

Representations, commutative algebra, and Hurwitz groups

Dedicated to Charles Leedham-Green on the occasion of his 65th birthday

W. Plesken, D. Robertz

1 Introduction

In this paper methods of commutative algebra are applied to study Hurwitz groups, i.e. finite epimorphic images of

$$G_{2,3,7} := \langle a, b \mid a^2, b^3, (ab)^7 \rangle.$$

The developed methods are much more general and can in principle be used to construct representations of any finitely presented group. One assigns matrices with indeterminate entries to the generators of the group so that the group relations become relations between commuting variables, as was already suggested in [PLS 97] and applied in [HPS 97]. Meanwhile rather effective methods for treating algebraic equations are developed so that it is worthwhile to come back to the old topic. In particular, we use an effective implementation of Janet's algorithm, an earlier and rather successful version of a Gröbner basis type algorithm, cf. [BCG 03], [BGY 01], [PIR 05], to deal with the equations. For the relevance of Hurwitz groups in the context of mathematics in general the reader is referred to [Mac 99], for its group theoretical relevance and history to [TaV 06].

There are essentially two situations to which the construction process for representations via algebraic equations is applied. First we construct representations for $G_{2,3,7}$ in low dimensions and draw conclusions from that to (finite) Hurwitz groups. Secondly, in case the representations depend on genuine parameters to be defined in Section 2, one can try to impose further relations on the group generators such that the parameters get more specialized, but still admitting solutions. Obviously, the lower the degree of the representations is, the less likely it is that parameters occur. In our case, we have to look at degrees 6 and 7.

In Section 2 two general remarks are made about the construction of representations. The first gives a normalization process for constructing irreducible or indecomposable representations which generalizes the construction of the companion matrix of a univariate polynomial. The second remark applies the *ultra product* construction to get a link

between representations in positive characteristic and characteristic zero. Section 3 constructs all irreducible representations of $G_{2,3,7}$ in characteristic zero up to degree 6 and Section 4 draws group-theoretic conclusions from that. For instance, it determines the precise number ϵ such that the direct product of ϵ copies of $\mathrm{PSL}(2, \mathbb{Z}/p^a\mathbb{Z})$ is a Hurwitz group for any prime p and any $a \in \mathbb{N}$. Section 5 classifies projective representations of degree 6 of $G_{2,3,7}$. Here for the first time the phenomenon of genuine parameters occurs. Some group-theoretic consequences of this are treated in Section 6. Finally, a two-dimensional variety of representations of degree 7 is studied in Section 7. Here, we find extra group relations, namely $(ab^2ab)^n = 1$ for $n \in \{10, 11, 12, 13, 17\}$ such that we get a representation of the resulting group, which is still infinite, over an algebraic number field. By passing to finite residue class fields or even residue class rings one obtains infinite families of finite Hurwitz groups satisfying this extra relation. It would be interesting to see, whether these results can be achieved using the classical character-theoretic approaches to the construction of Hurwitz groups.

The machinery for the extensive computations in this paper is Janet's algorithm. Since this is not the place to go into details about this useful algorithm for dealing with algebraic equations, or more generally with finitely generated modules over polynomial algebras, we only make a few remarks to stimulate group theoretician's interest. More details one can find in the introduction of [PIR 05]. Janet invented his algorithm in the context of linear partial differential equations, cf. [Jan 29] for a comprehensive presentation. If applied to linear pdes with constant coefficients it deals essentially with finitely generated modules over polynomial rings similar to Gröbner bases techniques, as pointed out by J.-F. Pommaret in 1990. The result is an explicit basis over the ground field, in fact in [PIR 05] it is shown that the Janet basis of a given finitely generated module provides a free resolution of the module. Under the name of involutive division V. Gerdt has developed the original idea into a strong computational tool which is a serious alternative to the conventional Gröbner bases algorithms, cf. e.g. [BGY 01]. More details on the implementations used for this paper and their present limits are explained in the very last paragraph. Like the Todd-Coxeter enumeration the method is a special case of the Knuth-Bendix procedure which however always terminates. Though this is not done in this paper, it could be used to prove infiniteness of certain finitely presented groups just by computing a representation with infinite image along the lines developed here.

The first author thanks A. Zalesskii for reviving his interest in Hurwitz groups. We are also grateful to him for pointing out errors and missing references in the first version of this paper. Both pro- p -groups and recognition of classical matrix groups played an important role in the preparation of this paper, which might not be visible from its final form. We thank Charles Leedham-Green for his contributions to these two topics which guided us. In return, this paper provides infinite families of matrix groups over finite fields which await recognition and also families of pro- p -groups arising as inverse limits of the Fitting subgroups of new Hurwitz groups.

2 Generalities

Let K be a field and $G := \langle g_1, \dots, g_k \mid r_i(g_1, \dots, g_k), i = 1, \dots, \rho \rangle$ a finitely presented group. The set of all representations

$$\Delta : G \rightarrow \mathrm{GL}(n, K)$$

can be viewed as the set $V_K(G, n)$ of K -rational points of an affine variety $V(G, n)$ defined over K , which is acted upon by $\mathrm{GL}(n, K)$ via conjugation. This is obvious, since Δ can be represented by

$$(\Delta(g_1), \dots, \Delta(g_k)) \in (K^{n \times n})^k \cong K^{n^2 k}$$

and the polynomial relations are given by the $n^2 \rho$ entries of $r_i(\Delta(g_1), \dots, \Delta(g_k)) - I_n$.^{*} Clearly, $V_K(G, n)$ only depends on G and not on the presentation of G . Although much has been said about the variety $V(G, n)$ in the literature, cf. e.g. [LuM 85], few examples have been worked out. For easy cases a dimension analysis can sometimes show that G is infinite. In the later sections we shall be interested in the case $G = G_{2,3,7}$ and small n .

Actually, we are not so much interested in all of $V_K(G, n)$ itself but only in the subset $\mathrm{Irr}_K(G, n)$ of all irreducible representations in $V_K(G, n)$. For an irreducible representation the following definition makes a first step to find a nice basis for the associated module. It is therefore more easily formulated in terms of modules than in terms of representations. Note the simple modules are among the cyclic ones.

Denote by F the free monoid generated by g_1, \dots, g_k . Passage from F to G via the obvious epimorphism goes without comment. In particular, any KG -module is automatically a KF -module.

Definition 2.1 *Let M be a cyclic KG -module of finite K -dimension.*

- 1.) *A total order \prec on the free monoid F is called admissible, if*
 - a) *$1 \prec g_i$ for $i = 1, \dots, k$ and*
 - b) *for each pair of words $(w_1, w_2) \in F^2$, $w_1 \prec w_2$ implies $g_i w_1 \prec g_i w_2$ for any $i = 1, \dots, k$.*
- 2.) *Fix an admissible total order \prec on F and let $v \in M$ with $KGv = M$. Then the natural K -basis (b_1, \dots, b_n) of M with respect to v and \prec is defined as follows: $b_1 := w_1 v$ with $w_1 := 1 \in F$. Suppose $(b_1 = w_1 v, \dots, b_i = w_i v)$ is already defined. Then the smallest $w_{i+1} \in F$ with $w_{i+1} v$ linearly independent of (b_1, \dots, b_i) yields $b_{i+1} := w_{i+1} v$. The sequence $\sigma_{v, \prec}(M) := (w_1 = 1, w_2, \dots, w_n)$ is called an associated sequence of M with respect to v and \prec .*
- 3.) *The matrix representation of KG associated to a cyclic KG -module M with respect to a natural basis is called a natural matrix representation.*

Clearly, these concepts are not restricted to group algebras but make sense for any finitely generated K -algebra. For instance, the cyclic $K[x]$ -modules of finite K -dimension have as their natural matrix representations $p(x) \mapsto p(m)$, where m is the companion matrix of some monic polynomial in $K[x]$. We apply the concept of associated sequences to stratify $V_K(G, n)$. In the sequel the admissible total order \prec will be fixed.

^{*}Sometimes these equations do not imply the invertibility of the matrices. Strictly speaking, one has to work in a localization defined by the nonvanishing of the k determinants.

Proposition 2.2 Fix a sequence $S = (w_1, \dots, w_n) \in F^n$ which occurs as associated sequence of some cyclic KG -module M . Let $V_K^S(G, n)$ be the set of all $\Delta \in V_K(G, n)$ such that the associated KG -module $K_\Delta^{n \times 1}$ defined by $G \times K_\Delta^{n \times 1} \rightarrow K_\Delta^{n \times 1} : (g, v) \mapsto \Delta(g)v$ is cyclic and has the standard basis (consisting of the columns e_i of the unit matrix) as a natural basis, i. e.:

$$(e_1, \dots, e_n) = (w_1 e_1, \dots, w_n e_1).$$

Then $V_K^S(G, n)$ forms the set of all K -rational points of a variety $V^S(G, n)$.

Proof: The vanishing ideal of $V^S(G, n)$ is the radical ideal of the ideal generated by three types of equations. The first type comes from the vanishing ideal of $V(G, n)$. Let $(A_1, \dots, A_k) \in V^S(G, n)$. The second type of equations comes from the definition of the associated natural basis: whenever $g_i w_j = w_k$, then the j -th column of A_i is equal to e_k . Finally, the third type of equations is as follows. For every $1 \leq i < n$ and every $w \in F$ with $w_i \prec w \prec w_{i+1}$ the additional polynomials for $V^S(G, n)$ are given by the determinants of the $(i+1) \times (i+1)$ -submatrices of the $n \times (i+1)$ -matrix formed by the columns $e_1, w_2 e_1, \dots, w_i e_1, w e_1$, where of course the matrix with indeterminates corresponding to $\Delta(g_i)$ is to be substituted into each w_j and w . q. e. d.

Note if one takes only the first and third type of equations in the last proof, one obtains a variety $\tilde{V}^S(G, n)$ most of whose K -rational points can be conjugated into $V_K^S(G, n)$ by $\text{GL}(n, K)$.

