Analyzing finitely presented groups by constructing representations

W. Plesken       B. Souvignier

1 Introduction

One idea how to prove that a finitely presented group $G$ is infinite is to construct suitable homomorphisms into infinite matrix groups. In [HoP 92] this is done by starting with a finite image $H$ of $G$ and solving linear equations to check whether the epimorphism onto $H$ can be lifted to a representation whose image is an extension of a $\mathbb{Z}$-lattice by $H$, thus exhibiting an infinite abelian section of $G$ in case it exists near the top of the group.

The variation of the idea presented here seems to be suitable for instance for some groups where the kernel of the epimorphism onto $H$ has a pro-$p$-completion of bounded width. The price to be paid is that algebraic rather than linear equations have to be solved. These are obtained from evaluating the relations on matrices with indeterminates as entries. This system of equations can be simplified by applying some representation theory, but it often remains too complicated for direct methods e.g. Gröbner base calculations or elimination of variables by taking resultants.

An alternative to the direct methods is to find a modular solution and to lift it to a solution over a $p$-adic field. Knowing a finite epimorphic image $H$ of $G$, $H$ and its modular representation theory might give us a hint which modular representation of $H$ one should try to lift to a $p$-adic representation of $G$.

A multi-dimensional version of Hensel’s lemma often assures that it is sufficient to lift a solution only a few steps to conclude that it can be lifted to a solution over a $p$-adic field. Note, although the initial equations are algebraic, each step of the lifting process is just a problem of solving linear equations over a finite field.

In general it is not clear that the lifting process leads to entries which are algebraic over $\mathbb{Q}$ even in the situation where each lift is equivalent to a representation whose entries are algebraic over $\mathbb{Q}$. To get a representation defined over a number field $K$ (with degree $[K : \mathbb{Q}]$ as small as possible), therefore involves two steps: To pass from the lifted representation to one with $p$-adic entries which are algebraic over $\mathbb{Q}$ and to identify the new entries as algebraic numbers. In the examples of this paper the first step turned out to be superfluous, since the lifted representation had already entries with rational minimal polynomials of small degree, see however [HPS 94] for a more ill-behaved example. The second step is discussed in Section 5.

Sometimes the lift does not work in characteristic 0, however is possible in the ring $\mathbb{F}_p[[x]]$ of Laurent series over $\mathbb{F}_p$. An even simpler method than the one for number fields yields a representation over the field of rational functions over $\mathbb{F}_p$. In both
cases one obtains infinitely many finite images of \( G \) by reducing modulo prime ideals of \( K \) resp. \( \mathbb{F}_p[[x]] \). These images are often simple and thus the method often provides infinitely many simple factor groups by starting with a single one at the beginning of the computation.

We give some examples to illustrate our methods. The groups in Examples 3 and 5 were already treated in [Wes 85] whereas infiniteness of the groups in the Examples 1, 2 and 4 was open. In [HPS 94] a representation of the group \((2, 3, 7; 11)\) of degree 7 is constructed by the method developed here.

Most computations were performed in MAPLE. However, it is clear that more adjusted programs are highly desirable. What is needed are: polynomial arithmetic over algebraic number fields and finite fields including Gröbner bases and resultants, \( p \)-adic arithmetic, matrix arithmetic over these domains, furthermore LLL-reduction and Gaussian elimination for very large numbers and a program for computing maximal orders and class numbers of algebraic number fields.

We thank D. Holt for providing us with the examples, A. Cohen for sharing his experience with Gröbner bases and resultants for solving algebraic equations with us, and M. Pohst for pointing out the reference [dWe 89] to us.

## 2 The direct method

Throughout this paper let \( G \) be a finitely presented group with presentation

\[ G := \langle g_1, \ldots, g_n | w_1(g_1, \ldots, g_n)^{r_1}, \ldots, w_m(g_1, \ldots, g_n)^{r_m} \rangle. \]

We want to find a representation of \( G \) of some degree \( d \).

A naive approach would be to map the generators \( g_k \) on matrices \( \gamma_k := \{x_{ij}^{(k)}\} \) in indeterminates \( x_{ij}^{(k)} \) and to take the entries of \( w_i(\gamma_1, \ldots, \gamma_n)^{r_i} - I_d \) as equations. This leads to a system of \( m \cdot d^2 \) equations in \( n \cdot d^2 \) indeterminates with a possibly very high degree. It will almost never be possible to solve such a system of equations by direct methods, but examples are known in the literature where a qualitative analysis of the equations leads already to results on \( G \).

The following two remarks can often be used to obtain a simpler system of algebraic equations:

1) If the relators \( w_1, \ldots, w_t \) only involve the generators \( g_1, \ldots, g_s \) and this restricted presentation defines a finite subgroup \( U \) of \( G \), then a representation of \( G \) must restrict to a representation of \( U \). Therefore representation theory of finite groups gives explicit candidates for the images \( \gamma_1, \ldots, \gamma_s \) of \( g_1, \ldots, g_s \). This reduces the number of equations, their degrees and the number of indeterminates.

2) One has only finitely many possibilities for the characteristic polynomial of \( w_i(\gamma_1, \ldots, \gamma_n) \) and therefore can take the coefficients of the characteristic polynomials of these matrices as equations. This reduces the number of equations and often their degrees.
By these two remarks one obtains a system of \((m - t) \cdot d\) equations in \((n - s) \cdot d^2\) indeterminates. Clearly each equation which is linear in one of the indeterminates can be used to reduce both the numbers of equations and of indeterminates by one. Especially for low matrix degrees \(d\) such a system of algebraic equations can sometimes be solved by one of the following direct methods:

1) The resultant method

The classical method to solve a system of equations is to eliminate indeterminates by taking resultants and then solve the system by backward substitution as described in [GCL 92], Chapter 9. Choosing different paths of elimination, one often succeeds in obtaining some equations in only one indeterminate. Let \(f_1, \ldots, f_l\) be such equations in the same indeterminate. Then these equations can be replaced by their greatest common divisor \(f\). If \(f = 1\) no solution in characteristic 0 is possible. In this case some of the resultants \(r_{ij} := \text{res}(f_i, f_j)\) are non-zero integers and the prime divisors of the greatest common divisor \(R\) of the \(r_{ij}\) are the candidates for prime numbers, where a modular solution exists, since taking resultants works over \(\mathbb{Z}\). This method was already used in [HoP 92], Section 5, to find prime numbers \(p\) such that \(PSL_2(p)\) is an image of a finitely presented group.

