New York Journal of Mathematics

New York J. Math. **17** (2011) 281–294.

Mild 2-relator pro-p-groups

Michael R. Bush, Jochen Gärtner, John Labute and Denis Vogel

Abstract. We give effective necessary and sufficient conditions for a quadratically defined 2-relator pro-p-group to be mild and apply these results to give examples of 2-extensions with restricted ramification over an imaginary quadratic base field for which the associated Galois group is a mild 2-relator pro-2-group.

Contents

1. Introduction 281
2. Computation of the holonomy algebra 282
3. The classification problem 283
4. Determining the mild orbits in the case $p = 2$, $d = 4$ 284
5. An algorithm for strong freeness 285
6. Examples of mild extensions 287
Appendix A. List of orbit representatives for the case $p = 2$, $d = 4$. 292
References 293

1. Introduction

Let G be a finitely presented pro-p-group and let $H^i(G) = H^i(G, \mathbb{Z}/p\mathbb{Z})$. Then $d = d(G) = \dim H^1(G)$ is the minimal number of generators of G and $r = r(G) = \dim H^2(G)$ is the minimal number of relators. Suppose that the cup product map

$$H^1(G) \otimes H^1(G) \longrightarrow H^2(G)$$

is surjective. In this case we say that G is *quadratically defined*. By duality, we get an injective mapping

$$\iota : H^2(G)^* \longrightarrow H^1(G)^* \otimes H^1(G)^*$$

Received November 20, 2010.

2000 *Mathematics Subject Classification.* 11R34, 20E15, 20E18, 12G10, 20F05, 20F14, 20F40.

Key words and phrases. Mild pro-p-groups, Galois groups, p-extensions, restricted ramification, Galois cohomology.

This research was partially supported by an NSERC Discovery Grant.

ISSN 1076-9803/2011

and hence an embedding of $W = H^2(G)^*$ into the tensor algebra $A = T(V)$ of $V = H^1(G)^*$ over $\mathbb{F}_p$. Let $B = A/(W)$, where (W) is the ideal of A generated by W. Then B is a finitely presented graded algebra over $\mathbb{F}_p$ with d generators and r quadratic relators; it is called the *holonomy algebra* of G. If $b_n = \dim B_n$, the n-th homogeneous component of B, the formal power series

$$B(t) = \sum_{n \geq 0} b_n t^n$$

is the Poincaré series of B. We have $B(t) \geq (1 - dt + rt^2)^{-1}$, cf. [1]. The pro-$p$-group G is called *mild* if the above inequality is an equality in which case the algebra B is also called mild. A basis of W is called *strongly free* if $B = A/(W)$ is mild.

Mild pro-p-groups have strong properties; for example, they are of cohomological dimension 2 and the Lie algebra associated to various central series of such groups can be computed, cf. [3], [5], [6].

Theorem 1. *A quadratically defined 2-relator pro-p-group is mild if $p \neq 2$.*

This is not the case when $p = 2$. However, we have the following result which gives an effective algorithm for determining the mildness of a quadratically defined pro-2-group.

Theorem 2. *A quadratically defined 2-relator pro-2-group is mild if and only if the codimension of the annihilator of $H^1(G)$ under the cup-product is > 2 and $\iota(H^2(G)^*)$ contains no nonzero square of an element of $T(H^1(G)^*)$.*

2. Computation of the holonomy algebra

Let $G = F/R = \langle x_1, \ldots, x_d \mid r_1, r_2 \rangle$ be a finitely presented pro-p-group with $r_1, r_2 \in F^p[F, F]$. Then $d(G) = d$. The completed $\mathbb{F}_p$-algebra of the free pro-p-group F can be identified with the algebra of noncommutative formal power series in $X_1, \ldots, X_d$ over $\mathbb{F}_p$. Under this identification, $x_i = 1 + X_i$. If $r \in R$ we have

$$r = \begin{cases} \displaystyle\prod_{i=1}^{d} x_i^{2c_{ii}} \prod_{i<j} [x_i, x_j]^{c_{ij}} \bmod F^4[F,F]^2[F,[F,F]] & \text{if } p = 2, \\ \displaystyle\prod_{i<j} [x_i, x_j]^{c_{ij}} \bmod F^p[F,[F,F]] & \text{if } p \neq 2, \end{cases}$$

so that

$$r = \begin{cases} \displaystyle\sum_{i=1}^{d} c_{ii} X_i^2 + \sum_{i<j} c_{ij}[X_i, X_j] \ \bmod \text{terms of degree} > 2 & \text{if } p = 2, \\ \displaystyle\sum_{i<j} c_{ij}[X_i, X_j] \ \bmod \text{terms of degree} > 2 & \text{if } p \neq 2. \end{cases}$$

Using the transpose of the inverse of the transgression isomorphism

$$\mathrm{tg} : H^1(R)^F = (R/R^p[R,F])^* \longrightarrow H^2(G),$$

the relator r defines a linear form ϕ_r on $H^2(G)$ such that, if $\chi_1, \dots, \chi_d$ is the basis of $H^1(F) = (F/F^p[F,F])^*$ with $\chi_i(x_j) = \delta_{ij}$, we have $\phi_r(\chi_i \cup \chi_j) = c_{ij}$ if $i \le j$, setting $c_{ii} = 0$ if $p \ne 2$; cf. [9], Prop. 3.9.13. If we identify x_i with its image in $V = F/F^p[F,F]$ the algebra $A = T(V)$ can be identified with the free associative algebra on $x_1, \dots, x_d$ over $\mathbb{F}_p$. Moreover,

$$\rho = \iota(\phi_r) = \begin{cases} \sum_{i=1}^{d} c_{ii}x_i^2 + \sum_{i<j} c_{ij}[x_i, x_j] & \text{if } p = 2, \\ \sum_{i<j} c_{ij}[x_i, x_j] & \text{if } p \ne 2, \end{cases}$$

which shows that ρ lies in $\wedge^2 V$ if $p \ne 2$. If $p = 2$ then ρ lies in $\mathrm{Sq}(V)$, the symmetric square of V, which is defined to be the subspace of $V \otimes V$ generated by elements of the form $x \otimes x$, $x \otimes y + y \otimes x$. Under our identification, $\wedge^2 V$ is the 2-component $\mathfrak{L}_2$ of the Lie subalgebra $\mathfrak{L}$ of A generated by $x_1, \dots, x_d$ and

$$\mathrm{Sq}(V) = \sum_{i=1}^{d} \mathbb{F}_2 x_i^2 + \mathfrak{L}_2$$

if $p = 2$. Let $c_{ji} = c_{ij}$ for $i < j$ if $p = 2$ and $c_{ji} = -c_{ij}$, $c_{ii} = 0$ if $p \ne 2$. Setting X to be the $1 \times d$ matrix $[x_1, \dots, x_d]$, we obtain a symmetric $d \times d$ matrix $C = [c_{ij}]$ such that $\rho = XCX^t$. This matrix is the matrix of the bilinear form b on $H^1(G)$ defined by $b(\chi, \psi) = \phi_r(\chi \cup \psi)$. The automorphism f of V defined by $X \mapsto XP$, where $P \in \mathrm{GL}_d(\mathbb{F}_2)$, extends to an automorphism $\hat{f}$ of A whose restriction to $\mathrm{Sq}(V)$ if $p = 2$ and to $\mathfrak{L}_2$ if $p \ne 2$ sends the element ρ to $\hat{f}(\rho) = XPCP^tX^t$.