Remark 2.3 There is a partial order on the set of all $V^S(G, n)$ defined as follows: $V^S(G, n) < V^T(G, n)$ iff $\tilde{V}^S(G, n) \subset \tilde{V}^T(G, n)$. The maximal elements are called generic. Different sequences give rise to different sets $\tilde{V}^S(G, n)$.

Example 2.4 Let G be any group generated by two elements a, b . We order F by $1 \prec a \prec b \prec \dots$, where the later elements do not matter, since we are only interested in $n = 2$. So the associated generic sequence is $(1, a)$ and the only other possibility is $(1, b)$. For the generic case we plug

$$A := \begin{pmatrix} 0 & a_{12} \\ 1 & a_{22} \end{pmatrix} \quad \text{and} \quad B := \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

into the relations for G and in the second case

$$A := \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \quad \text{and} \quad B := \begin{pmatrix} 0 & b_{12} \\ 1 & b_{22} \end{pmatrix}.$$

It is not true in general that any two representations in $V_K^S(G, n)$ are inequivalent. This can sometimes be achieved by choosing e_1 in a structurally rigid way.

Remark 2.5 There are only finitely many possibilities for the associated sequences with n and the presentation of G fixed.

Proof: Let $v \neq 0$ be some vector in M . Then $w_1 = 1$ and w_2 must be one of g_1, \dots, g_k by irreducibility. Say (w_1, w_2) is fixed and $\dim_K M > 2$, then w_3 must be of the form $g_i w_j$ with $j \leq 2$ and $1 \leq i \leq k$, again finitely many possibilities, and so on. q. e. d.

Some of the theoretical possibilities might end up with empty varieties. The choice of e_1 as vector for the definition above is not motivated yet by structural considerations. Very often one can introduce them by making use of some commutative subalgebra of KG .

Remark 2.6 *Let A be a commutative split semisimple subalgebra of KG . Then for each irreducible representation $\Delta \in \text{Irr}_K(G, n)$ there exists a representation δ of degree one of A such that (in the notation of Proposition 2.2)*

$$\text{Hom}_A(K_\delta^{1 \times 1}, K_{\Delta|_A}^{n \times 1}) \neq \{0\}.$$

Remark 2.7 *Let A be a subalgebra of KG and δ a one-dimensional representation of A . Each representation in*

$$V_K(G, n, \delta)_{\geq 1} := \{\Delta \in V_K(G, n) \mid \text{Hom}_A(K_\delta^{1 \times 1}, K_{\Delta|_A}^{n \times 1}) \neq \{0\}\}$$

is equivalent to a representation in

$$V_K(G, n, \delta, e_1) := \{\Delta \in V_K(G, n) \mid \Delta(a)e_1 = \delta(a)e_1 \text{ for all } a \in A\}.$$

$V_K(G, n, \delta, e_1)$ is the set of K -rational points of an algebraic variety $V(G, n, \delta, e_1)$. Whereas $V_K(G, n, \delta)_{\geq 1}$ is acted upon by all of $\text{GL}(n, K)$, only the stabilizer of Ke_1 in $\text{GL}(n, K)$ acts on $V_K(G, n, \delta, e_1)$.

Note, however, that the orbits under the stabilizer might contain more than one representation in the same equivalence class. The notion of genuine parameters from the introduction can be interpreted as the quotient $V_K(G, n)/\text{GL}(n, K)$ not being finite. The next result gives a method to cancel out the group action under good circumstances.

Proposition 2.8 *Let A be a subalgebra of KG , e.g. $A = KH$ for some subgroup H of G , and let δ be a representation of A of degree one.*

$\text{Irr}_K(G, n) \cap V_K(G, n, \delta)_{\geq 1}$ is acted upon by $\text{GL}(n, K)$ so that each of its representations has a representative in

$$\dot{\bigcup}_S (V_K(G, n, \delta, e_1) \cap V_K^S(G, n) \cap \text{Irr}_K(G, n)),$$

where the union is taken over all associated sequences $S \in F^n$ occurring among the irreducibles. In case $\dim_K \text{Hom}_A(K_\delta^{1 \times 1}, K_{\Delta|_A}^{n \times 1}) = 1$ for all $\Delta \in V_K(G, n, \delta)_{\geq 1}$ this set is a full set of representatives.

Note in the last proposition, each $V_K(G, n, \delta, e_1) \cap V_K^S(G, n)$ can be viewed as the set of K -rational points of the intersection $V(G, n, \delta, e_1) \cap V^S(G, n)$ of two varieties defined over K .

There are quite a few results derived by character theory of finite groups which allow us to predict representations of $G_{2,3,7}$.

Theorem 2.9 *Let G be a group and $\delta_i : G \rightarrow \mathrm{GL}(n, F_i)$ with i running through an infinite index set I , where each F_i is a field.*

1.) *If the characteristics are all different and positive, then there is a field F of characteristic zero and a representation $\Delta : G \rightarrow \mathrm{GL}(n, F)$ with the following properties:*

a) *If for some $a \in G$ and $p \in \mathbb{Z}[x_{11}, \dots, x_{nn}]$ one has $p(\delta_i(a)) = 0$ (resp. $\neq 0$) for all but finitely many $i \in I$, then $p(\Delta(a)) = 0$ (resp. $\neq 0$).*

b) *If $\delta_i(G)$ fixes some symmetric or skewsymmetric nondegenerate bilinear form on its natural module $F_i^{n \times 1}$ for all but finitely many $i \in I$, then there exists a bilinear form with the same properties on $F^{n \times 1}$ fixed by $\Delta(G)$. (The same applies to nonzero tensors in $(F_i^{n \times 1})^{\otimes k} \otimes ((F_i^{n \times 1})^*)^{\otimes k}$.)*

2.) *If the characteristics of all F_i are equal to p , then there is a field F of characteristic p and a representation $\Delta : G \rightarrow \mathrm{GL}(n, F)$ with the properties a) and b) above.*

Proof: This follows from the well known ultra product construction. One passes from the family of the fields F_i to the direct product ring $\prod_{i \in I} F_i$. This ring has an ideal N consisting of all those tuples (f_i) with $f_i = 0$ for all but finitely many $i \in I$. By Zorn's Lemma there exists a maximal ideal M of $\prod_{i \in I} F_i$ containing N . Let $F := \prod_{i \in I} F_i / M$. By identifying $\prod_{i \in I} F_i^{n \times n}$ with $(\prod_{i \in I} F_i)^{n \times n}$ one can pass over from $\prod \delta_i : G \rightarrow (\prod_{i \in I} F_i)^{n \times n}$ to $\Delta : G \rightarrow F^{n \times n}$ by taking the entries modulo M . Thus one easily obtains the result by noting that an element in $(f_i) \in \prod_{i \in I} F_i$ cannot lie in M if the set of all $i \in I$ with $f_i = 0$ is only finite, because it represents already a unit in $\prod_{i \in I} F_i / N$. Now a) and b) are easily checked. Clearly, the characteristic of F is zero under the assumption of 1.) and p under the assumption of 2.). q. e. d.

Typical integral polynomials to be taken in a) are $1 - \det$ or entries of $(x_{i,j})_{i,j=1,\dots,n}^k - I_n$, where I_n denotes the $(n \times n)$ -unit matrix. Typical tensors one can take in b) are products on the modules corresponding to δ_i viewed as elements of $F_i^{n \times 1} \otimes ((F_i^{n \times 1})^*)^{\otimes 2}$. Of course, the field constructed in the proof is too big to be interesting apart from a general existence result. In our applications, G will be finitely presented such as $G = G_{2,3,7}$. For this group one has for instance epimorphisms onto most $G_2(q)$ by [Mal 90]. Therefore one can expect non-trivial homomorphisms into $\mathrm{GL}(7, K)$ for some field K of characteristic zero. In fact we shall find an integral domain R with field of fractions $K = \mathbb{Q}(x_1, x_2)$ and a homomorphism of $G_{2,3,7}$ into a certain subgroup of $\mathrm{GL}(7, R)$ lying in a non-split form of $G_2(K)$, so that one can take various homomorphisms of R onto fields (also finite fields), not only to obtain explicit epimorphism of $G_{2,3,7}$ onto $G_2(q)$ but also onto groups, whose factor group modulo the biggest normal p -subgroup is $G_2(q)$. In these cases it is interesting to see whether one still gets a representation in characteristic zero, if one imposes further relations on the generators. We succeed in doing so for the extra relations $[a, b]^n = 1$ for $n = 10, 11, 12, 13$ such that the image group is still infinite. The case $n = 11$ was already treated in [HPS 97]. However, we have now more flexible tools to deal with the equations. Similarly we also construct projective representations of $G_{2,3,7}$ of degree 6 related to symplectic groups and special linear groups. In these cases we found no extra relations which could be imposed.

3 Representations of degree up to 6

Let $G := G_{2,3,7}$. It is our aim to construct irreducible representations of G of small degrees over a field K of characteristic zero. Note $a \mapsto a, b \mapsto b^2$ defines an automorphism of G . In the terminology of the previous section, we have the following ordering on the free monoid F generated by a, b :

$$1 \prec b \prec a \prec b^2 \prec ab \prec ba \prec a^2 \prec b^3 \prec ab^2 \prec bab \prec a^2b \prec b^2a \prec aba \prec \dots$$

Lemma 3.1 *Let K be a field. For an irreducible K -linear action of G on $K^{n \times 1}$ let v_1 be an eigenvector for ab . Define $v_2 := bv_1, v_3 := bv_2, v_4 := av_3, v_5 := bv_4, v_6 := bv_5, v_7 := av_5, v_8 := av_6$.*

- 1.) *If $n \leq 5$, then (v_1, v_2, \dots, v_n) is a K -basis for $K^{n \times 1}$.*
- 2.) *If $n > 5$, then (v_1, v_2, \dots, v_5) can be extended to a K -basis for $K^{n \times 1}$. In case v_6 is linearly independent of (v_1, v_2, \dots, v_5) , then (v_1, v_2, \dots, v_n) is a K -basis of $K^{n \times 1}$ for $n \leq 8$ or (v_1, v_2, \dots, v_8) can be extended to a K -basis for $K^{n \times 1}$ for $n > 8$.*

Proof: Let $abv_1 = \eta v_1$ for some $\eta \in K$. Assume $n \geq 2$. Since the action is irreducible, not both av_1 and bv_1 can be multiples of v_1 . But $v_2 = bv_1 = \eta av_1$. Hence (v_1, v_2) are linearly independent. Since $a^2 = 1$, the element av_2 is a multiple of v_1 . Again by irreducibility $v_3 := bv_2$ is linearly independent of (v_1, v_2) in case $n \geq 3$. Now $bv_3 = v_1$. Hence the argument can be repeated. q. e. d.

