Pacific Journal of Mathematics

DIHEDRAL GALOIS GROUPS OF EVEN DEGREE POLYNOMIALS

MARIA ÁNGELES GÓMEZ-MOLLEDA

Volume 229 No. 1 January 2007

PACIFIC JOURNAL OF MATHEMATICS
Vol. 229, No. 1, 2007

DIHEDRAL GALOIS GROUPS OF EVEN DEGREE POLYNOMIALS

MARIA ÁNGELES GÓMEZ-MOLLEDA

We present a new characterization of dihedral Galois groups of rational irreducible polynomials. It allows us to reduce the problem of deciding whether the Galois group of an even degree polynomial is dihedral, and its computation in the affirmative case, to the case of a quartic or odd degree polynomial, for which algorithms already exist. The characterization and algorithm are extended to permutation groups of order $2n$ containing an n-cycle.

1. Introduction

Given an irreducible polynomial $f \in \mathbb{Q}[x]$, we consider the problem of deciding whether its Galois group is dihedral, and, if so, we compute a minimal set of generators with its explicit action on the set of roots.

Methods are already known for polynomials of prime degree [Jensen and Yui 1982] and of odd degree [Williamson 1990]. Here we consider the case of even degree polynomials. For it, we provide a characterization of dihedral Galois groups, based on the behavior of f related to a quadratic subfield K of its splitting field and a certain prime number. The quadratic subfield must be determined in order to decide whether the Galois group is dihedral. In the affirmative case, the roots of f will be expressed as polynomials in a fixed root α and a primitive element of K over $\mathbb{Q}$. For computing K, we propose to transform f, after certain reductions, into either a quartic or an odd degree polynomial whose splitting field contains K. Such reductions are made from the nontrivial central elements of the Galois group.

In Section 2 we state the characterization of dihedral Galois groups, whereas Section 3 is devoted to the algorithm that decides whether the group is dihedral. Finally, in Section 4, we extend the results to groups of order $2n$ containing a cyclic subgroup of order n, taking advantage of their similarity to dihedral groups.

MSC2000: primary 12Y05; secondary 11R32.
Keywords: Dihedral Galois group, polynomials.
Partially supported by MCyT BFM 2002-04402-C02-0.

Since for every irreducible $f \in \mathbb{Q}[x]$ there exists a monic and irreducible polynomial in $\mathbb{Z}[x]$ with the same Galois group, we will assume throughout this paper that f is monic and irreducible with integer coefficients.

From now on, we will denote by Gal f the Galois group of f over $\mathbb{Q}$, whereas $\mathrm{Gal}_K f$ will represent the Galois group over a number field K.

If n is the degree of f, we will consider Gal f as a permutation group of degree n acting on the set of roots of f. By E_f we will denote the splitting field of f over $\mathbb{Q}$. If L is a subfield of E_f and H is a subgroup of Gal f, then L^H is the subfield of elements in L fixed by H. We denote by O_L the ring of integers of L and by $Z(H)$ the center of H.

2. Characterization of dihedral Galois groups

The dihedral group D_n, considered as a transitive subgroup of S_n, is generated by σ, τ, where σ is an n-cycle, τ has order 2 and $\tau\sigma\tau = \sigma^{-1}$.

Propositions 2.1 and 2.2 provide a characterization of dihedral Galois groups.

Proposition 2.1. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree $n > 2$ satisfying the following conditions*:

(i) *E_f has a quadratic subfield $K = \mathbb{Q}(\sqrt{a})$ for some squarefree $a \in \mathbb{Z}$.*

(ii) *$f \bmod p$ is irreducible for some odd prime $p \in \mathbb{Z}$, and $x^2 - a \bmod p$ splits*:

$$x^2 - a \equiv (x+b)(x+c) \bmod p$$

with b, c distinct modulo p.

(iii) *There exists $F \in K[x]$ such that*

$$F(x) \equiv A(\sqrt{a}+b)x^p - A(\sqrt{a}+c)x^{p^{n-1}} \bmod \big(p, f(x)\big),$$

where $A = (b-c)^{-1} \bmod p$, and $f\big(F(\alpha)\big) = 0$ for some root α of f.

Then Gal $f = D_n$.

Proof. By condition (i) and the Fundamental Theorem of Galois Theory, $\mathrm{Gal}_K f$ is a normal subgroup of Gal f of index 2.

Since $f \bmod p$ is irreducible, a Frobenius automorphism σ in Gal f over p is an n-cycle. Let Q be a prime ideal in O_{E_f} lying over p such that

$$\sigma(u) \equiv u^p \bmod Q \quad \text{for every } u \in O_{E_f}.$$

As $x^2 - a \bmod p$ splits, σ fixes K pointwise, so σ is in $\mathrm{Gal}_K f$. Therefore, $\mathrm{Gal}_K f$ is transitive of degree n, and f is irreducible over K.

Also by condition (ii), $(p, \sqrt{a}+b)$ and $(p, \sqrt{a}+c)$ are the prime ideals in O_K lying over p. We assume without loss of generality that Q lies over $(p, \sqrt{a}+c)$.