Proposition 1. *Let ϕ_i be the linear form on $H^2(G)$ associated to r_i and let $\rho_i = \iota(\phi_i)$. Then G is quadratically defined and $r(G) = 2$ if and only if ρ_1, ρ_2 are linearly independent over $\mathbb{F}_p$, in which case, the holonomy algebra of G is $A/(\rho_1, \rho_2)$ which implies that G is mild if and only if the sequence ρ_1, ρ_2 is strongly free.*

3. The classification problem

Let $\mathcal{Q}$ be the set of graded $\mathbb{F}_p$-algebras of the form $A/(\rho_1, \rho_2)$ with ρ_1, ρ_2 linearly independent elements of $\mathrm{Sq}(V)$ if $p = 2$ and $\mathfrak{L}_2$ if $p \ne 2$. Two algebras $A/(\rho_1, \rho_2)$, $A/(\rho_1', \rho_2') \in \mathcal{Q}$ are isomorphic if and only if there is an automorphism f of V and $Q \in \mathrm{GL}_2(\mathbb{F}_p)$ such that

$$\begin{bmatrix} \rho_1' \\ \rho_2' \end{bmatrix} = Q \begin{bmatrix} \hat{f}(\rho_1) \\ \hat{f}(\rho_2) \end{bmatrix}.$$

The vector space $\mathfrak{L}_2$ has dimension $\binom{d}{2}$ with basis

$$\{x_{ij} = [x_i, x_j] \mid 1 \le i < j \le d\}$$

which we order lexicographically. If $p = 2$ the symmetric square $\mathrm{Sq}(V)$ has dimension $(d^2 + d)/2$ over $\mathbb{F}_2$ with explicit basis

$$x_1^2 < \cdots < x_d^2 < x_{12} < x_{13} < \cdots < x_{23} < x_{24} < \cdots < x_{d-1,d}.$$

Each relator ρ_i is determined by its coordinates $Y = [c_{i1}, \ldots, c_{is}] \in \mathbb{F}_p^s$ with respect to this basis; here $s = \binom{d}{2}$ if $p \neq 2$ and $s = (d^2 + 2)/2$ if $p = 2$. If $f(x_j) = \sum_{i=1}^d p_{ij} x_i$ then, in terms of these coordinates the automorphism $\hat{f}$ sends Y to $Y\hat{P}$, where $\hat{P} \in \mathrm{GL}_s(\mathbb{F}_p)$ is determined by

$$\hat{f}(x_{ij}) = \sum_{r<s} (p_{ri}p_{sj} + p_{si}p_{rj}) x_{rs}$$

$$\hat{f}(x_i^2) = \sum_{j=1}^d p_{ji}^2 x_j^2 + \sum_{r<s} p_{ri}p_{si}x_{rs} \quad \text{if} \quad p = 2.$$

Each algebra in $\mathcal{Q}$ is determined by specifying a $2 \times s$ matrix over $\mathbb{F}_p$. Determining the isomorphism classes of elements of $\mathcal{Q}$ reduces to determining the orbit space of $2 \times s$ matrices C over $\mathbb{F}_p$ under the action of $\Gamma = \mathrm{GL}_2(\mathbb{F}_p) \times \mathrm{GL}_d(\mathbb{F}_p)$ where, for $(Q, P) \in \mathrm{GL}_2(\mathbb{F}_p) \times \mathrm{GL}_d(\mathbb{F}_p)$,

$$(Q, P)C = QC\hat{P}^t.$$

In the case $p = 2$, $d = 4$ computations with symbolic algebra package Magma [8] yield the following result.

Theorem 3. *There are* 54 *orbits of* $\mathcal{Q}$ *under the action of* Γ. *The size of each orbit together with a representative is given in Appendix A.*

An orbit is called *mild* if it has a strongly free representative. If one representative is strongly free then so are all the others.

4. Determining the mild orbits in the case $p = 2$, $d = 4$

Theorem 4. *The orbits* 19, 20, 21, 49, 50, 51, 52, 53, 54 *are the only nonmild orbits when* $d = 4$, $p = 2$.

These orbits are nonmild since the 4-th term of their Poincaré series is either 49 or 50 instead of 48.

To prove strong freeness for all but one of the remaining orbits we use Anick's criterion which is developed in [1], §6. In order to state Anick's criterion we have to define the notion of a combinatorially free sequence. A sequence of nonidentity monomials $\alpha_1, \ldots, \alpha_d$ in $x_1, \ldots, x_d$ is said to be combinatorially free if:

(1) No monomial α_i is a submonomial of α_j for $i \neq j$.
(2) If $\alpha_i = u_1 v_1$, $\alpha_j = u_2 v_2$ is a proper factorization with u_i, v_i monomials then $u_1 \neq v_2$.

Let an ordering of $x_1, \ldots, x_d$ be given and order the monomials lexicographically. By the leading term of a homogeneous polynomial $w \in A$ we mean the largest monomial appearing in w (with a nonzero coefficient).

Proposition 2 (Anick's Criterion)**.** *A sequence $\rho_1, \ldots, \rho_m$ of homogeneous elements of A of degree > 0 is strongly free if the sequence of leading terms of these elements is combinatorially free.*

As an example consider orbit 5 which is represented by

$$\rho_1 = x_1^2 + [x_1, x_2], \rho_2 = [x_1, x_3].$$

The leading terms for the ordering $x_1 < x_2 < x_3 < x_4$ are x_2x_1, x_3x_1 which are combinatorially free. The remaining orbits, except for orbit 28 are handled in this way.

To handle orbit 28 we need a more powerful criterion for mildness that was obtained by Patrick Forré [3]. There he proves a result on how sequences in A can be modified in a certain way such that strongly free sequences remain strongly free by assigning different weights $e = (e_1, e_2, e_3, e_4)$ to the basis $X = (x_1, x_2, x_3, x_4)$. Dealing with different gradings (X, e) at the same time together with Anick's criterion, this gives an alternative proof of the cup product criterion for cohomological dimension 2 (especially for pro-2-groups, cf. [6], Th. 1.1).

Proposition 3 (Forré's Theorem)**.** *Let $w_1 + v_1, \ldots, w_r + v_r$ be a sequence of homogenous elements of A. Then this sequence is strongly free in A if there is a grading (X, e) such that:*

(a) *$w_1, \ldots, w_r$ is a strongly free sequence of e-homogeneous elements of A.*
(b) *For each e-homogeneous component u of v_j, we have*

$$\deg_e u > \deg_e(w_j).$$

Proof. For a proof we refer to [3], Cor. 3.8 and 3.10. □

Orbit 28 is represented by $\rho_1 = x_1^2 + [x_1, x_3], \rho_2 = x_2^2 + [x_1, x_2]$. For the (X, e)-grading with $e_1 = 2, e_2 = 3, e_3 = e_4 = 1$ the e-homogeneous terms of lowest degree of ρ_1, ρ_2 are $[x_1, x_3], [x_1, x_2]$ whose highest terms for the ordering $x_1 < x_2 < x_3 < x_4$ are x_3x_1, x_2x_1, a combinatorially free sequence.

5. An algorithm for strong freeness

Theorem 5. *The Γ-orbit of an algebra in $\mathcal{Q}$ contains a representative $B = A/(\rho_1, \rho_2)$ with ρ_1, ρ_2 in exactly one of the following forms with $L, L_1, L_2 \in \mathfrak{L}_2$, $L_1, L_2 \neq 0$:*

(I) $\rho_1, \rho_2 \in \mathfrak{L}_2,\ \rho_1, \rho_2 \neq 0,\ \rho_1 \neq \rho_2$.
(II) $\rho_1 = x_1^2 + L_1,\ \rho_2 = L_2$, *with* $L_1 \neq L_2$.
(III) $\rho_1 = x_1^2,\ \rho_2 \in \mathfrak{L}_2,\ \rho_2 \neq 0$.