Hence, under the assumption of the lemma, the natural sequences for the generic cases with respect to an eigenvector for ab are the beginnings of the following sequence:

$$1 \prec b \prec b^2 \prec ab^2 \prec bab^2 \prec b^2ab^2 \prec abab^2 \prec ab^2ab^2 \prec \dots$$

and up to degree 6 there are no other natural sequences with respect to an eigenvector for ab .

Note the lemma is also correct for projective representations in the sense of I. Schur and will also be applied for them. We emphasize that the results of this section are for characteristic zero. Many papers, including [Mac 69] and [Coh 81] in view of the next two corollaries, deal exclusively with all positive characteristics. Either by direct inspection or by Theorem 2.9 these results have consequences for characteristic zero. Our point of view is, that for the simpler cases, one computation in characteristic zero together with some number theoretic observations as explained in the next section recover the uniform part of the results also in positive characteristics. Of course, the exceptional cases in positive characteristic need to be investigated separately. Indeed, as was pointed out to us, there is an extensive literature on this, cf. [DTZ 00], [TaV 05], [TaV 06], [TaZ 04], [ViZ 05], [Vse 04]. Many of these papers are not only concerned with the construction of representations, but also with the identification of their images, something that we follow up only for very few cases, cf. Sections 4, 6. Our point of view here is that a good portion of the work can be done simply by machine computation using Janet's algorithm, at least in characteristic zero (or in any fixed positive characteristic). We are confident however that an implementation of Janet's algorithm over \mathbb{Z} which is almost available

now might also be helpful to find the exceptional characteristics and the corresponding representations which of course are more exciting from the point of view of constructing new Hurwitz groups but need considerably more details to enumerate.

From Lemma 3.1 one has the following consequence for degree two. Note, since G is perfect, one cannot have a non-trivial (linear) representation of degree 2, as seen by looking at the eigenvalues for the matrix representing a . Throughout this section let ζ be a primitive 7-th root of unity.

Corollary 3.2 *One has the following irreducible projective representations $\Delta_{2,\zeta}$ of G into $L_2(\mathbb{Q}[\zeta])$:*

$$a \mapsto \begin{pmatrix} 0 & \zeta \\ -\zeta^6 & 0 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

$\Delta_{2,\zeta}$ and $\Delta_{2,\zeta^{-1}}$ are equivalent, so that one has three pairwise inequivalent representations, which however are Galois conjugate. Any projective representation of G into $L_2(\mathbb{C})$ is equivalent over \mathbb{C} to one of these three.

Proof: Let $\Delta : G \rightarrow \text{PSL}(2, \mathbb{C})$ be a projective representation. Let $\Delta(a), \Delta(b)$ be represented by matrices $A, B \in \text{SL}(2, \mathbb{C})$. Then $A^2, B^3, (AB)^7$ are scalar matrices of determinant 1, i.e. ± 1 . By replacing A or B by its negative, one can achieve $A^2 = -1, B^3 = 1, (AB)^7 = 1$, because $A^2 = 1$ gives either a scalar matrix or a matrix of determinant -1 . Now Lemma 3.1 can be applied and one immediately has the result. q. e. d.

Corollary 3.3 *One has the following irreducible representation $\Delta_{3,\zeta,c} : G \rightarrow \text{GL}_3(\mathbb{Q}[\zeta])$:*

$$a \mapsto \begin{pmatrix} 0 & \zeta & \zeta c \\ \zeta^6 & 0 & c \\ 0 & 0 & -1 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

with $c = c_1(\zeta) = \zeta^2 + \zeta^4$ or $c = c_2(\zeta) = 1 + \zeta^6$.[†]

For the first choice of c , the image is isomorphic to $L_2(7)$. The three representations $\Delta_{3,\zeta,c_1(\zeta)}, \Delta_{3,\zeta^2,c_1(\zeta^2)}, \Delta_{3,\zeta^4,c_1(\zeta^4)}$ are equivalent so that one has two inequivalent representations for this choice of c .

For the second choice of c , $\Delta_{3,\zeta,c_2(\zeta)}$ and $\Delta_{3,\zeta^{-1},c_2(\zeta^{-1})}$ are equivalent so that one obtains three inequivalent representations for this choice of c . However, $\Delta_{3,\zeta,c_2(\zeta)}$ is a constituent of $\Delta_{2,\zeta^3} \otimes \Delta_{2,\zeta^3}$, in particular it factors over $L_2(\mathbb{Q}[\zeta])$.

Any irreducible projective representation of degree 3 over \mathbb{C} is equivalent to one of the five linear ones above.

Proof: The proof is similar to degree 2. However, excluding the possibility $B^3 = \zeta_3$ for a primitive third root of unity ζ_3 , one has to use Lemma 3.1 once more, because it reduces B to a rather special monomial shape, contradicting the determinantal condition. q. e. d.

A completely analogous proof, however with slightly more computing, yields the complete list for degree 4:

[†]The eigenvalues of the image of ab in the first case are ζ, ζ^2, ζ^4 and $1, \zeta, \zeta^6$ in the second.

Corollary 3.4 *For degree 4 the irreducible representations $\Delta : G_{2,3,7} \rightarrow \mathrm{GL}(4, \mathbb{C})$ are equivalent to one of the three inequivalent representations $\Delta_{2,\zeta} \otimes \Delta_{2,\zeta^2}, \Delta_{2,\zeta} \otimes \Delta_{2,\zeta^3}, \Delta_{2,\zeta^2} \otimes \Delta_{2,\zeta^3}$, which take values in $\mathrm{GL}(4, \mathbb{Q}[\zeta])$ and which are Galois conjugate.*

The projective irreducible representations of degree 4 are up to equivalence the ones obtained from Δ_{2,ζ^i} by composing with the irreducible representation of degree 4 of $\mathrm{SL}_2(\mathbb{C})$, yielding three inequivalent Galois conjugate representations and a further one with image isomorphic to $L_2(7)$.

Proof: For the linear case Lemma 3.1 yields the following shape for the matrices:

$$a \mapsto \begin{pmatrix} 0 & \zeta & 0 & 0 \\ \zeta^6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & 0 & 1 & c_1 \\ 1 & 0 & 0 & c_2 \\ 0 & 1 & 0 & c_3 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

with $c_1 + c_2 + c_3 = 0$ and further algebraic equations. Running Janet's algorithm gives exactly three solutions:

$$\begin{aligned} c_1 &= -(\zeta + \zeta^3 + \zeta^4), & c_2 &= \zeta - \zeta^6, \\ c_1 &= -(\zeta + \zeta^2 + \zeta^5), & c_2 &= \zeta - \zeta^6, \\ c_1 &= -(1 + \zeta^3 + \zeta^5), & c_2 &= -\zeta^2 + \zeta^3 - \zeta^4 + \zeta^5. \end{aligned}$$

The first two solutions give irreducible representations and the third a reducible one with the scalar matrices as commuting algebra. In fact, the image in the third case is isomorphic to an extension of \mathbb{Z}^6 by $L_2(7)$.[‡] Again Lemma 3.1 easily helps one to identify two of the tensor products in the statement as equivalent to these two representations.

The projective case is similar.

q. e. d.

With more machine computation, one obtains the classification in degree 5, which can also be extracted from [TaZ 04].

Corollary 3.5 *The irreducible representations of degree 5 fall into three equivalence classes of Galois conjugate representations, all of which can be obtained from $\Delta_{3,\zeta^i,c_2(\zeta^i)}$ in Corollary 3.3 as the symmetric part of the tensor square. Any projective irreducible representation of degree 5 over \mathbb{C} , which is not linear, is equivalent to one of the following two:*

$$a \mapsto \begin{pmatrix} 0 & \eta^5 & 0 & 0 & r \\ \eta^2 & 0 & 0 & 0 & -\eta^{16}r \\ 0 & 0 & 0 & \eta^7 & -\eta^{21}u \\ 0 & 0 & 1 & 0 & u \\ 0 & 0 & 0 & 0 & \eta^{21} \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & 0 & 1 & 0 & c \\ 1 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & c \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

[‡]The eigenvalues of the image of ab are $\zeta, \zeta^3, \zeta^4, \zeta^6$ in the first case, $\zeta, \zeta^2, \zeta^5, \zeta^6$ in the second case, and $1, \zeta, \zeta^2, \zeta^4$ in the third case.

with r, u, c one of the following two:

$$\begin{aligned} r &= 1 + \eta^{12} - \eta - \eta^{18} + 2\eta^{17} - \eta^{16} - \eta^{13} - 2\eta^{11} + \eta^{10} - 2\eta^6 + \eta^5 + \eta^3 - \eta^4 - \eta^9 - \eta^{21}, \\ u &= 1 - \eta^{23} - \eta^{16} + \eta^{20} + \eta^{15} - \eta^9 - \eta^2 + \eta^{21}, \\ c &= -\eta^2 + \eta^4 - \eta^5 - \eta^{10} + \eta^{11} - \eta^{17} + \eta^{18} + \eta^{21} \end{aligned}$$

resp.

$$\begin{aligned} r &= -1 - 2\eta^7 - \eta^{14} - \eta^{12} + \eta^{23} + 2\eta^{18} + 2\eta^{13} + \eta^{11} - \eta^{10} + \eta^8 + \eta^6 - \eta^5 \\ &\quad + \eta^3 + \eta^4 - \eta^{19} - \eta^{21}, \\ u &= -\eta^5 - \eta^{20} - \eta^{15} + \eta^{21}, \\ c &= 1 - \eta^2 - \eta^4 + \eta^7 - \eta^9 + \eta^{10} - \eta^{11} + \eta^{12} - \eta^{16} + \eta^{17} - \eta^{18} + \eta^{21} - \eta^{23}, \end{aligned}$$

where η is a primitive 35-th root of unity.

