ISRAEL JOURNAL OF MATHEMATICS 96 (1996), 431–444

COVERING GROUPS OF ALMOST SIMPLE GROUPS AS GALOIS GROUPS OVER $\mathbb{Q}^{ab}(t)$

BY

GUNTER MALLE*

IWR, Im Neuenheimer Feld 368, D–69120 Heidelberg, Germany
e-mail: malle@kalliope.iwr.uni-heidelberg.de

AND

JACK SONN

Department of Mathematics, Technion, 32000 Haifa, Israel
e-mail: sonn@techunix.technion.ac.il

Dedicated to the memory of Shimshon Amitsur

ABSTRACT

In this paper we construct Galois extensions with the rigidity method and apply a criterion [15] for solving central embedding problems over $\mathbb{Q}^{ab}(t)$ to realize regularly the covering groups of most of the classical groups and the sporadic groups as Galois groups over $\mathbb{Q}^{ab}(t)$.

1. Introduction

Let $\mathbb{Q}^{ab}$ denote the maximal abelian extension of the rationals $\mathbb{Q}$. After $\mathbb{Q}$ itself, $\mathbb{Q}^{ab}$ is probably the most intensely studied ground field in inverse Galois theory, primarily because of Shafarevich's conjecture that its absolute Galois group is (profinite) free. At the same time, Hilbert's irreducibility theorem carries inverse Galois theory from $\mathbb{Q}$ to $\mathbb{Q}(t)$ (rational functions in t over $\mathbb{Q}$) and from $\mathbb{Q}^{ab}$ to $\mathbb{Q}^{ab}(t)$. It is therefore of interest to realize groups as Galois groups over $\mathbb{Q}^{ab}(t)$ by means of extensions

* The first author thanks the Deutsche Forschungsgemeinschaft for financial support. The second author would like to thank Professor B. H. Matzat and the IWR in Heidelberg for their hospitality during the period in which the collaboration leading to this paper took place.
Received November 15, 1994 and in revised form January 20, 1995

$K/\mathbb{Q}^{ab}(t)$ which are regular over $\mathbb{Q}^{ab}$, i.e., $\mathbb{Q}^{ab}$ is algebraically closed in K (the same of course holds for $\mathbb{Q}$, which is much more difficult). There is a local-global principle for central embedding problems over rational function fields [14] which is applied in [15] to formulate a simple criterion for solving central embedding problems over $\mathbb{Q}^{ab}(t)$ if the initial Galois extension is constructed by rigidity methods. This criterion is used in [15] to realize covering groups of two families of finite classical groups as Galois groups of extensions of $\mathbb{Q}^{ab}(t)$ which are regular over $\mathbb{Q}^{ab}$. If N is Galois over $\mathbb{Q}^{ab}(t)$ with Galois group G, and N is regular over $\mathbb{Q}^{ab}$, we will say that G is regular over $\mathbb{Q}^{ab}$, or that G occurs regularly as a Galois group over $\mathbb{Q}^{ab}(t)$, or that G is regularly realizable as a Galois group over $\mathbb{Q}^{ab}(t)$. In this paper we formulate the criterion purely group-theoretically and apply it to regularly realize most of the remaining covering groups of the classical groups over $\mathbb{Q}^{ab}(t)$, the main omission being the even dimensional orthogonal groups.

2. The criterion

Let K be any field, K_s its separable closure, $G_K := \mathrm{Gal}(K_s/K)$. An embedding problem over K is an exact diagram

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & A & \longrightarrow & \tilde{G} & \xrightarrow{e} & G & \longrightarrow & 1 \end{array}$$

with $\tilde{G}$ finite, $G = \mathrm{Gal}(L/K)$ for some field $L \leq K_s$. We will assume A to be abelian. A **(weak) solution** is a continuous homomorphism $f\colon G_K \to \tilde{G}$ such that $e \circ f = \mathrm{res}$. If f is surjective, f is called a **proper** solution, and the fixed field of $\ker f$ is a **solution .eld** N with $\mathrm{Gal}(N/K) \cong \tilde{G}$. It is known [4, p. 397] that if K is Hilbertian (and A ; abelian), then every embedding problem that has a solution has a proper solution.

:.1. CRITERION [15, THEOREM 5]: *Let k be any algebraic extension of $\mathbb{Q}^{ab}$, $K = :(t)$, L/K a finite Galois extension with group G. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the finite primes 'relative to t) of K that ramify in L, $\mathfrak{P}_i$ a prime divisor of $\mathfrak{p}_i$ in L of ramification 'ndex e_i, and let the inertia group of $\mathfrak{P}_i$ be generated by $\sigma_i \in G$, $i = 1, \ldots, r$. Given a central embedding problem as above with A finite cyclic of exponent m, suppose that for each $i = 1, \ldots, r$ either*

(a) $(e_i, m) = 1$ *or*

(b) $\langle \sigma_i \rangle$ *is its own centralizer in G.*

Then the embedding problem has a proper solution.