(IV) $\rho_1 = x_1^2 + L_1,\ \rho_2 = x_2^2 + L_2$ *with* $L_1 + L_2 \neq 0,\ [x_1, x_2]$ *or* $L_1 = L_2 \neq [x_1, x_2]$.
(V) $\rho_1 = x_1^2 + [x_1, x_2],\ \rho_2 = x_2^2 + [x_1, x_2]$.
(VI) $\rho_1 = x_1^2,\ \rho_2 = x_2^2 + L$.

The orbit is mild if and only if it is of type (I), (II) *or* (IV).

Proof. Let $B : H^1(G) \to H^2(G)$ be the linear mapping defined by $B(\chi) = \chi \cup \chi$ and let $t = \text{codimKer}(B)$. Let s be the codimension of the annihilator of $H^1(G)$ under the cup-product. Note that $p \neq 2$ can only occur for type (I).

The representative ρ_1, ρ_2 is of type (I) if and only if $t = 0$ in which case $s \geq 3$. After a change of variables we can assume that the largest term of ρ_2 is $[x_k, x_d]$. Let $a[x_i, x_j]$ with $i < j$ be the largest term of ρ_1. After possibly subtracting from ρ_1 a scalar multiple of ρ_2 we may assume that $[x_i, x_j] \neq [x_k, x_d]$. To prove mildness we use Anick's criterion. If $j = d$ then the highest monomials in ρ_1, ρ_2 are $x_d x_i, x_d x_k$ which are combinatorially free. If $j < d$, $j \neq k$, the highest monomials are $x_j x_i, x_d x_k$ which are combinatorially free. If $j < d$, $j = k$ then, for the ordering of $x_1, \ldots, x_d$ in which $x_d < x_k$ are largest, the highest monomials are $x_k x_i, x_k x_d$ which are combinatorially free. Hence type (I) is mild.

We are in types (II) or (III) if and only if $t = 1$ in which case we may assume, without loss of generality, that $\rho_1 = x_1^2 + L_1$, $\rho_2 = L_2$ with $L_1, L_2 \in \mathfrak{L}_2$. If $L_1 = 0$ we are in type (III); if $L_1 = L_2$ then after subtracting ρ_2 from ρ_1 we fall in type (III). To show that type (III) is not mild let $\mathfrak{R}$ be the ideal of A generated by ρ_1, ρ_2 and let I be the augmentation ideal of A. Since $[x_1, \rho_1] = 0$ we see that $x_1 \rho_1 \equiv 0 \bmod \mathfrak{R}I$ and hence that $\mathfrak{R}/\mathfrak{R}I$ is not a free B-module on the images of ρ_1, ρ_2. This implies that ρ_1, ρ_2 are not strongly free, cf. [3]. If ρ_1, ρ_2 are of type (II) we prove mildness exactly as for type (I).

We are in type (IV), (V), or (VI) if and only if $t = 2$. Type (VI) is not-mild which is proven in the same way as for type (III). Type (V) is not mild since $[x_2, \rho_1] + [x_1, \rho_2] = 0$.

Now suppose that ρ_1, ρ_2 are of type (IV) with $L_1 = L_2 = L$. If we add ρ_2 to ρ_1 and replace x_1 by $x_1 + x_2$ we get $\rho_1 = x_1^2 + [x_1, x_2]$, $\rho_2 = x_2^2 + L'$ with $L' \neq [x_1, x_2]$. Hence, after a change of variables, we can assume that the largest term of L' is $[x_k, x_d]$ with $d > 2$. The highest monomials in ρ_2, ρ_2 are $x_2 x_1$, $x_d x_k$ which are combinatorially free if $k \neq 2$. If $k = 2$ we apply Forré's Theorem with $e_1 = 3$, $e_2 = 2$, $e_d = 1$, $e_h = 2$ for $h \neq 1, 2, d$. In this case the homogeneous components of lowest degree for ρ_1, ρ_2 are $[x_1, x_2]$, $[x_2, x_d]$ whose highest monomials for the ordering in which $x_1 < x_d < x_2$ are the combinatorially free monomials $x_2 x_1$, $x_2 x_d$.

Now suppose that ρ_1, ρ_2 are of type (IV) with $L_1 \neq L_2$, $L_1 + L_2 \neq [x_1, x_2]$. Without loss of generality, we can assume the largest term of ρ_2 is $[x_k, x_d]$ with $d > 2$. Let $[x_i, x_j]$ with $i < j$ be the largest term of ρ_1.

Suppose first that $[x_i, x_j] \neq [x_k, x_d]$. If $j = d$ or $j \neq d$, $k \neq j$ the highest monomials of ρ_1, ρ_2 are $x_j x_i$, $x_d x_k$ which are combinatorially free. If $j \neq d$ and $k = j \neq 2$ then, for the ordering in which the largest variables are $x_d < x_j$, the highest monomials are $x_k x_i$, $x_k x_d$ which are combinatorially free. If $j \neq d$, $k = j = 2$ then

$$\rho_1 = x_1^2 + [x_1, x_2],\ \rho_2 = x_2^2 + \sum_{h=2}^{d} a_h [x_1, x_h] + \sum_{h=3}^{d-1} b_h [x_2, x_h] + [x_2, x_d].$$

If we apply Forré's Theorem with $e_1 = 3$, $e_2 = 2$, $e_d = 1$, $e_h = 2$ for $h \neq 1, 2, d$, the homogeneous components of lowest degree for ρ_1, ρ_2 are $[x_1, x_2]$, $[x_2, x_d]$ whose highest monomials for the ordering in which $x_1 < x_d < x_2$ are the combinatorially free monomials $x_2 x_1$, $x_2 x_d$.

Now suppose that $[x_i, x_j] = [x_k, x_d]$. If $i = k > 2$ then, after adding ρ_2 to ρ_1 and replacing x_1 by $x_1 + x_2$, the largest term of ρ_1 is a nonzero element of $\mathfrak{L}_2$ which is not equal to $[x_k, x_d]$, the largest term of ρ_2. This reduces us to the previous case in which that ρ_1, ρ_2 were strongly free. Now suppose $i = k = 2$. We have

$$\rho_1 = x_1^2 + M_1 + [x_2, x_d],\ \rho_2 = x_2^2 + M_2 + [x_2, x_d].$$

Since $L_1 + L_2 \neq 0, [x_1, x_2]$ exactly one of M_1, M_2, say M_1, has a term $[x_1, x_h]$ or $[x_2, x_h]$ with $h \neq 1, 2, d$ which we can assume to be the latter if both appear. If we change the ordering by making x_h largest, the highest monomials are $x_h x_2$, $x_d x_2$ which are combinatorially free. In the same way we can prove that ρ_1, ρ_2 are combinatorially free if $i = k = 1$. □

Theorems 1 and 2 follow immediately from this result.

6. Examples of mild extensions

Let k be a totally imaginary number field and S a finite set of primes of k. The pro-2-group $G_S(2) = \mathrm{Gal}(k_S(2)/k)$, i.e. the Galois group of the maximal 2-extension of k unramified outside S, contains interesting information on the arithmetic of k. In the case where the set of primes S_2 of k above 2 is contained in S - the wild case - it has been known for a long time that $G_S(2)$ is of cohomological dimension less than or equal to 2, see [9].

