ACTA ARITHMETICA
LXXXII.2 (1997)

On double covers of the generalized alternating group $\mathbb{Z}_d \wr \mathfrak{A}_m$ as Galois groups over algebraic number fields

by

Martin Epkenhans (Paderborn)

Let $\mathbb{Z}_d \wr \mathfrak{A}_m$ be the generalized alternating group. We prove that all double covers of $\mathbb{Z}_d \wr \mathfrak{A}_m$ occur as Galois groups over any algebraic number field. We further realize some of these double covers as the Galois groups of regular extensions of $\mathbb{Q}(T)$. If d is odd and $m > 7$, then every central extension of $\mathbb{Z}_d \wr \mathfrak{A}_m$ occurs as the Galois group of a regular extension of $\mathbb{Q}(T)$. We further improve some of our earlier results concerning double covers of the generalized symmetric group $\mathbb{Z}_d \wr \mathfrak{S}_m$.

1. Introduction and notations. Serre's formula on trace forms [15], [16] relates the obstruction to certain embedding problems

$$1 \to \mathbb{Z}_2 \to \widetilde{\mathcal{G}} \to \mathcal{G} \to 1$$

of a finite group $\mathcal{G}$ to invariants of the trace form of a field extension. Using this, N. Vila [19] realized the unique covering group $\widetilde{\mathfrak{A}}_m$ of $\mathfrak{A}_m, m \geq 8, m \equiv 0, 1 \bmod 8$ as the Galois group of a regular extension of the rational function field $\mathbb{Q}(T)$. J. F. Mestre [11] extended this result to all $m \geq 4$. Following Mestre's ideas, J. Sonn [18] improved one of his previous results on covering groups of the symmetric group $\mathfrak{S}_m$. We can summarize these results as follows.

Every finite central extension of $\mathfrak{S}_m$ and of $\mathfrak{A}_m$, $m \geq 4$, is realizable as the Galois group of a regular extension of $\mathbb{Q}(T)$.

Vila, Sonn and Schacher [19], [20], [17], [13] used trinomials $f(X) = X^m + aX^l + b$ with Galois group $\mathfrak{S}_m$, resp. $\mathfrak{A}_m$. We know the trace form of a trinomial [15], [3]. The trace form of a trinomial with square discriminant depends only on l. It is not always possible to choose $l < n$ such that the obstruction vanishes. This explains why Vila's results are not complete.

1991 *Mathematics Subject Classification*: Primary 12F12.

Mestre gave a one-parameter deformation of a polynomial of odd degree to an irreducible polynomial with the same trace form. Völklein [21] obtained Mestre's result on $\widetilde{\mathfrak{A}}_m$ without trace form considerations.

In a previous paper [4] we realized some of the double covers of the generalized symmetric group $\mathbb{Z}_d \wr \mathfrak{S}_m$ as Galois groups over $K(T)$, where K is an algebraic number field which contains the dth roots of unity.

In this paper we investigate double covers of the generalized alternating group as a Galois group over number fields and over rational function fields. Using Ishanov's theorem we prove that all double covers of $\mathbb{Z}_d \wr \mathfrak{A}_m$ and of $\mathbb{Z}_d \wr \mathfrak{S}_m$ occur as the Galois groups over any algebraic number field. If d is odd, then the unique non-trivial double cover of $\mathbb{Z}_d \wr \mathfrak{A}_m$ occurs as the Galois group of a regular extension of $\mathbb{Q}(T)$.

Kotlar, Schacher and Sonn [8, Theorem 6] reduced the question whether a central extension of $\mathfrak{S}_m$ is a Galois group over K to certain pull-backs of stem covers of $\mathfrak{S}_m$ with cyclic groups. Following their arguments we show that all central extensions of $\mathbb{Z}_d \wr \mathfrak{A}_m$ are the Galois groups of regular extensions of $\mathbb{Q}(T)$ if d is odd and $m > 7$.

Let us fix some notation. Let $\mathcal{G}$ be a finite group. Then $\mathcal{G}'$ denotes the commutator subgroup of $\mathcal{G}$ and $\mathrm{M}(\mathcal{G})$ is the Schur multiplier of $\mathcal{G}$. Let $\pi_1 : \mathcal{H}_1 \to \mathcal{G}$, $\pi_2 : \mathcal{H}_2 \to \mathcal{G}$ be homomorphisms of groups. Then $\mathcal{H}_1 \times_{\mathcal{G}} \mathcal{H}_2$ is the associated pull-back.

Let K be a field. Then $\overline{K}$ denotes an algebraic closure of K. $\mu_d \subset \overline{K}$ is the group of dth roots of unity. Let $f(X) \in K[X]$ be a polynomial. Then $\mathrm{dis}(f)$ is the discriminant of $f(X)$, and $\mathrm{Gal}(f)$ stands for its Galois group. Let T, U, V, X, Y denote indeterminates.

2. The embedding problem. Let K be a field of $\mathrm{char}(K) \neq 2$, K_{s} a separable closure of K, and $\Gamma_K := G(K_{\mathrm{s}}/K)$ the absolute Galois group of K. Let L/K be a separable field extension of finite degree n, $N \supset L$ a normal closure of L/K inside K_{s}, and $\mathcal{G} = G(N/K)$ the Galois group of N/K. By Galois theory we have homomorphisms $\varrho : \Gamma_K \to \mathcal{G}$ and $e : \Gamma_K \to \mathfrak{S}_n$. Let

$$0 \to \mathcal{A} \xrightarrow{\iota} \mathcal{E} \to \mathcal{G} \to 0$$

be a group extension of $\mathcal{G}$ with abelian kernel $\mathcal{A}$. We say the *embedding problem* with abelian kernel defined by the diagram

$$\begin{array}{ccccccccc} & & & & & & \Gamma_K & & \\ & & & & & & \big\downarrow{\scriptstyle\varrho} & & \\ 1 & \longrightarrow & \mathcal{A} & \longrightarrow & \mathcal{E} & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \end{array}$$

has a (proper) solution iff there is a (surjective) homomorphism $\varphi : \Gamma_K \to \mathcal{E}$ making the diagram commutative. If $\iota(\mathcal{A}) \subset Z(\mathcal{E})$, the center of $\mathcal{E}$, then we call it a *central embedding problem*. An abelian embedding problem over an algebraic number field has a proper solution if it has a solution (Ikeda's Theorem [6]). If the order $|\mathcal{A}|$ of $\mathcal{A}$ is a prime and if $\mathcal{E}$ is a non-trivial extension of $\mathcal{G}$, then every solution of the embedding problem is a proper solution.

Let $\mathrm{H}^m(\mathcal{G},\mathcal{A})$, $m \in \mathbb{Z}$, denote the mth cohomology group of the $\mathcal{G}$-module $\mathcal{A}$. The group extension $1 \to \mathcal{A} \to \mathcal{E} \to \mathcal{G} \to 1$ with abelian kernel $\mathcal{A}$ defines an element $\varepsilon \in \mathrm{H}^2(\mathcal{G},\mathcal{A})$. Let $\mathrm{Br}(K)$ be the Brauer group of K and let $\inf : \mathrm{H}^2(\mathcal{G},\mathcal{A}) \to \mathrm{Br}(K)$ be the inflation map induced by $\varrho : \Gamma_K \to \mathcal{G}$.

HOECHSMANN'S THEOREM. *The embedding problem associated with $\varepsilon \in \mathrm{H}^2(\mathcal{G},\mathcal{A})$ has a solution if and only if* $\inf(\varepsilon) = 0 \in \mathrm{Br}(K)$.

With the help of Serre's formula we are able to calculate the obstruction $\inf(\varepsilon)$ for some embedding problems. By Kummer theory we know $\mathrm{H}^1(\Gamma_K,\mathbb{Z}_2) \simeq \mathrm{Hom}(\Gamma_K,\mathbb{Z}_2) \simeq K^\star/K^{\star 2}$. For $a,b \in K^\star$, $(a,b)_K$ denotes the generalized quaternion algebra generated over K by i,j and satisfying $i^2 = a$, $j^2 = b$, $ij = -ji$. The class of $(a,b)_K$ in $\mathrm{Br}(K)$ is also denoted by $(a,b)_K$. Let ψ be a (non-degenerate) quadratic form over K. The *Hasse invariant* (second Stiefel–Whitney class) is defined by

$$w_2\psi := \bigotimes_{1\le i<j\le n} (a_i,a_j)_K \in \mathrm{Br}(K),$$

where $\psi \simeq_K \langle a_1,\dots,a_n\rangle$ is a diagonalization of ψ. Here $\simeq_K$ denotes the isometry of quadratic forms defined over K. The determinant of ψ is denoted by $\det_K \psi$.