2) The Gröbner base method

A second method is to compute a Gröbner basis (cf. [Buc 65]) for the ideal generated by the equations in the ring \(\mathbb{Z}[x_{ij}^{(k)}]\). There exists a solution in characteristic 0 if and only if the Gröbner basis does not collapse to \(1\), i.e. the ideal is not the whole ring. If the ideal is zero-dimensional (i.e. the residue class algebra is finite dimensional) one can choose a suitable basis for the residue class algebra and express the indeterminates in this basis by means of the unique normal form with respect to the Gröbner basis. If the ideal has a higher dimension one will usually first specialize indeterminates until the ideal becomes zero-dimensional. Namely, to prove infiniteness one does not need the most general solution, but one (for instance with algebraic entries) with an infinite image.

In practice it turned out to be fruitful to use a combination of these two methods. On the one hand one obtains by the Gröbner base method nice expressions for the entries if one uses the powers of a trace of some matrix as basis for the residue class algebra. On the other hand the resultant method often yields minimal polynomials for the entries of the matrices. Adding these to the equations makes it much easier to calculate a Gröbner basis.

The following two examples come from a family of presentations denoted by \((m, n, p; q)\) which is an abbreviation for \(\langle a, b | a^m, b^n, (ab)^p, [a, b]^q \rangle\).

**Example 1:** Let \(G = (3, 4, 8; 2)\), then the commutator subgroup \(G'\) has index 4 in \(G\) and a presentation \(\langle a, b, c, d | a^3, b^4, c^3, d^2, (a^{-1}d)^2, (b^{-1}a)^2, (c^{-1}b)^2, (d^{-1}c)^2, (abcd)^2 \rangle\).

We try to construct a projective representation of degree 2 of \(G'\), i.e. the images \(\alpha, \beta, \zeta, \delta\) of \(a, b, c, d\) satisfy the above relations only modulo scalar matrices. Since
$G'$ is perfect, one ought to assume that $\alpha, \beta, \zeta, \delta$ have determinant equal to 1.

Clearly $\langle a, b|a^3, b^3, (b^{-1}a)^2 \rangle \cong \text{Alt}(4)$, thus we start by mapping $a$ on $a := \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ and $b$ on $b := \begin{pmatrix} -1 & -i \\ -i & 0 \end{pmatrix}$, where $i^2 = -1$. Let $\zeta := \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$ and $\delta := \begin{pmatrix} x_3 & x_4 \\ y_3 & y_4 \end{pmatrix}$ be the images of $c$ and $d$, then $tr(\zeta) = tr(\delta) = -1$ since $c$ and $d$ have order 3. Hence $y_2 = -1 - x_1$ and $y_1 = -1 - x_3$. Furthermore from $tr(\zeta^{-1}\beta) = tr(\alpha^{-1}\delta) = 0$ one gets $y_1 = i + ix_1 - x_2$ and $y_3 = 1 + x_3 + x_4$. Thus one obtains the following system of nonlinear equations in $x_1, x_2, x_3, x_4$: $f_1 : det(\zeta) - 1 = 0$, $f_2 : det(\delta) - 1 = 0$, $f_3 : tr(\delta^{-1}\zeta) = 0$, $f_4 : tr(\alpha\beta\zeta\delta) = 0$.

By the resultant method over $\mathbb{Q}[i] \cong \mathbb{Q}[x]/(x^2 + 1)$ one succeeds in finding quadratic relations $m_j = m_j(x_j)$ for each $x_j$, which as polynomials in $\mathbb{Q}[i][x_j]$ are irreducible. Ideally the Gröbner base method over $\mathbb{Q}[i]$ now yields that $\mathbb{Q}[i][x_1, x_2, x_3, x_4]/(f_1, f_2, f_3, f_4, m_1, m_2, m_3, m_4) \cong \mathbb{Q}[i][x]/(x^2 + ix + i)$. Since no $\mathbb{Q}[i]$-Gröbner base implementation is available to us, Gröbner base methods applied to $\mathbb{Q}[y, x_1, x_2, x_3, x_4]/(y^2 + 1, f_1, \ldots, m_4)$ yield $\mathbb{Q}[x]/(x^4 + x^2 + 2x + 1)$, where $f_j$ etc. is obtained from $f_j$ by replacing $i$ by $y$.

The entries of the matrices can be expressed as: $i = \theta^3 - \theta^2 + \theta + 1$, $x_1 = -\frac{1}{2}\theta^3 - 2\theta - \frac{1}{2}$, $x_2 = \frac{3}{2}\theta^3 - \frac{5}{2}\theta^2 + \frac{5}{2}\theta + 1$, $x_3 = 2\theta^3 - \frac{5}{2}\theta^2 + \frac{7}{2}\theta + \frac{5}{2}$, $x_4 = -\frac{3}{2}\theta^3 - 2\theta - \frac{7}{2}$.

The fractions can be eliminated by conjugating the representation with the matrix

$$\begin{pmatrix}
1 + \theta^3 & -\theta + \theta^2 - \theta^3 \\
0 & 2
\end{pmatrix},$$

which gives the following representation over $\mathbb{Z}[\theta]$:

$$a \mapsto \begin{pmatrix}
2\theta - \theta^2 & -1 + 2\theta + \theta^2 - \theta^3 \\
1 - \theta + \theta^2 & 1 - 2\theta + 2\theta^2 - \theta^3
\end{pmatrix},

b \mapsto \begin{pmatrix}
-3 - \theta - \theta^3 & -2\theta + \theta^2 - \theta^3 \\
-3 + 3\theta + 2\theta^2 - 2\theta^3 & 2\theta + \theta^3
\end{pmatrix},

c \mapsto \begin{pmatrix}
-1 - 4\theta + 2\theta^2 - 2\theta^3 \\
3 + \theta^2
\end{pmatrix},

d \mapsto \begin{pmatrix}
6 + 7\theta - 3\theta^2 + 5\theta^3 & -9 - 5\theta + 2\theta^2 - 5\theta^3 \\
2 + 5\theta - 2\theta^2 + 3\theta^3 & 7 - 7\theta + 3\theta^2 + 5\theta^3
\end{pmatrix}.