By condition (iii), $F(x) \equiv x^p \bmod \big(p, \sqrt{a}+c, f(x)\big)$. In particular,

$$F(\alpha) \equiv \alpha^p \bmod Q.$$

Then, $F(\alpha) - \sigma(\alpha) \in Q$. If $F(\alpha) \neq \sigma(\alpha)$, then the discriminant $\operatorname{disc} f$ lies in $Q \cap \mathbb{Z} = p\mathbb{Z}$, but $f \bmod p$ is irreducible. Thus $F(\alpha) = \sigma(\alpha)$. As σ is an n-cycle, the equality holds for every root of f, so $\sigma \in Z(\operatorname{Gal}_K f)$; see [Fernández-Ferreirós and Gómez-Molleda 2004]. Thus, $\operatorname{Gal}_K f = \langle\sigma\rangle$. Moreover, the order of $\operatorname{Gal} f$ is $2n$. If τ is a representative of the nontrivial class of $\operatorname{Gal}_K f$ in $\operatorname{Gal} f$, then Q and $Q' = \tau Q$ are the prime ideals in O_{E_f} over p. Then

$$\tau^{-1}\sigma\tau(u) \equiv u^p \bmod Q' \quad \text{for every } u \in O_{E_f}$$

and

$$(\tau^{-1}\sigma\tau)^{n-1}(u) \equiv u^{p^{n-1}} \bmod Q' \quad \text{for every } u \in O_{E_f}.$$

Again by condition (iii), $F(\alpha) \equiv \alpha^{p^{n-1}} \bmod Q'$. Reasoning as above we have $F(\alpha) = (\tau^{-1}\sigma\tau)^{n-1}(\alpha)$ for every root α of f. Then $\tau^{-1}\sigma\tau = \sigma^{-1}$.

Finally, since σ is an n-cycle, τ is easily seen to have order 2. □

We state the converse of Proposition 2.1, strengthening the conditions:

Proposition 2.2. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree $n > 2$ such that $\operatorname{Gal}_{\mathbb{Q}} f = D_n$.*

(i) *There exists a unique quadratic subfield K of E_f such that f is irreducible over K and $\operatorname{Gal}_K f$ is cyclic.*

In fact, $K = E_f^{\langle\sigma\rangle}$ for every n-cycle $\sigma \in D_n$.

(ii) *The proportion of integer primes p such that f is irreducible modulo p is $\phi(n)/2n$, where ϕ is the Euler function.*

If a is a squarefree integer such that $K = \mathbb{Q}(\sqrt{a})$, then for every odd prime p under this condition, $x^2 - a$ splits modulo p, that is,

$$x^2 - a \equiv (x+b)(x+c) \bmod p$$

for some $b, c \in \mathbb{Z}$ distinct modulo p.

(iii) *There exists a unique polynomial $F \in K[x]$ of degree smaller than n such that $F(\alpha)$ is a root of f for every root α of f, and*

$$F(x) \equiv A(\sqrt{a}+b)x^p - A(\sqrt{a}+c)x^{p^{n-1}} \bmod \big(p, f(x)\big),$$

where $A = (b-c)^{-1} \bmod p$.

Proof. Let σ, τ be generators of D_n as a transitive subgroup of S_n, where σ is an n-cycle, τ has order 2 and $\tau\sigma\tau = \sigma^{-1}$.

(i) $\langle\sigma\rangle$ is the unique normal subgroup of index 2 in D_n that is cyclic and transitive in S_n. The statement follows from the Fundamental Theorem of Galois Theory.

(ii) By the Chebotarev Density Theorem, the proportion of primes p such that $f \bmod p$ is irreducible is the proportion of n-cycles in the Galois group. The number of n-cycles in D_n is exactly $\phi(n)$.

Since f is irreducible modulo p, the Frobenius automorphisms over p are n-cycles. Then they fix K pointwise, so $x^2 - a$ splits modulo p whenever p does not divide $4a$, the discriminant of $x^2 - a$. If p is odd and p divides $4a$, then p divides a, so it divides the discriminant of O_K, and therefore p is ramified in O_K. This is a contradiction since p is unramified in O_{E_f}.

(iii) As stated above, the Frobenius automorphisms of E_f over p belong to $\langle\sigma\rangle$. We can assume without loss of generality that σ is the Frobenius automorphism over the prime ideal $(p, \sqrt{a}+b)$ in O_K. Thus, for the prime Q in O_{E_f} over $(p, \sqrt{a}+b)$,

$$\sigma(u) \equiv u^p \bmod Q \quad \text{for every } u \in O_{E_f},$$

since the norm of $(p, \sqrt{a}+b)$ is p. Its conjugate, σ^{n-1}, satisfies the corresponding property for the other prime Q' over p:

$$\sigma^{n-1}(u) \equiv u^p \bmod Q' \quad \text{for every } u \in O_{E_f}.$$

Thus,

$$\sigma(u) \equiv u^{p^{n-1}} \bmod Q' \quad \text{for every } u \in O_{E_f}.$$

By the Chinese Remainder Theorem and because $pO_{E_f} = QQ'$,

$$\sigma(u) \equiv A(\sqrt{a}+b)u^p - A(\sqrt{a}+c)u^{p^{n-1}} \bmod p \quad \text{for every } u \in O_{E_f}.$$

On the other hand, since $\mathrm{Gal}_K f$ is cyclic and f is irreducible over K, the splitting field of f over K is $K(\alpha)$ for any root α of f. Then $\sigma(\alpha) \in K[\alpha]$, so there exists a unique polynomial $F \in K[x]$ of degree smaller than n such that $\sigma(\alpha) = F(\alpha)$. Since $\mathrm{Gal}_K f$ is transitive and abelian, the equality holds for every root of f.