In the tame case, where $S \cap S_2 = \varnothing$ and in the mixed case, where $\varnothing \subsetneq S \cap S_2 \subsetneq S_2$, only little had been known about the structure of $G_S(2)$ until recently. The results of [6] on mild pro-2-groups apply to an arithmetic result of Schmidt [10] which in turn yields a theorem that deals with all the above cases: For any given finite set S' of primes of k, there exists a finite set T of primes of k of odd norm such that for $S = S' \cup T$, the group $G_S(2)$ is of cohomological dimension 2. A natural question in this context is whether one can even prove the stronger property of mildness of $G_S(k)$ in some situations, in particular when we are given presentations that are

not of Koch-type. In the following, we will give some examples of mild pro-2-groups with 4 generators and 2 relators occuring as $G_S(2)$ for imaginary quadratic number fields, making use of our classification.

Finally we will also give an arithmetic example of a nonmild 4-generator 2-relator pro-2 group, which occurs as $G_S(2)$ over a cubic field. A good reference for a general discussion of the calculations we will carry out explicitly in our examples is section 11.4 of [4]. We will use the same notation and refer to this for more background and details.

Example 1. *Let* $k = \mathbb{Q}(\sqrt{-7})$, $S = \{\mathfrak{p}, \overline{\mathfrak{p}}, \mathfrak{q}\}$, *where* $\mathfrak{p} = \left(\frac{1+\sqrt{-7}}{2}\right)$ *and* $\overline{\mathfrak{p}} = \left(\frac{1-\sqrt{-7}}{2}\right)$ *are the primes of* k *above* 2 *and* $\mathfrak{q} = (2+\sqrt{-7})$ *is one of the primes of* k *above* 11. *Then* $G_S(2)$ *is a mild pro-2-group on* 4 *generators and* 2 *relators corresponding to orbit* 39 *in the list given in Appendix A.*

Proof. The ideal class group of k is trivial, and we have

$$V_\varnothing = \{\alpha \in k^\times \mid \alpha \in U_\mathfrak{l} k_\mathfrak{l}^{\times 2} \text{ for all primes } \mathfrak{l} \text{ of } k\}/k^{\times 2} \cong \{\pm 1\},$$

where $k_\mathfrak{l}$ denotes the completion of k at $\mathfrak{l}$ and $U_\mathfrak{l}$ denotes the unit group of $k_\mathfrak{l}$. Since -1 is not a square in $\mathbb{Q}_2 = k_\mathfrak{p}$, we have

$$V_S = \{\alpha \in k^\times \mid \alpha \in k_\mathfrak{l}^{\times 2} \text{ for } \mathfrak{l} \in S, \alpha \in U_\mathfrak{l} k_\mathfrak{l}^{\times 2} \text{ for } \mathfrak{l} \notin S\}/k^{\times 2} = 1.$$

Let U_S be the subgroup of the idele group I_k consisting of those ideles whose components for $\mathfrak{l} \in S$ are 1 and for $\mathfrak{l} \notin S$ are units. Then we have an exact sequence

$$0 \longrightarrow \{\pm 1\} \longrightarrow \prod_{\mathfrak{l} \in S} U_\mathfrak{l}/U_\mathfrak{l}^2 \longrightarrow I_k/(U_S I_k^2 k^\times) \longrightarrow 0$$

and an isomorphism

$$I_k/(U_S I_k^2 k^\times) \cong G_S(2)/G_S(2)_2.$$

In particular, the generator rank of $G_S(2)$ is given by

$$\dim_{\mathbb{F}_2} U_\mathfrak{p}/U_\mathfrak{p}^2 + \dim_{\mathbb{F}_2} U_{\overline{\mathfrak{p}}}/U_{\overline{\mathfrak{p}}}^2 + \dim_{\mathbb{F}_2} U_\mathfrak{q}/U_\mathfrak{q}^2 - 1 = 2 + 2 + 1 - 1 = 4.$$

We set $\alpha_{\mathfrak{p},1} = 5$, $\alpha_{\mathfrak{p},2} = -1$, $\alpha_{\overline{\mathfrak{p}},1} = 5$, $\alpha_{\overline{\mathfrak{p}},2} = -1$, $\alpha_\mathfrak{q} = -1$. Then $\{\alpha_{\mathfrak{p},1}, \alpha_{\mathfrak{p},2}\}$, $\{\alpha_{\overline{\mathfrak{p}},1}, \alpha_{\overline{\mathfrak{p}},2}\}$ and $\{\alpha_\mathfrak{q}\}$ are bases of $U_\mathfrak{p}/U_\mathfrak{p}^2$, $U_{\overline{\mathfrak{p}}}/U_{\overline{\mathfrak{p}}}^2$ and $U_\mathfrak{q}/U_\mathfrak{q}^2$, respectively. Let $\mathfrak{P}$ be fixed prime divisor of $\mathfrak{p}$ in k_S. Let $\tau_{\mathfrak{p},1}$ be an element of the inertia group of $\mathfrak{P}$ whose restriction to the maximal abelian subextension L/k of $k_S(2)/k$ equals $(\hat{\alpha}_{\mathfrak{p},1}, L/k)$, where $\hat{\alpha}_{\mathfrak{p},1}$ denotes the element of the idele group I_k of k whose $\mathfrak{p}$-component equals $\alpha_{\mathfrak{p},1}$ and all other components are equal to 1. In an analogous way we define $\tau_{\mathfrak{p},2}, \tau_{\overline{\mathfrak{p}},1}, \tau_{\overline{\mathfrak{p}},2}, \tau_\mathfrak{q}$. Then $\{\tau_{\mathfrak{p},1}, \tau_{\mathfrak{p},2}, \tau_{\overline{\mathfrak{p}},1}, \tau_{\overline{\mathfrak{p}},2}, \tau_\mathfrak{q}\}$ is a nonminimal set of generators of $G_S(2)$. We have to determine which one of the generators we can omit. In the group $I_k/(U_S I_k^2 k^\times)$ we have the identity

$$-1 \equiv \hat{\alpha}_{\mathfrak{p},2} \hat{\alpha}_{\overline{\mathfrak{p}},2} \hat{\alpha}_\mathfrak{q} \mod U_S I_k^2 k^\times,$$

and therefore

$$\tau_\mathfrak{q} \equiv \tau_{\mathfrak{p},2} \tau_{\overline{\mathfrak{p}},2} \mod G_S(2)_2.$$

So we can omit $\tau_{\mathfrak{q}}$, and $\{\tau_{\mathfrak{p},1}, \tau_{\mathfrak{p},2}, \tau_{\overline{\mathfrak{p}},1}, \tau_{\overline{\mathfrak{p}},2}\}$ is a minimal set of generators of $G_S(2)$. Now we have to deal with the relators. By [4], we have relators $r_{\mathfrak{p}}, r_{\overline{\mathfrak{p}}}, r_{\mathfrak{q}}$ (which we will determine shortly) of which we can omit any. We omit $r_{\mathfrak{q}}$, hence $G_S(2)$ has a minimal presentation (as pro-2-group)

$$G_S(2) = \langle \tau_{\mathfrak{p},1}, \tau_{\mathfrak{p},2}, \tau_{\overline{\mathfrak{p}},1}, \tau_{\overline{\mathfrak{p}},2} \mid r_{\mathfrak{p}} = r_{\overline{\mathfrak{p}}} = 1 \rangle.$$