Let G be a finite group, $\mathbf{C} = (C_1, \dots, C_s)$ a class vector in G, i.e., an s-tuple of conjugacy classes of G. Set

$$\bar{\Sigma}(\mathbf{C}) := \{(\sigma_1, \dots, \sigma_s) \in G^s \mid \sigma_i \in C_i,\ \sigma_1 \cdots \sigma_s = 1\},$$

and

$$\Sigma(\mathbf{C}) := \{(\sigma_1, \dots, \sigma_s) \in \bar{\Sigma}(\mathbf{C}) \mid \langle \sigma_1, \dots, \sigma_s \rangle = G\}.$$

G acts on $\bar{\Sigma}(\mathbf{C})$ and on $\Sigma(\mathbf{C})$ by conjugation. Define $n(\mathbf{C}) := |\bar{\Sigma}(\mathbf{C})/G|$, and $\ell(\mathbf{C}) := |\Sigma(\mathbf{C})/G|$. Since $\Sigma(\mathbf{C})/G \subseteq \bar{\Sigma}(\mathbf{C})/G$ we have $\ell(\mathbf{C}) \leq n(\mathbf{C})$. The class vector $\mathbf{C}$ is called **rigid** if $\ell(\mathbf{C}) = 1$. Let Z_m denote a cyclic group of order m.

2.2. CRITERION:

(a) *Let G be a finite group with a rigid class vector $\mathbf{C} = (C_1, \dots, C_s)$ and let $(\sigma_1, \dots, \sigma_s) \in \Sigma(\mathbf{C})$. Assume that the center of G has a complement in the normalizer $\mathcal{N}_G(\langle \sigma_i \rangle)$ for some $1 \leq i \leq s$. Then there exists a Galois extension $N/\mathbb{Q}^{\mathrm{ab}}(t)$ regular over $\mathbb{Q}^{\mathrm{ab}}$ with $\mathrm{Gal}(N/\mathbb{Q}^{\mathrm{ab}}(t)) \cong G$.*

(b) *Let further m be a positive integer and suppose that for each $i \in \{1, \dots, s\}$ with one possible exception either σ_i has order prime to m or σ_i generates its own centralizer in G. (These properties are clearly independent of the chosen representatives $\sigma_i \in C_i$.) Then the field N in* (a) *can be chosen so that every central embedding problem for $G \cong \mathrm{Gal}(N/\mathbb{Q}^{\mathrm{ab}}(t))$ given by an exact sequence*

$$1 \longrightarrow Z_m \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$$

has a proper solution.

Proof: By [13, II, §4, Folgerung 3] (the Basic Rigidity Theorem) the rigidity of $\mathbf{C}$ together with the normalizer condition implies the existence of a regular Galois extension $N/\mathbb{Q}^{\mathrm{ab}}(t)$ with $\mathrm{Gal}(N/\mathbb{Q}^{\mathrm{ab}}(t)) \cong G$, which is unramified outside a set $\mathbb{S}$ of prime divisors $\mathfrak{p}_i$, $1 \leq i \leq s$, of degree one of $\mathbb{Q}^{\mathrm{ab}}(t)$, which can be prescribed arbitrarily. Further, the inertia groups over the $\mathfrak{p}_i$ are generated by elements $\sigma_i \in C_i$.

We may choose $\mathfrak{p}_s$ to be the infinite prime (relative to t). Then the proof is completed by applying Criterion 2.1. ∎

In general we will be dealing with covering groups with cyclic kernel, but in certain exceptional cases the kernel is non-cyclic. We therefore give the following reduction to the case of cyclic kernel.

2.3. PROPOSITION: *Let K be a Hilbertian field containing the m-th roots of unity, L/K a finite Galois extension. Suppose every central embedding problem (over L/K) with kernel Z_m is solvable (hence properly solvable). Then every central embedding problem with kernel a finite abelian group of exponent m is (properly) solvable.*

Proof: Let A, abelian (noncyclic) of exponent m, be the kernel of a central embedding problem

$$\mathcal{E}\colon 1 \longrightarrow A \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1.$$

We proceed by induction on $|A|$. Without loss of generality we may assume that m is a prime power p^e. Write $A = B \times C$ where C is cyclic of order $m = p^e$. By induction the induced embedding problems $\mathcal{E}', \mathcal{E}''$ with kernels $A/B \cong C$ and $A/C \cong B$ have proper solutions. From the pullback diagram

$$\begin{array}{ccc} \tilde{G} & \longrightarrow & \tilde{G}/B \\ \downarrow & & \downarrow \\ \tilde{G}/C & \longrightarrow & G \end{array}$$