If $\tilde{F}$ also satisfies the same conditions as F, then $F(\alpha) - \tilde{F}(\alpha) \in pO_{E_f}$ for every root α of f. If $F(\alpha) \neq \tilde{F}(\alpha)$, then $\mathrm{disc}\, f \in p\mathbb{Z}$, which is impossible because f has no multiple root modulo p. Since the degrees of both polynomials are smaller than n, they must be equal. □

3. An algorithm to decide whether the Galois group is dihedral

We will describe an algorithm, based on the preceding characterization, to decide whether the Galois group of a given monic irreducible polynomial $f \in \mathbb{Z}[x]$ of even degree $n > 2$ is dihedral, and to determine explicitly the group in the affirmative case.

Essentially, the algorithm consists in checking whether or not the polynomial satisfies conditions (i)–(iii) in Proposition 2.1. In order to discuss condition (i), we will first determine the center of the Galois group.

The center of the dihedral Galois group. If n is even, the center of D_n has order 2. For determining the center, we use any odd prime $p \in \mathbb{Z}$ such that $f \bmod p$ is irreducible; the proportion of such primes in the dihedral case, according to Proposition 2.2, is $\phi(n)/2n$.

Proposition 3.1. *Let p be a prime such that $f \bmod p$ is irreducible and $\sigma_p \in \operatorname{Gal} f$ is a Frobenius automorphism over p. Then $Z(\operatorname{Gal} f) \subseteq \langle \sigma_p \rangle$.*

Moreover, σ_p^k is central if and only if there exists $H \in \mathbb{Q}[x]$ such that

$$H(x) \equiv x^{p^k} \bmod \big(p,\, f(x)\big),$$

and, given any root α of f, $H(\alpha)$ is a root of f.

When σ_p^k is central, the polynomial H describes the action of σ_p^k:

$$H(\alpha) = \sigma_p^k(\alpha) \quad \text{for every root } \alpha \text{ of } f.$$

Proof. This follows from the characterizations of $Z(\operatorname{Gal} f)$ given in [Fernández-Ferreirós and Gómez-Molleda 2004]. □

Lifting x^{p^k} up to a certain power of $\big(p,\, f(x)\big)$ and checking if the polynomial obtained permutes the roots of f, we determine the centrality of σ_p^k.

Construction of the quadratic subfield. We now show a procedure to either provide a quadratic subfield K of E_f such that f is irreducible over K, or to conclude that the Galois group is not dihedral. When the group is dihedral, K is precisely the unique subfield in condition (i) of Proposition 2.2.

In [Williamson 1990], assuming that n is odd, it is proved that if the irreducible factors of the resolvent $R(x_1 - x_2,\, f)$ are even polynomials of degree dividing $2n$, d is the independent coefficient of any of them and $-d$ is not a square in $\mathbb{Q}$, then $\mathbb{Q}(\sqrt{-d}\,)$ is a quadratic subfield of E_f, otherwise the Galois group is not dihedral.

The method of C. J. Williamson is not applicable to even degree polynomials. Next we solve the case of quartic polynomials, and give a procedure for reducing the problem of even degree to either quartic or odd degree polynomials.

Lemma 3.2. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree* 4.

(1) $\operatorname{Gal} f$ *equals D_4 if and only if the center of* $\operatorname{Gal} f$ *has order* 2.

(2) *If $\big\langle (1,3)(2,4) \big\rangle$ is the center of D_4, then $D_4 = \big\langle (1,2,3,4), (1,3) \big\rangle$.*

(3) *$K = E_f^{\langle (1,2,3,4) \rangle}$ is a quadratic subfield with f irreducible over K.*

The proof is straightforward.

Once it is known that Gal $f = D_4$, one can quickly determine a primitive element of E_f, since E_f is generated by two roots of f, and the number of subfields is only 8. If $\sigma = (1, 2, 3, 4)$ and γ is a primitive element of E_f, not every elementary symmetric function of $\{\gamma, \sigma(\gamma), \sigma^2(\gamma), \sigma^3(\gamma)\}$ is rational. Any of them not belonging to $\mathbb{Q}$ is a primitive element of K.

If $n > 4$ is even, we will reduce successively the problem to polynomials of smaller degree, which we call derived polynomials:

Definition 3.3. Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n, and let α be a root of f. If there exists a nontrivial element $\tau \in Z(\text{Gal } f)$, let β be an algebraic integer and primitive element of $\mathbb{Q}(\alpha)^{\langle\tau\rangle}$ over $\mathbb{Q}$, and let $g \in \mathbb{Z}[x]$ be its minimal polynomial. We call g a derived polynomial from f by τ.

The degree of g is n/r, where r is the order of τ. A proof can be found in [Fernández-Ferreirós and Gómez-Molleda 2004] along with a simple procedure to construct derived polynomials.

The following proposition provides a method to compute a quadratic subfield K of E_f for a given polynomial f, or to conclude that Gal f is not dihedral:

Proposition 3.4. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of even degree $n > 4$ such that* Gal $f = D_n$. *If g is a derived polynomial from f by the central element of order* 2, *then* Gal $g = D_{n/2}$ *and* $E_f^{\langle\sigma\rangle} = E_g^{\langle\overline{\sigma}\rangle}$, *where σ and $\overline{\sigma}$ are an n-cycle and an $n/2$-cycle in* Gal f *and* Gal g, *respectively.*

Proof. Let $D_n = \langle\sigma, \tau\rangle$ with $O(\sigma) = n$, $O(\tau) = 2$ and $\tau\sigma\tau = \sigma^{-1}$. The only nontrivial central element in D_n is $\rho = \sigma^{n/2}$, whose order is 2.