Example 2: Let $G = (3, 4, 14; 2)$, then the commutator subgroup $G'$ has index 2 in $G$ and a presentation $\langle a, b, c|a^3, b^3, c^2, (a^{-1}b), (a^{-1}b) \rangle$. Again we try to construct a projective representation of degree 2.
As in the above example we map $a$ on $\alpha := \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ and $b$ on $\beta := \begin{pmatrix} -1 & -i \\ -i & 0 \end{pmatrix}$, where $i^2 = -1$. Let $\zeta := \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$ be the image of $c$, then $\text{tr}(\zeta) = 0$, hence $y_2 = -x_1$ and $\text{tr}(\alpha \beta \zeta) = \xi_7 + \xi_7^{-1}$ where $\xi_7$ is a primitive 7th root of unity. One thus ends up with only two equations: $f_1 : \det(\zeta) = 1$ and $f_2 : \text{tr}(\alpha^{-1} \beta \zeta) = 0$.

By the resultant method over $\mathbb{Q}[i, \xi_7 + \xi_7^{-1}]$ one obtains relations $m_1, m_2$ of degree 4 for $x_1, x_2$. With Gröbner base methods one computes that the residue class algebra $\mathbb{Q}[i, \xi_7 + \xi_7^{-1}] / (f_1, f_2, m_1, m_2)$ is isomorphic to the field $\mathbb{Q}[i][x] / (m_0)$, where $m_0 := x^{12} - x^{11} - 6x^{10} + 7x^9 + 15x^8 - 18x^7 - 21x^6 + 18x^5 + 15x^4 - 7x^3 - 6x^2 + x + 1$ is the minimal polynomial of $\theta = tr(\alpha \zeta)$. The field $\mathbb{Q}[\theta]$ has a non-abelian Galois group of order $1536 = 2^9 \cdot 3$, discriminant $78 \cdot 13^4 \cdot 41$, classnumber 1, 4 real and 4 pairs of complex embeddings into $\mathbb{C}$ and maximal order $\mathbb{Z}[\theta]$. With respect to $\theta$ and $i$ one obtains:

$$\xi_7 + \xi_7^{-1} = 4\theta^{11} - 2\theta^{10} - 24\theta^9 + 15\theta^8 + 62\theta^7 - 35\theta^6 - 88\theta^5 + 14\theta^4 + 48\theta^3 + 8\theta^2 - 9\theta - 4,$$

$$x_1 = \frac{1}{3}((1 + 9i)\theta^{11} - (1 + 5i)\theta^{10} - (6 + 5i)\theta^9 + (7 + 3i)\theta^8 + (15 + 139i)\theta^7 - (18 + 88i)\theta^6 - (21 + 157i)\theta^5 + (18 + 4i)\theta^4 + (15 + 111i)\theta^3 + (-7 + 9i)\theta^2 - (5 + 239i)\theta + 1 - 7i),$$

$$x_2 = \frac{1}{12}(-5 + 3i)\theta^{11} + (3 + i)\theta^{10} + (30 + 18i)\theta^9 - (22 + 8i)\theta^8 - (77 + 47i)\theta^7 + (53 + 17i)\theta^6 + (109 + 67i)\theta^5 - (32 + 4i)\theta^4 - (63 + 33i)\theta^3 - (1 + 15i)\theta^2 + (13 + 3i)\theta + 3 + 5i).$$

Since $\text{tr}(\alpha \zeta)$ generates $\mathbb{Q}[\theta]$, the matrix $\alpha \zeta$ has infinite order. By conjugating the representation with the matrix $\begin{pmatrix} 1+i & -1+i+\theta^7-i\theta^7 \\ 0 & 2 \end{pmatrix}$, one obtains a representation over $\mathbb{Z}[i, \theta]$. The enveloping algebra of this representation, i.e. the $\mathbb{Q}$-algebra generated by $\alpha, \beta, \zeta$ has dimension 4 over its centre $\mathbb{Q}[\theta]$, therefore it is a skewfield over $\mathbb{Q}[\theta]$ which is the character field of the representation.

>From the above representation one obtains homomorphisms into $PSL_2(p)$ e.g. for $p = 13, 197, 281, 293, 337, 349, 433, \ldots$.

## 3 The use of finite images

In this section we demonstrate how finite images $H$ of $G$ can be used as a guideline to construct a representation of $G$. Note, even for the direct methods described in Section 2 one has to choose a degree for the representation. In the insoluble case there are essentially two methods available to find finite images. The first one is described in [HoP 89], Section 7.1, cf. also [HoR 93] for a description of an implementation and further details. This method finds homomorphisms from a finitely presented group into a given permutation group and works very well for images of orders up to $10^6$. The second method is the resultant method described in Section 2, which is rather powerful especially to obtain images $PSL_2(q)$, since it more or less computes $q$ rather than tests for solutions.

To get an idea what sort of information is useful, assume $\Delta : G \to SL_n(F)$ is a homomorphism, where $\Delta(G)$ is infinite and $F$ is a global field, i.e. a finite extension of $\mathbb{Q}$ or of $E_p(x)$. Since $G$ is finitely generated, the image $\Delta(G)$ must lie in an
Instead of taking the universal pro-\(p\) completion \(\lambda\) and maybe the type of the Lie algebra of the algebraic group, or if \(\text{char}(F) = 0\), Tschebotaròw’s density theorem (cf. [Tsc 26]) tells us that \(\varphi\) can be chosen such that \(R/\varphi \cong \mathbb{F}_p\) for some prime number \(p\). In any case let \(p = \text{char}(R/\varphi)\). Then the kernel \(K\) of \(\Delta_\varphi\) maps under \(\Delta\) into the congruence subgroup \(\{\gamma \in SL_n(R)\mid \gamma - I_n \equiv 0 \mod \varphi\}\) of \(SL_n(R)\) and therefore one expects \(X := \Delta(K)\) and hence also \(K\) to have a substantial pro-\(p\)-completion \(\overline{X} := \varinjlim X/\lambda^i(X)\) resp. \(\overline{K} := \varprojlim K/\lambda^i(K)\), where \((\lambda^i(\Gamma))\) denotes the lower \(p\)-central series of \(\Gamma\) defined by \(\lambda^1(\Gamma) := \Gamma\) and \(\lambda^{i+1}(\Gamma) := [\lambda^i(\Gamma), \Gamma]\lambda^i(\Gamma)^p\).