We have yet to determine $r_{\mathfrak{p}}$ and $r_{\overline{\mathfrak{p}}}$. We set $\pi_{\mathfrak{p}} = \frac{1+\sqrt{-7}}{2}$ and $\pi_{\overline{\mathfrak{p}}} = \frac{1-\sqrt{-7}}{2}$. Let $\sigma_{\mathfrak{p}}$ be a lift of the Frobenius automorphism of $\mathfrak{P}$ (with respect to the maximal subextension of k_S/k in which $\mathfrak{P}$ is unramified) whose restriction to L/k is given by $(\hat{\pi}_{\mathfrak{p}}, L/k)$. In an analogous way, we define $\sigma_{\overline{\mathfrak{p}}}$. We calculate the following Hilbert symbols in $k_{\mathfrak{p}}$: $(\alpha_{\mathfrak{p},1}, \alpha_{\mathfrak{p},2}) = 1$, $(\alpha_{\mathfrak{p},1}, \pi_{\mathfrak{p}}) = -1$, $(\alpha_{\mathfrak{p},2}, \pi_{\mathfrak{p}}) = -1$. For the Hilbert symbols in $k_{\overline{\mathfrak{p}}}$ we obtain $(\alpha_{\overline{\mathfrak{p}},1}, \alpha_{\overline{\mathfrak{p}},2}) = 1$, $(\alpha_{\overline{\mathfrak{p}},1}, \pi_{\overline{\mathfrak{p}}}) = -1$, $(\alpha_{\overline{\mathfrak{p}},2}, \pi_{\overline{\mathfrak{p}}}) = -1$. This means that $r_{\mathfrak{p}}$ is given by

$$r_{\mathfrak{p}} = \sigma_{\mathfrak{p}}^2 \tau_{\mathfrak{p},2}^2 [\tau_{\mathfrak{p},1}, \sigma_{\mathfrak{p}}],$$

and the relator $r_{\overline{\mathfrak{p}}}$ is given by

$$r_{\overline{\mathfrak{p}}} = \sigma_{\overline{\mathfrak{p}}}^2 \tau_{\overline{\mathfrak{p}},2}^2 [\tau_{\overline{\mathfrak{p}},1}, \sigma_{\overline{\mathfrak{p}}}]$$

(note that there is a mistake in [4] concerning the signs of the Hilbert symbols, as a consequence the squares of Frobenius are missing there). Computations in Magma [8] show that

$$\hat{\pi}_{\mathfrak{p}} \equiv \hat{\alpha}_{\overline{\mathfrak{p}},1} \hat{\alpha}_{\overline{\mathfrak{p}},2} \mod U_S I_k^2 k^{\times},$$

and

$$\hat{\pi}_{\overline{\mathfrak{p}}} \equiv \hat{\alpha}_{\mathfrak{p},1} \hat{\alpha}_{\mathfrak{p},2} \hat{\alpha}_{\mathfrak{q}} \mod U_S I_k^2 k^{\times},$$

so

$$\sigma_{\mathfrak{p}} \equiv \tau_{\overline{\mathfrak{p}},1} \tau_{\overline{\mathfrak{p}},2} \mod G_S(2)_2,$$

and

$$\sigma_{\overline{\mathfrak{p}}} \equiv \tau_{\mathfrak{p},1} \tau_{\mathfrak{p},2} \tau_{\mathfrak{q}} \equiv \tau_{\mathfrak{p},1} \tau_{\mathfrak{p},2} \tau_{\mathfrak{p},2} \tau_{\overline{\mathfrak{p}},2} \equiv \tau_{\mathfrak{p},1} \tau_{\overline{\mathfrak{p}},2} \mod G_S(2)_2.$$

We obtain that

$$\begin{aligned} r_{\mathfrak{p}} &= \sigma_{\mathfrak{p}}^2 \tau_{\mathfrak{p},2}^2 [\tau_{\mathfrak{p},1}, \sigma_{\mathfrak{p}}] \equiv (\tau_{\overline{\mathfrak{p}},1} \tau_{\overline{\mathfrak{p}},2})^2 \tau_{\mathfrak{p},2}^2 [\tau_{\mathfrak{p},1}, \tau_{\overline{\mathfrak{p}},1} \tau_{\overline{\mathfrak{p}},2}] \\ &\equiv \tau_{\mathfrak{p},2}^2 \tau_{\overline{\mathfrak{p}},1}^2 \tau_{\overline{\mathfrak{p}},2}^2 [\tau_{\mathfrak{p},1}, \tau_{\overline{\mathfrak{p}},1}] [\tau_{\mathfrak{p},1}, \tau_{\overline{\mathfrak{p}},2}] [\tau_{\overline{\mathfrak{p}},1}, \tau_{\overline{\mathfrak{p}},2}] \mod G_S(2)_3 \end{aligned}$$

and

$$\begin{aligned} r_{\overline{\mathfrak{p}}} &= \sigma_{\overline{\mathfrak{p}}}^2 \tau_{\overline{\mathfrak{p}},2}^2 [\tau_{\overline{\mathfrak{p}},1}, \sigma_{\overline{\mathfrak{p}}}] \equiv (\tau_{\mathfrak{p},1} \tau_{\overline{\mathfrak{p}},2})^2 \tau_{\overline{\mathfrak{p}},2}^2 [\tau_{\overline{\mathfrak{p}},1}, \tau_{\mathfrak{p},1} \tau_{\overline{\mathfrak{p}},2}] \\ &\equiv \tau_{\mathfrak{p},1}^2 [\tau_{\mathfrak{p},1}, \tau_{\overline{\mathfrak{p}},1}] [\tau_{\mathfrak{p},1}, \tau_{\overline{\mathfrak{p}},2}] [\tau_{\overline{\mathfrak{p}},1}, \tau_{\overline{\mathfrak{p}},2}] \mod G_S(2)_3. \end{aligned}$$

Therefore, $G_S(2)$ has a presentation by generators x_1, x_2, x_3, x_4 and relators whose initial forms ρ_1, ρ_2 are given by

$$\begin{aligned} \rho_1 &= x_2^2 + x_3^2 + x_4^2 + [x_1, x_3] + [x_1, x_4] + [x_3, x_4], \\ \rho_2 &= x_1^2 + [x_1, x_3] + [x_1, x_4] + [x_3, x_4]. \end{aligned}$$

One can check that this presentation belongs to orbit 39 and hence is mild. In fact, applying the automorphism f given by $f(x_1) = x_2$, $f(x_2) = x_2 +$

x_4, $f(x_3) = x_1 + x_3 + x_4$, $f(x_4) = x_2 + x_3$, yields the representative given for orbit 39 in Appendix A. □

Example 2. *Let* $k = \mathbb{Q}(\sqrt{-7})$, $S = \{\mathfrak{p}, \overline{\mathfrak{p}}, \mathfrak{q}\}$, *where* $\mathfrak{p} = \left(\frac{1+\sqrt{-7}}{2}\right)$ *and* $\overline{\mathfrak{p}} = \left(\frac{1-\sqrt{-7}}{2}\right)$ *are the primes of* k *above* 2 *and* $\mathfrak{q}$ *is the unique prime of* k *above* 3. *Then* $G_S(2)$ *is a mild pro-2-group on* 4 *generators and* 2 *relators corresponding to orbit* 17.