Gal $g = D_n/S = \langle\overline{\sigma}, \overline{\tau}\rangle$, where $S = \langle\rho_1, \ldots, \rho_{n/2}\rangle \cap D_n$, and $\rho_1, \ldots, \rho_{n/2}$ are the disjoint transpositions of ρ and $\overline{\sigma}$, $\overline{\tau}$ the classes of σ and τ, respectively. Since $\sigma^{n/2} \in S$ and there is no other power of σ of order 2, whereas every element of S has order 2, we get $O(\overline{\sigma}) = n/2$.

We know that g is irreducible of degree $n/2$, so $|\text{Gal } g| \geq n/2$. Thus, $|S| = 2$ or 4. If $|S| = 4$, then Gal $g = \langle\overline{\sigma}\rangle$ and $\overline{\tau}\,\overline{\sigma}\,\overline{\tau} = \overline{\sigma}$. But $\overline{\tau}\,\overline{\sigma}\,\overline{\tau} = \overline{\sigma}^{-1}$, and $\sigma S \neq \sigma^{-1} S$ (otherwise $n = 4$). Therefore Gal $g = D_{n/2}$.

As $E_g \subset E_f$, $\overline{\sigma} = \sigma\langle\rho\rangle$ and ρ fixes E_g pointwise, we conclude that $E_g^{\langle\overline{\sigma}\rangle} \subseteq E_f^{\langle\sigma\rangle}$. Both fields are quadratic over $\mathbb{Q}$, so they must coincide. □

As a consequence of Proposition 3.4, if the Galois group of the given polynomial is dihedral, the unique quadratic subfield in condition (i) of Proposition 2.2 is that of any derived polynomial.

In general, if we get a derived polynomial of odd degree or degree 4 whose Galois group is dihedral, its quadratic subfield K is also contained in E_f, and we have condition (i) in Proposition 2.1. Moreover, f is irreducible over K.

End of the algorithm. Let $p \in \mathbb{Z}$ be an odd prime such that $f \bmod p$ is irreducible (we have already obtained it for computing the center). If the Galois group is dihedral, then $x^2 - a \bmod p$ splits by condition (ii) in Proposition 2.2: $x^2 - a \equiv (x+b)(x+c) \bmod p$. To check condition (iii) in Proposition 2.1, we use quadratic Newton lifting, which allows the computation of $F \bmod p^{2^k}$ up to any k.

Notice that $F(x) = F_1(x) + \sqrt{a}F_2(x)$ with $F_1, F_2 \in \mathbb{Q}[x]$. Thus it is simpler to work in $\mathbb{Q}[x]$, and the Newton lifting in $\mathbb{Q}(\sqrt{a})[x]$ for the given polynomial is not much harder than in $\mathbb{Q}[x]$.

Bounds are known on the coefficients of F_1, F_2 (a straightforward generalization of the results in [Dixon 1990]). Thus, if the polynomial F in the required conditions exists, it is easily determined from $F \bmod p^{2^k}$ with k large enough.

Example 3.5. We consider the irreducible polynomial

$$\begin{aligned} f(x) = x^{30} &+ 15x^{28} - 20x^{27} + 135x^{26} - 228x^{25} + 895x^{24} - 1080x^{23} + 2010x^{22} \\ &- 1870x^{21} - 2682x^{20} - 840x^{19} + 6735x^{18} - 66690x^{17} + 132855x^{16} \\ &- 331936x^{15} + 637515x^{14} - 387270x^{13} + 1466250x^{12} - 1155870x^{11} \\ &+ 82710x^{10} - 2939470x^9 - 129075x^8 + 660750x^7 + 2836550x^6 \\ &+ 1971960x^5 + 1124850x^4 + 280300x^3 + 42300x^2 + 7500x + 725. \end{aligned}$$

We have checked that f remains irreducible mod 19. We compute the center, of order 2, and obtain the derived polynomial

$$\begin{aligned} g(x) = x^{15} &- 15x^{14} + 135x^{13} - 755x^{12} + 2550x^{11} - 4290x^{10} + 2395x^9 - 4875x^8 \\ &+ 39975x^7 - 74750x^6 + 33090x^5 + 15675x^4 - 6950x^3 - 1050x^2 - 1500x - 725. \end{aligned}$$

Since the degree of g is congruent to 3 mod 4, its discriminant is not a perfect square, otherwise the Galois group is not dihedral. Precisely,

$$K = \mathbb{Q}\big(\sqrt{\operatorname{disc} g}\,\big) = \mathbb{Q}(\sqrt{-15}\,)$$

is a quadratic subfield of the splitting field of g, and therefore a quadratic subfield of E_f. Moreover,

$$x^2 + 15 \equiv (x+2)(x+17) \bmod 19.$$

It remains to check whether there exists a polynomial satisfying the third condition in Proposition 2.1. By means of Newton lifting we obtain

$$\begin{aligned} F(x) = {} & \tfrac{78705199522740662980850936383320197413945663132536272567919488639}{34390727770780900149705596163521595177782209179717772991415373721887}\, x^{29} + \cdots \\ & \cdots\cdots\cdots + \tfrac{35163553259550871700540691155402908776210583552656812429856449486132}{42045090378070692972994302519665900060611478307491948171322870694 47} \\ & + \tfrac{45906483199164589345341721201472645340073265776270072931299700 2459}{13412383830604551058385182503773422119335061580089931466651995751535 93}\, i\sqrt{15}x^{29} + \cdots \\ & \cdots\cdots + \tfrac{10793822840327679259688966253357691052394007590393980279241368538 40}{78389151552335190288633445375648288248597671420747699980432470786 3}\, i\sqrt{15}, \end{aligned}$$

which transforms a root of f into another root.

