) = 2^6 \cdot 3^{42} \cdot 5^6$. We will now use our algorithm to show that $\mathrm{Gal}(\varphi)$ is dihedral of order 18 by verifying conditions (1)–(3) of the proposition.

When we verify condition (1) of the proposition, we find that

$$\begin{aligned} R(x_1 - x_2, \varphi)(x) = {} & (x^{18} - 8667x^{12} + 19842651x^6 + 19683) \\ & (x^{18} + 10773x^{12} + 2784051x^6 + 307546875) \\ & (x^6 + 108)^3\,(x^6 + 243)^3. \end{aligned}$$

We see that the irreducible factors are even polynomials and since $19683 = 3 \cdot 81^2$, $307546875 = 3 \cdot 10125^2$, $108 = 3 \cdot 6^2$, and $243 = 3 \cdot 9^2$, the quadratic field in question is, as we expect, $K = \mathbf{Q}(\sqrt{-3})$.

To verify condition (2), we first factor $\varphi(x)$ over K and find that it is irreducible over K. Next we need a resolvent of the form $R(e_1x_1+e_2x_2, \varphi)(x)$ with distinct roots. $R(x_1-x_2, \varphi)(x)$ has multiple roots, so we consider the resolvent $R(x_1+2x_2, \varphi)(x)$, which has distinct roots. The factorization of $R(x_1+2x_2, \varphi)(x)$ over $\mathbf{Q}(\sqrt{-3})$ is

$$\begin{gathered}
(x^9-(18\rho+9)\,x^6-4455x^3+(162\rho+81))\\
(x^9+(18\rho+9)\,x^6-4455x^3-(162\rho+81))\\
(x^9-(90\rho+45)\,x^6+2349x^3+(20250\rho+10125))\\
(x^9+(90\rho+45)\,x^6+2349x^3-(20250\rho+10125))\\
(x^9-(36\rho+261)\,x^6-(20412\rho-9153)\,x^3-(234900\rho+622647))\\
(x^9+(36\rho-225)\,x^6+(20412\rho+29565)\,x^3+(234900\rho-387747))\\
(x^9-(54\rho+189)\,x^6-(20412\rho+2187)\,x^3-(153090\rho+194643))\\
(x^9+(54\rho-135)\,x^6+(20412\rho+18225)\,x^3+(153090\rho-41553)),
\end{gathered}$$

where ρ is a primitive cube root of 1. This shows that the splitting field of $\varphi(x)$ over K has degree 9.

To verify condition (3), we take a prime $p \nmid \operatorname{disc}(\varphi)$ which remains inert in $\mathbf{Q}(\sqrt{-3})$. The first such prime is $p=11$ and

$$\begin{aligned}
\varphi(x) \equiv (x-5)&(x^2+1)(x^2-5x+1)\\
&(x^2+5x+1)(x^2+5x+3) \qquad (\mathrm{mod}\ 11).
\end{aligned}$$

Thus, we have shown that $\mathrm{Gal}(\varphi)$ is dihedral of order 18 and that $\mathbf{Q}(\sqrt{-3})$ is the unique quadratic subfield of the splitting field of $\varphi(x)$.

Since $\varphi(x)=x^9-15x^6-87x^3-125$ is a root sum polynomial, the resolvent $R(x_1-x_2, \varphi)(x)$ necessarily has multiple roots and it was therefore necessary to factor a second resolvent polynomial of the form $R(e_1x_1+e_2x_2, \varphi)(x)$. Since the amount of computer time required to factor these degree 72 polynomials is large compared to the time required to construct such polynomials, it is desirable, from the computational point of view, to construct another polynomial $\psi(x)$, whose roots generate the same extension as those of $\varphi(x)$, but such that the resolvent $R(x_1-x_2, \psi)(x)$ has *distinct* roots. This will essentially cut the computation time in half since $R(x_1-x_2, \psi)(x)$ will be the only resolvent which must be factored: we first factor the resolvent over $\mathbf{Q}$ (to determine the quadratic subfield $K=\mathbf{Q}(\sqrt{-3})$), then factor the irreducible factors thus obtained over K (to determine that the degree of the splitting field of $\psi(x)$ over K is 9). Since we started with specific extension in mind, it is an easy matter to construct such a polynomial $\psi(x)$. We note that the minimal polynomial of $\sqrt[3]{3}-\sqrt[3]{2}$ is $x^9-3x^6+165x^3-1$, so the minimal polynomial of $(\sqrt[3]{3}-\sqrt[3]{2})^{-1}$ is $\psi(x)=x^9-165x^6+3x^3-1$. Here $\operatorname{disc}(\psi)=2^6\cdot 3^{42}\cdot 5^6$ and $R(x_1-x_2, \psi)(x)$ has distinct roots.