Now we recall a definition of two covering groups of $\mathfrak{S}_n$. $\mathfrak{S}_n$ has a standard presentation with generators $t_1,\dots,t_{n-1}$ ($t_i = (i,i+1)$) and relations

$$t_i^2 = 1, \quad (t_it_{i+1})^3 = 1, \quad t_it_j = t_jt_i \quad \text{if } |i-j| \ge 2.$$

Let $\mathfrak{S}_n^-$ be the group generated by $\omega, \widetilde{t}_1,\dots,\widetilde{t}_{n-1}$ with relations

$$\widetilde{t}_i^{\,2} = 1 = \omega^2, \quad \omega\widetilde{t}_i = \widetilde{t}_i\omega, \quad (\widetilde{t}_i\widetilde{t}_{i+1})^3 = 1, \quad \widetilde{t}_i\widetilde{t}_j = \omega\widetilde{t}_j\widetilde{t}_i \quad \text{if } |i-j| \ge 2.$$

Let $\mathfrak{S}_n^+$ be the group generated by $\omega, \widetilde{t}_1,\dots,\widetilde{t}_{n-1}$ with relations

$$\widetilde{t}_i^{\,2} = \omega, \quad \omega^2 = 1, \quad \omega\widetilde{t}_i = \widetilde{t}_i\omega, \quad (\widetilde{t}_i\widetilde{t}_{i+1})^3 = 1, \quad \widetilde{t}_i\widetilde{t}_j = \omega\widetilde{t}_j\widetilde{t}_i \quad \text{if } |i-j| \ge 2.$$

Denote by $s_n^-, s_n^+ \in \mathrm{H}^2(\mathfrak{S}_n,\mathbb{Z}_2)$ the cohomology classes associated with these group extensions. The signature homomorphism $\varepsilon_n : \mathfrak{S}_n \to \mathbb{Z}_2$ is the unique non-zero element of $\mathrm{H}^1(\mathfrak{S}_n,\mathbb{Z}_2)$ if $n \ge 2$. We know $\mathrm{H}^2(\mathfrak{S}_n,\mathbb{Z}_2) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{0, s_n^+, s_n^-, \varepsilon_n \cup \varepsilon_n\}$ if $n \ge 4$. Here $\cup$ denotes the usual cup product of cohomology classes.

The trace map $\mathrm{tr}_{L/K} : L \to K$ defines a quadratic form over K on the K-vector space L by $x \mapsto \mathrm{tr}_{L/K}(x^2)$. We denote the associated quadratic space by $\langle L\rangle$. This form is usually called *trace form*. The homomorphism

$e : \Gamma_K \to \mathfrak{S}_n$ defines a homomorphism $e^\star : \mathrm{H}^2(\mathfrak{S}_n, \mathbb{Z}_2) \to \mathrm{Br}_2(K)$, where $\mathrm{Br}_2(K)$ is the subgroup of elements $x \in \mathrm{Br}(K)$ with $2x = 0$. Now Serre's formula asserts:

Proposition 1 (Serre [15]). 1. $e^\star(s_n^+) = (-2, \det_K\langle L\rangle)_K \otimes w_2\langle L\rangle$.
2. $e^\star(s_n^-) = (2, \det_K\langle L\rangle)_K \otimes w_2\langle L\rangle$.
3. $e^\star(\varepsilon_n \cup \varepsilon_n) = (\det_K\langle L\rangle, -1)_K$.

Let

$$\inf : \mathrm{H}^2(\mathcal{G}, \mathbb{Z}_2) \to \mathrm{H}^2(\Gamma_K, \mathbb{Z}_2)$$

be the inflation homomorphism induced by ϱ and let

$$\mathrm{res} : \mathrm{H}^2(\mathfrak{S}_n, \mathbb{Z}_2) \to \mathrm{H}^2(\mathcal{G}, \mathbb{Z}_2)$$

be the restriction homomorphism induced by the injection $\mathcal{G} \hookrightarrow \mathfrak{S}_n$. Then $e^\star = \inf \circ \mathrm{res}$. Combining Serre's formula with Hoechsmann's result we get

Proposition 2. *The embedding problem associated with the group extension* $\mathrm{res}(s_n^+)$ *(resp.* $\mathrm{res}(s_n^-)$*) has a solution iff*

$$w_2\langle L\rangle = (-2, \det_K\langle L\rangle)_K \ (\textit{resp. } w_2\langle L\rangle = (2, \det_K\langle L\rangle)_K).$$

3. The wreath product. The generalized alternating group $\mathbb{Z}_d \wr \mathfrak{A}_m$ is the wreath product of $\mathbb{Z}_d$ and $\mathfrak{A}_m$. We now recall the definition of the wreath product of groups.

Definition 1. Let $\mathcal{G}$ be a permutation group on a finite set Ω. Let $\mathcal{H}$ be a finite group and set $\mathcal{H}^\Omega = \{f : \Omega \to \mathcal{H}\}$. Then $f \mapsto {}^\pi f = f \circ \pi^{-1}$, $\pi \in \mathcal{G}$, defines an action of $\mathcal{G}$ on $\mathcal{H}^\Omega$. Now the *wreath product* $\mathcal{H} \wr \mathcal{G}$ of $\mathcal{H}$ and $\mathcal{G}$ is the semidirect product of $\mathcal{H}^\Omega$ and $\mathcal{G}$ induced by the action above.

In the sequel we need the commutator subgroup of a wreath product.

Lemma 1. *Let $\mathcal{G}$ be a permutation group of degree m, and $\mathcal{H}, \mathcal{H}_1, \mathcal{H}_2$ be groups.*

1. *If $\mathcal{G}$ acts transitively, then*

$$(\mathcal{H} \wr \mathcal{G})' = \{(h_1, \ldots, h_m; \sigma) \mid h_1 \ldots h_m \in \mathcal{H}',\ \sigma \in \mathcal{G}'\}$$

and

$$(\mathcal{H} \wr \mathcal{G})/(\mathcal{H} \wr \mathcal{G})' \simeq \mathcal{H}/\mathcal{H}' \times \mathcal{G}/\mathcal{G}'.$$

3. *If $\mathcal{G}'$ acts doubly transitively, then*

$$(\mathcal{H} \wr \mathcal{G})'' = \{(h_1, \ldots, h_m; \sigma) \mid h_1 \ldots h_m \in \mathcal{H}'',\ \sigma \in \mathcal{G}''\}.$$

3. $(\mathcal{H}_1 \wr \mathcal{G}) \times_{\mathcal{G}} (\mathcal{H}_2 \wr \mathcal{G}) \simeq (\mathcal{H}_1 \times \mathcal{H}_2) \wr \mathcal{G}$.

Proof. 1. Let $\pi_1 : \mathcal{H} \to \mathcal{H}/\mathcal{H}'$ and $\pi_2 : \mathcal{G} \to \mathcal{G}/\mathcal{G}'$ be the canonical projections. Let $[x, y] = xyx^{-1}y^{-1}$ be the commutator of x, y. Set $\mathcal{K} =$

$\{(h_1,\dots,h_m;\sigma) \mid h_1\dots h_m \in \mathcal{H}',\ \sigma \in \mathcal{G}'\}$. Since $\mathcal{H}/\mathcal{H}'$ is abelian,

$$\mathcal{H} \wr \mathcal{G} \to \mathcal{H}/\mathcal{H}' \times \mathcal{G}/\mathcal{G}' : (h_1,\dots,h_m;\sigma) \mapsto (\pi_1(h_1\dots h_m), \pi_2(\sigma))$$

is a homomorphism with kernel $\mathcal{K}$. Hence $(\mathcal{H} \wr \mathcal{G})' \subset \mathcal{K}$. Define $f_{i,a} : \Omega \to \mathcal{H}$, $a \in \mathcal{H}$, by $f_{i,a}(i) = a$, $f_{i,a}(k) = 1$ if $k \neq i$. Let $i \neq j$. Since $\mathcal{G}$ acts transitively, there is a permutation $\sigma \in \mathcal{G}$ with $\sigma(i) = j$. Then $[(f_{i,a};\mathrm{id}),(1;\sigma)] = (f_{i,a} \cdot f_{j,a^{-1}};\mathrm{id})$. Hence $\{(h_1,\dots,h_m;\mathrm{id}) \mid h_1\dots h_m = 1\} \subset (\mathcal{H} \wr \mathcal{G})'$. If $h_m \in \mathcal{H}'$, then $(1,\dots,1,h_m;\mathrm{id}) \in (\mathcal{H} \wr \mathcal{G})'$. We get the assertion from $(h;\mathrm{id})(1;\pi) = (h;\pi)$.

2. If $\mathcal{G}'$ acts doubly transitively on Ω, then we can choose $\sigma \in \mathcal{G}'$ with $\sigma(i) = i$, $\sigma(j) = k$, where $i \neq j,k$. Then

$$[(f_{i,a} \cdot f_{j,a^{-1}};\mathrm{id}),(1;\sigma)] = (f_{k,a} \cdot f_{j,a^{-1}},\mathrm{id}) \in (\mathcal{H} \wr \mathcal{G})''.$$

3. Define

$$\varphi : (\mathcal{H}_1 \wr \mathcal{G}) \times_{\mathcal{G}} (\mathcal{H}_2 \wr \mathcal{G}) \to (\mathcal{H}_1 \times \mathcal{H}_2) \wr \mathcal{G}$$

by $((h;\sigma),(g;\sigma)) \mapsto ((h_1,h_2);\sigma)$, where $(h_1,h_2) : \Omega \to \mathcal{H}_1 \times \mathcal{H}_2 : j \mapsto (h_1(j),h_2(j))$. Then φ is an isomorphism. ∎

In the following two lemmas we study inflation maps.