Therefore $E_f = \mathbb{Q}(\alpha, \sqrt{-15})$, where α is any root of f and Gal f is dihedral, generated by σ and τ such that

$$\sigma(\alpha) = F(\alpha), \quad \tau(\alpha) = \alpha, \quad \sigma(\sqrt{-15}) = \sqrt{-15}, \quad \tau(\sqrt{-15}) = -\sqrt{-15}.$$

Example 3.6. Let $f(x) = x^{12} + 10x^6 + 5$, which is irreducible modulo 7.

A derived polynomial from f by the order 2 central element is

$$g_1(x) = x^6 - 10x^3 + 5.$$

The polynomial g_1 is also irreducible modulo 7, and

$$g_2(x) = x^3 - 5$$

is a derived polynomial from g_1. Then $K = \mathbb{Q}\big(\sqrt{\operatorname{disc} g_2}\big) = \mathbb{Q}(\sqrt{-3})$ is a quadratic subfield of E_f. Moreover,

$$x^2 + 3 \equiv (x+2)(x+5) \bmod 7.$$

However, the third condition in Proposition 2.1 is not satisfied (the polynomial we obtain by Newton lifting does not permute the roots of f). Thus, by Propositions 2.2 and 3.4, Gal f is not dihedral.

Note. We could have stopped earlier, since $Z(\text{Gal } f)$ has order 4. Nonetheless, it is interesting to see that f "almost" satisfies every condition in Proposition 2.1:

$$F(x) = -\tfrac{7}{8}x + \tfrac{7}{8}\sqrt{-3}x - \tfrac{1}{8}x^7 + \tfrac{1}{8}\sqrt{-3}x^7 \in K[x]$$

permutes the roots of f, and

$$F(x) \equiv 5(\sqrt{-3}+5)x^7 - 5(\sqrt{-3}+2)x^{7^5} \bmod \big(7, f(x)\big).$$

It follows from Proposition 4.1 below that Gal f has order 24 and is generated by two elements σ, τ, where σ is an n-cycle and $\tau\sigma\tau^{-1} = \sigma^5$. Moreover, $E_f = \mathbb{Q}(\alpha, \sqrt{-3})$, where α is any root of f, and

$$\sigma(\alpha) = F(\alpha), \quad \tau(\alpha) = \alpha, \quad \sigma(\sqrt{-3}) = \sqrt{-3}, \quad \tau(\sqrt{-3}) = -\sqrt{-3}.$$

4. Groups of order $2n$ that contain a cyclic subgroup of order n

The characterization of dihedral Galois groups can be generalized to transitive subgroups of S_n, of order $2n$, containing an n-cycle.

Let G be one of these groups and $\sigma \in G$ an n-cycle. Then there exists an integer m such that $\tau^{-1}\sigma\tau = \sigma^m$ for every $\tau \in G - \langle\sigma\rangle$. Since there is no transitive abelian subgroup of S_n having order larger than n, we have $m \not\equiv 1$ modulo n.

The group G is determined by n and m mod n up to isomorphism, so we write $G = G(n, m)$. It is simple to prove that $(m, n) = 1$ and $m^2 \equiv 1 \bmod n$.

See [Hwang et al. 2003] for a detailed and more general classification of these groups, where they are not assumed to be subgroups of S_n.

Proposition 4.1. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree $n > 2$ satisfying the following conditions*:

(i) *E_f has a quadratic subfield $K = \mathbb{Q}(\sqrt{a})$ for some $a \in \mathbb{Z}$ squarefree.*

(ii) *$f \bmod p$ is irreducible for some odd prime $p \in \mathbb{Z}$, and $x^2 - a$ splits*:

$$x^2 - a \equiv (x+b)(x+c) \bmod p$$

with b, c distinct modulo p.

(iii) *There exists $F \in K[x]$ such that*

$$F(x) \equiv A(\sqrt{a}+b)x^p - A(\sqrt{a}+c)x^{p^m} \bmod (p,\, f(x)),$$

where $A = (b-c)^{-1} \bmod p$, and $f\big(F(\alpha)\big) = 0$ for some root α of f.

Then $\operatorname{Gal} f = G(n, m)$.

Proof. The proof is essentially the same as for Proposition 2.1. □

The converse cannot be strengthened as far as for dihedral groups, since the case $8 \mid n$ and $m = (n/2) + 1$ is peculiar:

Proposition 4.2. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree $n > 2$ such that* $\operatorname{Gal}_{\mathbb{Q}} f = G(n, m)$.