However, if we were merely given the polynomial $\varphi(x)=x^9-15x^6-87x^3-125$ without any information about the extension that its roots generate, we still would be able to find a polynomial $\psi(x)$ with the desired properties. If α is a roots of $\varphi(x)$, we can easily determine the minimal polynomial of α^2. (Multiplication by α is a linear map on the vector space $\mathbf{Q}(\alpha)$. We can determine the matrix of this map with respect to any basis, square the matrix, and then compute the characteristic polynomial of the resulting matrix.) In our case the polynomial is

$$\psi(x)=x^9-399x^6+3819x^3-15625.$$

It is clear that the roots of $\psi(x)$ generate the same extension as those of $\varphi(x)$ and one may verify that $R(x_1-x_2, \psi)(x)$ has distinct roots. Thus, $\psi(x)$ is a better polynomial to use to verify that the extension in question is dihedral.

It was easy to construct a $D_{3\times 3}$-extension of $\mathbf{Q}$ containing $\mathbf{Q}(\sqrt{-3})$ because $\mathbf{Q}(\sqrt{-3})$ is the field of cube roots of unity. However, it is not difficult to construct a $D_{3\times 3}$-extension of $\mathbf{Q}$ containing an arbitrary quadratic field K. We consider the D_3-polynomial

$$\varphi(x)=\varphi_{d,t,u}(x)=x^3-3(3dt^2+u^2)\,x+2u(3dt^2+u^2).$$

Since $\operatorname{disc}(\varphi)=[18t(3dt^2+u^2)]^2\,d$, if we choose d, t, $u\in\mathbf{Z}$ such that d is a non-square and $\varphi(x)$ is irreducible over $\mathbf{Q}$, then the splitting field $\operatorname{spl}(\varphi)$ is a D_3-extension of $\mathbf{Q}$ containing $K=\mathbf{Q}(\sqrt{d})$. By fixing d and varying t and u we will obtain various D_3-extensions of $\mathbf{Q}$ each containing K. We can obtain two such extensions which are linearly disjoint over K by constructing extensions in which different sets of primes ramify. Note that if $p\nmid 2u$ and p^1 is the exact power of p dividing $(3dt^2+u^2)$, then $\varphi(x)$ is an Eisenstein polynomial, hence is irreducible over $\mathbf{Q}$, and the primes of K lying over p are totally ramified in $\operatorname{spl}(\varphi)$. Thus, we may construct a $D_{3\times 3}$-extension by constructing a polynomial $\varphi_1(x)$ which is Eisenstein for some prime p and a second polynomial $\varphi_2(x)$ whose discriminant is not divisible by p. If we take $\varphi(x)=S(\varphi_1, \varphi_2)(x)$, then $\operatorname{Gal}(\varphi)$ is $D_{3\times 3}$. For instance, if we fix $d=2$, then for $t=u=1$ we obtain $\varphi_1(x)=x^3-21x+14$, which is Eisenstein for $p=7$, and for $t=1$ and $u=3$ we obtain $\varphi_2(x)=x^3-45x+90$, whose discriminant is not divisible by 7. Then $\varphi(x) = x^9-198x^7+312x^6+10233x^5-18504x^4-164328x^3+179712x^2+$

$761472x-326656$ is a $D_{3\times 3}$-polynomial whose splitting field contains $\mathbf{Q}(\sqrt{2})$.