we see that in order to solve properly the embedding problem $\mathcal{E}$, it suffices to solve properly the two induced embedding problems $\mathcal{E}', \mathcal{E}''$ in such a way that the two solution fields are linearly disjoint over L. Let $N' = L(J^{1/m})$ be a proper solution field to $\mathcal{E}'$, where $J \leq L^*/(L^*)^m$ (N'/L is a Kummer extension), and similarly let $N'' = L(x^{1/m})$, $x \in L^*/(L^*)^m$, be a solution field to $\mathcal{E}''$. By Kummer theory we see that the condition that needs to be fulfilled is that $J \cap \langle x \rangle = 1$. Suppose not. Then J contains the element $x^{p^{e-1}}$, which is nontrivial since x has order p^e. If $a \in K^*L^{*m}/L^{*m}$, then $N_1'' := L((xa)^{1/m})$ is also a solution to $\mathcal{E}''$. (This is classical, see [14, Prop. 2.5].) It therefore suffices to choose $a \in K^*L^{*m}/L^{*m}$ of order p^e such that $\langle a \rangle \cap J\langle x \rangle = 1$, since if a is so chosen, then $\langle xa \rangle \cap J \neq 1$ would imply $(xa)^{p^{e-1}} \in J$. Since by assumption also $x^{p^{e-1}} \in J$, we get $a^{p^{e-1}} \in J$, a contradiction. Also since $\langle a \rangle \cap \langle x \rangle = 1$, xa has order p^e. Now since K is Hilbertian and $N := L((J\langle x \rangle)^{1/m})$ is a finite extension of K, there is an element $a \in K^*$ such that $X^m - a$ is irreducible over N, by a refinement of Hilbert's Irreducibility Theorem (see e.g. [4, p. 145]) applied to the irreducible polynomial $X^m - Y \in N[X, Y]$. ∎

In the following favorable cases, we can thus solve all central embedding problems:

2.4. COROLLARY: *Let G be a finite group with a rigid class vector $\mathbf{C} = (C_1, \ldots, C_s)$. Assume there exists $r \in \{0, 1, ..., s\}$ such that elements from r of the*

classes C_i generate their proper centralizers, while the orders of elements from the remaining $s - r$ classes are pairwise coprime. Then there exists a Galois extension $N/\mathbb{Q}^{ab}(t)$ with Galois group G such that every central embedding problem for $N/\mathbb{Q}^{ab}(t)$ has a proper solution. In particular, every covering group of G is regular over $\mathbb{Q}^{ab}$.

Proof: This is an easy consequence of Criterion 2.2(b) and Proposition 2.3. ∎

3. Generating pairs in some classical groups

In this section we construct Galois realizations for unitary and odd-dimensional orthogonal groups which yield themselves to an application of the Criterion 2.1. This is achieved by application of the criterion of Belyi to suitable class vectors of these groups. Rather similar class vectors had been investigated in [12], the only difference being that those in *loc. cit.* belonged to the simple groups, while here we will be dealing with the groups of adjoint type. So most arguments from *loc. cit.* carry over and we will refer to it for those parts.

3.A. THE UNITARY GROUPS. We first consider the projective unitary groups. In [16] Walter states without proof that the unitary groups can be generated by a transvection and a regular semisimple element of a suitable order. Here we prove a slightly stronger result, using ideas from [12]. Let $G = \mathrm{PGU}_n(q)$, $q = p^\nu$, $n \geq 3$, be the projective general unitary group defined over the finite field $\mathbb{F}_{q^2}$ with q^2 elements. By [5, 3.3 and 6.7], G contains cyclic maximal tori T_1, T_2 of orders $|T_1| = (q^n - (-1)^n)/(q+1)$, $|T_2| = q^{n-1} - (-1)^{n-1}$. (These are parametrized by the partitions (n) and $(n-1,1)$ of n in the notation of *loc. cit.*) Denote by C_i the class of a generator of T_i, where in addition we assume that C_2 is chosen such that $C_1 \cdot C_2 \subseteq G' = \mathrm{U}_n(q)$, which is clearly possible since $G/G' \cong T_i/T_i'$ for $i = 1, 2$, where $T_i' := T_i \cap G'$. Further, let C_3 be the conjugacy class of the image in $\mathrm{PGU}_n(q)$ of a transvection in $\mathrm{GU}_n(q)$ and denote by $\mathbf{C} := (C_1, C_2, C_3)$ the corresponding class vector of G. Note that the tori T_1, T_2 chosen above are precisely the ones considered in [12, Th. 2.2]. For better reference we first cite a result from *loc. cit.* on overgroups in $G' = \mathrm{U}_n(q)$ of T_i' (see [12, Th. 1.1]):

3.1. PROPOSITION: *Let $G' = \mathrm{U}_n(q)$ with $n \geq 3$.*

(a) *If $n = 2k+1$ is odd, then a maximal subgroup $M < G'$ of G' containing a semisimple element of order $|T_1'| = (q^{2k+1}+1)/(d(q+1))$, where $d = \gcd(2k+1, q+1)$, either lies in the collection $\mathcal{C}_3$ of subgroups defined by*

Aschbacher, or we are in one of the cases

$$(M', G') \in \{(\mathrm{L}_2(7), \mathrm{U}_3(3)),\ (A_7, \mathrm{U}_3(5)),\ (\mathrm{L}_2(11), \mathrm{U}_5(2))\},$$

where M' denotes the derived group of M.