If $8 \nmid n$ or $m \neq (n/2) + 1$, then:

(i) *There exists a unique quadratic subfield K of E_f such that f is irreducible over K, and* $\operatorname{Gal}_K f$ *is cyclic.*

In fact, $K = E_f^{\langle\sigma\rangle}$ for every n-cycle $\sigma \in G(n, m)$.

(ii) *The proportion of integer primes p such that f is irreducible modulo p is $\phi(n)/2n$. If a is a squarefree integer such that $K = \mathbb{Q}(\sqrt{a})$, then for every odd prime p under this condition, $x^2 - a$ splits modulo p, that is, $x^2 - a \equiv (x+b)(x+c) \bmod p$ for some $b, c \in \mathbb{Z}$ distinct modulo p.*

(iii) *There exists a unique polynomial $F \in K[x]$ of degree smaller than n such that $F(\alpha)$ is a root of f for every root α of f, and*

$$F(x) \equiv A(\sqrt{a}+b)x^p - A(\sqrt{a}+c)x^{p^m} \bmod \big(p,\, f(x)\big),$$

where $A = (b-c)^{-1} \bmod p$.

If $8 \mid n$ and $m = (n/2) + 1$, there exists more than one cyclic subgroup of order n in $G(n, m)$. Therefore the quadratic subfield satisfying conditions (i)–(iii) *is not unique. In such a case $\phi(n)/2n$ is the proportion of primes p such that $f \bmod p$ is irreducible, and $x^2 - a$ splits modulo p for a given quadratic subfield $\mathbb{Q}(\sqrt{a})$. For such primes, condition* (iii) *holds.*

Proof. It can be proved that a cyclic subgroup of $G(n, m)$ of order n is generated by an n-cycle. Therefore, it is enough to prove that there exist n-cycles $\sigma, \tau \in G(n, m)$ such that $\langle\sigma\rangle \neq \langle\tau\rangle$ if and only if $8 \mid n$ and $m = (n/2) + 1$. The rest is essentially the same as for Proposition 2.2.

Let $\tau \notin \langle\sigma\rangle$.

If τ is an n-cycle and n is odd, then $\langle\tau\rangle = \langle\tau^2\rangle = \langle\sigma\rangle$. Assume then that n is even, $\sigma = (0, 1, \ldots, n-1)$ and $\tau(0) = a \in \{0, 1, \ldots, n-1\}$. Since $\tau\sigma\tau^{-1} = \sigma^m$, we have $\tau(i) = a + im \bmod n$ for every $i \in \{0, \ldots, n-1\}$. For $1 \leq k \leq n$,

$$\tau^k(0) = \begin{cases} \frac{1}{2}ka(m+1) \bmod n & \text{if } k \text{ is even,} \\ \frac{1}{2}(k+1)a + \frac{1}{2}(k-1)am \bmod n & \text{if } k \text{ is odd.} \end{cases}$$

If $m < (n/2) + 1$, take $k = 2(m-1) < n$. Since $m^2 \equiv 1 \bmod n$, we have $\tau^k(0) = 0$, and then τ is not an n-cycle. When $m > (n/2) + 1$ the same reasoning works for $k = 2(n - m + 1)$. Suppose then that $m = (n/2) + 1$ (which implies $n \equiv 0 \bmod 4$) and $n \not\equiv 0 \bmod 8$, then $m + 1 \equiv 0 \bmod 4$. Taking $k = n/2$ we have $\tau^k(0) = 0$, and again τ is not an n-cycle.

When $8 \mid n$ and $m = (n/2)+1$, we may take $a = 1$, and then $\tau^2 = \sigma^{a(m+1)} = \sigma^{m+1}$. Since $8 \mid n$, we have $\gcd(m + 1, n) = 2$. Thus σ^{m+1} has order $n/2$. Since $n/2$ is even and τ^2 has order $n/2$, we conclude that τ has order n. □

The problem again is how to determine the quadratic subfield.

When $4 \nmid n$ or $m \neq (n/2) + 1$, we can determine, as in the dihedral case, an irreducible polynomial g of degree smaller than n whose Galois group is the quotient by the center. The quadratic subfield of E_f is that of E_g.

When $4 \mid n$ and $m = (n/2) + 1$, such a polynomial does not exist. This is a consequence of the following lemma, which provides an important relation between the center and $G\big(n, (n/2) + 1\big)$:

Lemma 4.3. *Let $G = G(n, m)$ and let σ be any n-cycle in G.*

(i) *$Z(G)$ equals $\langle\sigma^i\rangle$, where i is the least positive integer such that*

$$i(m-1) \equiv 0 \bmod n.$$

(ii) *$Z(G)$ is trivial if and only if n is odd and G is dihedral.*

(iii) *$G/Z(G)$ is abelian $\Leftrightarrow \sigma^2 \in Z(G) \Leftrightarrow 4 \mid n$ and $m = (n/2) + 1$.*

Proof. (i) It can be easily proved that $Z(G)$ is a subgroup of $\langle\sigma\rangle$ for every n-cycle $\sigma \in G$. Now $\sigma^i \in Z(G)$ if and only if $\sigma^i = \tau^{-1}\sigma^i\tau = (\sigma^i)^m$ for any $\tau \notin \langle\sigma\rangle$, if and only if $i \equiv im \bmod n$.

(ii) Since $m^2 \equiv 1 \bmod n$, we have $\sigma^{m+1} \in Z(G)$. If $Z(G)$ is trivial, then σ^{m+1} is the identity and therefore $m \equiv -1 \bmod n$, so G is dihedral of odd degree. The converse is well-known.