To construct a D_9-extension of $\mathbf{Q}$, we first construct a D_9-extension of $\mathbf{Q}(t)$, where t is an indeterminate. We consider the elliptic curve

$$E: y^2+3xy+6y=x^3+6x^2,$$

which is defined over $\mathbf{Q}$ and has a $\mathbf{Q}$-rational point of order 9, namely, $P=(0,0)$. We let $\mathscr{L}=\mathbf{Q}(E)=\mathbf{Q}(x,y)$ be the function field of $E/\mathbf{Q}$. For $Q\in E(\mathbf{Q})$, let $T_Q: E\to E$ be the map $R\mapsto R+Q$, and let $T_Q^*: f\mapsto f\circ T_Q$ be the corresponding automorphism of $\mathbf{Q}(E)$. Let $\langle P\rangle$ be the subgroup of order 9 generated by P, let $H=\{T_Q^*: Q\in\langle P\rangle\}$, and let $\mathscr{K}=\mathscr{L}^H$, the fixed field of H. Then $\mathscr{K}=\mathbf{Q}(t,u)$, where

$$t=\mathrm{Tr}_{\mathscr{L}/\mathscr{K}}(x)=\frac{p(x)}{x^2(x+2)^2\,(x-6)^2\,(x+6)^2}$$

and

$$u=\mathrm{Tr}_{\mathscr{L}/\mathscr{K}}(y)=\frac{q(x)\,y+r(x)}{x^3(x+3)^3\,(x-6)^3\,(x+6)^3},$$

where $p(x)=x^9+378x^7+6804x^6+33048x^5+50544x^4+7776x^3+139968x^2+279936x+186624$ and $q(x)$, $r(x)\in\mathbf{Z}[x]$. Here t and u satisfy the relationship

$$u^2+3tu+54u=t^3+18t^2-2268t-59778.$$

$\mathscr{K}$ is the function field over $\mathbf{Q}$ of the quotient curve $E'=E/\langle P\rangle$ and the extension $\mathscr{L}/\mathscr{K}$ is cyclic of degree 9. Now let $\mathrm{inv}: E\to E$ be the map $R\mapsto -R$ and let $\tau=\mathrm{inv}^*$ be the corresponding automorphism of $\mathscr{L}$. Then $\tau: x\mapsto x$, $y\mapsto -y-3x-6$, so τ leaves x and, hence, t fixed, and therefore $\tau\in\mathrm{Gal}(\mathscr{L}/\mathbf{Q}(t))$. We see that $\tau\sigma\tau=\sigma^{-1}$ for any $\sigma=T_Q^*\in\mathrm{Gal}(\mathscr{L}/\mathscr{K})$ so $\mathrm{Gal}(\mathscr{L}/\mathbf{Q}(t))=D_9$. Therefore,

$$g(x,t)=p(x)-x^2(x+2)^2\,(x-6)^2\,(x+6)^2\,t$$

is irreducible over $\mathbf{Q}(t)$ and has Galois group D_9. By the Hilbert Irreducibility Theorem (see Lang [4]), $\varphi(x)=g(x,\alpha)$ is irreducible over $\mathbf{Q}$ and has Galois group D_9 for infinitely many values $\alpha\in\mathbf{Q}$. For instance, we may take $\alpha=0$ to obtain $\varphi(x)=p(x)=x^9+378x^7+6804x^6+33048x^5+50544x^4+7776x^3+139968x^2+279936x+186624$. Here $\mathrm{disc}(\varphi)=2^{108}\cdot 3^{70}$. Again we will use our algorithm to verify that $\mathrm{Gall}(\varphi)$ is dihedral of order 18.

To verify condition (1) in the proposition, we factor $R(x_1-x_2,\varphi)(x)$

over $\mathbf{Q}$ and obtain 4 irreducible even polynomials of degree 18, whose constant coefficients are

$$526486815369068544 = 725594112^2,$$

$$11555266180939776 = 107495424^2,$$

$$739537035580145664 = 859963392^2,$$

and

$$180551034077184 = 13436928^2.$$

Thus, the quadratic field in question is $\mathbf{Q}(\sqrt{-1})$.

To verify condition (2), we note that $\varphi(x)$ is irreducible over $\mathbf{Q}(\sqrt{-1})$ and then factor $R(x_1 - x_2, \varphi)(x)$ over $\mathbf{Q}(\sqrt{-1})$. Over $\mathbf{Q}(\sqrt{-1})$, $R(x_1 - x_2, \varphi)(x)$ factors into 8 irreducible polynomials, each of degree 9.

