Explicit determination of generalized symmetric and alternating Galois groups

M. Ángeles Gómez-Molleda

Dpto. Álgebra, Geometría y Topología, Universidad de Málaga, 29071 Málaga, Spain

Received 28 October 2005; received in revised form 9 January 2006
Available online 13 March 2006
Communicated by C.A. Weibel

Abstract

This paper shows a probabilistic algorithm to decide whether the Galois group of a given irreducible polynomial with rational coefficients is the generalized symmetric group $C_p \wr S_m$ or the generalized alternating group $C_p \wr A_m$. In the affirmative case, we give generators of the group with their action on the set of roots of the polynomial.

© 2006 Elsevier B.V. All rights reserved.

MSC: Primary: 12Y05; secondary: 11R32

1. Introduction

In a previous paper (see [4]) we proposed a method for determining the action of the centre of the Galois group of a given polynomial, without computing the whole group. This method extends the abelian case treated by Acciaro and Klüners [1], where they compute explicitly the action of the elements of the Galois group of an irreducible polynomial, knowing that it is abelian.

We are now concerned with the, in some sense, opposite case to abelian groups: those transitive permutation groups with nontrivial centre and as many elements as possible, the centralizers of prime order elements. These are representable as wreath products $C_p \wr S_m$ of the cyclic group $C_p$ of prime order $p$ and the symmetric group $S_m$ of degree $m$. The wreath products of cyclic and symmetric groups were called generalized symmetric groups by Osima [6].

The present paper shows how to decide whether the Galois group of a given irreducible polynomial with rational coefficients is the generalized symmetric group $C_p \wr S_m$. In the affirmative case, we give generators of the group with their action on the set of roots of the polynomial.

The method relies on a characterization of these groups: the Galois group of a given irreducible polynomial $f$ of degree $pm$ is $C_p \wr S_m$ if and only if the centre has order $p$, the Galois group contains a $p$-cycle, and a certain quotient of the group (depending on the centre) is $S_m$.

The search for $p$-cycles is made by factorizations of $f$ modulo primes. The density of primes with a suitable factorization to guarantee the existence of $p$-cycles is high in the case of generalized symmetric groups.
The determination of whether the quotient is symmetric is also essentially made by factorizations of \( f \) modulo primes, as quickly as proving whether the Galois group of a polynomial is symmetric. It is just necessary to interpret the factorizations of \( f \) as permutations in the quotient group, for which we need to know the order of the centre and sometimes the polynomial expression of any of its generators.

The method given in [4] for computing the centre consisted of searching for certain prime numbers among a set whose density depends on the order of the Galois group: the larger the group, the more difficult it is to determine the centre. In the present case, the order is the largest possible, so that determining the centre would take a long time. Here we improve the computation of the centre, using more prime numbers whose density in the case of our generalized symmetric groups is very high.

The method is extensible, with a few modifications, to generalized alternating groups \( C_p \triangleleft A_m \), as we show in the last section.

2. Preliminaries

Let \( G \) be a transitive permutation group of degree \( n \) and \( Z(G) \) its centre. Every nontrivial central element can be written as a product of disjoint cycles of the same length, with no fixed point.

Let \( p \) be a prime divisor of \( n \), \( n = pm \), and let us suppose that there exists \( \tau \in Z(G) \) of order \( p \). Assume, without loss of generality, that the disjoint cycles of \( \tau \) are

\[
\tau_i = (i, m + i, 2m + i, \ldots, (p - 1)m + i) \quad \text{for} \quad i = 1, \ldots, m.
\]

We denote \( T_i = \{i, m + i, 2m + i, \ldots, (p - 1)m + i\} \). The map

\[
\begin{align*}
\phi : & \quad G \to S_m \\
\sigma & \quad \to \quad \phi_\sigma
\end{align*}
\]

defined by \( \phi_\sigma(i) = j \), if \( \sigma(i) \in T_j \), is a group homomorphism with kernel \( \langle \tau_1, \ldots, \tau_m \rangle \cap G \). In virtue of the centrality of \( \tau \), the next result follows:

**Proposition 1.** Let \( \sigma \in G \) and \( c = (a_1, \ldots, a_l) \) any of its disjoint cycles. One of the following conditions holds:

1. \( c \) has at least two components, \( a_j, a_j \), belonging to the same set \( T_k \). Then \( p \) divides \( l \) and \( c^{l/p} = \tau^b \) on \( \{a_1, \ldots, a_l\} \) for some integer \( b \).
2. Each component of \( c \) belongs to a different set \( T_i \). Then there exist cycles \( c_2, \ldots, c_p \) of \( \sigma \) such that \( c_j = (\tau^{j-1}(a_1), \ldots, \tau^{j-1}(a_l)) \).

If \( c \) satisfies the second property, we say that \( c, c_2, \ldots, c_p \) are the copies of \( c \).

The cycle structure of \( \phi(\sigma) \) depends on the behaviour of the cycles of \( \sigma \), in the terms exposed in Proposition 1, as the next corollary states:

**Corollary 2.** Let \( c_1, \ldots, c_l \) be the cycles of \( \sigma \in G \), of lengths \( l_1, \ldots, l_l \), satisfying the first property in Proposition 1. Let \( c_{i,j}^j, i = 1, \ldots, s, \quad j = 1, \ldots, p \), denote the remaining cycles, where \( c_{i,1}, \ldots, c_{i,p} \) are the copies of \( c_{i,1} \), of length \( l_i' \). Then \( \phi(\sigma) \) is the product of \( t + s \) disjoint cycles of lengths

\[
\frac{l_1}{p}, \ldots, \frac{l_t}{p}, l_1', \ldots, l_s'.
\]

We are interested in the cycle structure of the elements of \( \phi(G) \), since \( \phi(G) \) and \( \tau \) provide generators for \( G \) in certain cases:

**Proposition 3.** Let \( \sigma \in C_{S_p}(\tau) \), the centralizer of \( \tau \) in \( S_p \), such that \( \sigma(i) \in T_{p_i} \) for some \( p_i \in \phi(G) \) and all \( i = 1, \ldots, m \). If \( G \) contains a \( p \)-cycle, then \( \sigma \in G \). In particular, if \( p_1, \ldots, p_s \) are generators of \( \phi(G) \) and \( G \) contains a \( p \)-cycle, then \( G \) is generated by \( \tau, \tau_1, \sigma_1, \ldots, \sigma_s \), where \( \sigma_i \) is any element in \( C_{S_p}(\tau) \) such that \( \sigma_i(i) \in T_{p_i} \) for every \( i \).
Lemma 4. Let $G$ be a subgroup of $S_4$. Let $c = (a_1, \ldots, a_p)$ be a $p$-cycle in $G$. Since $c \tau = \tau c$ and the order of $\tau$ is $p$, there exist $1 \leq k \leq m$, $1 \leq i \leq p$ such that $\tau_k = c^i$. Thus, $\tau_k \in G$ and, because of the transitivity of $G$, $\langle \tau_1, \ldots, \tau_m \rangle \subseteq G$. Therefore $\text{Ker} \phi = \langle \tau_1, \ldots, \tau_m \rangle$ and $\rho$ has $p^m$ preimages in $G$. The number of elements in $C_{S_n}(\tau)$, such that $\sigma(i) \in T_{\rho(i)}$ for every $i$, is also $p^m$, since there are exactly $p$ choices for the images of each $i = 1, \ldots, m$. They are, then, the preimages of $\rho$ in $G$. The rest of the statement follows immediately. \hfill $\Box$

Given $f \in \mathbb{Z}[x]$, a monic irreducible polynomial of degree $n$, we denote by $\text{Gal}(f)$ its Galois group over $\mathbb{Q}$. In [4] we exposed a method for computing central elements in the Galois group and constructing polynomials $g \in \mathbb{Z}[x]$, of degree $n/p$, whose Galois group is $\phi(\text{Gal}(f))$. If we are able to prove the existence of a $p$-cycle in $\text{Gal}(f)$ then, by the above proposition, $\text{Gal}(f)$ is the wreath product of the cyclic group of order $p$ and $\text{Gal}(g)$. The problem of giving generators for $\text{Gal}(f)$ is reduced to $\text{Gal}(g)$. Although this procedure is always possible, it is frequently slow, specially in the case of big $p$-groups.