Proof: The linear case is straightforward. The projective case can be normalized such that $B^3 = 1$, $(AB)^7 = 1$ and A^2 is a primitive 5-th root of unity, which we have chosen to be η^7 . The rest is in theory clear, but in practice one has to calculate over $\mathbb{Q}[\eta]$ as ground field, which is of degree 24 over the rationals. In both cases AB has an eigenvalue 1, so that it is possible to repeat the calculation in the 5-th cyclotomic number field. But then the formulas are even worse: r, u, c lie in the subfield of $\mathbb{Q}[\eta]$ containing $\mathbb{Q}[\eta^7]$ of degree 12 over the rationals. It also turns out that the two solutions listed above are up to Galois conjugacy equivalent under the automorphism mentioned at the beginning of this section. q. e. d.

Corollary 3.6 *The irreducible linear representations of degree 6 over \mathbb{C} are all equivalent and factor over $L_2(7)$.*

Proof: We have two possibilities for the basis according to Lemma 3.1: (v_1, \dots, v_6) , which is the generic case, or (v_1, \dots, v_5, av_5) . The second case immediately yields determinant -1 for the matrix representing a , contradicting the perfectness of $G_{2,3,7}$. In the generic case, v_1, v_2, v_3 are cyclically permuted by b as well as v_4, v_5, v_6 . The matrix A representing the action of a with respect to our basis has its first four columns determined. As for the last two columns, its bottom 2×2 -submatrix must square to I_2 and have determinant 1, hence it can only be I_2 or $-I_2$. Both cases leave us with 8 indeterminates for the remaining entries, which quickly reduce to 4 because of $A^2 = I_6$. Running Janet's algorithm yields one solution in the first case and two in the second. The first case gives the irreducible representation factoring over $L_2(7)$ and the second two yield reducible representations, a decomposable one also factoring over $L_2(7)$ and an indecomposable one factoring over a space group with point group $L_2(7)$. q. e. d.

As for the projective representations of degree 6, the story is complicated and is treated in Section 5.

4 Group-theoretical consequences

The existence of the two-dimensional projective representation of $G_{2,3,7}$ has the following immediate consequence.

Definition 4.1 *Let H, U be any groups. Define $\epsilon(H, U)$ to be the biggest $z \in \mathbb{Z}_{\geq 0}$ such that the direct product U^z of z copies of U is an epimorphic image of H .*

The following theorem is a group theoretic formulation of an old result by Macbeath [Mac 69] with a new proof and a new corollary.

Theorem 4.2

$$\epsilon(G_{2,3,7}, L_2(q)) = \begin{cases} 1, & q = 7, \\ 1, & q = p^3, p \neq 7 \text{ prime}, p \not\equiv \pm 1 \pmod{7}, \\ 3, & q \text{ prime}, q \equiv \pm 1 \pmod{7}, \\ 0, & \text{otherwise.} \end{cases}$$

Proof: Analyzing the enveloping algebra of the representation $\Delta_{2,\zeta}$ yields that $\Delta_{2,\zeta}(\mathbb{Q}G_{2,3,7})$ is a non-split quaternion algebra over $\mathbb{Q}[\zeta + \zeta^6]$, which is ramified over its center only at two primes, both of which are infinite. (The third infinite prime gives the representation into the real projective group $\mathrm{PSL}_2(\mathbb{R})$ studied by Hurwitz, which also shows that the representation is faithful.) The center can be read off from the fact that $\Delta_{2,\zeta}$ and $\Delta_{2,\zeta^{-1}}$ are equivalent. The Gram matrix of the trace bilinear form with respect to the basis $(\Delta_{2,\zeta}(1), \Delta_{2,\zeta}(a), \Delta_{2,\zeta}(b), \Delta_{2,\zeta}(ab))$ is easily checked to have signature $(3, 1)$ for one and $(1, 3)$ for the two other embeddings of $\mathbb{Q}[\zeta + \zeta^6]$ into the reals \mathbb{R} . Also the determinant of the Gram matrix is a unit in $\mathbb{Z}[\zeta + \zeta^6]$ which shows that there is no ramification over the center at the finite primes.

Observe that 7 is the only ramified prime in $\mathbb{Q}[\zeta + \zeta^6]$. Hence, for any decomposed prime p , i.e. $p \equiv \pm 1 \pmod{7}$, our representation yields a homomorphism into $\mathrm{PSL}_2(\mathbb{Z}_p)^3$, where \mathbb{Z}_p denotes the ring of p -adic integers, and for the other primes, i.e. the inert ones, one gets a homomorphism into $\mathrm{PSL}_2(R_p)$, where R_p is the unramified extension of degree 3 of \mathbb{Z}_p . Taking these homomorphisms modulo p yields $\epsilon(G_{2,3,7}, L_2(q)) \geq 1$ resp. 3 in these cases, since the subgroups of $L_2(q)$ are well known. That there are no more epimorphisms onto $L_2(q)$ can be easily seen from Lemma 3.1. In any case $\Delta_{2,\zeta}$ and $\Delta_{2,\zeta^{-1}}$ are equivalent. In case $7 \mid p - 1$ all the roots ζ lie in \mathbb{F}_p , leaving $3 = 6/2$ choices, no two of which are conjugate under an automorphism of $L_2(p)$. In case $p \neq 7, 7 \nmid p - 1$ one needs a field extension F of degree 3 of \mathbb{F}_p to realize $\zeta + \zeta^{-1}$ (the trace of ab) as element of F . Since the Schur index must be one in positive characteristic, one gets a realization over F . Again the six possibilities for the representations are equivalent in pairs, but the remaining three are Galois conjugate and Galois conjugation induces a group automorphism on $L_2(p^3)$ so that one gets only one copy of $L_2(p^3)$ as epimorphic image.

The remaining case $q = 7^n$ can be dealt with directly using Lemma 3.1 by remarking that ζ has to be equal to 1 in this case and hence $n = 1$. q. e. d.

The above proof was not carried out in positive characteristic but rather via characteristic zero in order to show the following corollary at the same time.

Corollary 4.3 *Let $p \neq 7$ be a prime number ≥ 5 and R_p the unramified extension of degree 3 of \mathbb{Z}_p . One has $\epsilon(G_{2,3,7}, L_2(R_p/p^k R_p)) = 1$ for p a prime, $p \not\equiv 1 \pmod{7}$ and $\epsilon(G_{2,3,7}, L_2(\mathbb{Z}_p/p^k \mathbb{Z}_p)) = 3$ for p a prime, $p \equiv 1 \pmod{7}$, where k is an arbitrary natural number.*

Proof: From the above proof one gets a homomorphism of $G_{2,3,7}$ into $\mathrm{PSL}_2(\mathbb{Z}_p)^3$ resp. into $\mathrm{PSL}_2(R_p)$. By an old result of Wall, cf. [HoP 89], Theorem 2.3.37, the extension $\mathrm{PSL}_2(\mathbb{Z}/p^2\mathbb{Z})$ of the simple $L_2(p)$ -module $(\mathbb{Z}/p\mathbb{Z})^3$ by $L_2(p)$ does not split for primes $p \geq 5$. Hence, the result follows from the last proof for primes $p \geq 5, p \neq 7$. For $p = 2, 3$ an explicit computation becomes necessary, which is left to the reader. q. e. d.

Obviously, there are also results for $p \in \{2, 3, 7\}$. One has to do some calculations in $\mathrm{PSL}_2(R)$, where R is the p -adic completion of $\mathbb{Z}[\omega]$ with $\omega := \zeta + \zeta^6$. For the convenience of the reader, who wants to go into details, we mention that the projective representation can be written as

$$a \mapsto \begin{pmatrix} a_1 & a_2 \\ a_3 & -a_1 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

where one has $a_2 - a_3 + a_1 - \omega, a_2^2 - a_2 a_3 + a_3^2 - 2a_2 \omega + 2a_3 \omega + 1 + \omega^2$. Here a_3 can be chosen arbitrarily. Then the second equation determines a_2 and after this the first a_1 . For instance $a_3 := -\omega$ is a good choice for the 2-adic situation, because one can then do a Newton iteration for a_2 with starting value $1 - \omega - \omega^2$ to work with an arbitrary precision.

As a consequence, one obtains that $G_{2,3,7}$ is virtually a residual p -by- $L_2(p)^3$ -group resp. a p -by- $L_2(p^3)$ -group. At the same time one has infinitely many Hurwitz groups H with $H/O_p(H) \cong L_2(q)$ with $q = p$ or $q = p^3$ as above (and correspondingly in the other cases).

One also gets negative results from this classification. They are an immediate consequence of Theorem 2.9 and our classification of the representations up to degree 6 in characteristic zero.