Finally, to verify condition (3), we take $p \nmid \operatorname{disc}(\varphi)$ which remains inert in $\mathbf{Q}(\sqrt{-1})$. The first such prime is $p = 7$ and

$$\begin{aligned}\varphi(x) \equiv (x-3)(x^2+2)(x^2-3x-1)&\\ (x^2-3x+1)(x^2+2x+3) &\qquad (\text{mod } 7).\end{aligned}$$

Thus, we have shown that $\operatorname{Gal}(\varphi)$ is dihedral of order 18 and that $\mathbf{Q}(\sqrt{-1})$ is the unique quadratic subfield of the splitting field of $\varphi(x)$.

While the algorithm determines if the Galois group is dihedral, it does not determine the structure of the abelian subgroup of index 2. We will not treat this problem in general in this paper, but we will give several methods to treat the special case of a dihedral group of order 18.

PROPOSITION 5. *Suppose that* $\varphi(x) \in \mathbf{Z}[x]$ *is monic, irreducible, and of degree* 9 *with* $\operatorname{Gal}(\varphi)$ *dihedral of order* 18. *If the resolvent* $R(x) = R(x_1 + x_2 + x_3, \varphi)(x)$ *has distinct roots, then we may determine the structure of* $\operatorname{Gal}(\varphi)$ *by factoring* $R(x)$ *over* $\mathbf{Q}$. *Specifically,*

1. *if* $\operatorname{Gal}(\varphi) = D_9$, *then* $R(x)$ *factors into a product of* 1 *irreducible of degree* 3, 3 *irreducibles of degree* 9, *and* 3 *irreducibles of degree* 18, *and*

2. *if* $\operatorname{Gal}(\varphi) = D_{3\times 3}$, *then* $R(x)$ *factors into a product of* 4 *irreducibles of degree* 3 *and* 4 *irreducibles of degree* 18.

Proof. First suppose that $\operatorname{Gal}(\varphi) = D_9$. To represent $\operatorname{Gal}(\varphi)$ as a subgroup of S_9, we note that $\operatorname{Gal}(\varphi)$ has a 9-cycle, say $\sigma = (1\ 2 \cdots 9)$. If τ is an element of order 2 which fixes α_1, then from $\tau\sigma\tau = \sigma^{-1}$, we see that $\tau = (2\ 9)(3\ 8)(4\ 7)(5\ 6)$. These elements generate D_9, so we may write down all elements of D_9 and determine the action of D_9 on the collection of (unordered) sets of 3 roots of $\varphi(x)$. We find that there are 1 orbit of length 3, 3 orbits of length 9, and 3 orbits of length 18. McKay and Soicher's results [5] then imply that $R(x)$ factors as described in statement 1 of the proposition.

Similarly, if $\mathrm{Gal}(\varphi)=D_{3\times 3}$, then we may represent $\mathrm{Gal}(\varphi)$ as the subgroup of S_9 generated by $(1\,2\,3)(4\,5\,6)(7\,8\,9)$, $(1\,4\,7)(2\,5\,8)(3\,6\,9)$, and $(2\,3)(4\,7)(5\,9)(6\,8)$ and again determine the action of the group on the collection of sets of 3 roots of $\varphi(x)$. This time there are 4 orbits of length 3 and 3 orbits of length 18. Thus, the factorization of $R(x)$ is as described in statement 2 of the Proposition. ▮

The problems with this test are that $R(x)$ has degree 84 and it is quite time consuming to construct and factor this polynomial, and that $R(x)$ may have multiple roots in which case it would be necessary to find another field generator with minimal polynomial $\psi(\mathrm{x})$ such that the resolvent $R(x_1+x_2+x_3, \psi)(x)$ has distinct roots.

We now let $\varphi_1(x)$ be the D_9-polynomial $x^9+378x^7+6804x^6+33048x^5+50544x^4+7776x^3+139968x^2+279936x+186624$, and let $\varphi_2(x)$ be the $D_{3\times 3}$-polynomial $x^9-15x^6-87x^3-125$.