We will be concerned, from now on, with generalized symmetric and alternating Galois groups. Their special structure allows, in spite of their high order, a fast determination of the Galois group. The procedure consists, essentially, of factorizations of $f$ modulo primes and quadratic Newton-lifting, while it is unnecessary to reduce the problem to any other polynomial.

3. Generalized symmetric group

Let us consider the wreath product $C_p \wr S_m$ of the cyclic group of order $p$ and $S_m$, called a generalized symmetric group [6]. Such a group is the centralizer of $\tau$ in $S_n$, where $n = pm$, and has order $p^m m!$.

Although the order of the group is high, the computation of the centre is fast, as we will show in Section 3.1. Next, we will study the proportion of elements that assures the existence of a $p$-cycle, so that it can be determined by means of the factorization of $f$ modulo a few primes. We will make good use of these factorizations to obtain the type of the images by $\phi$ of the Frobenius automorphisms in order to decide whether $\phi(G)$ is symmetric.

3.1. The centre

The number of $n$-cycles in $C_p \wr S_m$ is $p^{m-1}(p-1)(m-1)!$, a proportion of $\frac{p-1}{n}$. The $n$-cycles have the following property, which is useful to compute the centre:

Lemma 4. Let $G$ be a subgroup of $S_n$ and $\sigma$ an $n$-cycle in $G$.

Then $Z(G)$ is a subgroup of $\langle \sigma \rangle$.

Proof. Let $N$ be the number of conjugates of $\sigma$ in $S_n$ and $C_{S_n}(\sigma)$ its centralizer. The order of $C_{S_n}(\sigma)$ is $n!/N$. Since the conjugates of $\sigma$ are all $n$-cycles, $N = (n-1)!$ and then $|C_{S_n}(\sigma)| = n$. Thus, $C_{S_n}(\sigma) = \langle \sigma \rangle$ and so is the centralizer in any group $G$ containing $\sigma$. Therefore, $Z(G) \leq \langle \sigma \rangle$. \hfill $\Box$

If $q$ is a prime number, we denote by $\sigma_q$ any of the permutations in the conjugacy class of Frobenius automorphisms of $q$ in $\text{Gal}(f)$. It is well known that the degrees of the irreducible factors of $f \mod q$ are the cycle lengths of $\sigma_q$. By the Tchebotarev density theorem (see [5]), the frequency of primes giving a certain type of factorization is the proportion of the corresponding cycle shape in the Galois group. If $\text{Gal}(f)$ is the generalized symmetric group $C_p \wr S_m$, a prime $q$ such that $f \mod q$ be irreducible appears within a frequency of $(p-1)/pm$. In such a case, $\sigma_q$ is an $n$-cycle and, by Lemma 4, every central element in $\text{Gal}(f)$ is a power of $\sigma_q$.

Proposition 5. Let $q$ be a prime such that $f \mod q$ is squarefree. $\sigma_q^k$ is central if and only if there exists $F \in \mathbb{Q}[x]$ such that

$$F(x) \equiv x^{q^k} \mod (q, f(x))$$

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

In the affirmative case, the polynomial $F$ describes the action of $\sigma_q^k$:

$$F(\alpha) = \sigma_q^k(\alpha) \quad \text{for every root } \alpha \text{ of } f.$$
The preceding proposition follows from the characterizations of $Z(\text{Gal}(f))$ given in [4]. Lifting $x^{q^k}$ up to a certain power of $(q, f(x))$ and checking whether the obtained polynomial permutes the roots of $f$, we determine the centrality of $\sigma_q^k$.