Corollary 4.4 *Let $3 \leq n \leq 6$. There are only finitely many primes p such that $\mathrm{SL}(n, p^\alpha)$ or $\mathrm{SU}(n, p^\alpha)$ for some α is a Hurwitz group. Let $\overline{\mathbb{F}_p}$ be the algebraic closure of \mathbb{F}_p . Then, except for at most finitely many primes p , the only irreducible Hurwitz subgroups of $\mathrm{GL}(n, \overline{\mathbb{F}_p})$ are modulo their centers isomorphic to certain direct products of $L_2(q)$ with q as in Theorem 4.2.*

This agrees with the more explicit results in [DTZ 00]. Note projective groups of degree 5 were considered in [TaZ 04]. Some of the projective cases in degree 6 will be considered in the next chapter. As far as representations in positive characteristic are concerned, our implementation of Janet's algorithm in [BCG 03] meanwhile can also handle polynomials over \mathbb{Z} . This enables us for instance to find all characteristics where there are representations of a given degree, and to find these representations, thus dealing with the details left open by the last corollary. However, here we concentrate on characteristic zero.

5 Projective representations of degree 6

In this section we construct irreducible projective representations Δ of $G_{2,3,7}$. More precisely we construct matrices $A, B \in \text{GL}(6, K)$ satisfying

$$A^2 = -1, \quad B^3 = 1, \quad (AB)^7 = 1$$

for a suitable field K of characteristic zero such that $\Delta(a) := A$, $\Delta(b) := B$ defines an irreducible projective representation of $G_{2,3,7}$. According to Lemma 3.1 one can assume that A, B take one of the following two possible forms:

$$(*) \quad A = \begin{pmatrix} 0 & r & 0 & 0 & c_1 & d_1 \\ -r^6 & 0 & 0 & 0 & c_2 & d_2 \\ 0 & 0 & 0 & -1 & c_3 & d_3 \\ 0 & 0 & 1 & 0 & c_4 & d_4 \\ 0 & 0 & 0 & 0 & a_1 & a_2 \\ 0 & 0 & 0 & 0 & a_3 & -a_1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

in which case v_6 is linearly independent of v_1, \dots, v_5 in Lemma 3.1 or in the other case

$$(**) \quad A = \begin{pmatrix} 0 & r & 0 & 0 & 0 & 0 \\ -r^6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 1 & 0 & c & d_1 \\ 1 & 0 & 0 & 0 & c & d_2 \\ 0 & 1 & 0 & 0 & c & d_3 \\ 0 & 0 & 0 & 0 & -1 & d_4 \\ 0 & 0 & 0 & 1 & -1 & d_5 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

where r is a seventh root of unity, i.e. the eigenvalue of AB of the eigenvector which is the first standard basis column corresponding to v_1 .[§] In this last case $B^3 = I_6$ is equivalent to $d_1 = -(d_2 + d_3 + c(d_4 + d_5))$.

Lemma 5.1 *AB has at least four different eigenvalues. In particular, it has one eigenvalue of multiplicity 1.*

Proof: Clearly, AB has at least one eigenvalue which is a primitive seventh root of unity, say ζ . Therefore, one can choose $r = \zeta$ in the above matrices A . Since the characteristic is zero, AB is diagonalizable and, assuming AB has at most three eigenvalues, it therefore satisfies

$$(AB - \zeta^i I_6)(AB - \zeta^j I_6)(AB - \zeta^k I_6) = 0,$$

where $\zeta^i, \zeta^j, \zeta^k$ are the eigenvalues, i.e. $0 \leq i < j < k \leq 6$. These are 6^2 algebraic equations for the unknown coefficients in the matrices above, in addition to the equations coming from $A^2 + I_6 = 0$ resp. $B^3 - I_6 = 0$. Janet's algorithm very quickly shows that there are no solutions in any of the possible cases. q. e. d.

This lemma allows us to introduce computable names for the irreducible projective representations as follows. Let ζ be a fixed primitive seventh root of unity.

[§]The associated sequence in the sense of Definition 2.1 is $(1, b, b^2, ab^2, bab^2, b^2ab^2)$ in the first case and $(1, b, b^2, ab^2, bab^2, abab^2)$ in the second case.

Definition 5.2 Let Δ be a projective irreducible representation of $G_{2,3,7}$ mapping a^2 onto -1 , and each of $b^3, (ab)^7$ onto 1.

- 1) $e(\Delta)$ denotes the smallest integer $i \geq 0$ such that $\Delta(ab)$ has eigenvalue ζ^i with multiplicity 1.
- 2) $\tau(\Delta)$ denotes the type of Δ . It is g (from “generic”) if v_6 is linearly independent of v_1, \dots, v_5 , where v_6 is defined in Lemma 3.1 for the case that v_1 is the eigenvector of $\Delta(ab)$ for the eigenvalue $\zeta^{e(\Delta)}$. Otherwise it is s (from “special”).
- 3) Choose $r := \zeta^{e(\Delta)}$. Then the parameters of Δ are the values for the tuple $(a_1, \dots, d_4) \in K^{11}$ in $(*)$ in case $\tau(\Delta) = g$, resp. the values of $(c, d_1, \dots, d_5) \in K^6$ in $(**)$ in case $\tau(\Delta) = s$.

Since the eigenspace of $\Delta(ab)$ for the eigenvalue $r = \zeta^{e(\Delta)}$ is one-dimensional, one gets the following remark by Proposition 2.8.

Remark 5.3 The type together with the parameters are uniquely determined by the equivalence class of a projective representation of $G_{2,3,7}$. The parameters lie in the affine variety $P(*)$ resp. $P(**)$, whose polynomial equations result from $A^2 = -1, B^3 = 1, (AB)^7 = 1$. Any irreducible projective representation can be transformed to normal form.

Corollary 5.4 The projective irreducible representations Δ of $G_{2,3,7}$ as specified above, i.e. mapping a^2 onto -1 , and each of $b^3, (ab)^7$ onto 1, are equivalent to exactly one among the following:

- 1) $\Delta_{2,\zeta^i} \otimes \Delta_{3,\zeta^j,c_1(\zeta^j)}$ with $i = 1, 2, 3, j = 1, 3$, yielding six Galois conjugate projective representations over $\mathbb{Q}[\zeta]$ with $\tau(\Delta) = g$.[¶]
- 2) $\Delta_{2,\zeta^i} \otimes \Delta_{3,\zeta^i,c_2(\zeta^i)}$ with $i = 1, 2, 3$, yielding three Galois conjugate projective representations over $\mathbb{Q}[\zeta]$ with $\tau(\Delta) = g$.
- 3) $\Delta(a) = A, \Delta(b) = B$ as in $(*)$, i.e. $\tau(\Delta) = g$, with $r = \zeta$ and characteristic polynomial of AB the seventh cyclotomic polynomial. These form a 2-dimensional variety of representations with the parameters $(a_1, \dots, d_4) \in K^{11}$ subject to $(*_{eqn1})$ to $(*_{eqn3})$ listed in the middle of Section 6.
- 4) $\Delta(a) = A, \Delta(b) = B$ as in $(**)$, i.e. $\tau(\Delta) = s$, with $r = \zeta$ and characteristic polynomial of AB the seventh cyclotomic polynomial. These form a 1-dimensional variety of representations with the parameters $(c, d_1, \dots, d_5) \in K^6$ subject to $(**_{eqn})$ listed at the beginning of Section 6.

Proof: We first assume that 1 is eigenvalue of AB with multiplicity 1. We can therefore choose $r = 1$ in $(*)$ resp. $(**)$. Also a new variable n is introduced with relation $n \det(AB - 1) - 1 = 0$. This equation together with the ones from $(AB)^7 - I_6 = 0$ and $A^2 + I_6 = 0$ in case of $(*)$ resp. $B^3 - I_6 = 0$ in case of $(**)$ yield 12 solutions for $(*)$, more precisely a residue class ring of $\mathbb{Q}[a_1, \dots, n]$ of \mathbb{Q} -vector space dimension 12, and no solutions for $(**)$. This computation takes place over \mathbb{Q} , no ζ is needed. Factoring the minimal polynomial of the coset of n yields two factors $p_i(\lambda)$, each of degree 6. We end up with two prime ideals in the primary decomposition by adding $p_1(n)$ resp. $p_2(n)$ to

[¶]Note $\Delta_{3,\zeta^j,c_1(\zeta^j)}$ factors over $L_2(7)$.

the relations. In both cases the discriminant of the characteristic polynomial of AB is zero. We therefore choose ζ as an eigenvalue of AB with multiplicity at least two and now continue the computation over $\mathbb{Q}[\zeta]$. This now gives a unique solution in each case with eigenvalues $1, \zeta, \zeta, \zeta^2, \zeta^4, \zeta^6$ resp. $1, \zeta, \zeta, \zeta^3, \zeta^4, \zeta^5$. Because of Galois action we are done. However, the first case yields a reducible representation and therefore drops out. The remaining case yields the six Galois conjugate representations of case 1).

We next assume that 1 is eigenvalue of AB with multiplicity 2. In this case we may assume by Galois action and Lemma 5.1 that ζ is eigenvalue of multiplicity 1 of AB and hence may assume $r = \zeta$ in (*) resp. (**). These conditions lead to no solutions in case of (**) quite quickly by a computation over \mathbb{Q} with $\sum_{i=0}^6 \zeta^i$ as extra relation. However, the case (*) has to be split up into cases, one for each possible spectrum for AB . So we get equations from the coefficients of the characteristic polynomial of AB and, instead of the equations from $(AB)^7 - I_6$ we insert AB in its minimal polynomial, which is the multiplicity-free version of the characteristic polynomial. These computations can again be performed over \mathbb{Q} with $\sum_{i=0}^6 \zeta^i$ as extra relation. It turns out that in case (*) there are no solutions except for the spectrum $1, 1, \zeta, \zeta^2, \zeta^5, \zeta^6$ or $1, 1, \zeta, \zeta^3, \zeta^4, \zeta^6$. Because there are no solutions in (**), one can conclude that these two cases are Galois conjugate. We end up with the three Galois conjugate representations of case 2).