When we applied the above test to $\varphi_1(x)$, there was no problem: the resolvent $R(x_1+x_2+x_3, \varphi_1)(x)$ had distinct roots and its factorization over $\mathbf{Q}$ was as predicted by the proposition. However, $R(x_1+x_2+x_3, \varphi_2)(x)$ had multiple roots and it was necessary to find another irreducible degree 9 polynomial with the same splitting field as $\varphi_2(x)$. We used $\varphi_3(x)=x^9-177x^6-648x^5-1620x^4-2355x^3-2106x^2-1134x-773$, the minimal polynomial of $\sqrt[3]{2}+\sqrt[3]{3}+\sqrt[3]{6}+\sqrt[3]{12}$. (Constructing this polynomial was simple, but was possible only because we know the field extension in question.) Then $R(x_1+x_2+x_3, \varphi_3)(x)$ had distinct roots and its factorization over $\mathbf{Q}$ was as predicted by the proposition.

We would like to note other methods to distinguish between $D_{3\times 3}$ and D_9. These methods are somewhat *ad hoc*, but are considerably more efficient computationally.

First we note that $\varphi_1(x)$ is irreducible (mod 5). Thus, when we reduce modulo primes lying over 5, we have a residue field extension of degree 9. Hence, $\mathrm{Gal}(\varphi_1)$ must have a element of order 9, so $\mathrm{Gal}(\varphi_1)=D_9$.

Next we note that $R(x_1-x_2, \varphi_2)(x)$ has 2 irreducible factors of degree 6, $\rho_1(x)=x^6+108$ and $\rho_2(x)=x^6+243$. These are the minimal polynomials of certain elements of the splitting field of $\varphi_2(x)$. For $i=1, 2$, let γ_i be a root of $\rho_i(x)$. Now assume that $\mathrm{Gal}(\varphi_2)=D_9$. In this case, $\mathrm{spl}(\varphi_2)$ has only one subextension of degree 6 over $\mathbf{Q}$, so we must have $\mathbf{Q}(\gamma_1)=\mathbf{Q}(\gamma_2)$. Thus, $\gamma_1+\gamma_2$ can have degree at most 6 over $\mathbf{Q}$. But the minimal polynomial of $\gamma_1+\gamma_2$ is an irreducible factor of the root sum polynomial $\rho(x)=S(\rho_1, \rho_2)(x)$ and the factorization of $\rho(x)$ over $\mathbf{Q}$ is

$$(x^{18} - 8667x^{12} + 19842651x^6 + 19683)$$
$$(x^{18} + 10773x^{12} + 2784051x^6 + 307546875).$$

This contradiction establishes that $\mathrm{Gal}(\varphi_2) = D_{3\times 3}$.

5.3. *The Case $n = 15$*

We will construct a polynomial with Galois group D_{15} as follows: let $\varphi_1(x) \in \mathbf{Z}[x]$ be a polynomial with Galois group D_5 whose splitting field contains a quadratic field K and let $\varphi_2(x) \in \mathbf{Z}[x]$ be a polynomial with Galois group D_3 whose splitting field contains the same quadratic field K. Then if $\varphi(x)$ is the root sum polynomial $S(\varphi_1, \varphi_2)(x)$, then $\mathrm{Gal}(\varphi) = D_{5\times 3} = D_{15}$. We would like $\varphi(x)$ to have relatively small coefficients, so we will try to take $\varphi_1(x)$ and $\varphi_2(x)$ with coefficients that are small and zero whenever possible. Roland, Yui, and Zagier [7] give the polynomial $x^5 - 5x + 12$, whose splitting field is a D_5-extension of $\mathbf{Q}$ containing $\mathbf{Q}(\sqrt{-10})$. This will be $\varphi_1(x)$. To produce a D_3-extension of $\mathbf{Q}$ containing $\mathbf{Q}(\sqrt{-10})$, we will use the polynomial $\varphi_{d,t,u}(x)$ introduced in the last section. We take $d = -10$, $t = 2$, and $u = 11$ to obtain $\varphi_2(x) = x^3 - 3x + 22$. The root sum polynomial $S(\varphi_1, \varphi_2)(x)$ is then $\varphi(x) = x^{15} - 15x^{13} + 110x^{12} + 75x^{11} - 1284x^{10} + 4495x^9 + 11430x^8 - 66840x^7 + 76600x^6 + 164844x^5 + 153720x^4 + 1175520x^3 - 1060800x^2 - 5179200x + 6187904$. We now use our algorithm to verify that $\mathrm{Gal}(\varphi)$ is dihedral.