Instead of taking the universal pro-\(p\)-completion \(\overline{X}\) of \(X\) one can also look at the \(\varphi\)-adic completion \(X_\varphi\) of \(X \subseteq SL_n(R)\) or even of \(\Delta(G)\) itself in \(SL_n(R_\varphi)\), where \(R_\varphi := \varprojlim R/\varphi^i\). This will also be a compact pro-\(p\)-group, namely a (continuous) image of \(\overline{X}\). No matter whether or not \(X_\varphi, \overline{X}\) and \(\overline{K}\) are isomorphic it is reasonable to assume that \(X_\varphi\) is of finite index in a maximal compact subgroup of the group of \(F_\varphi\)-rational points of some reductive group defined over the field of fractions \(F_\varphi\) of \(R_\varphi\). Note, the reductive groups over local fields are classified in characteristic 0 in [Kne 65] and [Sat 71], for characteristic 0 and \(p > 0\) in [BrT 72] and [Tit 79], where also their maximal compact subgroups are investigated. For guessing a good candidate for the reductive group and the field \(K_\varphi\) it is very helpful not only to have the finite image \(H\) (assumed to be isomorphic to \(\Delta_\varphi(G)\) or at least to \(\Delta_\varphi(G)/O_p(\Delta_\varphi(G))\)), but also a power commutator presentation of \(K/\lambda^i(K)\) for some \(i\) (particularly if \(X_\varphi, \overline{X}\) and \(\overline{K}\) are isomorphic). For instance if the sequence \(\vert \lambda^i(K)/\lambda^{i+1}(K)\vert = p^i\) is bounded and becomes periodic one can guess the dimension and maybe the type of the Lie algebra of the algebraic group, or if \(\overline{K}\) is powerful, the characteristic of \(F\) must be zero. But much more information such as ramification index etc. can be extracted. Having guessed the algebraic group one knows which is the smallest matrix degree to try.

We note that our assumptions open up new possibilities where the existing methods - e.g. looking for a free abelian section or applying refinements of the Golod-Šafarevič-bound (cf. e.g. [GaN 70]) - do not work.

The next example shows that this information alone might sometimes suffice to get the direct method started, though the finite factor group \(SL_2(7)\) one has at the beginning turns out to be a proper epimorphic image of \(\Delta_\varphi(G)\).

**Example 3:** The group \(G := \langle a, b, c | a^3, b^3, c^3, ababa^{-1}b^{-1}, bcceb^{-1}c^{-1}, cacac^{-1}a^{-1}\rangle\) was investigated in connection with buildings of type \(A_2\) in [Wes 85].

D. Holt checked that this group has a map onto \(SL_2(7)\) for which the kernel \(K\) has a lower 7-central series with a repeating sequence of layers \(7^2, 7^1, 7^2, 7^3\) at least down to class 16 and where \(\lambda^4(K)\) is powerful. Since \(2 + 1 + 2 + 3 = \text{dim}(A_2)\), this indicates that the group might have a Lie group structure of type \(A_2\), hence we try a representation of degree 3 in characteristic 0.

Clearly \(\langle a, b \rangle \cong \langle b, c \rangle \cong \langle c, a \rangle \cong \text{Frob}(21)\). Thus one may map \(a\) on the matrix...
\[ \alpha := \begin{pmatrix} \theta & -1 & -1 \\ 0 & 0 & 1 \\ -1 & 1 & -\theta \end{pmatrix} \text{ and } b \text{ on } \beta := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ \theta & -1 & -1 \end{pmatrix}, \text{ where } \theta^2 + \theta + 2 = 0, \text{ then } \langle \alpha, \beta \rangle \cong \text{Frob}(21). \]

\[ \zeta = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix} \]

be the image of \( c \). Since \( c \) has order 3 we must have \( tr(\zeta) = 0 \). In \( \langle a, c \rangle \) the element \( a^2 c \) has order 3, hence \( tr(a^2 \zeta) = 0 \) and the same argument for \( \langle b, c \rangle \) gives \( tr(b^2 \zeta) = 0 \). The elements \( bc \) and \( ca \) have order 7, hence \( tr(\beta \zeta) \) and \( tr(\zeta \alpha) \) are \( \theta \) or \( -1 - \theta \). Here one has to make a choice and we assume both traces to be \( \theta \). By each of these 5 linear equations one can eliminate one indeterminate and one finally comes up with a system of 6 non-linear equations in the indeterminates \( x_2, x_3, x_4, x_6 \).

Using the resultant method one obtains the solution \( \zeta = \begin{pmatrix} -1 - \theta & 1 - \frac{1}{2} \theta & - \theta \\ \frac{1}{2} \theta & 1 + \frac{1}{2} \theta & 1 \\ -1 & \frac{1}{2} \theta & 0 \end{pmatrix} \).

The denominators cannot be eliminated, since \( tr(\alpha \beta \zeta) = \frac{1}{2} (1 - \theta) \), which is not an algebraic integer in \( \mathbb{Q}[\theta] \). This proves as well that the image is infinite.

With respect to complex conjugation the above representation fixes the positive definite hermitian form \( F := \begin{pmatrix} 3 & \theta & \overline{\theta} \\ \theta & 3 & \theta \\ \overline{\theta} & \theta & 3 \end{pmatrix} \) of determinant 7.

\[ \phi \text{ from this representation one obtains epimorphisms onto } SL_3(p) \text{ for } p \equiv 1, 2, 4 \text{ mod } 7 \text{ and onto } SU_3(p) \text{ for } p \equiv 3, 5, 6 \text{ mod } 7. \]

For \( p = 7 \) one obtains the affine group \( \text{Aff}_2(7) \cong 7^2 > \text{SL}_2(7) \). This explains the strange pattern of the lower 7-central series of the kernel of \( G \to SL_3(7) \), which after all is the sort of pattern one would expect for a group coming close to the pro-\( p \)-Sylow subgroup of a parahoric subgroup of a unitary group (cf. [BrT 72], [Tit 79]).

It can happen that the image \( H \) of \( G \) is too large to obtain a presentation of the kernel (e.g. if the resultant method yields an image \( PSL_2(p) \) for a big prime number \( p \)). In this situation one can still try to obtain some more modest information from \( H \). The following lemma shows how to decide whether for an arbitrary epimorphic image \( H \) of \( G \) an epimorphism can be lifted to a split extension of a \( \mathbb{F}_p H \)-module by \( H \).

**Lemma 3.1** Let \( \phi \) be an epimorphism of \( G \) onto \( H \) and \( V \) a simple \( \mathbb{F}_p H \)-module. Then the maximum number \( a \) such that \( \phi \) can be lifted to an epimorphism onto the split extension \( V^a \cdot H \) is \( a = \dim(\text{Der}(G, V)) - \dim(\text{Der}(H, V)) \).