In the final case we assume that 1 does not occur as eigenvalue of AB . Again, by Galois action we may assume $r = \zeta$ as eigenvalue with multiplicity 1. In both cases one checks the various possibilities for the minimal polynomial of AB as done earlier, possibly by taking into account the coefficients of the characteristic polynomial. Note the degree of the minimal polynomial must be bigger than 3 by Lemma 5.1. It also cannot be 5, because then exactly one eigenvalue has multiplicity 2 which quickly leads to a contradiction to the determinant being 1. The case of exactly four different eigenvalues has to be excluded as in Lemma 5.1. The only cases left for both (*) and (**) are $\zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, \zeta^6$. Here one can start with the equations coming from $A^2 + I_6 = 0$ resp. $B^3 - I_6 = 0$ and the coefficients of the characteristic polynomial of AB all being 1. A slightly lengthy run of Janet's algorithm gives a two-dimensional variety for (*) and a less lengthy one a one-dimensional variety for (**). q. e. d.

We discuss some group-theoretical consequences of these results.

6 Further group-theoretical consequences

We discuss some of the projective representations of the last section from the point of view of finite Hurwitz groups. The representations in the first two groups are not so interesting because of their tensor product structure.

We start with the (simpler) one-dimensional family (of type s , i.e. (**)). Here is an explicit parametrization of the representations with c as parameter and ζ the fixed primitive 7-th

root of unity as in the previous section:

$$(**_{eqn}) \quad \begin{cases} d_1 = \zeta + \zeta^2 + \zeta^3 + \zeta^4 - \zeta c \\ d_2 = 2 - \zeta^3 - \zeta^4 + (1 + 3\zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5)c + c^2, \\ d_3 = -2 - \zeta - \zeta^2, \\ d_4 = -\zeta - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5 - c, \\ d_5 = -1 - \zeta. \end{cases}$$

Moreover one finds that this representation fixes a symplectic form over $K[c]$. Its Gram matrix can be written over $\mathbb{Z}[\zeta][c]$ and has determinant

$$\zeta^5(4 + \zeta^2 - 3\zeta^3 - 3\zeta^4 + \zeta^5 + (2\zeta^3 + 2 + 4\zeta + 2\zeta^4 + 2\zeta^5 + 2\zeta^2)c + c^2)^4.$$

If this determinant becomes zero upon specialization to a residue class field of $\mathbb{Q}[\zeta][c]$, the form does not become zero but only singular, i.e. the representation becomes reducible. We have not worked out the other values of c for which the representation becomes reducible, though this can be done. Galois conjugation usually turns our type s representation into a type g representation. Again the values for which this is not the case can be computed. Here is the trace of AB^2AB , which will be needed below:

$$c^2 + (2\zeta^3 + 2 + 4\zeta + 2\zeta^4 + 2\zeta^5 + 2\zeta^2)c + 2 + \zeta^2 + \zeta^5.$$

Now, no fractions turn up in the above parametrization. Therefore we can view the whole setup over $\mathbb{Z}[\zeta][c]$, where $\mathbb{Z}[\zeta]$ is the ring of algebraic integers in the 7-th cyclotomic number field.

Remark 6.1 *Every finite residue class ring of $\mathbb{Z}[\zeta][c]$ defines a finite Hurwitz group.*

Example 6.2 1) Take $\mathbb{Z}[\zeta][c]/\langle \zeta - 7, 29, c - 1 \rangle$ to obtain $\mathrm{PSp}(6, 29)$ as factor group of $G_{2,3,7}$.

2) Let $M := \{1, 2, 3, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\}$ and take

$$\mathbb{Z}[\zeta][c]/\langle \zeta - 7, 29, \prod_{i \in M} (c - i) \rangle$$

to obtain $\mathrm{PSp}(6, 29)^{15}$ as factor group of $G_{2,3,7}$, i.e. $\epsilon(G_{2,3,7}, \mathrm{PSp}(6, 29)) \geq 15$, cf. Lemma 4.1.

3) Take $\mathbb{Z}[\zeta][c]/\langle \zeta - 7, 29, (c - 1)^k \rangle$ to obtain $\mathrm{PSp}(6, \mathbb{F}_{29}[x]/\langle x^k \rangle)$ for any $k \in \mathbb{N}$ as factor group.

4) Take $\mathbb{Z}[\zeta][c]/\langle \zeta - (7 + 22 \cdot 29 + 5 \cdot 29^2 + 3 \cdot 29^4 \dots), 29^k, c - 1 \rangle$ to obtain $\mathrm{PSp}(6, \mathbb{Z}/\langle 29^k \rangle)$ for any $k \in \mathbb{N}$ as factor group.

Proof: 1) This residue class ring is the field \mathbb{F}_{29} and the classical group recognition routine in Magma, cf. [BCP 97], [NiP 98], [Lee 01], immediately returns $\mathrm{Sp}(6, 29)$ for the specialization of our representation above.

2) For each of the specializations $c \mapsto i \in M$ onto \mathbb{F}_{29} one gets $\mathrm{PSp}(6, 29)$ as image as in 1). No two of these representations are conjugate under automorphisms of $\mathrm{PSp}(6, 29)$, since they all yield different traces for the element ab^2ab as given above.

3) For the specialization in 1) ab^2ab gets the order 871. In the representation modulo $\langle \zeta - 7, 29, (c - 1)^2 \rangle$ one gets a non-trivial image for $(ab^2ab)^{871}$. Since $\mathrm{Sp}(6, 29)$ acts irreducibly on its Lie algebra in characteristic 29, one obtains an epimorphism onto $\mathrm{PSp}(6, \mathbb{F}_{29}[x]/\langle x^2 \rangle)$. By general principles, cf. [KLP 97] Chapters III and V, one gets from taking commutators and using the irreducibility of the $\mathrm{Sp}(6, 29)$ -actions on the sections an epimorphism onto $\mathrm{PSp}(6, \mathbb{F}_{29}[x]/\langle x^k \rangle)$ for any k .

4) As in 3) except that no extra computation is needed since $\mathrm{PSp}(6, \mathbb{Z}/\langle 29^2 \rangle)$ does not split. The expansion is understood to converge to the 29-adic 7-th root of unity. q. e. d.

Of course, by doing some more calculations one now gets many more results. We just mention one, which we happen to notice. For the primes $p \in \{29, 547, 701\}$ one gets similarly as above $\epsilon(G_{2,3,7}, \mathrm{PSp}(6, p)) \geq (p + 1)/2$. The question arises for which other primes $p \equiv 1 \pmod{7}$ this is true. Of course, one also gets results for the primes which are not split in $\mathbb{Q}[\zeta]$ and a big variety of extension fields arises because the parameter c , respectively its minimal polynomial, can be arbitrarily specialized. The details have to be worked out along the lines of Section 4.

We now proceed to the two-dimensional family, which is more expensive from the point of view of computing time than the other examples treated in this paper. Taking the relations from (*) via $A^2 + I_6 = 0$ and characteristic polynomial of AB being the seventh cyclotomic polynomial, Janet's algorithm over $\mathbb{Q}[\zeta]$ yields a residue class ring of Krull dimension 2 of $\mathbb{Q}[\zeta][a_1, \dots, d_4]$. As a first consequence of this run, one can make the following linear substitutions:

$$(*_{eqn1}) \quad \begin{cases} d_4 = -a_3 - \zeta - \zeta^2 - \zeta^3 - \zeta^4 - \zeta^5, \\ d_3 = -c_2 - 1 - \zeta - \zeta^2, \\ c_4 = -a_2 - 1 - \zeta, \\ c_3 = -d_1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4. \end{cases}$$

After this one can make the following nonlinear substitutions:

$$(*_{eqn2}) \quad \begin{cases} d_1 = -a_3^2 + (1 + \zeta^6) a_3 - a_1 a_2 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 - a_1 \zeta - a_1, \\ c_1 = (c_2 a_1 + d_2 a_3) \zeta, \\ c_2 = (a_3 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5) a_1 - a_2^2 + (-\zeta - 1) a_2 - \zeta - 1 - \zeta^2. \end{cases}$$

Now a new run of Janet's algorithm yields the following relations for the remaining variables a_1, a_2, a_3, d_2 :

$$(*_{eqn3}) \quad \begin{cases} a_1^2 + a_2 a_3 + 1, \\ d_2 a_1 + ((1 - a_3) a_2 - 1 - \zeta^6) a_1 + a_2^3 + (\zeta + 1) a_2^2 + (\zeta^2 + 1 + \zeta) a_2 \\ - \zeta^6 a_3^2 + (-1 - \zeta^3 - \zeta - \zeta^4 - \zeta^2) a_3 + \zeta^3 + 1 + \zeta + \zeta^2, \\ (-1 - a_2 a_3) d_2 + (-a_3 + a_3^2) a_2^2 + (-1 + (\zeta^6 + 2) a_3) a_2 + 1 + \zeta^6 + \\ (a_2^3 + (\zeta + 1) a_2^2 + (\zeta^2 + 1 + \zeta) a_2 - \zeta^6 a_3^2 + (\zeta^5 + \zeta^6) a_3 - \zeta^4 - \zeta^5 - \zeta^6) a_1, \end{cases}$$

which describe an integral domain which is an integral extension of $K[a_3, d_2]$ with $K[a_3, d_2]$ -basis $(1, a_1, a_2, a_1 a_2, a_2^2, a_1 a_2^2)$. Hence, for any generic choice of the parameters a_3, d_2 one gets 6 solutions.