To verify condition (1) we note that the factorization of $R(x_1 - x_2, \varphi)(x)$ over $\mathbf{Q}$ is of the form $A^5 \cdot B^3 \cdot C^3 \cdot D \cdot E \cdot F \cdot G$, where $A, \ldots, G$ are irreducible and even with $\deg(A) = 6$, $\deg(B) = \deg(C) = 10$, and $\deg(D) = \deg(E) = \deg(F) = \deg(G) = 30$. The constant coefficients of these factors are

$$12960 = 10 \cdot 36^2,$$
$$4000 = 10 \cdot 20^2,$$
$$16000 = 10 \cdot 40^2,$$
$$442676506546929664000 = 10 \cdot 6653393920^2,$$
$$489870267788099584000 = 10 \cdot 6999073280^2,$$
$$34333741918544896000 = 10 \cdot 1852936640^2,$$

and

$$1480380926952411136000 = 10 \cdot 12167090560^2,$$

so the quadratic field in question is, as we expect, $\mathbf{Q}(\sqrt{-10})$.

To verify condition (2), we note that $\varphi(x)$ is irreducible over $\mathbf{Q}(\sqrt{-10})$, that $R(x_1 + 2x_2, \varphi)(x)$ has distinct roots, and that over $\mathbf{Q}(\sqrt{-10})$ this resolvent polynomial factors into 14 irreducible polynomials of degree 15.

To verify condition (3), we take a prime $p \nmid \operatorname{disc}(\varphi)$ which remains inert in $\mathbf{Q}(\sqrt{-10})$. The first such prime is $p=17$ and

$$\begin{aligned} \varphi(x) \equiv (x+7)(x^2-5x-5)(x^2-5x+8) \\ (x^2-x+6)(x^2+4x-2)(x^2+5x-1) \\ (x^2+6x+3)(x^2+6x+6) \qquad \pmod{17}. \end{aligned}$$

We have shown that $\operatorname{Gal}(\varphi)$ is dihedral of order 30 and that $\mathbf{Q}(\sqrt{-10})$ is the unique quadratic subfield of the splitting field of $\varphi(x)$.

5.4. *The Case $n=21$*

We will treat the Galois group D_{21} in much the same way as we treated the Galois group D_{15}: we will let $\varphi_1(x) \in \mathbf{Z}[x]$ be a polynomial with Galois group D_7 whose splitting field contains a quadratic field K and let $\varphi_2(x) \in \mathbf{Z}[x]$ be a polynomial with Galois group D_3 whose splitting field contains the same quadratic field K. Then if $\varphi(x)$ is the root sum polynomial $S(\varphi_1, \varphi_2)(x)$, then $\operatorname{Gal}(\varphi) = D_{7 \times 3} = D_{21}$. We let

$$\varphi_1(x) = x^7 - 2x^6 - x^5 + x^4 + x^3 + x^2 - x - 1.$$

This polynomial is given in Weber [10]. Its splitting field is the Hilbert Class Field of $\mathbf{Q}(\sqrt{-71})$. In particular, $\operatorname{Gal}(\varphi_1) = D_7$ and $\operatorname{spl}(\varphi_1) \supseteq \mathbf{Q}(\sqrt{-71})$. To construct a D_3-extension containing $\mathbf{Q}(\sqrt{-71})$, we again use the polynomial $\varphi_{d,t,u}(x)$. We take $d=-71$, $t=1$, and $u=15$ to obtain $x^3-36x+360$. We let $\varphi_2(x) = x^3 - 9x + 45$, which clearly generates the same extension. The root sum polynomial $S(\varphi_1, \varphi_2)(x)$ is then

$$\begin{aligned} \varphi(x) = x^{21} &- 6x^{20} + 240x^{19} - 1240x^{18} + 24696x^{17} - 108945x^{16} \\ &+ 1410773x^{15} - 5256357x^{14} + 48234981x^{13} - 149580758x^{12} \\ &+ 982724424x^{11} - 2487762960x^{10} + 10891586000x^{9} \\ &- 21984384291x^{8} + 46779215985x^{7} - 74840673504x^{6} \\ &- 63114954528x^{5} + 46891819239x^{4} + 41626168828x^{3} \\ &+ 50133555678x^{2} - 41816335086x - 52220177731. \end{aligned}$$