(b) *If $n = 2k$ is even, then a maximal subgroup $M < G'$ of G' containing a semisimple element of order $|T_2'| = (q^{2k-1}+1)/(d(q+1))$, $d = \gcd(2k, q+1)$, either lies in the family $\mathcal{C}_1$, or*

$$(M', G') \in \{(A_7, \mathrm{U}_4(3)),\ (\mathrm{L}_3(4), \mathrm{U}_4(3)),\ (\mathrm{M}_{22}, \mathrm{U}_6(2))\},$$

or $G' = \mathrm{U}_4(2)$.

See [9] for the definition of the collections $\mathcal{C}_i$ and some of their properties. Now as in [12] we obtain:

3.2. PROPOSITION: *The class vector $\mathbf{C}$ of $\mathrm{PGU}_n(q)$, $n \geq 3$, $(n,q) \neq (3,2)$, satisfies $\ell(\mathbf{C}) = 1$. In particular, $\mathrm{GU}_n(q)$ is generated by a transvection and an element of order $q^n - (-1)^n$.*

Proof: We use a result in [12] together with the criterion of Belyi. For this we first evaluate the character theoretic formula for the normalized structure constant $n(\mathbf{C})$ of the class vector $\mathbf{C}$ (see [13, II, §6]):

$$n(\mathbf{C}) = \frac{|G|}{|\mathcal{C}_G(\sigma_1)||\mathcal{C}_G(\sigma_2)||\mathcal{C}_G(\sigma_3)|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(\sigma_1)\chi(\sigma_2)\chi(\sigma_3)}{\chi(1)}, \tag{3.1}$$

where $(\sigma_1, \sigma_2, \sigma_3) \in \tilde{\Sigma}(\mathbf{C})$ and the sum runs over the irreducible complex characters of $G = \mathrm{PGU}_n(q)$. Denote by $T_i' := T_i \cap G'$ the intersection of T_i with the derived group $G' = \mathrm{U}_n(q)$. In [12, Th. 2.2(a)] it was shown that if one replaces the classes C_i by the classes C_i' of generators of T_i', then only two irreducible characters of G' do not vanish on both C_1', C_2'. The argument proceeded in two steps. First, since the tori T_1' and T_2' have coprime orders, it follows from the Deligne–Lusztig theory of characters of reductive groups (see [1], for example) that only the so-called unipotent characters of G' can possibly not vanish on both classes. Secondly, by considering the prime divisors of the degrees of the unipotent characters it followed that every unipotent character different from the trivial and the Steinberg character has degree divisible by a prime dividing either $|T_1'|$ or $|T_2'|$. This then implied the required assertion, since it

is also known that the values of unipotent characters on regular semisimple elements in a torus of given type are constants independent of q (see again [1], for example).

The irreducible characters of G not vanishing on C_i, $i = 1, 2$, are extensions of irreducible characters of G'. Again, as in [12] the Deligne–Lusztig theory immediately shows that at most the extensions of unipotent characters of G' to G can take non-zero values on both C_1 and C_2. Moreover, since these are extensions of the unipotent characters of G', the above statement about the divisibility of their degrees by suitable primes remains correct. It thus follows again that at most the extensions of the trivial and of the Steinberg character do contribute to $n(\mathbf{C})$.

Let χ be the extension to G of an irreducible character of G'. Any other character χ' of G having the same restriction to G' as χ differs from χ by multiplication with a linear character. Since by definition we have $C_1 \cdot C_2 \subseteq G'$, the product $\chi(C_1)\chi(C_2)$ is the same as $\chi'(C_1)\chi'(C_2)$. As $C_3 \subseteq G'$ we also have $\chi(C_3) = \chi'(C_3)$. Thus we obtain the structure constant by evaluating the contribution of a single extension to G of each character of G' and then multiplying the result by the index $(G\colon G')$.

The value of the Steinberg character St on a semisimple element $\sigma \in G$ is known to be given, up to sign, by the p-part of its centralizer order:

$$\mathrm{St}(\sigma) = \pm|\mathcal{C}_G(\sigma)|_p, \tag{3.2}$$

while St vanishes on all non-semisimple elements [1]. As the elements in C_1 and C_2 are regular this implies that $\mathrm{St}(\sigma_i) = \pm 1$ for $\sigma_i \in C_i$, $i = 1, 2$. Further, for any non-central element σ (like the ones in C_3) this shows that $|\mathrm{St}(\sigma)| < \mathrm{St}(1)$. Evaluation of the formula (3.1) for $n(\mathbf{C})$ thus gives $n(\mathbf{C}) > 0$.

Now take $\boldsymbol{\sigma} := (\sigma_1, \sigma_2, \sigma_3) \in \tilde{\Sigma}(\mathbf{C})$ and let $H := \langle \boldsymbol{\sigma} \rangle$, $H' := H \cap G'$. Thus H contains generators of T_i, and H' contains generators of T_i', $i = 1, 2$. We can hence use Proposition 3.1 to investigate the possibilities for H'. As there, we distinguish two cases. Let first $n = 2k + 1$ be odd, so Proposition 3.1(a) applies. By [9, Table 3.5.B], the groups in $\mathcal{C}_3$ are stabilizers of extension fields, so their preimages in $\mathrm{GU}_{2k+1}(q)$ have the structure $\mathrm{GU}_m(q^r)$ for $2k + 1 = mr$, $r \geq 3$ prime, and are embedded in the natural way. But it is clear that under this embedding these subgroups cannot contain transvections of G. Further with the Atlas [2] it is easy to check that none of the exceptional maximal subgroups in Proposition 3.1(a) contains transvections. Having thus excluded all possibilities for maximal subgroups M of G' as overgroups of H' we conclude $H' = G'$, and hence also $H = G$ since $G/G' \cong T_i/T_i'$. Thus any pair of a transvection and a regular semisimple element in the Coxeter torus T_1 of order $(q^{2k+1} + 1)/(q + 1)$ generates G.