LEMMA 2. *Let* $\mathcal{G}$ *be a permutation group of degree* m, *and let* $\mathcal{H}$ *be a finite group. Let* $\mathcal{A}$ *be a finite abelian group, considered as a trivial* $\mathcal{G}$*-module. Then the inflation map*

$$\inf : \mathrm{H}^2(\mathcal{G},\mathcal{A}) \to \mathrm{H}^2(\mathcal{H} \wr \mathcal{G},\mathcal{A})$$

induced by the canonical projection $\varrho : \mathcal{H} \wr \mathcal{G} \to \mathcal{G}$ *is injective.*

Proof. An element $\varepsilon \in \mathrm{H}^2(\mathcal{G},\mathcal{A})$ corresponds to a central extension of $\mathcal{G}$ with kernel $\mathcal{A}$. The image of ε under the inflation map corresponds to a pull-back, i.e. there is a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{A} \arrow[r] \arrow[d, equal] & \mathcal{E} \times_{\mathcal{G}} (\mathcal{H} \wr \mathcal{G}) \arrow[r] \arrow[d] & \mathcal{H} \wr \mathcal{G} \arrow[r] \arrow[d, "\varrho"] \arrow[dl, "\varphi"'] & 1 \\
1 \arrow[r] & \mathcal{A} \arrow[r] & \mathcal{E} \arrow[r, "\pi"] & \mathcal{G} \arrow[r] & 1
\end{tikzcd}$$

We know $\inf(\varepsilon) = 0$ if and only if the upper sequence splits. By the universal property of the pull-back this is equivalent to the existence of a homomorphism $\varphi : \mathcal{H} \wr \mathcal{G} \to \mathcal{E}$ making the above diagram commutative. We know $\iota : \mathcal{G} \to \mathcal{H} \wr \mathcal{G} : \sigma \mapsto (0;\sigma)$ is a monomorphism. Now $\varphi((0;\sigma)) = e$ gives $\sigma = \varrho((0;\sigma)) = \mathrm{id}$. Hence $\mathcal{G} \simeq \varphi \circ \iota(\mathcal{G})$ is a subgroup of $\mathcal{E}$. Let $x \in \mathcal{A} \cap \varphi \circ \iota(\mathcal{G})$. Then $x = \varphi((0;\sigma))$ and $\pi(x) = \mathrm{id} = \pi \circ \varphi((0;\sigma)) = \sigma$ gives $x = e$. Hence $\mathcal{E} \simeq \mathcal{A} \times \mathcal{G}$. ∎

The next lemma reduces our approach to double covers of $\mathbb{Z}_d \wr \mathcal{G}$, where $d = 2^f \geq 1$.

LEMMA 3. *Let $\mathcal{G}$ be a permutation group of degree m. Let $\pi : \mathcal{H}_1 \to \mathcal{H}_2$ be an epimorphism of finite groups $\mathcal{H}_1, \mathcal{H}_2$. Let $\mathcal{A}$ be an abelian group with order relatively prime to the order of* $\ker(\pi)$*. Then the inflation map*

$$\inf : \mathrm{H}^2(\mathcal{H}_2 \wr \mathcal{G}, \mathcal{A}) \to \mathrm{H}^2(\mathcal{H}_1 \wr \mathcal{G}, \mathcal{A})$$

induced by $\varrho : \mathcal{H}_1 \wr \mathcal{G} \to \mathcal{H}_2 \wr \mathcal{G} : (h; \sigma) \mapsto (\pi \circ h; \sigma)$ is an isomorphism.

Proof. The sequence

$$1 \to \ker(\pi)^m \to \mathcal{H}_1 \wr \mathcal{G} \to \mathcal{H}_2 \wr \mathcal{G} \to 1$$

is exact. Since the order of $\mathcal{A}$ is relatively prime to the order of $\ker(\pi)$, we get $\mathrm{H}^1(\ker(\pi)^m, \mathcal{A}) = \mathrm{H}^2(\ker(\pi)^m, \mathcal{A}) = 0$ (see [1, II.10.2]). Hence

$$0 \to \mathrm{H}^2(\mathcal{H}_2 \wr \mathcal{G}, \mathcal{A}) \xrightarrow{\inf} \mathrm{H}^2(\mathcal{H}_1 \wr \mathcal{G}, \mathcal{A}) \xrightarrow{\mathrm{res}} \mathrm{H}^2(\ker(\pi)^m, \mathcal{A}) = 0$$

is an exact sequence (see [14, VII, §7, Proposition 5]). ■

4. The restriction map res : $\mathrm{H}^2(\mathfrak{S}_{md}, \mathbb{Z}_2) \to \mathrm{H}^2(\mathbb{Z}_d \wr \mathfrak{A}_m, \mathbb{Z}_2)$**.** The image of the restriction map determines the double covers which can be shown to be Galois groups by the use of Serre's formula.

We know

$$\mathrm{H}^2(\mathcal{G}, \mathcal{A}) \simeq ((\mathcal{G}/\mathcal{G}') \otimes \mathcal{A}) \times (\mathrm{M}(\mathcal{G}) \otimes \mathcal{A}),$$

with an abelian group $\mathcal{A}$ (see [7, 2.1.20]). In [7, Theorem 6.3.13] we found a list of the relevant Schur multipliers. Together with Lemma 1 we get

$$\mathrm{H}^2(\mathbb{Z}_d \wr \mathfrak{A}_m, \mathbb{Z}_2) \simeq \begin{cases} \mathbb{Z}_2 & \text{if } d \equiv 1 \bmod 2, \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 & \text{if } d \equiv 0 \bmod 2, \end{cases}$$

and $m \geq 4$. We further know

$$\begin{aligned} \mathbb{Z}_d \wr \mathfrak{A}_m = \langle s_1, \ldots, s_{m-2}, w_1, \ldots, w_m \mid s_1^3 = s_j^2 = (s_{j-1}s_j)^3 = 1,& \\ 1 < j \leq m-2;\ (s_i s_j)^2 = 1,\ 1 \leq i < j-1,\ j \leq m-2;\ w_j^d = 1;& \\ w_i w_j = w_j w_i;\ s_i w_j = w_j s_i,\ j \neq 1, 2, i+1, i+2;& \\ s_i w_{i+1} = w_{i+2} s_i,\ i = 2, \ldots, m-2;& \\ s_1 w_3 = w_1 s_1;\ s_i w_1 = w_2 s_i,\ i = 1, \ldots, m-2\rangle.& \end{aligned}$$

Let $1 \to \{1, \omega\} \to \mathcal{E} \to \mathbb{Z}_d \wr \mathfrak{A}_m \to 1$ be an exact sequence. Then $\widetilde{g} \in \mathcal{E}$ denotes a preimage of $g \in \mathbb{Z}_d \wr \mathfrak{A}_m$ in $\mathcal{E}$. We can choose a set of generators $s_1, \ldots, s_{m-2}; w_1, \ldots, w_m$ of $\mathbb{Z}_d \wr \mathfrak{A}_m$ such that

$$\begin{aligned} \mathcal{E} = \langle \omega, \widetilde{s}_1, \ldots, \widetilde{s}_{m-2}, \widetilde{w}_1, \ldots, \widetilde{w}_m \mid \omega^2 = 1;\ \omega\widetilde{s}_i = \widetilde{s}_i\omega;\ \omega\widetilde{w}_j = \widetilde{w}_j\omega;& \\ \widetilde{s}_1^{\,3} = 1;\ \widetilde{s}_j^{\,2} = \lambda_3;\ (\widetilde{s}_{j-1}\widetilde{s}_j)^3 = 1,\ j = 2, \ldots, m-2;\ (\widetilde{s}_i\widetilde{s}_j)^2 = \lambda_3,& \\ 1 \leq i < j-1,\ j \leq m-2;\ \widetilde{w}_j^{\,d} = \lambda_2;\ \widetilde{w}_i\widetilde{w}_j = \lambda_4\widetilde{w}_j\widetilde{w}_i,\ i \neq j;& \\ \widetilde{s}_i\widetilde{w}_j = \widetilde{w}_j\widetilde{s}_i,\ j \neq 1, 2, i+1, i+2;\ \widetilde{s}_i\widetilde{w}_{i+1} = \widetilde{w}_{i+2}\widetilde{s}_i,\ i \neq 1;& \\ \widetilde{s}_1\widetilde{w}_3 = \widetilde{w}_1\widetilde{s}_1;\ \widetilde{s}_i\widetilde{w}_1 = \widetilde{w}_2\widetilde{s}_i\rangle,& \end{aligned}$$

where $\lambda_2, \lambda_3, \lambda_4 \in \{1, \omega\}$ (our notation agrees with the notation in [4]). If d is odd, we can choose $\lambda_2 = \lambda_4 = 1$. Therefore the one-to-one correspondence between all central extensions of $\mathbb{Z}_d \wr \mathfrak{A}_m$ with kernel $\mathbb{Z}_2$ and all elements of $\mathrm{H}^2(\mathbb{Z}_d \wr \mathfrak{A}_m, \mathbb{Z}_2)$ is given by $\mathcal{E} \mapsto (\lambda_2, \lambda_3, \lambda_4)$ if d is even; and by $\mathcal{E} \mapsto \lambda_3$ if d is odd. If d is odd, then $\lambda_3 = \omega$ gives the unique non-trivial extension of $\mathbb{Z}_d \wr \mathfrak{A}_m$ with kernel $\mathbb{Z}_2$.