Proof. We proceed in the same way as in Example 1, except that we set $\alpha_{\mathfrak{q}} = \zeta_8$ where ζ_8 denotes a primitive eighth root of unity in $k_{\mathfrak{q}}$. Then $\{\tau_{\mathfrak{p},1}, \tau_{\mathfrak{p},2}, \tau_{\overline{\mathfrak{p}},1}, \tau_{\overline{\mathfrak{p}},2}, \tau_{\mathfrak{q}}\}$ is a nonminimal set of generators of $G_S(2)$. In the group $I_k/(U_S I_k^2 k^\times)$ we have the identity

$$-1 \equiv \hat{\alpha}_{\mathfrak{p},2}\hat{\alpha}_{\overline{\mathfrak{p}},2} \mod U_S I_k^2 k^\times,$$

and therefore

$$\tau_{\mathfrak{p},2} \equiv \tau_{\overline{\mathfrak{p}},2} \mod G_S(2)_2.$$

So we can omit $\tau_{\overline{\mathfrak{p}},2}$, and $\{\tau_{\mathfrak{p},1}, \tau_{\mathfrak{p},2}, \tau_{\overline{\mathfrak{p}},1}, \tau_{\mathfrak{q}}\}$ is a minimal set of generators of $G_S(2)$. By [4], we have relators $r_{\mathfrak{p}}, r_{\overline{\mathfrak{p}}}, r_{\mathfrak{q}}$, and we can omit any of them. We choose to omit $r_{\overline{\mathfrak{p}}}$. We have yet to determine $r_{\mathfrak{p}}$ and $r_{\mathfrak{q}}$. We set $\pi_{\mathfrak{p}} = \frac{1+\sqrt{-7}}{2}$ and $\pi_{\mathfrak{q}} = 3$ and define $\sigma_{\mathfrak{p}}$ and $\sigma_{\mathfrak{q}}$ as in Example 1. The relator $r_{\mathfrak{p}}$ is given as in Example 1 by

$$r_{\mathfrak{p}} = \sigma_{\mathfrak{p}}^2 \tau_{\mathfrak{p},2}^2 [\tau_{\mathfrak{p},1}, \sigma_{\mathfrak{p}}].$$

The relator $r_{\mathfrak{q}}$ is given by

$$r_{\mathfrak{q}} = \tau_{\mathfrak{q}}^{N(\mathfrak{q})-1}[\tau_{\mathfrak{q}}, \sigma_{\mathfrak{q}}] = \tau_{\mathfrak{q}}^8[\tau_{\mathfrak{q}}, \sigma_{\mathfrak{q}}].$$

Using Magma [8] we obtain that

$$\hat{\pi}_{\mathfrak{p}} \equiv \hat{\alpha}_{\overline{\mathfrak{p}},1}\hat{\alpha}_{\overline{\mathfrak{p}},2}\hat{\alpha}_{\mathfrak{q}} \mod U_S I_k^2 k^\times,$$

and

$$\hat{\pi}_{\mathfrak{q}} \equiv \hat{\alpha}_{\mathfrak{p},1}\hat{\alpha}_{\mathfrak{p},2}\hat{\alpha}_{\overline{\mathfrak{p}},1}\hat{\alpha}_{\overline{\mathfrak{p}},2} \mod U_S I_k^2 k^\times.$$

Hence,

$$\sigma_{\mathfrak{p}} \equiv \tau_{\overline{\mathfrak{p}},1}\tau_{\overline{\mathfrak{p}},2}\tau_{\mathfrak{q}} \equiv \tau_{\mathfrak{p},2}\tau_{\overline{\mathfrak{p}},1}\tau_{\mathfrak{q}} \mod G_S(2)_2,$$

and

$$\sigma_{\mathfrak{q}} \equiv \tau_{\mathfrak{p},1}\tau_{\mathfrak{p},2}\tau_{\overline{\mathfrak{p}},1}\tau_{\overline{\mathfrak{p}},2} \equiv \tau_{\mathfrak{p},1}\tau_{\overline{\mathfrak{p}},1} \mod G_S(2)_2.$$

It follows that

$$\begin{aligned} r_{\mathfrak{p}} &= \sigma_{\mathfrak{p}}^2\tau_{\mathfrak{p},2}^2[\tau_{\mathfrak{p},1}, \sigma_{\mathfrak{p}}] \equiv (\tau_{\mathfrak{p},2}\tau_{\overline{\mathfrak{p}},1}\tau_{\mathfrak{q}})^2\tau_{\mathfrak{p},2}^2[\tau_{\mathfrak{p},1}, \tau_{\mathfrak{p},2}\tau_{\overline{\mathfrak{p}},1}\tau_{\mathfrak{q}}] \\ &\equiv \tau_{\overline{\mathfrak{p}},1}^2\tau_{\mathfrak{q}}^2[\tau_{\mathfrak{p},1}, \tau_{\mathfrak{p},2}][\tau_{\mathfrak{p},1}, \tau_{\overline{\mathfrak{p}},1}][\tau_{\mathfrak{p},1}, \tau_{\mathfrak{q}}][\tau_{\mathfrak{p},2}, \tau_{\overline{\mathfrak{p}},1}][\tau_{\mathfrak{p},2}, \tau_{\mathfrak{q}}][\tau_{\overline{\mathfrak{p}},1}, \tau_{\mathfrak{q}}] \mod G_S(2)_3 \end{aligned}$$

and

$$r_{\mathfrak{q}} = \tau_{\mathfrak{q}}^8[\tau_{\mathfrak{q}}, \sigma_{\mathfrak{q}}] \equiv [\tau_{\mathfrak{q}}, \tau_{\mathfrak{p},1}\tau_{\overline{\mathfrak{p}},1}] \equiv [\tau_{\mathfrak{q}}, \tau_{\mathfrak{p},1}][\tau_{\mathfrak{q}}, \tau_{\overline{\mathfrak{p}},1}] \mod G_S(2)_3.$$

Therefore, $G_S(2)$ has a presentation by generators x_1, x_2, x_3, x_4 and relators whose initial forms ρ_1, ρ_2 are given by

$$\rho_1 = x_3^2 + x_4^2 + [x_1, x_2] + [x_1, x_3] + [x_1, x_4] + [x_2, x_3] + [x_2, x_4] + [x_3, x_4],$$
$$\rho_2 = [x_1, x_4] + [x_3, x_4].$$

Applying Anick's criterion with $x_4 < x_3 < x_2 < x_1$, we see that $G_S(2)$ is mild. More precisely, applying the automorphism f given by $f(x_1) = x_1 + x_4,\ f(x_2) = x_1 + x_3,\ f(x_3) = x_1 + x_2 + x_4,\ f(x_4) = x_2 + x_4$ we obtain the representative for orbit 17 in Appendix A. □

Example 3. *Let $k = \mathbb{Q}(\sqrt[3]{3})$, $S = \{\mathfrak{p}, \overline{\mathfrak{p}}, \mathfrak{q}\}$, where $\mathfrak{q}$ denotes the real prime of k and $\mathfrak{p} = (\sqrt[3]{3} - 1)$ and $\overline{\mathfrak{p}} = (1 + \sqrt[3]{3} + \sqrt[3]{3}^2)$ are the primes of k above 2. Then $G_S(2)$ is pro-2-group on 4 generators and 2 relators corresponding to the nonmild orbit 54.*

Proof. First let us remark that since the field k is not totally imaginary and S contains the real prime of k, complex conjugation induces a nontrivial 2-torsion element in $G_S(2)$. In particular, it follows that $G_S(2)$ has infinite cohomological dimension and therefore cannot be mild. In the following we show that $d(G_S(2)) = 4,\ r(G_S(2)) = 2$ and in fact $G_S(2)$ belongs to orbit 54. Again k has trivial ideal class group, and it follows that a $\mathbb{F}_2$-basis for $V_\varnothing$ is given by the residue classes of $-1, -\varepsilon$ modulo $k^{\times 2}$, where $\varepsilon = 4 + 3\sqrt[3]{3} + 2\sqrt[3]{3}^2$ is a fundamental unit. Clearly $-1, -\varepsilon$ are not squares in $k_\mathfrak{q} = \mathbb{R}$ and furthermore ε is not a square in $k_\mathfrak{p} = \mathbb{Q}_2$. Hence it follows that $V_S = 1$. The primes $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ have inertia degrees 1 and 2 respectively and by chapter 11 of [4] it follows that $d(G_S(2)) = 4$, $r(G_S(2)) \leq 2$. We set

$$\alpha_{\mathfrak{p},1} := 5,\ \alpha_{\mathfrak{p},2} := -1,\ \alpha_{\overline{\mathfrak{p}},1} := 1 + 4\sqrt[3]{3},\ \alpha_{\overline{\mathfrak{p}},2} := -1,\ \alpha_{\overline{\mathfrak{p}},3} := \varepsilon,\ \alpha_\mathfrak{q} := -1.$$