**Proof:** This follows from [Ple 87], Section 2. \( \blacksquare \)

**Remark 3.2** Let \( \phi \) be an epimorphism of \( G \) onto \( H \). If defining relations for \( H \) in terms of the \( \phi(g_i) \) are known the problem of calculating the dimensions of the spaces of derivations can be reduced to a linear problem over \( \mathbb{F}_p \) by using Fox-derivatives (cf. [HoP 89], Section 4.2).
For the rest of this section we assume that $G$ has a homomorphism $\varphi$ onto $PSL_2(p)$ for some prime $p$. That this is not too much a restriction follows from the following two observations:

1) "Most" simple groups are of this type (e.g. 50% of the groups of order less than $10^6$).

2) If $G$ has a 2-dimensional representation over any field of characteristic 0 then it follows from Tschebotaröw’s density theorem (cf. [Tsc 26]), that there are infinitely many primes $p$ such that $G$ maps into $PSL_2(p)$.

The next lemma gives a lower bound for the degree of the representation to construct in case the field is of characteristic $p$ or ramified over $\mathbb{F}_p$.

**Lemma 3.3** Assume that $V$ is a simple $\mathbb{F}_pPSL_2(p)$ module of dimension $d > 1$ such that $\varphi$ can be lifted to the split extension $V : PSL_2(p)$. Then this lift can not be realized in $PSL_k(\mathbb{F}_p[x]/x^2\mathbb{F}_p[x])$ for $k < (d+1)/2$.

**Proof:** Denote by $V_k$ the $k$-dimensional simple $\mathbb{F}_pSL_2(p)$ module and by $\Delta_k$ the corresponding representation of $SL_2(p)$. Then the module for the action of $\Delta_k(SL_2(p))$ on $(x\mathbb{F}_p[x]/x^2\mathbb{F}_p[x])^{k^2}$ is the tensor square of $V_k$, since $V_k$ is selfdual. But the largest simple composition factor of $V_k \otimes V_k$ is $2k-1$ as an easy calculation with Brauer characters shows.

We now want to decide whether an epimorphism lifts to a non-split extension $V.PSL_2(p)$ for a simple $\mathbb{F}_pPSL_2(p)$-module $V$.

**Lemma 3.4** Assume $p > 3$ and let $V_i$ be the simple $\mathbb{F}_pPSL_2(p)$-module of dimension $i$. Then

i) $H^2(PSL_2(p), V_i) = \{0\}$ if $i \neq 3$.

ii) $H^2(PSL_2(p), V_3) \cong \mathbb{F}_p$.

**Proof:** Let $V$ be any finite $\mathbb{F}_pPSL_2(p)$-module, $I(V)$ its injective hull and $\Omega^{-1}V$ the cokernel of $V \to I(V)$, i.e. the inverse of the Heller operator. Since $I(V)$ is projective, $\hat{H}^i(I(V)) = 0$, and therefore by the long exact sequence for Tate cohomology $\hat{H}^i(V) \cong \hat{H}^{i-1}(\Omega^{-1}V)$ (cf. [CuR 90] §8D). In particular $H^2(V) \cong \hat{H}^2(V) \cong \hat{H}^0(\Omega^{-2}V)$. One can easily read off $\Omega^{-2}V_i$ from the Brauer tree (cf. [Alp 86]):

$$
\bullet V_1 \bullet V_{p-2} \bullet V_3 \bullet V_{p-4} \cdots \bullet V_{(p+\varepsilon)/2}
$$

where $\varepsilon = \pm 1$ with $p \equiv \varepsilon$ mod 4 and the multiplicity of the exceptional vertex is 2. Clearly $H^2(V_1) = \{0\}$, since the Schur multiplier of $PSL_2(p)$ is isomorphic to $C_2$, $H^2(V_p) = \{0\}$, since $V_p$ is injective and $\hat{H}^0(\Omega^{-2}V_n) = \{0\}$ if $\Omega^{-2}V_n$ does not have $V_1$ in its socle. The only critical cases are the modules $V_{p-2}$ and $V_3$. In obvious notation giving the socle series one has: $\Omega^{-2}V_{p-2} = V_1 V_3 V_{p-2} V_3 V_{p-4}$ and $\Omega^{-2}V_3 = V_{p-2} V_3 V_{p-4} V_5$ for $p > 5$ resp. $\Omega^{-2}V_3 = V_1 V_3 V_3 V_1$ for $p = 5$. In
particular $\hat{H}^0(\Omega^{-2}_V) = \{0\}$ for $i \neq 3$ and $\hat{H}^0\Omega^{-2}_V \cong \mathbb{F}_q$, since in our situation $\hat{H}^0(\Omega^{-2}_V) \cong H^0(\Omega^{-2}_V)$.

**Lemma 3.5** For $p > 3$ an epimorphism $\varphi$ of $G$ onto $PSL_2(p)$ lifts to a non-split extension $V_3$. $PSL_2(p)$ if and only if the projective representation of $\varphi$ of $G$ can be lifted to a projective representation of $G$ onto $PSL_2(\mathbb{Z}_p/p^2\mathbb{Z}_p)$.

**Proof:** This follows immediately from the preceding lemma and Theorem 2.3.37 in [HoP 89] (cf. also [Wal 68]).

### 4 The lifting procedure

For this section we fix the following notation: let $R$ be a complete discrete valuation ring with maximal ideal $\varphi = \pi R$, residue class field $\mathbb{F}_q$ and field of fractions $K$, which is a finite extension of $\mathbb{Q}_p$ or $\mathbb{F}_q((x))$ with ramification index $e$ in the first case. Set $e = \infty$ in the second case.

We assume that we have a homomorphism $\varphi$ from $G$ into $PSL_k(\mathbb{F}_q)$. We want to lift $\varphi$ to a homomorphism of $G$ into $PSL_k(R)$ such that $\varphi$ is the composition of that homomorphism with the natural projection from $R$ to $R/\varphi$.

First we describe how $\varphi$ can be lifted (if such a lift is possible) to a homomorphism into $PSL_k(R/\varphi^c)$ for some finite $c > 1$ by solving linear equations over $\mathbb{F}_q$.

**Lemma 4.1** Let $f_1, \ldots, f_m \in R[X_1, \ldots, X_n]$ and assume that for $y = (y_1, \ldots, y_n) \in R^n$ one has $f_i(y) \equiv 0 \mod \varphi^d$ for $1 \leq i \leq m$. Let $z = (z_1, \ldots, z_n) \in R^n$ and define $e' := \min(d,e)$. Then the conditions $f_i(z) \equiv 0 \mod \varphi^{d+e'}$ for $1 \leq i \leq m$ and $z_j \equiv y_j \mod \varphi^d$ for $1 \leq j \leq n$ are equivalent to a certain $\mathbb{F}_q$-linear system of equations in $\pi^{-d}(z_j - y_j) \mod \varphi^{e'}$.