Let $1 \to \{1, \omega\} \to \widetilde{\mathfrak{S}}_n \xrightarrow{\widetilde{\Phi}} \mathfrak{S}_n \to 1$, $n = md$, be an exact sequence. We know

$$\widetilde{S}_n = \langle \omega,\ \widetilde{t}_1, \ldots, \widetilde{t}_{n-1} \mid \omega^2 = 1,\ \omega \widetilde{t}_i = \widetilde{t}_i \omega,\ \widetilde{t}_i^{\,2} = \varepsilon_1,\ (\widetilde{t}_i \widetilde{t}_{i+1})^3 = 1,$$
$$(\widetilde{t}_i \widetilde{t}_j)^2 = \varepsilon_2 \text{ if } |i - j| \geq 2\rangle.$$

If $n \geq 4$, we get $\mathfrak{S}_n^- = (1, \omega)$, $\mathfrak{S}_n^+ = (\omega, \omega)$ and $\mathfrak{S}_n^0 := (\omega, 1)$. If $\widetilde{\mathfrak{S}}_n = \mathfrak{S}_n^+$, then $\widetilde{\Phi}^{-1}(\mathbb{Z}_d \wr \mathfrak{A}_m) =: (\mathbb{Z}_d \wr \mathfrak{A}_m)^+$. $(\mathbb{Z}_d \wr \mathfrak{A}_m)^-$ and $(\mathbb{Z}_d \wr \mathfrak{A}_m)^0$ are defined similarly.

Proposition 3. *Let*

$$\mathrm{res} : \mathrm{H}^2(\mathfrak{S}_{md}, \mathbb{Z}_2) \to \mathrm{H}^2(\mathbb{Z}_d \wr \mathfrak{A}_m, \mathbb{Z}_2)$$

be the restriction map, $m \geq 4$. *Then* res *can be identified with the map*

$$(\varepsilon_1, \varepsilon_2) \mapsto \begin{cases} \lambda_3 = \varepsilon_1 & \text{if } d \equiv 1 \bmod 2, \\ (\lambda_2, \lambda_3, \lambda_4) = (\varepsilon_1^{d/2} \varepsilon_2^{d(d-2)/8}, 0, \varepsilon_2) & \text{if } d \equiv 0 \bmod 2. \end{cases}$$

If $d \equiv 1 \bmod 2$, *then* res *is surjective*, *but not injective. If* $d \equiv 2 \bmod 4$, *then* res *is injective*, *but not surjective.*

If $d \equiv 0 \bmod 8$, *then* $\mathrm{res}(\mathfrak{S}_{md}^+) = \mathrm{res}(\mathfrak{S}_{md}^-) = (0, 0, \omega)$.

If $d \equiv 4 \bmod 8$, *then* $\mathrm{res}(\mathfrak{S}_{md}^+) = \mathrm{res}(\mathfrak{S}_{md}^-) = (\omega, 0, \omega)$.

If d is odd, then $\widetilde{\mathfrak{A}}_m \times_{\mathfrak{A}_m} (\mathbb{Z}_d \wr \mathfrak{A}_m)$ is the unique non-trivial double cover of $\mathbb{Z}_d \wr \mathfrak{A}_m$ (see Lemma 2). If $m > 7$ and if $m = 5$ and $d \equiv 1, 5 \bmod 6$ we get $\mathrm{M}(\mathbb{Z}_d \wr \mathfrak{A}_m) = \mathbb{Z}_2$. Hence $\widetilde{\mathfrak{A}}_m \times_{\mathfrak{A}_m} (\mathbb{Z}_d \wr \mathfrak{A}_m)$ is the unique covering group of $\mathbb{Z}_d \wr \mathfrak{A}_m$. If d is even, then $\widetilde{\mathfrak{A}}_m \times_{\mathfrak{A}_m} (\mathbb{Z}_d \wr \mathfrak{A}_m)$ corresponds to the tuple $(0, \omega, 0) \in \mathrm{H}^2(\mathbb{Z}_d \wr \mathfrak{A}_m, \mathbb{Z}_2)$.

5. The main theorems. We are now able to formulate the main results of this paper.

Theorem 1. *Let K be an algebraic number field. Then all double covers of $\mathbb{Z}_d \wr \mathfrak{A}_m$ and of $\mathbb{Z}_d \wr \mathfrak{S}_m$ are realizable as Galois groups over K.*

Theorem 2. *Let $m \geq 5, d \in \mathbb{N}$ be integers. Let K be an algebraic number field.*

1. *The non-trivial double cover $\widetilde{\mathfrak{A}}_m \times_{\mathfrak{A}_m} (\mathbb{Z}_d \wr \mathfrak{A}_m)$ of $\mathbb{Z}_d \wr \mathfrak{A}_m$ occurs as the Galois group of a regular extension of the rational function field $K(T)$. This is the unique non-trivial double cover of $\mathbb{Z}_d \wr \mathfrak{A}_m$ if d is odd.*

2. *Let* $d = 2^f \cdot d'$, $2 \nmid d'$.
   (a) *If* $d \equiv 2 \bmod 4$, *then* $(\mathbb{Z}_d \wr \mathfrak{A}_m)^0$ *occurs as the Galois group of a regular extension of* $K(T)$.
   (b) *If* $d \equiv 2 \bmod 4$ *and* m *is even, then* $(\mathbb{Z}_d \wr \mathfrak{A}_m)^+$ *and* $(\mathbb{Z}_d \wr \mathfrak{A}_m)^-$ *occur as the Galois groups of regular extensions of* $K(T)$.
   (c) *If* $d \equiv 0 \bmod 4$ *and* $\mu_{2^f} \subset K^\star$, *then* $(\mathbb{Z}_d \wr \mathfrak{A}_m)^+ = (\mathbb{Z}_d \wr \mathfrak{A}_m)^-$ *occurs as the Galois group of a regular extension of* $K(T)$. *The double cover which corresponds to the tuple* $(\omega^{d/4}, \omega, \omega)$ *is the Galois group of a regular extension of* $K(T)$.

THEOREM 3. *Let* d *be odd*, $m > 7$. *Then every central extension of* $\mathbb{Z}_d \wr \mathfrak{A}_m$ *is the Galois group of a regular extension of* $\mathbb{Q}(T)$.

6. Some reduction lemmas. First we recall a fact from group theory.

LEMMA 4. *A central extension of an abelian group is nilpotent.*

Proof. Let $1 \to \mathcal{A} \to \mathcal{E} \to \mathcal{G} \to 1$ be a central extension with $\mathcal{G}$ an abelian group. Then $\mathcal{E}' \subset \mathcal{A} \subset Z(\mathcal{E})$. By a theorem of Gaschütz (see [5, III.Satz 3.12]) we know $\mathcal{E}' = \mathcal{E}' \cap Z(\mathcal{E}) \subset \Phi(\mathcal{E})$, the Frattini subgroup of $\mathcal{E}$. Hence $\mathcal{E}$ is nilpotent by a result of Wielandt ([5, Satz 3.11]). ∎

PROPOSITION 4. *Let* K *be an algebraic number field. Let* $\mathcal{G}$ *be a permutation group of degree* m *and let* $\mathcal{H} \wr \mathcal{G}$ *be a wreath product of groups. Suppose*

$$1 \to \mathcal{A} \to \widetilde{\mathcal{H} \wr \mathcal{G}} \xrightarrow{\pi} \mathcal{H} \wr \mathcal{G} \to 1$$

is a central extension with

1. *the preimage* $\mathcal{N}$ *of* $\mathcal{H}^m$ *in* $\widetilde{\mathcal{H} \wr \mathcal{G}}$ *nilpotent and*
2. *the preimage* $\widetilde{\mathcal{G}}$ *of* $\mathcal{G}$ *in* $\widetilde{\mathcal{H} \wr \mathcal{G}}$ *realizable as a Galois group over* K.

Then $\widetilde{\mathcal{H} \wr \mathcal{G}}$ *occurs as a Galois group over* K.

Proof. Consider the semidirect product $\mathcal{N} \rtimes \widetilde{\mathcal{G}}$ defined by conjugation of $\widetilde{\mathcal{G}}$ on $\mathcal{N}$. Then

$$\mathcal{N} \rtimes \widetilde{\mathcal{G}} \to \widetilde{\mathcal{H} \wr \mathcal{G}} : (n, g) \mapsto ng$$

defines an epimorphism. If $\widetilde{n} \in \mathcal{N}$ and $\widetilde{g} \in \widetilde{\mathcal{G}}$, then $\pi(\widetilde{n}) = (n, \mathrm{id})$ and $\pi(\widetilde{g}) = (1, g)$. We get $\pi(\widetilde{g}\widetilde{n}\widetilde{g}^{-1}) = (1, g)(n, \mathrm{id})(1, g^{-1}) = (1, g)(n, g^{-1}) = {}^{\pi(\widetilde{g})}\pi(\widetilde{n})$. The conditions 1 and 2 are the assumptions of Ishanov's theorem [16, Claim 2.2.5]. Hence $\mathcal{N} \rtimes \widetilde{\mathcal{G}}$ and its epimorphic image $\widetilde{\mathcal{H} \wr \mathcal{G}}$ occur as Galois groups over K. ∎

Let $\mathcal{A} = \mathbb{Z}_2$ and $\mathcal{H} = \mathbb{Z}_d$. Then condition 1 is satisfied by Lemma 4. This reduces our approach to double covers of $\mathcal{G}$. By results of Mestre and of Sonn we are done if $\mathcal{G} = \mathfrak{A}_m, \mathfrak{S}_m$. This gives Theorem 1.

Now we prove a regularity lemma.