To verify condition (1) we note that the factorization of $R(x_1 - x_2, \varphi)(x)$ over $\mathbf{Q}$ is of the form $A^7 \cdot B^3 \cdot C^3 \cdot D^3 \cdot E \cdot F \cdot G \cdot H \cdot I \cdot J$, where $A, \ldots, J$ are irreducible and even with $\deg(A) = 6$, $\deg(B) = \deg(C) = \deg(D) = 14$, and

$\deg(E)=\deg(F)=\deg(G)=\deg(H)=\deg(I)=\deg(J)=42$. The constant coefficients of these factors are

$$51759=71\cdot 3^6,\ 71,\ 71,\ 71,$$

$$152307032219773256686529638120543 1=71\cdot 4631597421931369^2,$$

$$1023102650741521612883649360868151=71\cdot 3796036945199191^2,$$

$$1134801959955874058911508218451231=71\cdot 3997890218172781^2,$$

$$1128450079872082230725796754592879=71\cdot 3986685728370107^2,$$

$$1034032826936881438519101873768071=71\cdot 3816260294177249^2,$$

and

$$974018896215133459307616416140199=71\cdot 3703859608979537^2,$$

so the quadratic field in question is, as we expect, $\mathbf{Q}(\sqrt{-71})$.

To verify condition (2), we note that $\varphi(x)$ is irreducible over $\mathbf{Q}(\sqrt{-71})$, that $R(x_1+2x_2, \varphi)(x)$ has distinct roots, and that over $\mathbf{Q}(\sqrt{-71})$ this resolvent polynomial factors into 20 irreducible polynomials of degree 21.

To verify condition (3), we take a prime $p \nmid \operatorname{disc}(\varphi)$ which remains inert in $\mathbf{Q}(\sqrt{-71})$. The fist such prime is $p=13$ and

$$\begin{aligned}\varphi(x)\equiv{}&(x-1)(x^2-6x-6)(x^2-6x-2)\\&(x^2-6x+3)(x^2-4x+6)(x^2-x+5)\\&(x^2+2x-6)(x^2+2x+6)(x^2+4x-3)\\&(x^2+4x-1)(x^2+6x+1)\pmod{13}.\end{aligned}$$

We have shown that $\operatorname{Gal}(\varphi)$ is dihedral of order 42 and that $\mathbf{Q}(\sqrt{-71})$ is the unique quadratic subfield of the splitting field of $\varphi(x)$.

5.5. *The Case $n=25$*

We will construct a $D_{5\times 5}$-extension by starting with two D_5-polynomials whose splitting fields contain the same quadratic field. Roland, Yui, and Zagier's family [7] contains the polynomials $\varphi_1(x)=x^5-5x+12$ and $\varphi_2(x)=x^5+11275x+61500$. For $i=1,2$, $\operatorname{Gal}(\varphi_i)=D_5$ and $\operatorname{spl}(\varphi_i)\supseteq \mathbf{Q}(\sqrt{-10})$. Now the root sum polynomial $\varphi(x)=S(\varphi_1,\varphi_2)(x)$ is

$$\begin{aligned}&x^{25}+56350x^{21}+307560x^{20}+1277739625x^{17}+13912159800x^{16}\\&\quad+37376011440x^{15}+14327060755000x^{13}+235578171264000x^{12}\\&\quad+1294343053466400x^{11}+2412562855697280x^{10}\\&\quad+79873363709050000x^{9}+174240615596712000 0x^{8}\end{aligned}$$

$$+ 14222055194387580000x^7 + 51625642989217651200x^6$$
$$+ 251977508487372743680x^5 + 497927658525327360000x^4$$
$$+ 543034855856362867200000x^3 + 2962586569934658078720000x^2$$
$$+ 806828758126280636313600x + 87785383535209242456883 2.$$

We verified that $\varphi(x)$ is irreducible over $\mathbf{Q}$, so it follows immediately that $\mathrm{spl}(\varphi_1)$ and $\mathrm{spl}(\varphi_2)$ are linearly disjoint over $\mathbf{Q}(\sqrt{-10})$. Hence, $\varphi(x)$ is a $D_{5\times 5}$-polynomial.