(iii) The quotient $G/Z(G)$ is abelian if and only if, for any $\tau \notin \langle\sigma\rangle$, $\tau^{-1}\sigma\tau Z(G) = \sigma Z(G)$. This is equivalent to $\sigma^{m-1} \in Z(G)$, or yet to $\sigma^2 \in Z(G)$, because the proof of (ii) showed that $\sigma^{m+1} \in Z(G)\big)$. Further, $\sigma^2 \in Z(G) \iff 2(m-1) = 0 \bmod n$ (from the proof of (i)). Since $1 < m < n$, this last condition is the same as $m = (n/2) + 1$. This implies that n is even, so m is odd, which implies $n/2$ is even, so $4 \mid n$. □

Proposition 4.4. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree $n > 2$ such that* $\operatorname{Gal} f = G(n, m)$ *and $Z(\operatorname{Gal} f)$ is not trivial. Let g be a derived polynomial from f by $Z(\operatorname{Gal} f)$. Then*

$$\operatorname{Gal} g = \operatorname{Gal} f / Z(\operatorname{Gal} f) \Leftrightarrow \big|Z(\operatorname{Gal} f)\big| < n/2.$$

If $\big|Z(\operatorname{Gal} f)\big| < n/2$, then $\operatorname{Gal} g = G(n', m')$, *where $n' = n/\big|Z(\operatorname{Gal} f)\big|$ and $m' \equiv m \bmod n'$. Moreover, $E_f^{\langle\sigma\rangle} = E_g^{\langle\overline{\sigma}\rangle}$, where σ is an n-cycle in* $\operatorname{Gal} f$ *and $\overline{\sigma}$ its class in the quotient.*

Proof. Assume that $\big|Z(\operatorname{Gal} f)\big| < n/2$. Then $\operatorname{Gal} g = (\operatorname{Gal} f)/S$, where

$$S = \big\{\rho \in \operatorname{Gal} f : \rho(\beta) = \beta \ \text{ for every } \beta \in E_g\big\} \supseteq Z(\operatorname{Gal} f).$$

Let σ be an n-cycle in $\operatorname{Gal} f$. If $\sigma^k \in S$, then σ^k fixes

$$\big(x - \sigma^i(\alpha)\big)\big(x - \sigma^{2i}(\alpha)\big) \ldots \big(x - \sigma^{|Z(\operatorname{Gal} f)|i}(\alpha)\big),$$

and therefore $\sigma^k \in \langle\sigma^i\rangle = Z(\operatorname{Gal} f)$.

If $S \neq Z(\operatorname{Gal} f)$, then $\tau \in S$ for some $\tau \notin \langle\sigma\rangle$. Since $\tau^{-1}\sigma\tau = \sigma^m$ and S is normal in $\operatorname{Gal} f$, then $\sigma^{m-1} \in S$. Thus $\sigma^{m-1} \in Z(\operatorname{Gal} f)$.

We refer to the proof of Lemma 4.3 to conclude that $\sigma^2 \in Z(\operatorname{Gal} f)$, a contradiction. Therefore $S = Z(\operatorname{Gal} f)$.

Assume that $\operatorname{Gal} g = \operatorname{Gal} f / Z\big(\operatorname{Gal} f\big)$. If $\big|Z(\operatorname{Gal} f)\big| \geq n/2$, then by Lemma 4.3 $\operatorname{Gal} f/Z(\operatorname{Gal} f)$ is abelian. But then its order is

$$\deg g = \frac{n}{\big|Z(\operatorname{Gal} f)\big|},$$

a contradiction.

For the rest we refer to the proof of Proposition 3.4. □

Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree $n > 2$. In order to determine whether its Galois group is $G(n, m)$ for some m, we propose to construct a chain of derived polynomials up to a polynomial g whose Galois group has a trivial center or $\big|Z(\operatorname{Gal} g)\big| = \frac{1}{2}\deg g$.

If $Z(\operatorname{Gal} g)$ is trivial, then either $\operatorname{Gal} f$ is not $G(n, m)$ or, by Lemma 4.3, the degree of g is odd and $\operatorname{Gal} g$ is dihedral. In this case, its unique quadratic subfield K is computable [Williamson 1990] and, by Proposition 4.4, K is a quadratic subfield of E_f.

If $\big|Z(\operatorname{Gal} g)\big| = \frac{1}{2}\deg g$, we assume that $4 \mid \deg g$, otherwise $\operatorname{Gal} f$ is not $G(n, m)$ by Lemma 4.3(c). Let $\rho \in Z(\operatorname{Gal} g)$ be the order 2 element, and compute h a derived polynomial from g by ρ. Since $\operatorname{Gal} h$ is cyclic, all the roots of h are expressible as polynomials in a fixed root γ. Now, $\gamma \in \mathbb{Q}(\beta)$ for some root β of g. Since $|\operatorname{Gal} g| > \deg g$, there must exist another root β_i of g such that

$$(x - \beta_i)(x - \rho\beta_i) \in \mathbb{Q}(\gamma)[x] \subset \mathbb{Q}(\beta)[x]$$

is irreducible over $\mathbb{Q}(\beta)$, so $\mathbb{Q}(\beta, \beta_i)$ has degree $2 \deg g$ over $\mathbb{Q}$.