LEMMA 5. *Let $N/K(T)$ be a regular Galois extension with Galois group $\mathcal{G}$. Let M/N be an abelian extension such that $M/K(T)$ is a Galois extension with Galois group $\mathcal{H}$.*

1. *Then $M/K(T)$ is a regular extension if and only if $M^{\mathcal{H}'}/K(T)$ (the maximal abelian subextension of $M/K(T)$) and $N/K(T)$ are regular extensions.*

2. *If $\mathcal{H}$ is a non-trivial double cover of $\mathcal{G} = \mathbb{Z}_d \wr \mathfrak{A}_m$, $m \geq 5$, then $M/K(T)$ is a regular extension.*

Proof. 1. Let $M/K(T)$ be a regular extension. Then $N/K(T)$ and $M^{\mathcal{H}'}/K(T)$ are regular extensions [9, Corollary 1, p. 57]. Conversely let K' be the algebraic closure of K in M. Then $K' \cap N = K$. Hence $K'(T)/K(T)$ is an abelian extension contained in $M^{\mathcal{H}'}$.

2. If $G(M/N) < G(M/K(T))'$, then $\mathcal{H}/\mathcal{H}' \simeq \mathcal{G}/\mathcal{G}'$. This gives $M^{\mathcal{H}'} = N^{\mathcal{G}'}$. Now let $\mathcal{H}$ be a double cover of $\mathcal{G}$ with $G(M/N) \cap G(M/K(T))' = \{\mathrm{id}\}$. The number of these extensions is $|\mathrm{H}^2(\mathcal{G}/\mathcal{G}', \mathbb{Z}_2)| = |\mathrm{H}^2(\mathbb{Z}_d, \mathbb{Z}_2)| = \gcd(d, 2)$ (see [7, 2.1.17]). If $\mathcal{H}$ is a non-trivial extension, then $d \equiv 0 \bmod 2$, and $\mathcal{H}$ corresponds to the tuple $(\omega, 0, 0)$ (see Section 4). But then $\mathcal{H}/\mathcal{H}' \simeq \mathbb{Z}_{2d}$, which completes the proof. ∎

PROPOSITION 5. *Let K be a field. Let $\mathcal{G}$ be a transitive permutation group of degree m and let $\mathcal{H}$ be a finite group. Let*

$$E: \quad 1 \to \mathcal{A} \to \widetilde{\mathcal{G}} \to \mathcal{G} \to 1$$

be a non-trivial central group extension with $|\mathcal{A}|$ a prime. Let N/K be a Galois extension with Galois group $\mathcal{G}$.

1. *Let $\widetilde{N}/K$ and L/K be Galois extensions with $N = L^{\mathcal{U}}$, $\mathcal{U} = \{(t_1, \ldots \ldots, t_m; \mathrm{id}) \mid t_i \in \mathcal{H}\} \lhd \mathcal{H} \wr \mathcal{G}$, such that $\widetilde{N} \supset N$ and with Galois groups $G(\widetilde{N}/K) \simeq \widetilde{\mathcal{G}}$ and $G(L/K) \simeq \mathcal{H} \wr \mathcal{G}$ respectively. Then $G(\widetilde{N}L/K) \simeq \widetilde{\mathcal{G}} \times_{\mathcal{G}} \mathcal{H} \wr \mathcal{G}$.*

2. *Let K be a Hilbertian field of characteristic 0 and let $\mathcal{H}$ be a group which is realizable as the Galois group of a regular extension of K. Suppose there is a Galois extension $\widetilde{N}/K$ with Galois group $\widetilde{\mathcal{G}}$. Then there is a Galois extension M/K with $G(M/K) \simeq \widetilde{\mathcal{G}} \times_{\mathcal{G}} (\mathcal{H} \wr \mathcal{G})$.*

Let $\mathcal{A} \subset \widetilde{\mathcal{G}}'$ and let K be a rational function field. If $\widetilde{N}/K$ is a regular extension, then we can choose a regular extension M/K.

Proof. 1. We prove $\widetilde{N} \cap L = N$. Suppose $\widetilde{N} \cap L \neq N$. Then $\widetilde{N} \subset L$, since $|G(\widetilde{N}/N)|$ is a prime. Since $G(L/K) \simeq \mathcal{H} \wr \mathcal{G}$ is a semidirect product of $G(L/N) = \mathcal{H}^m$ and $\mathcal{G}$, there is a subgroup $\mathcal{G}_0 \simeq \mathcal{G}$ of $G(L/K)$ such that $\mathcal{G}_0 \cap G(L/N) = \{\mathrm{id}\}$ and $G(L/K) = \mathcal{G}_0 \cdot G(L/N)$. Set $N_0 = L^{\mathcal{G}_0}$. Obviously

$$\varphi : \mathcal{G}_0 \to G(\widetilde{N}/K) : \sigma \mapsto \sigma_{|\widetilde{N}}$$

is a monomorphism. Now $\sigma \in G(L/K)$ with $\sigma_{|\widetilde{N}} \in \varphi(\mathcal{G}_0) \cap G(\widetilde{N}/N)$ implies $\sigma_{|N_0 N} = \mathrm{id}$. Since $N_0 N = L$, the sequence E splits, contrary to our hypothesis.

2. Set $N = \widetilde{N}^{\mathcal{A}}$. There is a (regular) Galois extension L/K with $L \supset N$ and $G(L/K) \simeq \mathcal{H} \wr \mathcal{G}$ (see [10, Satz 1, Zusatz 1, p. 228]).

$\mathcal{A} \subset \widetilde{\mathcal{G}}'$ implies $(\widetilde{\mathcal{G}} \times_{\mathcal{G}} (\mathcal{H} \wr \mathcal{G}))/(\widetilde{\mathcal{G}} \times_{\mathcal{G}} (\mathcal{H} \wr \mathcal{G}))' \simeq \mathcal{H}/\mathcal{H}' \times \mathcal{G}/\mathcal{G}'$. Hence the maximal abelian subextensions of L/K and of N/K coincide. Now apply Lemma 5. ∎

Let $\mathcal{H}$ be an abelian group and let $\mathcal{G}$ be a permutation group with trivial center. Then $\varphi : \mathcal{H} \wr \mathcal{G} \to \mathcal{G} : (t_1, \dots, t_m; \sigma) \mapsto \sigma$ is the unique epimorphism from $\mathcal{H} \wr \mathcal{G}$ onto $\mathcal{G}$. Hence $G(L/K) \simeq \mathcal{H} \wr \mathcal{G}$ and $N \subset L$ with $G(N/K) \simeq \mathcal{G}$ gives $G(L/N) \simeq \mathcal{H}^m$.

PROPOSITION 6. *Let K be a rational function field of characteristic* 0. *Let $\mathcal{G}$ be a transitive permutation group of degree m, and let d_0, d_1 be relatively prime integers. Let*

$$E : \quad 1 \to \mathcal{A} \to \mathcal{E} \to \mathbb{Z}_{d_1} \wr \mathcal{G} \to 1$$

be a central group extension with $\gcd(|\mathcal{A}|, d_0) = 1$. *Let $\widetilde{N}/K$ be a* (*regular*) *Galois extension with Galois group $\mathcal{E}$. Then there is a* (*regular*) *Galois extension M/K with Galois group*

$$G(M/K) \simeq (\mathbb{Z}_{d_0 d_1} \wr \mathcal{G}) \times_{\mathbb{Z}_{d_1} \wr \mathcal{G}} \mathcal{E}.$$

The sequence

$$1 \to \mathcal{A} \to G(M/K) \to \mathbb{Z}_{d_0 d_1} \wr \mathcal{G} \to 1$$

corresponds to the image of the sequence E under the inflation map induced by the canonical projection $\mathbb{Z}_{d_0 d_1} \wr \mathcal{G} \to \mathbb{Z}_{d_1} \wr \mathcal{G}$.

Proof. Set $N_1 = \widetilde{N}^{\mathcal{A}}$ and $N = N_1^{\mathcal{U}}$, where $\mathcal{U} = \{(t_1, \dots, t_m; \mathrm{id})\} \triangleleft \mathbb{Z}_{d_1} \wr \mathcal{G}$. From [10, Satz 1, Zusatz 1, p. 228 and Satz 1, p. 224] we know that there is a (regular) Galois extension N_0/K with $N_0 \supset N$ and $G(N_0/K) \simeq \mathbb{Z}_{d_0} \wr \mathcal{G}$. Since d_0 and d_1 are relatively prime, we get

$$\begin{aligned} G(N_0 N_1/K) &\simeq G(N_0/K) \times_{G(N/K)} G(N_1/K) \\ &\simeq (\mathbb{Z}_{d_0} \wr \mathcal{G}) \times_{\mathcal{G}} \mathcal{G}(\mathbb{Z}_{d_1} \wr \mathcal{G}) \simeq \mathbb{Z}_{d_0 d_1} \wr \mathcal{G}. \end{aligned}$$

Set $M := \widetilde{N} N_0 = \widetilde{N}(N_0 N_1)$. Then M/K is a Galois extension. Since $\gcd(d_0, |\mathcal{A}|) = 1$, we get $\widetilde{N} \cap N_0 N_1 = N_1$. Hence

$$G(M/K) \simeq G(N_0 N_1/K) \times_{G(N_1/K)} G(\widetilde{N}/K) \simeq (\mathbb{Z}_{d_0 d_1} \wr \mathcal{G}) \times_{\mathbb{Z}_{d_1} \wr \mathcal{G}} \mathcal{E}.$$

If $\widetilde{N}/K$ and N_0/K are regular extensions, then so is M/K, because d_0 and the order of $\mathcal{A}$ are relatively prime. ∎