Of course, all the possibilities indicated for the previous representation can be imposed. However, it turns out that one can impose further relations on A, B and still gets solutions in characteristic zero. For the relations $(A^{-1}B^{-1}AB)^n = I_6$ and $(A^{-1}B^{-1}AB)^n = -I_6$ we list the K -dimensions $d^+(n)$ resp. $d^-(n)$ of the resulting residue class rings, which however were only computed in various positive characteristics like 701 and 7001, giving evidence that they should be valid in characteristic zero as well:

n	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$d^+(n)$	0	0	0	0	2	0	4	0	4	4	2	4	2	0	0	0
$d^-(n)$	2	0	2	2	0	0	0	0	2	0	0	0	0	0	2	0

Of course, $d^-(4) = d^+(8) = d^-(12) = d^+(16)$ yield $L_2(7)$ as factor group. All three, $d^-(6)$ together with one half of $d^+(12)$, and $d^-(7) = d^+(14)$, and $d^+(13)$ yield $L_2(13)$ as factor group. (Recall from Theorem 4.2, $\epsilon(G_{2,3,7}, L_2(13)) = 3$.)

The first interesting case that has a chance to yield an infinite group is $n = 10$. However, some of the specializations modulo 701 yield the second Janko group J_2 , which yields evidence that the group itself is already J_2 . A rigorous proof requires more work. (Lifting the representation to characteristic zero can best be done by computing the characteristic polynomial of the commutator in finite characteristic first, then deduce from that its characteristic polynomial in characteristic zero and turn its coefficients into relations to be added to $(*_{eqn3})$, because the matrix entries of $(A^{-1}B^{-1}AB)^n$ are too difficult to compute in characteristic zero directly. Of course, this method only works if the characteristic polynomial is multiplicity-free, which it is in the present case.) The second half of $d^+(12)$ also seems to yield J_2 . All of $d^+(15)$ seems to yield J_2 . This proves that $\epsilon(G_{2,3,7}, J_2) \geq 3$, but the desired phenomenon of producing an infinite group factor group of $G_{2,3,7}$ with an extra relation via a six-dimensional representation has to wait for a more thorough investigation. For degree 7 this occurs quite naturally, as the next section shows.

There is one other type of specialization, which can even be pursued in characteristic zero. The representation fixes a symplectic form which is unique up to multiples by certain factors in the field of fraction of the ground ring. Choosing a particular form to be zero, namely the one with entry $1 + \zeta^6 a_3$ in its Gram matrix in position (1, 2), leads to a specialization of the representation as follows:

$$\begin{aligned}
a_3 &= -\zeta, \\
a_2 &= \zeta^6(1 + a_1^2), \\
d_2 &= -\zeta^4 a_1^5 + (\zeta^2 + \zeta^3 + \zeta + 1 - 2\zeta^4) a_1^3 + (\zeta^3 + \zeta^4 + \zeta + \zeta^2 + \zeta^5) a_1^2 \\
&\quad + (2\zeta + \zeta^5 + 2 + 3\zeta^2 + 3\zeta^3) a_1
\end{aligned}$$

with a_1 as parameter. However, it turns out that this representation again fixes a symplectic form, which becomes degenerate only for finitely many values of a_1 , where of course the representation becomes reducible. In any case one only gets representations taking values in the symplectic group of degree 6. Note the trace of AB^2AB in this representation depends on a_1 :

$$-\zeta^4 a_1^5 + (-\zeta^5 - 3\zeta^4) a_1^3 + (-\zeta^6 - 2) a_1^2 + (1 + \zeta^2 - \zeta^5 + \zeta^3 - 2\zeta^4 + \zeta) a_1 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2$$

and hence this representation is also suitable for the purposes of Example 6.2.

7 Degree 7

In this section we construct one family of representations of $G_{2,3,7}$ which depends on two parameters and has rich group-theoretical consequences. The representations we want to consider belong to the generic case of Lemma 3.1 and are therefore of the form

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & a_1 & 0 \\ 1 & 0 & 0 & 0 & 0 & a_1 & 0 \\ 0 & 0 & 0 & 1 & 0 & a_2 & 0 \\ 0 & 0 & 1 & 0 & 0 & a_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & a_3 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & a_3 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & b_1 \\ 1 & 0 & 0 & 0 & 0 & 0 & b_2 \\ 0 & 1 & 0 & 0 & 0 & 0 & -b_1 - b_2 \\ 0 & 0 & 0 & 0 & 0 & 1 & b_3 \\ 0 & 0 & 0 & 1 & 0 & 0 & b_4 \\ 0 & 0 & 0 & 0 & 1 & 0 & -b_3 - b_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Instead of taking the entries of $(AB)^7 - I_7$ to be zero, we impose stronger relations by requiring that the characteristic polynomial of AB is $\lambda^7 - 1$. One gets the following consequences:

$$\begin{aligned} a_2 &= -b_3 - 1 + a_3 b_3 - b_4, \\ b_1 &= a_3 b_3 + 2 b_4 b_3 - b_4 a_3 b_3 + b_4^2 - a_3 b_3^2 - b_2 + b_3^2 + b_3, \\ a_1 &= -2 b_4 b_3 - b_4 + 3 b_4 a_3 b_3 - b_4^2 - b_3^2 - 2 b_3 + 2 a_3 b_3^2 + a_3 b_4^2 \\ &\quad - 1 + a_3^2 b_3 - b_4 a_3^2 b_3 - a_3^2 b_3^2 - b_2 a_3 + a_3 b_3, \end{aligned}$$

and, by running Janet's algorithm, one is left with the following presentation on the remaining four variables:

$$\begin{aligned} &-a_3 + a_3 b_4 + a_3 b_3 - b_4 - 1, \\ &b_3^3 + b_4 b_3^2 + b_3 b_4^2 + b_2 a_3 + b_3^2 + b_2 b_4 + b_4 b_3 + b_4^2 - b_3, \\ &a_3 b_4^3 - a_3^2 b_2 - b_4 b_2 a_3 - b_4 b_3^2 - 3 a_3 b_4^2 - b_4^3 - b_3^2 + 2 a_3 b_4 - 2 b_4 b_3 - a_3 - 2 b_3 - 1. \end{aligned}$$

They present an integral domain of Krull dimension 2 over K and can be embedded into $K(b_3, b_4)$ as follows:

$$\begin{aligned} a_3 &= \frac{1 + b_4}{-1 + b_4 + b_3}, \\ b_2 &= -\frac{(-1 + b_4 + b_3)(b_3 b_4^2 + b_4^2 + b_4 b_3 + b_4 b_3^2 + b_3^3 - b_3 + b_3^2)}{b_4 b_3 + b_4^2 + 1}. \end{aligned}$$

The representation (over $K(b_3, b_4)$) fixes a nondegenerate symmetric bilinear form and a skewsymmetric product, both unique up to multiples. This indicates that our representation maps into a certain form of the algebraic groups G_2 .

Clearly, the constructions from Example 6.2 can be carried over to the present situation, where $\mathrm{PSp}(6, q)$ has to be replaced by $G_2(q)$ for suitable q . However, what goes beyond

the projective six-dimensional case is the following. We can impose extra relations of the form $(AB^2AB)^n = 1$ to define non-trivial residue class rings of our ring above for certain n and still get infinite groups represented this way. The resulting representations are then over algebraic number fields so that one can take them modulo prime ideals in these number fields as long as they avoid the denominators coming up in the representations. Here is the story for some smaller numbers n we checked. Of course, the case $n = 11$ was dealt with in [HPS 97]. Naturally some finite groups show up such as $L_2(7)$ for $n = 4$ and multiples, $L_2(13)$ for $n = 6, 7, 13$ and multiples, and $L_2(8)$ for $n = 9$ and multiples.^{||} Here is a list of representations we obtained.

For $n = 10$, we find up to Galois conjugation exactly two representations. In both cases ρ satisfies $\rho^2 - \rho - 1 = 0$, i.e. $\rho = \zeta_5 + \zeta_5^{-1}$ for a primitive 5-th root of unity. For the first one the eigenvalues of AB^2AB are 1, two primitive 5-th roots of unity which are inverse to each other, and all primitive 10-th roots of unity. The representation takes values in a quadratic extension of $\mathbb{Q}[\rho] = \mathbb{Q}[\sqrt{5}]$ with defining equation $5 - 5b_4 - 3b_4^3 + 6b_4^2 + b_4^4$ over \mathbb{Q} , which is at the same time the minimal equation for b_4 over \mathbb{Q} and has Galois group D_8 .

$$\begin{aligned} b_3 &= -1 - \rho, \\ b_2 &= 2 - b_4 + \rho, \\ a_3 &= -\frac{4}{5}b_4 + \frac{1}{5} + \frac{1}{10}\rho + \frac{1}{10}b_4\rho, \\ 0 &= b_4^2 + 2 - b_4 - b_4\rho + \rho. \end{aligned}$$

For the second one the eigenvalues of AB^2AB are 1, and -1 with multiplicity 2, two primitive 5-th roots of unity which are inverse to each other, and their negatives. Again the field of definition is quadratic over $\mathbb{Q}[\sqrt{5}]$ and b_4 has $-\frac{395}{361} + \frac{48}{19}b_4^3 + \frac{2266}{361}b_4^2 + \frac{40}{361}b_4 + b_4^4$ as its minimal equation over \mathbb{Q} , the latter having D_8 as Galois group.

$$\begin{aligned} b_3 &= \frac{20}{19}\rho + \frac{14}{19}, \\ b_2 &= -\frac{35}{76}\rho - \frac{15}{76} - \frac{1}{4}b_4\rho - \frac{1}{4}b_4, \\ a_3 &= -\frac{17}{20} + \frac{6}{5}\rho + \frac{6}{5}b_4\rho - \frac{37}{20}b_4, \\ 0 &= b_4^2 + \left(\frac{20}{19}\rho + \frac{14}{19}\right)b_4 + \frac{577}{361} + \frac{1036}{361}\rho. \end{aligned}$$

The case $n = 11$ was already treated in [HPS 97] (in a slightly different setup). We add here that we found only one solution up to Galois conjugation. The field of definition is a quadratic extension of $\mathbb{Q}[\zeta_{11} + \zeta_{11}^{-1}]$.