**Example 6.** Let $f(x) = x^{12} - x^6 - 3x^4 + 2x^2 + 2$. Since it is irreducible modulo 3, every central element in $\text{Gal}(f)$ must be a power of $\sigma_3$, a Frobenius automorphism of 3. Lifting $x^3$ modulo $(3, f(x))$, we obtain

$$F(x) = \frac{9}{5}x^5 + \frac{1}{5}x^3 - \frac{3}{5}x^5 - \frac{1}{5}x^7 - \frac{3}{5}x^9 + \frac{1}{5}x^{11},$$

the polynomial representation of $\sigma_3^2$, a central element of order 4.

The polynomial $f(x) = x^{12} - 4x^{11} + 4x^{10} - 50x^4 + 120x^3 - 112x^2 + 48x - 8$ is also irreducible modulo 3. It can be proved that no power of $\sigma_3$ is central. Therefore, $Z(\text{Gal}(f))$ is trivial in this case.

None of the polynomials of the preceding example has a generalized symmetric Galois group. The proportion of $n$-cycles in $C_p \wr S_m$ is high and Newton-lifting is fast, so that the centre will be computed quickly. Of course, the high proportion of $n$-cycles also guarantees that their existence can be refused with high probability in a few steps.

There are some types of elements that indicate the triviality of the centre. Let us go back to Proposition 1 and consider the polynomial

$$f(x) = x^{12} - x^{11} + x^{10} + x^9 + x^7 + x^6 + 3x^4 - x^3 + x^2 + 1.$$

Since $f(x) \equiv (x^3 + x^2 + x + 2)(x^3 + x^8 + 2x^7 + 2x^6 + x^4 + 2x^3 + 2x + 2) \mod 3$, if $\tau \in Z(\text{Gal}(f))$ has prime order $p$, then $p = 3$. Otherwise, there would be $p$ irreducible factors of the same degree. Factoring modulo 5, we obtain

$$f(x) \equiv (x^4 + 3x^3 + 2x^2 + 1)(x^6 + 4x^5 + 4x^3 + x^2 + 2x + 2)(x^2 + 2x + 3) \mod 5.$$

Now $p$ should be 2. Therefore, $Z(\text{Gal}(f))$ is trivial.

Finally, there are some other types of factorization that allow us to determine the whole centre from the Frobenius automorphism of a unique prime. We do not propose it here, because it is much faster to work with $n$-cycles; we refer to Section 4.

3.2. $p$-cycles

Let $\sigma_1, \ldots, \sigma_s$ be the decomposition of $\sigma \in G$ into disjoint cycles and $l_i$ the length of $\sigma_i$, $i = 1, \ldots, s$. We say that $(l_1, \ldots, l_s)$ is the type of $\sigma$. This notation is unique up to permutation of the $l_i$.

If the type of $\sigma \in G$ is $(p, a_1, \ldots, a_l)$, with $(a_i, p) = 1$ for $i = 1, \ldots, l$, then $\sigma^a$ is a $p$-cycle, where $a = \text{lcm}(a_1, \ldots, a_l)$. We will see that the proportion of these types of elements in $C_p \wr S_m$ is high, so that the existence of a $p$-cycle will be quickly determined by just factoring $f$ modulo several primes.

If $\sigma \in C_p \wr S_m$, with $(a_i, p) = 1$, Proposition 1 imposes that $a_i$ appears repeated $p$ times in the type of $\sigma$. We then write the type of $\sigma$ in the form

$$(p, a_1, a_2, \ldots, a_s)$$

where $a_1, \ldots, a_s$ are different and $\sigma$ has exactly $pl_i$ cycles of length $a_i$.

By Proposition 1 and a simple exercise of combinatorics, the number of elements of type $(p, a_1, \ldots, a_i, a_2, \ldots, a_s, \ldots, a_s)$ in $C_p \wr S_m$ is

$$\frac{(p - 1)p^{m-(1+l_1+\ldots+l_s)}m!}{l_1! \ldots l_s!a_1^{l_1} \ldots a_s^{l_s}}.$$.