COROLLARY 1. *Let K be a rational function field of characteristic 0. Let d be an odd number, $f \in \mathbb{N}, f \geq 1$, $\mathcal{G} = \mathfrak{A}_m, \mathfrak{S}_m$.*

1. *If $(\mathbb{Z}_{2^f} \wr \mathcal{G})^+$, $(\mathbb{Z}_{2^f} \wr \mathcal{G})^-$ and $(\mathbb{Z}_{2^f} \wr \mathcal{G})^0$ are Galois groups over K, then so are $(\mathbb{Z}_{2^f \cdot d} \wr \mathcal{G})^+, (\mathbb{Z}_{2^f \cdot d} \wr \mathcal{G})^-$ and $(\mathbb{Z}_{2^f \cdot d} \wr \mathcal{G})^0$.*
2. *If every double cover of $\mathbb{Z}_{2^f} \wr \mathfrak{A}_m$ occurs as the Galois group of a (regular) extension of K, then every double cover of $\mathbb{Z}_{2^f \cdot d} \wr \mathfrak{A}_m$ with d odd is realizable as the Galois group of a (regular) extension of K.*

Proof. We know $\mathrm{H}^2(\mathbb{Z}_{2^f} \wr \mathfrak{A}_m, \mathbb{Z}_2) = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. With the notation as in Section 4 we get

$$\inf : \mathrm{H}^2(\mathbb{Z}_{2^f} \wr \mathfrak{A}_m, \mathbb{Z}_2) \to \mathrm{H}^2(\mathbb{Z}_{2^f \cdot d} \wr \mathfrak{A}_m, \mathbb{Z}_2)$$

is defined by $(\lambda_2, \lambda_3, \lambda_4) \mapsto (\lambda_2, \lambda_3, \lambda_4)$. Now apply Proposition 6. If $\mathcal{G} = \mathfrak{S}_m$, then see [4, Section 4]. ∎

7. Trinomials, trace forms and the Galois group of $f(X^d)$. Let $\mathcal{G}$ be a transitive permutation group of degree m. Then the wreath product $\mathbb{Z}_d \wr \mathcal{G}$ appears in a natural way as the Galois group of a polynomial. For further details we refer to [2].

PROPOSITION 7. *Let K be a field and let $f(X) \in K[X]$ be an irreducible and separable polynomial of degree $m \geq 4$ with Galois group $\mathcal{G}$.*

1. *Let $d \in \mathbb{N}$ be an integer with $\mu_d \subset K^\star$ and* $\mathrm{char}(K) = 0$ *or* $\mathrm{char}(K) \nmid d$ *and $\mu_d \subset K^\star$.*
   (a) *Then* $\mathrm{Gal}(f(X^d))$ *is a subgroup of $\mathbb{Z}_d \wr \mathcal{G}$.*
   (b) $\mathrm{Gal}(f(X^d)) \simeq \mathbb{Z}_d \wr \mathcal{G}$ *if and only if* $\mathrm{Gal}(f(X^p)) \simeq \mathbb{Z}_p \wr \mathcal{G}$ *for all primes $p \mid d$.*
2. *Let p be a prime with $p \neq \mathrm{char}(K)$ and $\mu_p \subset K^\star$. Suppose $\mathcal{G} \simeq \mathfrak{A}_m$ or $\mathcal{G} \simeq \mathfrak{S}_m$. If $\mathcal{G} \simeq \mathfrak{A}_4, \mathfrak{A}_5$, then let $p \neq 3$. Let N_0 be a splitting field of $f(X)$. Then* $\mathrm{Gal}(f(X^p)) \simeq \mathbb{Z}_p \wr \mathcal{G}$ *if and only if*
   (a) *p divides m and $(-1)^m f(0) \notin N_0^{\star p}$ or*
   (b) *$p \nmid m$, $(-1)^m f(0) \notin N_0^{\star p}$ and $f(X^p)$ is irreducible over the field $K(\sqrt[p]{(-1)^m f(0)})$.*

If $p \nmid m$, then $(-1)^m f(0) \notin N_0^{\star p}$ if and only if $\mathrm{Gal}(f(X^p)) \simeq \mathbb{Z}_p \times \mathcal{G}$ *or* $\mathrm{Gal}(f(X^p)) \simeq \mathbb{Z}_p \wr \mathcal{G}$. *Then* $\mathrm{Gal}(f(X^p)) \simeq \mathbb{Z}_p \times \mathcal{G}$ *iff $f(X^p)$ factors over $K(\sqrt[p]{(-1)^m f(0)})$ into a product of p prime polynomials of degree m.*

This is proven in [2, Corollary 1, Theorem 2 and Corollary 7].

LEMMA 6. *Let K be an algebraic number field. Let $m, l, d \in \mathbb{N}$, $s, t \in \mathbb{Z}$ be integers with $1 \leq l < m$, $\gcd(l, m) = 1$, $ms + tl = 1$, $\gcd(t, d) \in \{1, 2\}$ and $\mu_d \subset K^\star$. Choose $u, D \in K^\star$. Set*

$$H(X, U, V) = X^m + mU^{m-l}V^{s+t}X^l + (m-l)U^mV^t \in K(U, V)[X].$$

Let $H(X,Y)\in K(Y)[X]$ be the polynomial obtained by making in $H(X,u,V)$ the substitution

$$V=\begin{cases} l^l mDY^2-l^{-l} & \text{if } m \text{ is odd},\\ ((m-l)DY^2+l^l)^{-1} & \text{if } m \text{ is even}.\end{cases}$$

Suppose $-(m-l)u, (-1)^{(m+1)/2}(m-l)Du\notin K^{\star 2}$ if $m\not\equiv d\equiv t\equiv 0 \bmod 2$. The Galois group of $H(X^d,Y)$ over $K(Y)$ is isomorphic to $\mathbb{Z}_d\wr\mathfrak{S}_m$ iff $(-1)^{m(m-1)/2}D\notin K^{\star 2}$, and it is isomorphic to $\mathbb{Z}_d\wr\mathfrak{A}_m$ iff $(-1)^{m(m-1)/2}D\in K^{\star 2}$. If t is odd, then the splitting field N of $H(X^d,Y)$ is a regular extension of $K(\sqrt{(-1)^{m(m-1)/2}D})(Y)$.

Proof. The polynomial $X^m+mV^{s+t}X^l+(m-l)V^t\in K(V)[X]$ is absolutely irreducible and has Galois group $\mathfrak{S}_m$ over $K(V)$ (see [4, Proposition 6] and [19]). Set $L=K(\sqrt{(-1)^{m(m-1)/2}D})$. Let N and N_d be the splitting fields of $H(X,Y)$ and of $H(X^d,Y)$ over $K(Y)$ respectively. Then $N/L(Y)$ is a regular extension. From Lemma 1 we get $N_d^{(\mathbb{Z}_d\wr\mathfrak{A}_m)'}=L(\sqrt[d]{(-1)^m(m-l)u^mV^t},Y)$, which is regular over $L(Y)$ if $\gcd(t,d)=1$. Now apply Lemma 5. ∎

Proposition 8. *Let K be a field of characteristic 0 and consider the irreducible and separable polynomial $f(X):=X^n+aX^k+b\in K[X]$ with $a\neq 0$. Set $L:=K[X]/(f)$, $d:=\gcd(n,k)$, $md:=n$, $ld:=k$. Let d be even. Then the quadratic space $\langle L\rangle$ factorizes as follows.*

1. $\langle L\rangle\simeq_K\langle n,nk(n-k),-k(n-k)x,-bx\rangle\perp\frac{n-4}{2}\langle 1,-1\rangle$ *if m is odd;*
2. $\langle L\rangle\simeq_K\langle n,-n\cdot x,-kab,kax\rangle\perp\frac{n-4}{2}\langle 1,-1\rangle$ *if m is even,*

where

$$\begin{aligned} x&=n^mb^{m-1}+(-1)^{m-1}(n-k)^{m-l}k^la^mb^{l-1}\\ &=(-1)^{m(m-1)/2}d^m\cdot\operatorname{dis}(X^m+aX^l+b).\end{aligned}$$

This is proven in [3, Theorem 1]. There we also find a diagonalization in the case of d odd, which we do not need in this context.

9. Proof of Theorem 2. 1. Mestre [11, Théorème 1] gave a polynomial $F_T(X)\in\mathbb{Q}(T)[X]$ with Galois group $\mathfrak{A}_m, m\geq 5$, such that the splitting field of $F_T(X)$ is a regular extension of $\mathbb{Q}(T)$, contained in a regular extension with Galois group $\widetilde{\mathfrak{A}}_m$ and such that

$$\langle\mathbb{Q}(T)[X]/(F_T(X))\rangle\simeq_{\mathbb{Q}(T)} m\cdot\langle 1\rangle.$$

Now apply Proposition 5. Thus $\widetilde{\mathfrak{A}}_m\times_{\mathfrak{A}_m}(\mathbb{Z}_d\wr\mathfrak{A}_m)$ occurs as the Galois group of a regular extension of $K(T)$. If d is odd, then this is the unique non-trivial double cover of $\mathbb{Z}_d\wr\mathfrak{A}_m$ (see Lemma 3).

2. By Corollary 1 we can assume $d=2^f\geq 2$.

(b) $m\equiv 2 \bmod 4$, $d=2$. Choose $l\in\mathbb{N}$ with $1\leq l<m, \gcd(l,m)=1$.