Then the sets $\{\alpha_{\mathfrak{p},1}, \alpha_{\mathfrak{p},2}\}$, $\{\alpha_{\overline{\mathfrak{p}},1}, \alpha_{\overline{\mathfrak{p}},2}, \alpha_{\overline{\mathfrak{p}},3}\}$, $\{\alpha_\mathfrak{q}\}$ are bases of $U_\mathfrak{p}/U_\mathfrak{p}^2$, $U_{\overline{\mathfrak{p}}}/U_{\overline{\mathfrak{p}}}^2$ and $U_\mathfrak{q}/U_\mathfrak{q}^2$ respectively. As in the previous examples we may choose a corresponding nonminimal set of generators $\{\tau_{\mathfrak{p},1}, \tau_{\mathfrak{p},2}, \tau_{\overline{\mathfrak{p}},1}, \tau_{\overline{\mathfrak{p}},2}, \tau_{\overline{\mathfrak{p}},3}, \tau_\mathfrak{q}\}$ of $G_S(2)$. By class field theory the identities of ideles

$$\begin{aligned} -1 &\equiv \hat{\alpha}_{\mathfrak{p},2}\hat{\alpha}_{\overline{\mathfrak{p}},2}\hat{\alpha}_{\mathfrak{q},2} && \mod U_S I_k^2 k^\times, \\ \varepsilon &\equiv \hat{\alpha}_{\mathfrak{p},2}\hat{\alpha}_{\overline{\mathfrak{p}},3} && \mod U_S I_k^2 k^\times \end{aligned}$$

yield

$$\tau_{\mathfrak{p},2} \equiv \tau_{\overline{\mathfrak{p}},3} \equiv \tau_{\overline{\mathfrak{p}},2}\tau_\mathfrak{q} \mod G_S(2)_2$$

and hence $\{\tau_{\mathfrak{p},1}, \tau_{\overline{\mathfrak{p}},1}, \tau_{\overline{\mathfrak{p}},2}, \tau_\mathfrak{q}\}$ is a minimal set of generators of $G_S(2)$. By [4], we have relators $r_\mathfrak{p}, r_{\overline{\mathfrak{p}}}, r_\mathfrak{q}$, and we can omit any of them. We choose to omit $r_{\overline{\mathfrak{p}}}$. The relator $r_\mathfrak{q}$ belonging to the infinite prime is given by

$$r_\mathfrak{q} = \tau_\mathfrak{q}^2.$$

We set $\pi_\mathfrak{p} = \sqrt[3]{3} - 1$ and define $\sigma_\mathfrak{p}$ as in Example 1 and 2. We calculate the following Hilbert symbols in $k_\mathfrak{p}$: $(\alpha_{\mathfrak{p},1}, \alpha_{\mathfrak{p},2}) = 1$, $(\alpha_{\mathfrak{p},1}, \pi_\mathfrak{p}) = -1$, $(\alpha_{\mathfrak{p},2}, \pi_\mathfrak{p}) =$

1. Therefore $r_{\mathfrak{p}}$ is given by

$$r_{\mathfrak{p}} = \tau_{\mathfrak{p},2}^2[\tau_{\mathfrak{p},1}, \sigma_{\mathfrak{p}}] \equiv \tau_{\overline{\mathfrak{p}},2}^2 \tau_{\mathfrak{q}}^2[\tau_{\mathfrak{p},1}, \sigma_{\mathfrak{p}}][\tau_{\overline{\mathfrak{p}},2}, \tau_{\mathfrak{q}}] \mod G_S(2)_3.$$

Note that, contrary to the previous examples, the Hilbert symbol $(\alpha_{\mathfrak{p},2}, \pi_{\mathfrak{p}})$ being trivial implies that there is no square of the Frobenius.

Using Magma [8] we find that

$$\hat{\pi}_{\mathfrak{p}} \equiv \hat{\alpha}_{\overline{\mathfrak{p}},1} \mod U_S I_k^2 k^\times,$$

so

$$\sigma_{\mathfrak{p}} \equiv \tau_{\overline{\mathfrak{p}},1} \mod G_S(2)_2$$

and we obtain

$$r_{\mathfrak{p}} \equiv \tau_{\overline{\mathfrak{p}},2}^2 \tau_{\mathfrak{q}}^2[\tau_{\mathfrak{p},1}, \tau_{\overline{\mathfrak{p}},1}][\tau_{\overline{\mathfrak{p}},2}, \tau_{\mathfrak{q}}] \mod G_S(2)_3.$$

Therefore $G_S(2)$ admits a presentation by generators x_1, x_2, x_3, x_4 and two relators with initial forms ρ_1, ρ_2 given by

$$\rho_1 = x_3^2 + x_4^2 + [x_1, x_2] + [x_3, x_4],$$
$$\rho_2 = x_4^2.$$

By making the successive substitutions $x_1 \leftrightarrow x_4$, $x_2 \leftrightarrow x_3$, $x_2 \mapsto x_1 + x_2$ one checks that this presentation belongs to orbit 54. □

Appendix A. List of orbit representatives for the case $p = 2$, $d = 4$.

This is a list of orbit representatives followed by the size and type of the orbit for the case $p = 2$, $d = 4$.

(1) $[x_1, x_2]$, $[x_1, x_3]$, 630, (I)
(2) $[x_1, x_2], [x_3, x_4]$, 1680, (I)
(3) $[x_1, x_2]$, $[x_1, x_4] + [x_2, x_3]$, 1260, (I)
(4) $[x_1, x_2] + [x_3, x_4]$, $[x_1, x_3] + [x_2, x_4] + [x_3, x_4]$, 336, (I)
(5) $x_1^2 + [x_1, x_2]$, $[x_1, x_3]$, 1890, (II)
(6) $x_1^2 + [x_1, x_2]$, $[x_3, x_4]$, 10080, (II)
(7) $x_1^2 + [x_1, x_2]$, $[x_1, x_2] + [x_3, x_4]$, 10080, (II)
(8) $x_1^2 + [x_1, x_2]$, $[x_1, x_4] + [x_2, x_3]$, 7560, (II)
(9) $x_1^2 + [x_1, x_3]$, $[x_2, x_3]$, 7560, (II)
(10) $x_1^2 + [x_1, x_3] + [x_2, x_4]$, $[x_2, x_3]$, 15120, (II)
(11) $x_1^2 + [x_1, x_3] + [x_2, x_4]$, $[x_1, x_2] + [x_2, x_4] + [x_3, x_4]$, 15120, (II)
(12) $x_1^2 + [x_1, x_4] + [x_2, x_3]$, $[x_1, x_2]$, 3780, (II)
(13) $x_1^2 + [x_1, x_4] + [x_2, x_3]$, $[x_1, x_2] + [x_3, x_4]$, 181440, (II)
(14) $x_1^2 + [x_2, x_3]$, $[x_1, x_3]$, 3780, (II)
(15) $x_1^2 + [x_2, x_3]$, $[x_1, x_4]$, 10080, (II)
(16) $x_1^2 + [x_2, x_3]$, $[x_1, x_4] + [x_2, x_4]$, 30240, (II)
(17) $x_1^2 + [x_3, x_4]$, $[x_2, x_4]$, 15120, (II)
(18) $x_1^2 + [x_3, x_4], [x_1, x_2] + [x_1, x_4] + [x_2, x_3]$, 15120, (II)