**Example 7.** Let us suppose that we are given an irreducible polynomial of degree 18 whose Galois group has centre of order 3. We desire to know whether $\text{Gal}(f)$ is $C_3 \wr S_6$. For this, we must determine the existence of a 3-cycle. By the above formula, we know that $C_3 \wr S_6$ has

1620 elements with type $(3, 2, 2, 2, 2, 2, 2, 2, 1, 1, 1)$
Corollary 2

The proportion is $973/14580 \approx 1/15$. Factoring the polynomial modulo 100 primes, we could say, with probability 0.999, that $\text{Gal}(f)$ has no 3-cycle.

Let us consider, to simplify, only the elements of type $(p, m - 1, \ldots, m - 1)$ when $p$ does not divide $m - 1$ and $(p, m - 2, \ldots, m - 2, 1, \ldots, 1)$ otherwise. In the first case, the number of elements is $(p - 1)p^{m - 2}m(m - 2)!$ and the proportion is

$$\frac{p - 1}{p^2(m - 1)}.$$ 

The worst case is $p = 2$, $m$ big, and the proportion is around $1/2n$. In the second case, the number of elements is $(p - 1)p^{m - 3}m(m - 1)(m - 2)!$ Thus the proportion is

$$\frac{p - 1}{p^3(m - 2)}.$$ 

The worst case is now above $1/4n$.

3.3. Determination of $\phi(G)$

Davenport and Smith [3] give a fast algorithm for recognizing symmetric and alternating Galois groups. This also consists of factoring the polynomials modulo primes to obtain the cycle structure of its elements.

In our case, we desire to know whether $\phi(\text{Gal}(f))$ is symmetric (or alternating; see Section 4). We will obtain the cycle type of the elements $\phi(\text{Gal}(f))$ from the factorizations of $f$ modulo primes.

Let $f = f_1 \cdot \ldots \cdot f_s \mod q$ be the factorization of $f$ into distinct irreducibles modulo $q$. Let $\alpha$ be a root of $f$ such that $f_j(\alpha) \equiv 0 \mod q$. The other roots of $f_j$ are the images of $\alpha$ under the $q$-Frobenius automorphism $x \mapsto x^q$.

Let us denote by $\sigma_j$ the $q$-Frobenius automorphism as a permutation on the roots of $f$, and by $\sigma_i$ the corresponding cycle of length $\deg(f_j)$. In order to determine the cycle type of $\phi(\sigma_i)$, we will apply Corollary 2. For this, given a cycle $\sigma_i$ such that $p$ divides $\deg(f_j)$, we must know whether it moves more than one point in the same set $T_j$.

We must decide whether, among the roots of $f_1 \mod q$, there is more than one root of $f$ in the same cycle of $\tau$, that is to say, whether being $\alpha$ a root of $f_1 \mod q$, $F_\tau(\alpha)$ is also a root of $f_1$. Since the roots of $f_1$ are of the form $\alpha q^k$ with $0 \leq k \leq \deg(f_1) - 1$, we have to decide whether $F_\tau(x) - x^{q^k}$ is zero when evaluating in a root of $f_1$, that is, whether

$$F_\tau(x) - x^{q^k} \equiv 0 \mod (q, f_1(x))$$

for some $k \in \{0, \ldots, \deg(f_1) - 1\}$.

**Example 8.** Let us consider the irreducible polynomial

$$f(x) = x^9 - 45x^7 + 30x^6 + 1539x^5 - 2052x^4 - 15219x^3 + 31806x^2 - 21204x + 4712.$$ 

The polynomial

$$F(x) = -\frac{1116155}{576} + \frac{3641815}{576}x - \frac{11846471}{2304}x^2 - \frac{323413}{1152}x^3 + \frac{1144411}{2304}x^4 - \frac{197}{144}x^5$$

$$-\frac{33009}{2304}x^6 + \frac{287}{1152}x^7 + \frac{745}{2304}x^8$$

represents an order 3 element in $Z(\text{Gal}(f))$.