STEP 1. Let $a, b, c, d \in K^\star$ be elements with

$$a^2 + cb^2 = (m-l)l^l - \frac{c}{d}$$

and $-d, -c \notin K^{\star 2}$. Set

$$F(Y) = (Y^2 + c)^2 + d((Y^2 - c)b + 2aY)^2.$$

Then $F(Y) \notin \overline{\mathbb{Q}}[Y]^{\star 2}$.

Proof. Assume $xF(Y) = (G(Y))^2$ for some $x \in K^\star$ and $G(Y) \in K[Y]$. Let $\alpha \in \overline{K}$ be a root of $F(Y)$. $F(0) = 0$ contradicts $-d \notin K^{\star 2}$, and $\alpha^2 + c = 0$ gives $cb - a\alpha = 0$, hence $\alpha \in K$, which contradicts $-c \notin K^{\star 2}$. The formal derivative of $F(Y)$ is

$$F(Y)' = 4(Y^2 + c)Y + 4d((Y^2 - c)b + 2aY)(bY + a).$$

From $F(\alpha) = F(\alpha)' = 0$ we get

$$(\alpha^2 - c)b + 2a\alpha = -\frac{\alpha(\alpha^2 + c)}{d(b\alpha + a)}$$

and

$$0 = F(\alpha) = (\alpha^2 + c)^2 + \frac{d\alpha^2(\alpha^2 + c)^2}{d^2(b\alpha + a)^2},$$

which gives $d(b\alpha + a)^2 + \alpha^2 = 0$. Since $-d \notin K^{\star 2}$ and $\alpha \neq 0$, the polynomial

$$G(Y) = Y^2 + d(bY + a)^2 \in K[Y]$$

is irreducible and has root α, hence divides $F(Y)$. We get

$$(1 + db^2)F(Y) = G(Y)^2.$$

Hence $(1 + db^2)F(Y)' = (G(Y)^2)' = 4(Y^2 + d(bY + a)^2)(Y + bd(bY + a))$, which implies $(1 + db^2)F'(0) = -4abcd(1 + db^2) = 4a^3bd^2$. Thus

$$\frac{c}{d} + cb^2 = -a^2 = (m-l)l^l - a^2,$$

a contradiction.

STEP 2. We consider $(\mathbb{Z}_2 \wr \mathcal{G})^+$ and $(\mathbb{Z}_2 \wr \mathcal{G})^-$. Choose $s, t \in \mathbb{Z}$ with $ms + tl = 1$, $s \equiv 1 \bmod 2$. Let $\varepsilon \in \{1, -1\}$. There is a prime $q \equiv 1 \bmod 4$ such that $q \nmid lm$ and

1. $q \not\equiv -ml \bmod \mathbb{Q}_p^{\star 2}$ if $p \mid l$;
2. $q \not\equiv -m(m-l) \bmod \mathbb{Q}_p^{\star 2}$ if $p \mid m$ and $p \neq 2$.

By [12, 71:19] there is an element $P \in \mathbb{Z}$ with $P \neq -1, 0, 1$ and

1. $(P, -mlq)_{\mathbb{Q}} \otimes (-1, \varepsilon lq)_{\mathbb{Q}} = 0$,
2. $P, -lmqP \notin \mathbb{Q}^{\star 2}$.

Using the Hasse–Minkowski Principle we see there are elements $a, b, c \in \mathbb{Q}$ with

$$a^2 + lmqPb^2 = (m-l)l^l - Pc^2.$$

We can choose $a, b, c \neq 0$. Set $V = (l^l - (m-l)T^2)^{-1}$ and

$$T = (m-l)^{-1} \frac{((Y^2 - lmqP)a - 2lmqPbY)^2}{(Y^2 + lmqP)^2}.$$

Then $-lmq, -lmqP \notin \mathbb{Q}^{\star 2}$ implies

$$\begin{aligned}(m-l)V^{-1} &= (m-l)l^l - (m-l)^2T^2 \\ &= Pc^2 + lmqP\frac{((Y^2 - lmqP)b + 2aY)^2}{(Y^2 + lmqP)^2} \notin \overline{\mathbb{Q}}[Y]^{\star 2}.\end{aligned}$$

Now set $F(X^2, Y) = H(X^2, -\varepsilon q, V)$ and $L = K(Y)[X]/(F(X^2, Y))$. Proposition 8 gives

$$w_2\langle L\rangle = (-1, \varepsilon lq)_{K(Y)} \otimes ((m-l)V, 2lmq\varepsilon)_{K(Y)} = (\det_{K(Y)}\langle L\rangle, -2\varepsilon)_{K(Y)}.$$

Hence $e^\star(s^\pm_{2m}) = 0$.

(b), (c) $m \equiv 0 \bmod 2$, $md \equiv 0 \bmod 8$. Let l be an integer with $1 \leq l < m$ and $\gcd(l, m) = 1$. Choose $s, t \in \mathbb{Z}$ with $ms + tl = 1$, $s \equiv 0 \bmod 2$. Set

$$V = (l^l + (-1)^{m/2}(m-l)Y^2)^{-1} \quad \text{and} \quad u^\pm = \mp 2m(m-l)ld.$$

Then the splitting field of $F(X^d, Y) = H(X^d, u^\pm, V)$ over $K(Y)$ is a regular extension of $K(Y)$ with Galois group $\mathbb{Z}_d \wr \mathfrak{A}_m$. Set $L = K(Y)[X]/(F(X^d, Y))$. Proposition 8 gives

$$w_2\langle L\rangle = ((m-l)V, \mp 2)_{K(Y)} = (\mathrm{dis}(F(X^d, Y)), \mp 2)_{K(Y)}.$$

(c) $m \equiv 1 \bmod 2$, $d = 2^f \geq 4$. Let $l \in \mathbb{N}$ be an element with $l \in \mathbb{Q}^{\star 2}$ and $1 \leq l < m$, $\gcd(l, m) = 1$. Choose $s, t \in \mathbb{Z}$ with $ms + tl = 1$ and t even. Set $V = (-1)^{(m-1)/2} l^l m Y^2 - l^{-l}$. The splitting field of

$$G(X^d, U, Y) = H(X^d, (m-l)(U^2 - 2), V)$$

over $K(U, Y)$ is a regular extension with Galois group $\mathbb{Z}_d \wr \mathfrak{A}_m$. By Hilbert's Irreducibility Theorem there are elements $u, y \in K^\star$ such that $G(X^d, u, y)$ has Galois group $\mathbb{Z}_d \wr \mathfrak{A}_m$ over K. Since

$$\mathrm{Gal}(G(X^d, u, y)) = \mathbb{Z}_d \wr \mathfrak{A}_m < \mathrm{Gal}(G(X^d, uy^{-1}Y, Y)) < \mathbb{Z}_d \wr \mathfrak{A}_m,$$

the polynomial $G(X^d, uy^{-1}Y, Y)$ has Galois group $\mathbb{Z}_d \wr \mathfrak{A}_m$ over $K(Y)$. The splitting field of $G(((uy^{-1}Y)^2 - 2)X, uy^{-1}Y, Y)$ over $K(Y)$ is a regular extension of $K(Y)$. Since t is even, $G(0, uy^{-1}Y, Y) \notin \overline{K}(Y)^{\star 2}$. Hence the splitting field of $G(X^d, uy^{-1}Y, Y)$ is a regular extension of $K(Y)$. Set $L = K(Y)[X]/(G(X^d, uy^{-1}Y, Y))$. Proposition 8 gives

$$w_2\langle L\rangle = ((uy^{-1}Y)^2 - 2, 2^f)_{K(Y)} = (\mathrm{dis}(G(X^d, uy^{-1}Y, Y)), 2^f)_{K(Y)} = 0,$$

since $-1 \in K^{\star 2}$. Hence $e^\star(s_{md}^{\pm}) = 0$.

Now consider the double cover $(\omega^{d/4}, \omega, \omega) = (0, \omega, 0) + (\omega^{d/4}, 0, \omega) = (0, \omega, 0) + \mathrm{res}(\mathfrak{S}_{md}^{-})$. Set

$$L' = K(Y)[X]/(F(X, Y)), \qquad L := K(Y)[X]/(F(X^d, Y))$$

if m is even and $L' = K(Y)[X]/(G(X, Y))$, $L := K(Y)[X]/(G(X^d, Y))$ if m is odd. Let N, N' be normal closures of $L/K(Y)$, $L'/K(Y)$ resp. By the above $N/K(Y)$ and $N'/K(Y)$ are regular extensions. We further know $G(N'/K(Y)) \simeq \mathfrak{A}_m$ and $G(N/K(Y)) \simeq \mathbb{Z}_d \wr \mathfrak{A}_m$. Since $-1 \in K^{\star 2}$, Proposition 8 gives $w_2\langle L'\rangle = 0$. Hence $N'/K(Y)$ is contained in a regular Galois extension $\widetilde{N}/K(Y)$ with Galois group $\widetilde{\mathfrak{A}}_m$. By Proposition 5, $\widetilde{N}N/K(Y)$ is a solution of the embedding problem defined by $N/K(Y)$ and $(0, \omega, 0)$. We get $\inf((0, \omega, 0)) = 0$. From $w_2\langle L\rangle = 0$ we conclude $\inf((\omega^{d/4}, 0, \omega)) = 0$. Hence $(\omega^{d/4}, \omega, \omega)$ is in the kernel of the inflation map induced by $F(X^d, Y)$ resp. $G(X^d, Y)$.