If $n = 2k$ is even we have to exclude the groups M occurring in Proposition 3.1(b). If $G = \mathrm{PGU}_4(2)$, then we have $\mathbf{C} = (2A, 5A, 9A)$ in Atlas notation, and by [2] no maximal subgroup of G contains elements of orders 5 and 9, giving the result. In the proof of [12, Th. 3.1], it is shown that the groups in $\mathcal{C}_1$ cannot occur except possibly for $(n, q) = (6, 2)$. Also, the exceptional cases are excluded apart from $(n, q) = (4, 3)$. But a look at [2] reveals that none of the two possibilities for $M < \mathrm{PGU}_4(3)$ contains transvections. We are left with $G = \mathrm{PGU}_6(2)$ and $\mathbf{C} = (2A, 21A, 33A)$. By order considerations, all maximal subgroups of $G' = \mathrm{U}_6(2)$ apart from M_{22} can be excluded. But the latter group does not extend to $\mathrm{PGU}_6(2)$, and again we obtain generation.

Until now we have shown $\emptyset \neq \bar{\Sigma}(\mathbf{C}) = \Sigma(\mathbf{C})$. The transvections of $\tilde{G} := \mathrm{GU}_n(q)$ have an $(n-1)$-dimensional eigenspace for the eigenvalue 1 in the irreducible matrix representation $\tilde{G} \hookrightarrow \mathrm{GL}_n(q^2)$, and clearly the normalizer of $\tilde{G}$ in $\mathrm{GL}_n(q^2)$ is generated by $\tilde{G}$ and the center $\mathcal{Z}(\mathrm{GL}_n(q^2))$ of $\mathrm{GL}_n(q^2)$. These are the assumptions of the criterion of Belyi [13, II, §5, Satz 1] which thus applies to a preimage of $\mathbf{C}$ in $\tilde{G}$, yielding $\ell(\mathbf{C}) = 1$. ∎

An application of the rigidity criterion now gives the desired Galois extensions.

3.3. PROPOSITION: *Let $n \geq 3$ and $(n, q) \neq (3, 2)$. Then there exists a Galois extension $N/\mathbb{Q}^{\mathrm{ab}}(t)$ regular over $\mathbb{Q}^{\mathrm{ab}}$ with group $\mathrm{PGU}_n(q)$ and ramified in three points such that generators of the inertia groups at two of these points are semisimple elements generating their proper centralizers. The fixed field of $\mathrm{U}_n(q)$ inside this extension is a rational function field $\mathbb{Q}^{\mathrm{ab}}(u)$, yielding a regular realization $N/\mathbb{Q}^{\mathrm{ab}}(u)$ of this group.*

Proof: By Proposition 3.2 the class vector $\mathbf{C} = (C_1, C_2, C_3)$ of $G = \mathrm{PGU}_n(q)$ defined above is rigid. Furthermore, the center of G is trivial. The first assertion then follows from the first part of Criterion 2.2.

The fixed field K of the normal subgroup $G' = \mathrm{U}_n(q)$ of G is Galois over $\mathbb{Q}^{\mathrm{ab}}(t)$ with Galois group the cyclic group G/G' of order $\gcd(n, q+1)$. Since the class C_3 lies already inside G', only two points are ramified in $K/\mathbb{Q}^{\mathrm{ab}}(t)$, and then the Hurwitz genus formula gives $g(K) = 0$. ∎

3.B. THE ODD-DIMENSIONAL ORTHOGONAL GROUPS. We now turn to the orthogonal groups in odd dimension. Let p be an odd prime and $G := \mathrm{SO}_{2n+1}(q)$, $q = p^\nu$, the special orthogonal group in dimension $2n+1$ over the finite field $\mathbb{F}_q$ with q elements. For $n \geq 3$ the commutator subgroup $G' = \mathrm{O}_{2n+1}(q)$ is a simple group and has index 2 in G.