To verify condition (1) we note that the factorization of $R(x_1 - x_2, \varphi)(x)$ over $\mathbf{Q}$ is of the form $A^5 \cdot B^5 \cdot C^5 \cdot D^5 \cdot E \cdot F \cdot G \cdot H \cdot I \cdot J \cdot K \cdot L$, where $A, ..., L$ are irreducible and even with $\deg(A) = \deg(B) = \deg(C) = \deg(D) = 10$, and $\deg(E) = \deg(F) = \deg(G) = \deg(H) = \deg(I) = \deg(J) = \deg(K) = \deg(L) = 50$. The constant coefficients of these factors are

$$10 \cdot 40^2,\ 10 \cdot 20^2,\ 10 \cdot 237800^2,\ 10 \cdot 127100^2$$
$$10 \cdot 335447250038508485376000000^2$$
$$10 \cdot 700519733626559523225600000 0^2$$
$$10 \cdot 739727881002484000358400000 0^2$$
$$10 \cdot 442892793497191588944000000 0^2$$
$$10 \cdot 282983447059982057472000000 0^2$$
$$10 \cdot 802240075038861882731200000 00^2$$
$$10 \cdot 802314798738412489804800000 00^2$$
$$10 \cdot 280627349505366532608000000 0^2,$$

so the quadratic field in question is $\mathbf{Q}(\sqrt{-10})$.

To verify condition (2), we note that $\varphi(x)$ is irreducible over $\mathbf{Q}(\sqrt{-10})$, that $R(x_1 + 2x_2, \varphi)(x)$ has distinct roots, and that the factorization of this resolvent polynomial over $\mathbf{Q}(\sqrt{-10})$ is over $\mathbf{Q}(\sqrt{-10})$; this resolvent polynomial factors into 24 irreducible polynomials of degree 25.

To verify condition (3), we take a prime $p \nmid \mathrm{disc}(\varphi)$ which remains inert in $\mathbf{Q}(\sqrt{-10})$. The first such prime is $p = 17$ and

$$\begin{aligned} \varphi(x) \equiv (x-4)(x^2-3)(x^2-7x-3) \\ (x^2-7x-2)(x^2-6x-5)(x^2-6x-3) \\ (x^2-6x+2)(x^2-x-7)(x^2-x+3) \\ (x^2+3x+5)(x^2+5x-3)(x^2+5x+7) \\ (x+8x+4) \qquad (\mathrm{mod}\ 17). \end{aligned}$$

We have shown that $\mathrm{Gal}(\varphi)$ is dihedral of order 50 and that $\mathbf{Q}(\sqrt{-10})$ is the unique quadratic subfield of the splitting field of $\varphi(x)$.

References

1. C. U. Jensen, Remark on a characterization of certain ring class fields by their absolute Galois group, *in* "Proceedings, Amer. Math. Soc.", Vol. 14, No. 5 pp. 738–741, Providence, RI, 1963.
2. Christian U. Jensen and Noriko Yui, Polynomials with D_p as Galois group, *J. Number Theory* **15** (1982), 347–375.
3. Serge Lang, "Algebra," Addison–Wesley, Reading, MA, 1965.
4. Serge Lang, "Fundamentals of Diophantine Geometry," Springer-Verlag, New York/Berlin, 1983.
5. John McKay and Leonard Soicher, Computing Galois groups over the rationals, *J. Number Theory* **20** (1985), 273–281.
6. Jean-François Mestre, Courbes elliptiques et groups de classes d'idéaux de certains corps quadratiques, *J. Reine Angew. Math.* **343** (1983), 23–35.
7. G. Roland, N. Yui, and D. Zagier, A parametric family of quintic polynomials with Galois group D_5, *J. Number Theory* **15** (1982), 137–142.
8. Leonard Soicher, M. Comp. Sci. thesis, Concordia University, Montréal, 1981.
9. B. L. van der Waerden, "Algebra," Ungar, New York, 1970.
10. Heinrich Weber, "Lehrbuch der Algebra," Vol. 3, 2nd ed., Braunschweig,