We consider $\tilde{g}$ the minimal polynomial of a primitive element of $\mathbb{Q}(\beta, \beta_i)$ over $\mathbb{Q}$, which is easily constructible from the p-adic expressions of β and β_i, where p is a prime such that $g \bmod p$ has at least one linear factor, but does not split completely. Notice that $\tilde{g}$ and g have the same splitting field over $\mathbb{Q}$.

Then compute a derived polynomial $\tilde{h}$ from $\tilde{g}$ by the whole center. It has degree 4 with Galois group $\operatorname{Gal} g / Z(\operatorname{Gal} g)$, which is known to be abelian. If $\operatorname{Gal} f = G(n, m)$, then $\operatorname{Gal} g = G\big(\deg g, \frac{1}{2}\deg g + 1\big)$. In these conditions, it is not difficult to prove that $\operatorname{Gal} \tilde{h} = C_2 \times C_2$.

Now let p be a prime such that f is irreducible $\bmod p$. Let $\sigma_p \in \operatorname{Gal} \tilde{h}$ be the Frobenius automorphism over p, which is the class of a certain n-cycle σ in $\operatorname{Gal} f$. The derived polynomial from $\tilde{h}$ by σ_p has degree 2. Its splitting field is $E_{\tilde{h}}^{\langle\sigma_p\rangle} = E_f^{\langle\sigma\rangle}$, the quadratic subfield we are looking for.

It is important to choose p such that $f \bmod p$ is irreducible, in order to avoid problems with the nonuniqueness of the required quadratic subfields.

Example 4.5. We consider the irreducible polynomial

$$\begin{aligned} f(x) = {} & x^{20} + 16x^{19} - 28x^{18} - 1472x^{17} - 2632x^{16} + 51140x^{15} \\ & + 151148x^{14} - 782420x^{13} - 2812591x^{12} + 4620332x^{11} + 21703286x^{10} \\ & - 1147220x^9 - 48329142x^8 - 1527032x^7 + 116408438x^6 + 80220212x^5 \\ & - 3606076x^4 - 7107004x^3 + 150730188x^2 + 152657360x + 149376809. \end{aligned}$$

We have checked that $Z(\operatorname{Gal} f)$ has order 10, so m must be 11.

Since there is a central element of order 5 prime to 2, we can compute a derived polynomial of degree 4 whose Galois group is of the same type and such that its quadratic subfield is that of f. Such a polynomial is

$$g(x) = x^4 - 16x^3 + 96x^2 - 256x + 1506.$$

Using its central element of order 2, we have computed a polynomial of degree 8 with the same splitting field:

$$h(x) = x^8 - 96\,x^7 + 4032\,x^6 - 96768\,x^5 + 1434020\,x^4 - 13094592\,x^3 + 68487552\,x^2 - 165694464\,x + 1043664196.$$

Constructing a derived polynomial by the center we obtain a quartic polynomial and then a quadratic one whose splitting field is precisely the quadratic subfield sought, $\mathbb{Q}(i)$. The polynomial

$$F(x) = \frac{-2036578469291666316402543692876065961398037676972 04}{2376071543855246405784871933571129920385636353833225630750 7}x^{19} + \cdots\cdots\cdots\cdots\cdots\cdots\cdots - \frac{1331914423856209977719674839761939577042364719993942995112 52}{2376071543855246405784871933571129920385636353833225630750 7} + \frac{6152086964541718808900648055367126359050484928}{1782098210346693471675445836324255546677894212730237479}\,i\,x^{19} + \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots - \frac{2683013494208127229718816803849187289290345630472785 84}{1782098210346693471675445836324255546677894212730237479}\,i$$

satisfies the third condition in Proposition 4.1.

Acknowledgment

I thank the referee for his helpful comments and suggestions.

References

[Dixon 1990] J. D. Dixon, "Computing subfields in algebraic number fields", *J. Austral. Math. Soc. Ser. A* **49**:3 (1990), 434–448. MR 91h:11156 Zbl 0727.11049

[Fernández-Ferreirós and Gómez-Molleda 2004] P. Fernández-Ferreirós and M. A. Gómez-Molleda, "Deciding the nilpotency of the Galois group by computing elements in the centre", *Math. Comp.* **73**:248 (2004), 2043–2060. MR 2005c:12005 Zbl 1065.11101

[Hwang et al. 2003] Y.-S. Hwang, D. B. Leep, and A. R. Wadsworth, "Galois groups of order $2n$ that contain a cyclic subgroup of order n", *Pacific J. Math.* **212**:2 (2003), 297–319. MR 2004m:12002 Zbl 1051.12001

[Jensen and Yui 1982] C. U. Jensen and N. Yui, "Polynomials with D_p as Galois group", *J. Number Theory* **15**:3 (1982), 347–375. MR 84g:12011 Zbl 0496.12004

[Williamson 1990] C. J. Williamson, "Odd degree polynomials with dihedral Galois groups", *J. Number Theory* **34**:2 (1990), 153–173. MR 91d:12008 Zbl 0814.11054

Received May 17, 2005.

MARIA ÁNGELES GÓMEZ-MOLLEDA
DEPARTAMENTO DE ÁLGEBRA, GEOMETRÍA Y TOPOLOGÍA
UNIVERSIDAD DE MÁLAGA
29071 MÁLAGA
SPAIN

gomezma@agt.cie.uma.es