Let T be a maximal torus of G with $|T| = q^n+1$. (So it is parametrized by the pair of partitions $(-,(n))$ in the notation of [5].) We denote by C_T the conjugacy class of some generator τ of the cyclic group T. The embedding $\mathrm{GO}_2(q^n) \leq \mathrm{GO}_{2n}(q) < \mathrm{SO}_{2n+1}(q)$ shows that the torus T contains outer elements, so in particular C_T is a conjugacy class in $G \setminus G'$. Let further S be a maximal torus of G of order $|S| = q^n - 1$ (parametrized by $((n),-)$) and $\sigma \in S$ a generator of the (cyclic) 2-prime part of S. The conjugacy class of some such σ is denoted by C_S. By [9, Table 3.5] the orthogonal group G contains maximal subgroups of type $\mathrm{O}_1(q) \perp \mathrm{O}^{\epsilon}_{2n}(q)$, for $\epsilon = \pm$, as stabilizers of orthogonal decompositions of the natural underlying space. These are hence the centralizers of their central involutions. The class with centralizer $\mathrm{O}_1(q) \perp \mathrm{O}^{\epsilon}_{2n}(q)$ lies in $G \setminus G'$ precisely if $q^n \equiv -\epsilon 1 \pmod 4$. Let C_2 denote this outer class of involutions. From the above description of the centralizers it is clear that such involutions have $2n$ eigenvalues -1 in the natural $(2n+1)$-dimensional matrix representation of G.

Let $\mathbf{C} = (C_2, C_S, C_T)$ be the class vector of G formed by the three conjugacy classes defined above. Note that by construction C_T and C_2 lie in the outer coset of G' in G, while C_S is contained in G'. Note also that T and S are precisely the tori T_1 and T_2 considered in [12, Th. 2.4].

For the proof of generation we again appeal to a result classifying the overgroups of the maximal torus T inside G (see [12, Th. 1]):

3.4. PROPOSITION: *Let $T' := T \cap G'$ and $T' \leq M < G'$ be a maximal subgroup of G' containing T'. Then one of the following holds:*

(a) *$M \in \mathcal{C}_1$ as defined in [9],*

(b) *$(M, G') = (S_9, \mathrm{O}_7(3))$.*

3.5. PROPOSITION: *The class vector $\mathbf{C}$ of $G = \mathrm{SO}_{2n+1}(q)$ satisfies $\ell(\mathbf{C}) = 1$.*

Proof: This is proved by combining a result in [12] with the Belyi criterion. We first evaluate the character theoretic formula (3.1) for the normalized structure constant $n(\mathbf{C})$. In [12, Th. 2.3(a)] this was done for a class vector where the first class C_T is replaced by the class C'_T of a generator of $T' := T \cap G'$. It was shown that in this case only the trivial character and the Steinberg character of G' take non-zero values on both C'_T and C_S. The arguments were essentially the same as those explained in the proof of Proposition 3.2. Thus, as there, they carry over to the extension group G of G', yielding that only the extensions of the trivial character and the Steinberg character of G' to G do not vanish on any of the three classes of $\mathbf{C}$. Evaluating the Steinberg character with the formula (3.2), using that both C_T and C_S contain

regular elements, one obtains with (3.1) that $n(\mathbf{C}) \neq 0$. (This is true since the first class C_2 is non-central.)

Now take $\boldsymbol{\sigma} \in \bar{\Sigma}(\mathbf{C})$ and let $H := \langle \boldsymbol{\sigma} \rangle$, $H' := H \cap G'$. If possible, let M be a maximal subgroup of G' containing H'. Since H contains a generator of T, we have $T' \leq M$ and we are in the situation of Proposition 3.4. By Table 3.5 in [9] the groups in the family $\mathcal{C}_1$ are the maximal parabolic subgroups and the reducible subgroups

$$\mathrm{O}_m(q) \perp \mathrm{O}^{\epsilon}_{2n+1-m}(q), \quad 1 \leq m < 2n+1,\ m \text{ odd},\ \epsilon = \pm,$$

corresponding to an orthogonal decomposition of the natural $(2n+1)$-dimensional orthogonal space for G. We can now proceed exactly as in the proof of [12, Th. 3.1] to exclude the remaining possibilities for M, since the order of elements in class C_S is by definition divisible by a primitive prime divisor of $q^n - 1$, which is the only property needed in *loc. cit.* The two preceding results show that there exist triples $\boldsymbol{\sigma} \in \bar{\Sigma}(\mathbf{C})$ and that such triples always generate G. Since elements in class C_2 have a $2n$-dimensional eigenspace for the eigenvalue -1, the criterion of Belyi applies and yields $\ell(\mathbf{C}) = 1$. ∎

We are now in a position to prove a Galois realization for the odd-dimensional orthogonal groups.

3.6. PROPOSITION: *Let $n \geq 3$. Then there exists a Galois extension of $\mathbb{Q}^{\mathrm{ab}}(t)$ regular over $\mathbb{Q}^{\mathrm{ab}}$ with group $\mathrm{SO}_{2n+1}(q)$ and generators of the inertia groups lying in the classes of $\mathbf{C} = (C_2, C_S, C_T)$. The fixed field of $\mathrm{O}_{2n+1}(q)$ inside this extension is a rational function field $\mathbb{Q}^{\mathrm{ab}}(u)$, yielding a regular realization of this group.*

Proof: By Proposition 3.5 we have $\ell(\mathbf{C}) = 1$. According to the Basic Rigidity Theorem (Criterion 2.2) the assertion for $\mathrm{SO}_{2n+1}(q)$ then follows since G has trivial center. The descent to the commutator subgroup $G' = \mathrm{O}_{2n+1}(q)$ of index 2 is done by the same standard argument as in the proof of Proposition 3.3 for $\mathrm{U}_n(q)$. ∎

Remark: Note that Propositions 3.3 and 3.6 give a new proof of the result of Belyi, reproved by Walter [16], that the groups $\mathrm{PGU}_n(q)$, $n \geq 3$, and $\mathrm{SO}_{2n+1}(q)$ for q odd, $n \geq 3$, occur regularly as Galois groups over $\mathbb{Q}^{\mathrm{ab}}(t)$.