(19) $x_1^2,\ [x_1,x_2]$, 630, (III)
(20) $x_1^2,\ [x_2,x_3]$, 2520, (III)
(21) $x_1^2,\ [x_1,x_4]+[x_2,x_3]$, 2520, (III)
(22) $x_1^2+[x_1,x_2],\ x_2^2+[x_1,x_3]$, 3780, (IV)
(23) $x_1^2+[x_1,x_2],\ x_2^2+[x_3,x_4]$, 10080, (IV)
(24) $x_1^2+[x_1,x_2],\ x_2^2+[x_1,x_2]+[x_3,x_4]$, 10080, (IV)
(25) $x_1^2+[x_1,x_2],\ x_2^2+[x_1,x_4]+[x_2,x_3]$, 7560, (IV)
(26) $x_1^2+[x_1,x_2]+[x_3,x_4],\ x_2^2+[x_1,x_3]+[x_2,x_4]+[x_3,x_4]$, 60480 (IV)
(27) $x_1^2+[x_1,x_2]+[x_2,x_3],\ x_2^2+[x_1,x_3]+[x_2,x_4]+[x_3,x_4]$, 60480, (IV)
(28) $x_1^2+[x_1,x_3],\ x_2^2+[x_1,x_2]$, 7560, (IV)
(29) $x_1^2+[x_1,x_3],\ x_2^2+[x_2,x_3]$, 2520, (IV)
(30) $x_1^2+[x_1,x_3],\ x_2^2+[x_2,x_4]$, 15120, (IV)
(31) $x_1^2+[x_1,x_3],\ x_2^2+[x_1,x_4]+[x_2,x_4]$, 30240, (IV)
(32) $x_1^2+[x_1,x_3]+[x_2,x_4],\ x_2^2+[x_1,x_3]+[x_1,x_4]+[x_2,x_3]$, 5040, (IV)
(33) $x_1^2+[x_1,x_3]+[x_3,x_4],\ x_2^2+[x_1,x_3]+[x_2,x_3]+[x_2,x_4]$, 120960, (IV)
(34) $x_1^2+[x_1,x_4],\ x_2^2+[x_3,x_4]$, 60480, (IV)
(35) $x_1^2+[x_1,x_4],\ x_2^2+[x_1,x_3]+[x_2,x_4]$, 15120, (IV)
(36) $x_1^2+[x_1,x_4],\ x_2^2+[x_2,x_3]+[x_3,x_4]$, 30240, (IV)
(37) $x_1^2+[x_1,x_4],\ x_2^2+[x_1,x_3]+[x_2,x_3]+[x_2,x_4]+[x_3,x_4]$, 30240, (IV)
(38) $x_1^2+[x_1,x_4]+[x_2,x_3],\ x_2^2+[x_1,x_3]+[x_2,x_3]+[x_2,x_4]$, 5040, (IV)
(39) $x_1^2+[x_1,x_4]+[x_2,x_4],\ x_2^2+[x_1,x_3]+[x_2,x_3]+[x_3,x_4]$, 60480, (IV)
(40) $x_1^2+[x_1,x_4]+[x_2,x_4],\ x_2^2+[x_1,x_3]+[x_1,x_4]+[x_2,x_3]$, 30240, (IV)
(41) $x_1^2+[x_2,x_3],\ x_2^2+[x_1,x_3]$, 7560, (IV)
(42) $x_1^2+[x_2,x_3],\ x_2^2+[x_1,x_3]+[x_2,x_3]$, 5040, (IV)
(43) $x_1^2+[x_2,x_3],\ x_2^2+[x_1,x_4]+[x_2,x_3]$, 30240, (IV)
(44) $x_1^2+[x_2,x_4],\ x_2^2+[x_1,x_3]$, 15120, (IV)
(45) $x_1^2+[x_2,x_4],\ x_2^2+[x_2,x_3]$, 15120, (IV)
(46) $x_1^2+[x_3,x_4],\ x_2^2+[x_1,x_4]$, 60480, (IV)
(47) $x_1^2+[x_3,x_4],\ x_2^2+[x_2,x_3]+[x_2,x_4]+[x_3,x_4]$, 60480, (IV)
(48) $x_1^2+[x_3,x_4],\ x_2^2+[x_1,x_2]+[x_1,x_4]+[x_2,x_3]+[x_2,x_4]+[x_3,x_4]$, 60480, (IV)
(49) $x_1^2+[x_1,x_2],\ x_2^2+[x_1,x_2]$, 210, (V)
(50) $x_1^2,\ x_2^2$, 630, (VI)
(51) $x_1^2,\ x_2^2+[x_1,x_3]$, 3780, (VI)
(52) $x_1^2,\ x_2^2+[x_1,x_4]+[x_2,x_3]$, 7560, (VI)
(53) $x_1^2,\ x_2^2+[x_2,x_3]$, 7560, (VI)
(54) $x_1^2, x_2^2+[x_3,x_4]$, 20160, (VI)

References

[1] Anick, David J. Noncommutative graded algebras and their Hilbert series. *J. Algebra* **78** (1982), 120–140. MR0677714 (84g:16001), Zbl 0502.16002.

[2] Bush, Michael R.; Labute, John. Mild pro-p groups with 4 generators, *J. Algebra* **308** (2007), 828–839. MR2295092 (2008g:20054), Zbl 1119.20033.

[3] Forré, Patrick. Strongly free sequences and pro-p-groups of cohomological dimension 2. *J. Reine Angew. Math.*, to appear.

[4] Koch, Helmut. Galois theory of p-extensions. With a foreword by I. R. Shafarevich. Translated from the 1970 German original by Franz Lemmermeyer. With a postscript by the author and Lemmermeyer. Springer Monographs in Mathematics. *Springer-Verlag, Berlin*, 2002. xiv+190 pp. ISBN: 3-540-43629-4. MR1930372 (2003f:11181), Zbl 1023.11002.

[5] Labute, John. Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$. *J. Reine Angew. Math.* **596** (2006), 155–182. MR2254811 (2007j:11158), Zbl 1122.11076.

[6] Labute, John; Mináč, Ján. Mild pro-2-groups and 2-extensions with restricted ramification. *J. Algebra* **332** (2011), 136–158.

[7] Lazard, M. Groupes analytiques p-adiques. *Inst. Hautes tudes Sci. Publ. Math.* No. 26 (1965), 389–603. MR0209286 (35 #188), Zbl 0139.02302.

[8] Bosma, Wieb; Cannon, John. Handbook of Magma functions. School of Mathematics and Statistics, University of Sydney, 1996.

[9] Neukirch, Jürgen; Schmidt, Alexander; Wingberg, Kay. Cohomology of number fields. Second edition. Grundlehren der mathematischen Wissenschaften 323. *Springer Verlag, Berlin*, 2008. xvi+825 pp. ISBN: 978-3-540-37888-4. MR2392026 (2008m:11223), Zbl 1136.11001.

[10] Schmidt, Alexander. Über Pro-p-Fundamentalgruppen markierter arithmetischer Kurven. *J. Reine Angew. Math.* **640** (2010), 203–235. MR2629694, Zbl 1193.14041.

Dept. of Mathematics & Statistics, Smith College, Northampton, MA 01062, USA
mbush@smith.edu

Universität Heidelberg, Mathematisches Institut, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany
gaertner@mathi.uni-heidelberg.de

Dept. of Mathematics & Statistics, McGill University, Burnside Hall, 805 Sherbrooke Street West, Montreal, QC H3A 2K6, Canada
labute@math.mcgill.ca

Universität Heidelberg, Mathematisches Institut, Im Neuenheimer Feld 288, 69120 Heidelberg, Germany
vogel@mathi.uni-heidelberg.de

This paper is available via http://nyjm.albany.edu/j/2011/17-14.html.