$$f(x) \equiv (x^3 + 5x^2 + 6)(x^3 + x^2 + 6x + 3)(x^3 + x^2 + x + 2) \mod 7.$$ 

We have checked that neither $F(x) - x^7 \equiv 0 \mod (7, x^3 + 5x^2 + 6)$ nor $F(x) - x^7 \equiv 0 \mod (7, x^3 + 5x^2 + 6)$. Then, the first factor represents a cycle of length 3 whose elements belong to different sets $T_j$. The other cycles must
Proposition 1. Therefore, \( \phi(\tau) \) is a 3-cycle.

\[
f(x) \equiv (x + 8) \left( x^3 + 14x + 6 \right) (x + 21) \left( x^3 + 16x + 20 \right) (x + 17) \mod 23.
\]

Since there are less than three factors of degree 3, we can conclude without any other proof that \( \phi(\tau) \) is the identity.

By Proposition 1, in the case that \( \tau \) moves more than one root in the same \( T_i \), then \( 1 \neq \sigma_1^{\deg(f_i)/p} \in \langle \tau \rangle \). Therefore, \( \sigma_1^{\deg(f_i)/p} \) has order \( p \) and so \( \tau \in \langle \sigma_1^{\deg(f_i)/p} \rangle \). Thus, it is enough to check the above relation only for those \( k \) multiple of \( \deg(f_i)/p \).

4. Generalized alternating group

The method presented above for computing the centre relied on the existence of an \( n \)-cycle. Such elements do not always belong to \( C_p \wr A_m \):

Lemma 9. Let \( p, m \) be integers, \( p \) a prime.

1. \( C_p \wr A_m \) has \( pm \)-cycles if and only if \( m \) is odd.
2. If \( m \) is even, then \( C_p \wr A_m \) has elements of type \( (p, p(m-1)) \).

The proof follows immediately from Proposition 1.

The elements of type \( (p, p(m-1)) \), whose proportion in \( C_p \wr A_m \) (\( m \) even) is

\[
\frac{2(p-1)^2}{p^2(m-1)},
\]

are also useful to determine the centre quickly.

Proposition 10. Let \( G \) be a transitive subgroup of \( S_n \), \( n = pm \), \( p \) prime, \( m \neq 2 \). Let \( \rho \) and \( \sigma \) be disjoint cycles in \( S_n \), of lengths \( p \) and \( p(m-1) \) respectively, such that \( \rho \sigma \in G \). Then every element \( \tau \in Z(G) \) satisfies

\[
\tau = \rho^i \sigma^j \quad \text{for some integers } i, j.
\]

If \( m = 2 \), \( p \neq 2 \) and \( G = C_p \wr S_2 \), then the above property also holds.

Proof. Suppose first that \( G \) is any transitive subgroup of \( S_n \), \( m \neq 2 \). We can assume, without loss of generality, that

\[
\rho = (1, 2, \ldots, p) \quad \text{and} \quad \sigma = (p + 1, \ldots, n).
\]

If \( \tau(1) \in \{ p + 1, \ldots, n \} \) then, for every \( k = 1, \ldots, p \),

\[
\tau(k) = \tau \rho^{k-1}(1) = \tau (\rho \sigma)^{k-1}(1) = (\rho \sigma)^{k-1} \tau(1).
\]

Since \( \tau(1) = \tau \rho \sigma (p) = \rho \sigma \tau (p) = (\rho \sigma)^p \tau (1) \), the order of \( \tau_1 \sigma \), \( p(m-1) \), must divide \( p \). But \( m \neq 2 \), so that \( \tau(1) = i \in \{1, \ldots, p\} \). Thus, for every \( j = 1, \ldots, p \),

\[
\tau(j) = \tau (\rho \sigma)^{j-1}(1) = (\rho \sigma)^{j-1} \tau(1) = (\rho \sigma)^{j-1}(\rho \sigma)^{\rho^i}(1) = (\rho \sigma)^{\rho^i}(j) = \rho^i (j).
\]

That is to say, \( \tau \) is equal to \( \rho^j \) on \( \{1, \ldots, p\} \). Therefore, \( \tau \) permutes the set \( \{ p + 1, \ldots, n \} \), commuting with \( \sigma \). As in Lemma 4, \( \tau = \sigma^s \) on \( \{ p + 1, \ldots, n \} \) for some integer \( s \).