4. Galois realizations of covering groups of simple groups

We are now going to verify Criterion 2.2(b) for a number of almost simple groups. In this connection it is useful to note the following: Let S be a non-abelian simple group,

$S \leq G \leq \mathrm{Aut}(S)$ with G/S cyclic. Then the Schur multiplier $M(G)$ is a subgroup of the Schur multiplier $M(S)$ of S (see [15, Lemma 6]). A **covering group** or **stem extension** of G is a central extension

$$1 \longrightarrow A \longrightarrow \tilde{G} \longrightarrow G \longrightarrow 1$$

with A contained in the commutator subgroup of $\tilde{G}$. A **stem cover** of G is a covering group of G with $A \cong M(G)$. Every covering group of G is a factor group of a stem cover of G [8, pp. 628–655].

4.1. LEMMA: *Let $L/k(t)$ be a finite Galois extension, regular over k, with Galois group G, and let $\tilde{G}$ be a covering group of G. If N is a Galois extension of $k(t)$ containing L with $G(N/k(t)) \cong \tilde{G}$, then N is regular over k.*

Proof: Let k' be the algebraic closure of k in N. Then since L is regular over k, $k'(t) \cap L = k(t)$, so k'/k is abelian. But since $\tilde{G}$ is a covering group of G, the abelian extension $k'(t)$ of $k(t)$ must be contained in the fixed field of $\tilde{G}'$, which is contained in L. Hence $k' = k$. ∎

4.2. THEOREM:

(a) *Let $\mathrm{U}_n(q) \leq G \leq \mathrm{PGU}_n(q)$ for $n \geq 3$, $(n,q) \neq (3,2)$. Then any covering group of G occurs regularly as a Galois group over $\mathbb{Q}^{\mathrm{ab}}(t)$.*

(b) *Any covering group of $\mathrm{O}_{2n+1}(q)$ and of $\mathrm{SO}_{2n+1}(q)$, $n \geq 3$, occurs regularly as a Galois group over $\mathbb{Q}^{\mathrm{ab}}(t)$.*

Proof: We apply Criterion 2.2 to the Galois realizations found above. For (a) we start from Proposition 3.3, where we obtained regular Galois realizations of $G = \mathrm{PGU}_n(q)$ for the class vector (C_1, C_2, C_3). The elements from classes C_1 and C_2 are regular by [12, Th. 2.2(b)], so the tori they generate are already their full centralizers in G. Hence the assertion follows by Corollary 2.4 and Lemma 4.1.

In case (b) we may assume that q is odd, since $\mathrm{O}_{2n+1}(2^m) \cong \mathrm{S}_{2n}(2^m)$, and this case was already treated in [15]. So we can utilize the Galois realization in Proposition 3.5 defined by the class vector (C_2, C_S, C_T) of $\mathrm{SO}_{2n+1}(q)$. Since elements from C_T generate their full centralizer, while the orders of elements from C_2 and C_S are coprime, the result follows by Corollary 2.4 and Lemma 4.1. ∎

Together with the results in [15] this shows that the covering groups of all classical groups, with the possible exception of the orthogonal groups in even dimension, have regular Galois realizations over $\mathbb{Q}^{\mathrm{ab}}(t)$. For the group $\mathrm{S}_6(2)$, which was not treated

in [15], a regular Galois realization of the covering group $2 \cdot S_6(2)$ over $\mathbb{Q}(t)$ is already contained in [6, Satz 3.4]. Also, the group $U_3(2)$ is solvable and hence not of interest here.

For the exceptional groups of Lie type the following intermediate result may be deduced from the Galois realizations of simple groups contained in the literature:

4.3. THEOREM: *Let* $E_7(q) \leq G \leq E_7(q)_{ad}$, *where* $q = p^\nu$ *for* $p \geq 5$. *Then any covering group of* G *occurs regularly as a Galois group over* $\mathbb{Q}^{ab}(t)$.