The case $n = 12$ has many solutions. There are the solutions yielding $L_2(7)$ over \mathbb{Q} and $L_2(13)$ over $\mathbb{Q}[\sqrt[2]{13}]$, which we do not record here. The remaining solutions fall into three

^{||}The rational representation of $L_2(8)$ does not show up here. It seems that it must come up in the other case of Lemma 3.1.

classes under Galois conjugation. For the first one the eigenvalues of AB^2AB are 1, -1 with multiplicity 2, and all primitive 12-th roots of unity, so that one would expect \mathbb{Q} as field of definition. But it is quadratic, namely $\mathbb{Q}[\sqrt{-3}] = \mathbb{Q}[\zeta_3]$, where ζ_3 is a primitive third root of unity:

$$\begin{aligned} b_4 &= -1 - \frac{4}{5} \zeta_3, \\ b_3 &= \frac{6}{5}, \\ b_2 &= \frac{3}{5} + \frac{3}{5} \zeta_3, \\ a_3 &= 1 + \zeta_3. \end{aligned}$$

For the second one the eigenvalues of AB^2AB are 1, the primitive third and fourth roots of unity, and two primitive 12-th roots of unity which are inverse to each other. The field of definition is the 12-th cyclotomic number field $\mathbb{Q}[\zeta_{12}]$, where ζ_{12} is a primitive 12-th root of unity.

$$\begin{aligned} b_4 &= \zeta_{12} + \zeta_{12}^2, \\ b_3 &= -1 + \zeta_{12}^3 - 2\zeta_{12}, \\ b_2 &= -2\zeta_{12}^3 + 2\zeta_{12} - \zeta_{12}^2 + 2, \\ a_3 &= -\zeta_{12}^2. \end{aligned}$$

For the third class the eigenvalues of AB^2AB are 1, the primitive fourth and sixth roots of unity, and two primitive 12-th roots of unity which are inverse to each other, so that $\mathbb{Q}[\tau]$ with $\tau^2 = 3$ lies inside the field of definition. In fact, one needs again a quadratic extension of this field, where the minimal equation of b_4 over \mathbb{Q} is $-\frac{27}{121} - \frac{234}{121} b_4 + \frac{366}{121} b_4^2 + \frac{6}{11} b_4^3 + b_4^4$ with Galois group D_8 .

$$\begin{aligned} b_3 &= \frac{3}{11} - \frac{5}{11} \tau, \\ b_2 &= \frac{9}{22} + \frac{1}{2} b_4 \tau - \frac{3}{2} b_4 + \frac{7}{22} \tau, \\ a_3 &= -\frac{133}{314} \tau + \frac{1}{314} - \frac{133}{314} b_4 \tau - \frac{313}{314} b_4, \\ 0 &= b_4^2 + \left(\frac{3}{11} - \frac{5}{11} \tau \right) b_4 + \frac{216}{121} - \frac{129}{121} \tau. \end{aligned}$$

We do not record the results for $n > 12$ in detail. For instance, for $n = 13$ there are up to Galois conjugation two solutions. The first one has finite image $L_2(13)$ and the second one involves a quadratic extension of the maximal real subfield of the 13-th cyclotomic number field. Because $n = 17$ has no solution for the projective representation of degree 6, we tested $n = 17$ for the present representation and found solutions.

One word should be said about the rather heavy computations necessary to get these representations using Janet's algorithm. There are two implementations available to us, namely one in Maple and one in C++, also part of the Maple package [BCG 03]. At

present the C++-version, which is faster than the Maple version by a considerable factor, only deals with prime fields as coefficients. So the computations were first done modulo some prime $p \equiv 1 \pmod{7}$ so that we could use the fast C++-version. From the results we could compute the characteristic polynomials of AB^2AB and with these the computation could be performed in characteristic 0 usually over $\mathbb{Q}[\zeta_7]$ with the Maple version. Of course, there is always the slight chance of picking a bad prime, which then could occur in the denominator of the representation. To minimize the small risk of missing a representation in characteristic zero, we have repeated the calculation with other big primes. In doing so we found that the risk is even smaller than we originally thought, because a prime p in the denominator does not necessarily mean that one does not find the representation when working modulo p . The reason for this is that there is usually more than one prime ideal above p in the arising algebraic number field and typically only one is responsible for p to occur in the denominator. But anyhow, a rigorous completeness proof can either be performed by running through all possible minimal polynomials of AB^2AB or has to wait a fast C++-implementation of Janet's algorithm working over number fields.

References

- [BCG 03] Y. A. Blinkov, C. F. Cid, V. P. Gerdt, W. Plesken, D. Robertz. *The MAPLE Package "Janet": I. Polynomial Systems*. In *Proc. of Computer Algebra in Scientific Computing CASC 2003*, edited by V. G. Ganzha, E. W. Mayr, E. V. Vorozhtsov, 31–40. Garching, Germany: Institut für Informatik, TU München, 2003. Also available together with the package from WWW (<http://wwwb.math.rwth-aachen.de/Janet>).
- [BGY 01] Y. A. Blinkov, V. P. Gerdt, D. A. Yanovich. *Construction of Janet bases, II. Polynomial Bases*, in V. G. Ganzha, E. W. Mayr, E. V. Vorozhtsov (eds.). *Computer Algebra in Scientific Computing CASC 2001*. Springer, 2001, 249–263.
- [BCP 97] W. Bosma, J. J. Cannon, C. Playoust. *The Magma algebra system I: The user language*. *J. Symbolic Computation* **24** (1997), 235–265 (<http://magma.maths.usyd.edu.au/magma/MagmaInfo.html>).
- [Coh 81] J. Cohen. *On non-Hurwitz groups and noncongruence subgroups of the modular group*. *Glasgow Math. J.* **22** (1981), no. 1, 1–7.
- [DTZ 00] L. Di Martino, M. C. Tamburini, A. E. Zalesskii. *On Hurwitz groups of low rank*. *Comm. Algebra* **28** (2000), no. 11, 5383–5404.
- [HoP 89] D. F. Holt, W. Plesken. *Perfect Groups*. Oxford University Press, 1989.
- [HPS 97] D. F. Holt, W. Plesken, B. Souvignier. *Constructing a Representation of the Group (2, 3, 7, 11)*. *J. Symbolic Computation* **24** (1997), 489–492.
- [Jan 29] M. Janet, *Leçons sur les systèmes des équationes aux dérivées partielles*. Cahiers Scientifiques IV, Gauthiers-Villars, Paris, 1929.

- [KLP 97] G. Klaas, C. R. Leedham-Green, W. Plesken. *Linear pro- p -groups of finite width*. Lecture Notes in Mathematics 1674. Berlin: Springer (1997).
- [Lee 01] C. R. Leedham-Green. *The computational matrix group project*, in W. M. Kantor et al. (ed.), *Groups and computation III. Proceedings of the international conference at the Ohio State University, Columbus, OH, USA, June 15-19, 1999*. Berlin: Walter de Gruyter. Ohio State Univ. Math. Res. Inst. Publ. 8, 229–247 (2001).
- [LuM 85] A. Lubotzky, A. R. Magid. *Varieties of representations of finitely generated groups*. Mem. Amer. Math. Soc. 58 (1985), no. 336.
- [Mac 69] A. M. Macbeath. *Generators of linear fractional groups*. Proceedings of Symposia in Pure Mathematics (AMS) **12** (1969), 14–32.
- [Mac 99] A. M. Macbeath. *Hurwitz Groups and Surfaces*. in S. Levy (ed.) *The Eightfold Way*. Cambridge University Press 1999, 103–113.
- [Mal 90] G. Malle. *Hurwitz groups and $G_2(q)$* . Canad. Math. Bull. **33** (1990), no. 3, 349–357.
- [NiP 98] A. C. Niemeyer, C. E. Praeger. *A recognition algorithm for classical groups over finite fields*. Proc. London Math. Soc. (3) **77** (1998), no. 1, 117–169.
- [PIS 97] W. Plesken, B. Souvignier. *Analyzing finitely presented groups by constructing representations*. J. Symbolic Computation **24** (1997), 335–349.
- [PIR 05] W. Plesken, D. Robertz. *Janet’s approach to presentations and resolutions for polynomials and linear pdes*. Arch. Math. **84**:1 (2005), 22–37.
- [TaV 06] M. C. Tamburini, M. Vsemirnov. *Hurwitz groups and Hurwitz generation*. Handbook of Algebra, vol. 4, edited by M. Hazewinkel, Elsevier. Preprint: <http://www.dmf.unicatt.it/semmat/preprints/2003>.
- [TaV 05] M. C. Tamburini, M. Vsemirnov. *Irreducible $(2, 3, 7)$ -Subgroups of $\mathrm{PGL}_n(\mathbb{F})$, $n \leq 7$* . submitted to J. Algebra, July 2005. Preprint: <http://www.dmf.unicatt.it/semmat/preprints/2005>.
- [TaZ 04] M. C. Tamburini, A. E. Zalesski. *Classical groups in dimension 5 which are Hurwitz*. in: C. Y. Ho, P. Sin, P. H. Tiep and A. Turull (eds.). *Finite groups 2003. Proceedings of the conference held in Gainesville, FL, March 6–12, 2003*. Walter de Gruyter, Berlin, 2004, 363–371.
- [ViZ 05] R. Vincent, A. E. Zalesski. *Non-Hurwitz classical groups*. preprint (2005).
- [Vse 04] M. Vsemirnov. *Groups of $G_2(p)$, $p \geq 5$ as Quotients of $(2, 3, 7; 2p)$* to appear in Transformation Groups. Preprint: <http://www.pdmi.ras.ru/preprint/2004/04-17.html>.

Authors' addresses:

W. Plesken and D. Robertz
Lehrstuhl B für Mathematik
RWTH Aachen

Templergraben 64

52062 Aachen, Germany

e-mail: plesken@momo.math.rwth-aachen.de, daniel@momo.math.rwth-aachen.de