**Proof:** For $1 \leq j \leq n$ write $z_j = y_j + \pi^d r_j$ with $r_j \in R$. Expanding $f_i(z)$ around $y$ and omitting terms divisible by $\pi^{2d}$ yields $f_i(y) + \pi^d \sum_{j=1}^n l_{ij} r_j \equiv 0 \mod \varphi^{2d}$, where $l_{ij} \in R$. These are linear congruences for the $r_j$. Dividing by $\pi^d$ and reducing modulo $\varphi^{e'}$ gives $\sum_{j=1}^n l_{ij} r_j \equiv -\pi^{-d} f_i(y)$, which can be interpreted as $\mathbb{F}_q$-linear equations, since $R/\varphi^{e'}$ is an $\mathbb{F}_q$-algebra.

**Remark 4.2** (i) Obviously one has quadratic convergence for the characteristic $p > 0$ case. The same can be achieved in characteristic 0, if one is prepared to work in residue class rings of increasing size.

(ii) It pays, however, to lift by more than one step if possible, because not every lift from $R/\varphi^d$ to $R/\varphi^{d+1}$ can be lifted further to $R$, but it might be that for $h > 1$ for every lift from $R/\varphi^d$ to $R/\varphi^{d+h}$ the restriction to $R/\varphi^{d+1}$ can be lifted to $R$. This trick - an analogue of the famous "Echternacher Springprozession" - was already used by M. Wursthorn (cf. [Wur 93]) to calculate automorphisms of $p$-groups.

Concerning (non-)uniqueness of the lifting one should be aware of the following.

From one homomorphism $\varphi$ of $G$ into $PSL_k(R/\varphi^{d+1})$ one obtains further ones
by conjugating the image with matrices $\xi$ from $SL_k(R)$. If $\xi \equiv I_k \bmod \wp^d$ the homomorphisms $\varphi$ and $\xi \varphi \xi^{-1}$ agree modulo $\wp^d$ and can be viewed as lifting of the same homomorphism into $PSL_k(R/\wp^d)$. We give more precise details for the lifting from $R/\wp^d$ to $R/\wp^{d+1}$. Besides the homomorphism $\varphi_d : G \to PSL_k(R/\wp^d)$ one has $\gamma_1, \ldots, \gamma_s$ as images of $g_1, \ldots, g_s$ in $SL_k(R)$ in the notation of Section 2. Let $\mathcal{L}(\varphi_d)$ be the set of all homomorphisms $\varphi : G \to PSL_k(R/\wp^{d+1})$ with $g_i \varphi \equiv \gamma_i \bmod \wp^{d+1}$ for $i = 1, \ldots, s$ and $g_i \varphi \equiv g_i \varphi_d$ mod $\wp^d$ for $i = s+1, \ldots, n$ (ignoring the scalar matrices to be factored out). $\mathcal{L}(\varphi_d)$ can be viewed as an affine space over $R/\wp = \mathbb{F}_q$, because of the previous lemma. Let $C = \{X \in R^{k \times k} | X \gamma_i \equiv \gamma_i X \bmod \wp \text{ for } i = 1, \ldots, s\}$, and $C_0 := \{X \in C | X g_i \varphi_d \equiv g_i \varphi_d X \bmod \wp \text{ for } i = s+1, \ldots, n\}$. Note, both $C$ and $C_0$ only depend on $\varphi_d$ modulo $\wp$ (and are therefore constant throughout the computation). $C$ acts on $\mathcal{L}(\varphi_d)$ as follows: $c \in C$ maps $\varphi \in \mathcal{L}(\varphi_d)$ to $\varphi^{[c]}$, which is the composition of $\varphi$ with conjugation by $I_k + \pi^d c$. The crucial observation is

$$g_i \varphi^{[c]} \equiv g_i \varphi + \pi^d (c(g_i \varphi) - (g_i \varphi)c) \bmod \wp^{d+1} \text{ (and modulo scalar matrices).}$$

One easily verifies:

**Lemma 4.3** Let $C$ act on $\mathcal{L}(\varphi_d)$ as described above.

i) $C_0$ is the kernel of this action, more precisely each $C$-orbit on $\mathcal{L}(\varphi_d)$ is in bijection with the $\mathbb{F}_q$-vector space $C/C_0$.

ii) The $C$-action respects liftability (to $R/\wp^{d+2}$ or even to $R$).

Thus let $\alpha := \dim_{\mathbb{F}_q} C/C_0$ and let $\mathcal{L}^h(\varphi_d)$ be the set of all $\varphi \in \mathcal{L}(\varphi_d)$ which lift to a homomorphism into $PSL_k(R/\wp^{d+h})$. $\mathcal{L}^h(\varphi_d)$ is an affine subspace of $\mathcal{L}(\varphi_d) = \mathcal{L}^1(\varphi_d)$ for $h \leq d$. Denote its dimension by $\beta_h$. If $\alpha < \beta_1$ there is the danger that not everything lifts, i.e. $\mathcal{L}^h(\varphi_d) \neq \mathcal{L}(\varphi_d)$ for some $h > 1$. In this situation Remark 4.2(ii) should be taken seriously.

The following lemma is a multi-dimensional analogue of Hensel’s lemma. It gives an explicit value $d_0$ such that an epimorphism into $PSL_k(R/\wp^d)$ can be lifted to $PSL_k(R)$ for each $d > d_0$.

**Lemma 4.4** ([Bou 72], Chapter III, §4.6, Corollary 3)

Let $f_1, \ldots, f_m \in R[X_1, \ldots, X_n]$ where $n \geq m$. Denote by $M_f$ the Jacobian matrix $(\partial f_i/\partial X_j)$ and by $J_f^{(m)}(X_1, \ldots, X_n)$ the determinant of the last $m$ columns of $M_f$.

Let $y = (y_1, \ldots, y_n) \in R^n$ and assume that $f_i(y) \equiv 0 \bmod \wp^{i+2d}$ for $1 \leq i \leq m$, where $d$ is such that $\wp^d = J_f^{(m)}(y)R$. Then there exists $z = (z_1, \ldots, z_n) \in R^n$ such that $z_j \equiv y_j \bmod \wp^{i+2d}$ for $1 \leq j \leq n$ and $f_i(z) = 0$ for $1 \leq i \leq m$.