(a) Consider $(\mathbb{Z}_2 \wr \mathfrak{A}_m)^0$. If $m \equiv 0 \bmod 2$, choose $a, b, c \in \mathbb{Q}^\star$ with

$$a^2 + b^2 = (m - l)l^l - c^2$$

and set

$$V = (l^l + (-1)^{m/2}(m - l)T^2)^{-1} \quad \text{and} \quad T = (m - l)^{-1}\frac{((Y^2 - 1)a - 2bY)^2}{(Y^2 + 1)^2}.$$

Then

$$(m - l)V^{-1} = c^2 + \frac{((Y^2 - 1)b + 2aY)^2}{(Y^2 + 1)^2} \notin \overline{\mathbb{Q}}[Y]^{\star 2},$$

since $-1 \notin \mathbb{Q}^{\star 2}$. Thus $((m - l)V, -1)_{K(Y)} = 0$. Now consider $F(X^2, Y) = H(X^2, 1, V)$.

If $m \equiv 1 \bmod 2$, then use the polynomial $H(X^2, -(m - l)(U^2 + 1), V)$, t even, $V = (-1)^{(m-1)/2} l^l m Y^2 - l^{-l}$ and proceed as in (c). ■

10. Central extensions of $\mathbb{Z}_d \wr \mathfrak{A}_m$, d odd. The unique non-trivial double cover of $\mathbb{Z}_d \wr \mathfrak{A}_m$, where d is odd and $m > 7$, is a covering group of $\mathbb{Z}_d \wr \mathfrak{A}_m$. Following the arguments of Kotlar, Schacher and Sonn [8], we can reduce the question whether all central extensions of $\mathbb{Z}_d \wr \mathfrak{A}_m$, d odd and $m > 7$, are Galois groups over an algebraic number field to certain pull-backs. This method gives an affirmative answer to the problem.

The central extension $1 \to \mathcal{A} \to \mathcal{E} \to \mathcal{G} \to 1$ is called a *stem extension* of $\mathcal{G}$ if $\mathcal{A} \subset \mathcal{E}'$. If in addition $\mathcal{A} \simeq \mathrm{M}(\mathcal{G})$, then we call it a *stem cover* of $\mathcal{G}$. Theorem 6 of [8] generalizes as follows.

PROPOSITION 9. *Let $\mathcal{G}$ be a group satisfying*

1. $\mathcal{G}' = \mathcal{G}''$.

2. *$\mathcal{G}/\mathcal{G}'$ is cyclic of order d and there is an element $\sigma \in \mathcal{G}$ of order d which generates $\mathcal{G}/\mathcal{G}'$.*

Let K be a (*rational function*) *field with the following properties.*

1. *If the finite group $\mathcal{H}$ is the Galois group of a* (*regular*) *extension of K, then so is $\mathcal{H} \times \mathcal{A}$ for every finite abelian group $\mathcal{A}$.*

2. *Every factor group of the Galois group of a* (*regular*) *extension of K is the Galois group of a* (*regular*) *extension of K.*

If for every stem cover $\widetilde{\mathcal{G}}$ of $\mathcal{G}$ and every d' with $d \mid d'$ and such that $p \mid d'$ iff $p \mid d$ the pull-back

$$\widetilde{\mathcal{G}} \times_{\mathcal{G}/\mathcal{G}'} \mathbb{Z}_{d'}$$

is the Galois group of a (*regular*) *extension of K, then every central extension of $\mathcal{G}$ is the Galois group of a* (*regular*) *extension of K.*

Here $\widetilde{\mathcal{G}} \times_{\mathcal{G}/\mathcal{G}'} \mathbb{Z}_{d'}$ stands for the pull-back of $\widetilde{\mathcal{G}}$ and $\mathbb{Z}_{d'}$ along the homomorphisms $\widetilde{\mathcal{G}} \to \mathcal{G} \to \mathcal{G}/\mathcal{G}'$ and $\mathbb{Z}_{d'} \to \mathbb{Z}_d \simeq \mathcal{G}/\mathcal{G}'$. We just have to imitate the proof of Theorem 6 in [8].

Proof of Theorem 3. $\sigma = (0, \ldots, 0, 1; \mathrm{id}) \in \mathbb{Z}_d \wr \mathfrak{A}_m$ has order d and generates $(\mathbb{Z}_d \wr \mathfrak{A}_m)/(\mathbb{Z}_d \wr \mathfrak{A}_m)'$. Hence we can apply Proposition 9 (see [10, Zusatz 1, p. 226]). Let $d' \in \mathbb{N}$ be any odd integer with $d \mid d'$. By Lemma 3 and Section 4 the pull-back $\widetilde{\mathfrak{A}}_m \times_{\mathfrak{A}_m} (\mathbb{Z}_d \wr \mathfrak{A}_m)$ is the unique stem cover of $\mathbb{Z}_d \wr \mathfrak{A}_m$. We already know that there is a regular Galois extension L/K with Galois group $\mathfrak{A}_m$, contained in regular Galois extensions $\widetilde{N}/K$, M/K with $G(\widetilde{N}/K) \simeq \widetilde{\mathfrak{A}}_m$ and $G(M/K) \simeq \mathbb{Z}_{d'} \wr \mathfrak{A}_m$. We get $\widetilde{N} \cap M = L$ and $G(\widetilde{N}M/K) \simeq \widetilde{\mathfrak{A}}_m \times_{\mathfrak{A}_m} (\mathbb{Z}_{d'} \wr \mathfrak{A}_m)$. Set $M_{ab} = M^{(\mathbb{Z}_{d'} \wr \mathfrak{A}_m)'}$ and $M_0 = M^{\mathcal{U}}$, $\mathcal{U} = \{(t_1, \ldots, t_m; \mathrm{id}) \mid t_i \in \ker(\mathbb{Z}_{d'} \to \mathbb{Z}_d)\}$. Then $G(M_0/K) \simeq \mathbb{Z}_d \wr \mathfrak{A}_m$. We further get

$$M_0 \cap M_{ab} = M^{\mathcal{U} \cdot (\mathbb{Z}_{d'} \wr \mathfrak{A}_m)'} = M_0^{(\mathbb{Z}_d \wr \mathfrak{A}_m)'}.$$

The Galois extension $\widetilde{N}M_{ab}/K$ has Galois group $(\widetilde{\mathfrak{A}}_m \times_{\mathfrak{A}_m} (\mathbb{Z}_d \wr \mathfrak{A}_m)) \times_{\mathbb{Z}_d} \mathbb{Z}_{d'}$. ∎

References

[1] K. S. Brown, *Cohomology of Groups*, Grad. Texts in Math. 87, Springer, New York, 1982.

[2] M. Epkenhans, *On the Galois group of $f(X^d)$*, Comm. Algebra, to appear.

[3] —, *Trace forms of trinomials*, J. Algebra 155 (1993), 211–220.

[4] M. Epkenhans, *On double covers of the generalized symmetric group* $\mathbb{Z}_d \wr \mathfrak{S}_m$ *as Galois groups over algebraic number fields* K *with* $\mu_d \subset K$, J. Algebra 163 (1994), 404–423.

[5] B. Huppert, *Endliche Gruppen I*, Grundlehren Math. Wiss. 137, Springer, Berlin, 1967.

[6] M. Ikeda, *Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem für galoissche Algebren*, Abh. Math. Sem. Univ. Hamburg 24 (1960), 126–131.

[7] G. Karpilovsky, *The Schur Multiplier*, London Math. Soc. Monographs (N.S.), Clarendon Press, London, 1987.

[8] D. Kotlar, M. Schacher and J. Sonn, *Central extension of symmetric groups as Galois groups*, J. Algebra 124 (1989), 183–198.

[9] S. Lang, *Introduction to Algebraic Geometry*, Addison-Wesley, 1972.

[10] B. H. Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Math. 1284, Springer, Berlin, 1987.

[11] J. F. Mestre, *Extensions régulières de* $\mathbb{Q}(T)$ *de groupe de Galois* $\tilde{A}_n$, J. Algebra 131 (1990), 483–495.

[12] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer, Berlin, 1963.

[13] M. Schacher and J. Sonn, *Double covers of the symmetric groups as Galois groups over number fields*, J. Algebra 116 (1988), 243–250.

[14] J. P. Serre, *Corps Locaux*, Hermann, Paris, 1968.

[15] —, *L'invariant de Witt de la forme* $Tr(x^2)$, Comment. Math. Helv. 59 (1984), 651–676.

[16] —, *Topics in Galois Theory*, 1, Res. Notes in Math. 1, Jones and Bartlett, Boston, 1992.

[17] J. Sonn, *Central extensions of* S_n *as Galois groups via trinomials*, J. Algebra 125 (1989), 320–330.

[18] —, *Central extensions of* S_n *as Galois groups of regular extensions of* $\mathbb{Q}(T)$, ibid. 140 (1991), 355–359.

[19] N. Vila, *On central extensions of* A_n *as Galois group over* $\mathbb{Q}$, Arch. Math. (Basel) 44 (1985), 424–437.

[20] —, *On stem extensions of* S_n *as Galois group over number fields*, J. Algebra 116 (1988), 251–260.

[21] H. Völklein, *Central extensions as Galois groups*, ibid. 146 (1992), 144–152.

Fb Mathematik
Universität-Gesamthochschule Paderborn
D-33095 Paderborn, Germany
E-mail: martine@uni-paderborn.de

Received on 8.6.1996 (3002)