Proof: In [10, Th. 8.1] the groups $E_7(q)_{ad} = E_7(q) \cdot 2$ for $q = p^\nu$, $p \geq 5$, were realized as Galois groups with a class vector $\mathbf{C} = (C_1, C_2, C_3)$, where elements in C_1 have p-power order, while those in C_2 and C_3 have orders 2, $(q - \delta)(q^6 + \delta q^3 + 1)$ respectively, where $q \equiv -\delta \pmod 3$, $\delta \in \{1, -1\}$. The Schur multiplier of $E_7(q)$ has order $\gcd(2, q - 1)$ (see [2], for example). The order of elements in C_1 is prime to 2, and it follows from the remarks in the proof of Prop. 8.1 in [10] that elements in C_3 generate their full centralizers. Thus the Criterion 2.1 applies. ∎

For the sporadic simple groups we similarly obtain:

4.4. THEOREM: *Let* $S \leq G \leq \mathrm{Aut}(S)$ *for a sporadic simple group* $S \neq M_{22}$. *Then any covering group of* G *occurs regularly as a Galois group over* $\mathbb{Q}^{ab}(t)$. *For* $G = M_{22}$, *this is true at least for the three-fold covering.*

Proof: The groups S themselves have been known to occur as Galois groups for quite some time (even over $\mathbb{Q}$ for $S \neq M_{23}$). We refer the reader to [11, II.9] for a list of references. For the 3-fold coverings of $\mathrm{Aut}(S)$ where

$$S \in \{M_{22}, McL, Suz, ON, Fi_{22}, Fi'_{24}\}$$

regular Galois realizations over $\mathbb{Q}$ have been obtained by Feit [3]. We treat the remaining cases with non-trivial multiplier by exhibiting a Galois realization of $\mathrm{Aut}(S)$ in which three points are ramified such that two of the classes in the corresponding class vector satisfy the assumptions listed in Criterion 2.2. This verifies the assertion for $G = \mathrm{Aut}(S)$. Since in all cases the simple group has index at most two in its automorphism group, an easy descent argument applies to obtain the result for S itself (see the proof of Proposition 3.3).

In the table below we collect Galois realizations for the remaining sporadic groups with non-trivial Schur multiplier. The second column gives the corresponding class vector in Atlas notation, while the third lists the literature where these realizations

were first proved. For J_3 it is easy to verify that $(2B, 3A, 34A)$ provides a semi-rational rigid class vector of $\mathrm{Aut}(J_3)$.

For Ru and Co_1, Corollary 2.4 applies since all three element orders are coprime. In all other cases, elements from the first two classes have coprime orders, while those in the third class generate their full centralizer by [2]. Thus again an application of Corollary 2.4 yields the desired result. ∎

Aut(S)	C	
M_{12}: 2	$(2C, 3A, 12A)$	[13, II, §6, Satz 2]
J_2: 2	$(3A, 8C, 14A)$	[7]
HS: 2	$(2C, 5C, 30A)$	[7]
Ru	$(2A, 5A, 13A)$	[11]
Suz: 2	$(2C, 3B, 28A)$	[7]
J_3: 2	$(2B, 3A, 34A)$	see above
Fi_{22}: 2	$(2D, 5A, 42A)$	[11]
Co_1	$(3A, 5C, 13A)$	[11]
B	$(2C, 3A, 55A)$	[11]

For $2 \cdot M_{22}$: 2 there does not seem to exist a rigid class vector of M_{22}: 2 satisfying the assumptions of Criterion 2.2 with $s = 3$, so the case of even-order covers of $\mathrm{Aut}(M_{22})$ has to be left open at present.

References

[1] R. W. Carter, *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*, Wiley, New York, 1985.

[2] J. H. Conway et al., *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[3] W. Feit, *Some finite groups with nontrivial centers which are Galois groups*, in *Group Theory, Proceedings of the 1987 Singapore Conference*, W. de Gruyter, Berlin/New York, 1989, pp. 87–109.

[4] M. Fried and M. Jarden, *Field Arithmetic*, Springer, Berlin, 1986.

[5] P. C. Gager, *Maximal tori in finite groups of Lie type*, Thesis, University of Warwick, 1973.

[6] F. Häfner, *Einige orthogonale und symplektische Gruppen als Galoisgruppen über* $\mathbb{Q}$, Mathematische Annalen **292** (1992), 587–618.

[7] D. C. Hunt, *Rational rigidity and the sporadic groups*, Journal of Algebra **99** (1986), 577–592.

[8] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin–New York, 1967.

[9] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, Cambridge University Press, Cambridge, 1990.

[10] G. Malle, *Exceptional groups of Lie type as Galois groups*, Journal für die reine und angewandte Mathematik **392** (1988), 70–109.

[11] G. Malle and B. H. Matzat, *Inverse Galois Theory*, Springer-Verlag, to appear.

[12] G. Malle, J. Saxl and Th. Weigel, *Generation of classical groups*, Geometriae Dedicata **49** (1994), 85–116.

[13] B. H. Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Mathematics **1284**, Springer, Berlin–Heidelberg–New York, 1987.

[14] J. Sonn, *Brauer groups, embedding problems, and nilpotent groups as Galois groups*, Israel Journal of Mathematics **85** (1994), 391–405.

[15] J. Sonn, *Rigidity and embedding problems over* $\mathbb{Q}^{ab}(t)$, Journal of Number Theory **47** (1994), 398–404.

[16] J. H. Walter, *Classical groups as Galois groups*, in *Proceedings of the Rutgers Group Theory Year, 1983–1984* (M. Aschbacher et al., eds.), Cambridge University Press, Cambridge, 1985, pp. 357–383.