This lemma can be applied to a system of equations where the number of equations is not bigger than the number of indeterminates. But the reduction of the number of equations as outlined in Section 2 often suffices to fulfil this hypothesis. However, in all examples we have treated up to now, we could do in the end without this lemma, because we succeeded to pass from the representation modulo $\wp^c$ to a global representation as discussed in the next section.
5 From local to global representations

Since the entries of a representation of $G$ are solutions of a system of algebraic equations, one can usually arrange for a representation in characteristic 0 that it can be realized over some algebraic number field $K$. The required extension of $\mathcal{Q}$ can be determined from the $p$-adic expansion of the solutions by the following method (cf. [LLL 82], [dWe 89]):

**Lemma 5.1** Let $x = \sum_{i=0}^{\infty} a_i p^i$ be a $p$-adic number which is algebraic over $\mathcal{Q}$ and denote the $n$-th partial sum of $x$ by $x_n$. Define $L_{m,n} := \{ v = (v_0, v_1, \ldots, v_m) \in \mathbb{Z}^{m+1} | \sum_{i=0}^{m} v_i x_n^i \equiv 0 \mod p^{n+1} \}$ and let $L_m := \cap_{n=0}^{\infty} L_{m,n}$.

Then $|\mathcal{Q}[x] : \mathcal{Q}| = \min\{ m \in \mathbb{N} \mid L_m \neq \{0\} \}$.

**Proof:** Let $m_x = \sum_{i=0}^{d} c_i t^i$ be the minimal polynomial for $x$. Then clearly the vector $(c_0, \ldots, c_d, 0, \ldots, 0)$ lies in $L_m$ for all $m \geq d$. Suppose now $m < d$ and $v \in L_m$. Then for all $n \in \mathbb{N}$ one has $\sum_{i=0}^{m} v_i x_n^i \equiv 0 \mod p^{n+1}$, hence $\sum_{i=0}^{m} v_i x^i = 0$, which implies $v = 0$ since $m < d$.

The vector $v_x$ of coefficients of the minimal polynomial of $x$ can be calculated using the LLL-algorithm (cf. [LLL 82]) as follows:

The lattice $L_{m,n}$ has index $p^{n+1}$ in $\mathbb{Z}^{m+1}$ and a $\mathbb{Z}$-basis of $L_{m,n}$ is $(e_0, e_1, \ldots, e_m)$, where $e_0 = (p^{n+1}, 0, \ldots, 0)$ and $e_i = (-x_n^{i-1}, \ldots, 1, \ldots)$ with the 1 at position $i$. If $m = d$ the vector $v_x$ lies in $L_{m,n}$ for all $n$. Now for growing $n$ the Euclidean norms of the vectors in $L_{m,n}$ which are linearly independent from $v_x$ increase. Thus for $n$ sufficiently large $v_x$ can be found as a vector which is much shorter than all others by means of the LLL-algorithm. In our examples a faster pair-reduction applying usual Minkowski-reduction for dimension 2 to every pair of basis vectors yields already the desired shortest vector.

The above method can be used as well to express an algebraic number $y$ in terms of powers of $x$. For that one replaces the basis vector $e_m$ by $(-y, \ldots, 1)$. Then the LLL-algorithm yields the coefficients of a linear combination of $1, x, \ldots, x^{m-1}$ representing $y$.

**Example 4:** Let $G$ be given by $\langle a, b | a^3, b^3, bab^{-1}b^{-1}ab^{-1}ab^{-1}a^{-1} \rangle$. This group was on the one hand investigated by G. Rosenberger and L. Lévai in connection with generalized triangle groups and on the other hand by V. Metaftsis as a group with two generators of order 3 and one additional short relator. Its infiniteness was still open.

D. Holt checked that $G$ has a map onto $SL_2(5)$ for which the kernel has a lower 5-central series with a repeating sequence of layers $5^2, 5^1, 5^2, 5^3$ at least down to class 16. This indicates that the group is connected with a Lie group of type $A_2$. Furthermore the structure of the central series implies that some subgroup is powerful. Hence we try a representation of degree 3 in characteristic 0.

In this case the system of algebraic equations is too complicated for the direct methods. After fixing the image of $a$ and using the trace of $b$ there remain 8 indeterminates. The remaining 2 coefficients in the characteristic polynomial of $b$ give 2 nice
equations. If one uses the characteristic polynomial of the third relator one obtains 2 further equations with 222 resp. 5800 terms and degree 5 resp. 10. Alternatively one can use the entries of the third relator, then one gets 9 further equations with about 100 terms and degree 5.

Instead we look for primes $p$ such that $G$ maps onto $SL_3(p)$. Of course $G$ maps into $SL_3(5)$ with various homomorphisms factoring over $SL_2(5)$. Indeed the situation in the end turns out to be analogous to Example 3 at $p = 7$. It is more convenient to work with the prime 11, namely $G$ maps onto $SL_3(11)$ by $a \mapsto \alpha := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$

and $b \mapsto \beta_0 := \begin{pmatrix} 0 & 0 & 1 \\ -2 & 1 & 5 \\ -1 & 0 & -1 \end{pmatrix}$. This modular solution can be lifted to a solution $\beta$ over the ring $\mathbb{Z}_{11}$ of 11-adic integers. In each step of the lift one has 3 free parameters. Choosing the first row of $\beta$ as $(0, 0, 1)$ the lift becomes unique.

By the method described in Lemma 5.1 one now calculates that $\theta := tr(\alpha \beta \alpha)$ has minimal polynomial $m_\theta = x^6 - 3x^3 + 1$ and that the other entries of $\beta$ can be expressed in terms of $\theta$. The field $\mathcal{Q}[\theta]$ has Galois group $D_{12}$, classnumber 1, discriminant $3^6 \cdot 5^3$, 2 real and 2 pairs of complex embeddings into $\mathcal{C}$ and maximal order $\mathbb{Z}[\theta]$. The fact that $(\alpha \beta)^2 \neq 1$ and $tr((\alpha \beta)^2) = 3$ proves that the image is infinite. To write the representation over $\mathbb{Z}[\theta]$ one has to conjugate with a suitable matrix and finally obtains:

$$a \mapsto \begin{pmatrix} -3\theta^4+8\theta & -4\theta^4+11\theta & 2\theta^3.6 \\ 0 & 0 & 0 \\ -5\theta^5+14\theta^2 & -7\theta^5+19\theta^2 & 3\theta^4.8\theta \end{pmatrix}, b \mapsto \begin{pmatrix} -5\theta^5+14\theta^2 & -7\theta^5+19\theta^2 & 3\theta^4.8\theta \\ 3\theta^5.9\theta^2 & 5\theta^5-14\theta^2 & -2\theta^4+6\theta \\ 1 & 0 & 0 \end{pmatrix}.$$

Denote by $\theta$ the Galois automorphism of $\mathcal{Q}[\theta]$ that maps $\theta$ on $\theta^{-1} = -\theta^5 + 3\theta^2$.