If \( m = 2 \), \( p \) odd and \( G = C_p \wr S_2 \), the order of \( Z(G) \) is \( p \) and any nontrivial central element \( \tau \) is the product of \( 2 \) \( p \)-cycles. Since \( p > 2 \), both \( \rho \) and \( \sigma \) move elements of the same set \( T_i \) (as defined in Section 2). By Proposition 1, our claim holds. \( \Box \)

Let \( q \) be a prime such that \( f \equiv f_1 f_2 \mod q \), where \( f_1 \) and \( f_2 \) have degrees \( p \) and \( p(m-1) \), respectively. The Frobenius automorphism \( \sigma_q \) is the disjoint product of a \( p \)-cycle \( \rho \) and a \( p(m-1) \)-cycle \( \sigma \). We can assume that \( \rho \) permutes the roots of \( f_1 \), and \( \sigma \) those of \( f_2 \). Since \( \tau = \rho^a \) on the roots of \( f_1 \), which are of the form \( \alpha, \alpha^q, \ldots, \alpha^{q^{p-1}} \), we have that

\[
F_\tau(x) \equiv x^{q^a} \mod (q, f_1(x)),
\]
where $F_\tau$ is the polynomial in $\mathbb{Q}[x]$ representing the action of $\tau$ on the roots of $f$. Analogously,

$$F_\tau(x) \equiv x^{q^b} \mod (q, f_2(x))$$

for some integer $b$.

There exist $p_1, p_2 \in \mathbb{Z}[x]$ such that $p_1(x)f_1(x) + p_2(x)f_2(x) \equiv 1 \mod q$. By the Chinese Remainder Theorem,

$$F_\tau(x) \equiv x^{q^b} p_1(x)f_1(x) + x^{q^a} p_2(x)f_2(x) \mod q. \quad (1)$$

Applying Newton-lifting to Eq. (1), the polynomial $F_\tau$ is computed. The procedure is similar to that given by Allombert [2] to determine diagonal automorphisms.

**Remark 11.** Assume $1 \neq \tau = \rho^a\sigma^b \in Z(G)$ of order $p$. Then

$$p = O(\sigma^b) = \frac{pm}{\gcd(b, pm)},$$

so that $\gcd(b, pm) = m$ and there exist $t, s$ such that $tb + spm = m$. Thus

$$1 \neq \tau^t = \tau_1^a\sigma^b = \tau_1^a\sigma^m$$

and $\tau^t$ would also generate $Z(G)$ since it has order $p$. Therefore, it is enough to check pairs $(a, b)$ with $b = m$ and $a = 1, \ldots, p - 1$.

In order to determine the existence of $p$-cycles, the strategy is the same as for generalized symmetric groups. It is necessary, nevertheless, to take into account the possible types of elements belonging to the generalized alternating group, depending on $p$ and $m$. In this sense, the elements of the type $(p, a_1, \ldots, a_1, a_s, \ldots, a_s)$, where $a_1, \ldots, a_s$ are prime to $p$ and such that $(a_1, \ldots, a_s)$ belong to $A_m$, guarantee the existence of $p$-cycles in the group. The proportions, in the worst cases, are greater than $\frac{1}{8^m}$.

As for the determination of $\phi(\text{Gal}(f))$, we wish to remark that, if $p \neq 2$, then $C_p \leq A_m$ is a subgroup of $A_{pm}$. This fact can be useful in the following way: Davenport and Smith [3], looking at the cycle types of the permutations, decide only whether the Galois group is $A_m$ or $S_m$, or not. The discriminant of the given polynomial $f$ (a perfect square or not), can make the difference also in $\phi(\text{Gal}(f))$ when $p$ is odd.

**Acknowledgement**

The author was partially supported by MCyT BFM 2002-04402-C02-0.

**References**