With respect to this automorphism the above representation fixes the hermitian form

$$\begin{pmatrix} 4 & \theta^3.5 & \theta^2 \\ \theta^2.5 & 4 & \theta \\ \theta & \theta & 4 \end{pmatrix}$$

of determinant 5.

From this representation one obtains epimorphisms onto $SL_3(p)$ for $p = 11, 29, 41, 59, 71, 89, \ldots$ and onto $SU_3(p)$ for $p = 3, 7, 13, 37, 43, 47, 67, 73, 97, \ldots$ depending on the fact whether the polynomial $m_\theta$ has irreducible linear or quadratic factors over $\mathbb{F}_p$. For $p = 5$ one obtains the affine group $Aff\binom{2}{5} \cong 5^2 \rtimes SL_2(5)$.

In characteristic $p$ one will try to construct from a representation over $\mathbb{F}_p[[x]]$ one over the field of rational functions over $\mathbb{F}_p$. The following lemma, which was probably already known to Frobenius (cf. e.g. [Gan 59], Chapter XV, §10), gives an easy method for this.

**Lemma 5.2** There exists a bijection between periodic power series expansions in $\theta$ over $\mathbb{F}_p$ and rational functions over $\mathbb{F}_p$ not having a pole in $0$.

**Proof:** Let $r := \frac{f}{g}$ be a rational function in $x$, $gcd(f, g) = 1$, $p$ a prime such that $p|x(0)$. If $f$ is irreducible over $\mathbb{F}_p$ one has $f \mid x^{q-1} - 1$, where $q = deg(f)$. If $f = h^b$ where $h$ is irreducible and $b \in \mathbb{N}$ it follows for $q = deg(h)$ and $p^r \geq b$ that
f \mid x^{(q-1)p} - 1, \text{ since } (x^{q-1} - 1)^p = x^{(q-1)p} - 1 \text{ in characteristic } p. \text{ Finally assume } f_1, f_2 \in \mathbb{F}_p[x], a, b \in \mathbb{N} \text{ such that } gcd(f_1, f_2) = 1 \text{ and } f_1 \mid x^a - 1 \text{ and } f_2 \mid x^b - 1. \text{ Then } f_1 f_2 \mid x^{\text{lcm}(a,b)} - 1. \text{ Hence it follows by induction that } r \text{ can be written as } 1 + \frac{a}{1-x^n} \text{ for some } a \in \mathbb{N} \text{ and } h \in \mathbb{F}_p[x] \text{ which gives a periodic expansion of } r \text{ by means of the geometric series.}

The opposite direction follows immediately from the geometric series. The periodic expansion given by the coefficients \((a_0, a_1, \ldots, a_s, b_1, \ldots, b_n)\) with \(a_i, b_j \in \mathbb{F}_p\) is the power series expansion of the function \(r = \sum_{i=0}^{s} a_i x^i + x^{s+1} \frac{\sum_{j=1}^{n} b_j x^{j-1}}{1 - x^n}. \)

The following example was already studied in [Wes 85]. We want to show how a representation of this group can be obtained by our method of \(\wp\)-adic expansion.

**Example 5:** Let \(G := \langle a, b, c | a^3, b^3, c^3, aba^{-1}ba^{-1}b^{-1}, bcb^{-1}cb^{-1}c^{-1}, aca^{-1}ca^{-1}c^{-1} \rangle.\)

The commutator subgroup \(G'\) has index 3 in \(G\) and \(G''\) has index 72 in \(G'.\) Applying the nilpotent quotient algorithm for \(p = 2\) to \(G''\) gives a recurring sequence of layers \(2^6, 2^6, 2^4.\) This indicates a Lie group structure of type \(A_2 \times A_2.\) Furthermore a closer analysis of the central series shows that this Lie algebra must have characteristic 2.

We therefore try a representation of degree 3 over the field \(\mathbb{F}_2[[x]]\) of Laurent series over \(\mathbb{F}_2.\)

Clearly \(\langle a, b \rangle \cong \langle b, c \rangle \cong \langle c, a \rangle \cong \text{Frob}(21).\) Thus one may map \(a\) on the matrix \(\alpha := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}\) and \(b\) on \(\beta := \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},\) then \(\langle \alpha, \beta \rangle \cong \text{Frob}(21).\) Let \(\zeta := \begin{pmatrix} x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 \\ x_7 & x_8 & x_9 \end{pmatrix}\) be the image of \(c.\) Like in Example 3 one concludes that \(\text{tr}(\zeta) = \text{tr}(\alpha \zeta) = \text{tr}(\beta \zeta) = 0\) which gives the equations \(x_9 = x_1 + x_5, x_8 = x_5 + x_6\) and \(x_7 = x_2 + x_4 + x_5.\) A solution modulo the maximal ideal of \(\mathbb{F}_2[[x]]\) is \(\zeta_0 := \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.\)

This solution can be lifted to a solution \(\zeta\) in \(\text{SL}_3(\mathbb{F}_2[[x]]).\) Furthermore it turns out that this is possible in such a way that the entries of \(\zeta\) have periodic expansions. By the method described in Lemma 5.2 one now finds the following solution over the field of rational functions over \(\mathbb{F}_2:\) \(\zeta := u^{-1} \begin{pmatrix} 0 & u & u(1+x) \\ 1 & x^2 & 1+x^2 \\ x & 1 & x^2 \end{pmatrix},\) where \(u := 1 + x + x^2.\)

The matrix \(\alpha \beta \zeta\) has infinite order, since \(\text{tr}(\alpha \beta \zeta) = u^{-1}(1 + x)^3.\)

## 6 Bibliography


[HPS 94] D.F. Holt, W. Plesken, B. Souvignier, *Constructing a representation of the group (2,3,7;11)*. These proceedings


Lehrstuhl B für Mathematik
Rheinisch-Westfälische Technische Hochschule Aachen
Templergraben 64
D-52062 Aachen
Germany