Abstract

In this note we compute the (uni)versal deformation of two types of mod 3 Galois representations \( \bar{\rho}: \text{Gal}(\mathbb{Q}_3/\mathbb{Q}_3) \to \text{GL}_2(\mathbb{F}_3) \). In the cases considered the (uni)versal ring is not formally smooth over a ring of Witt vectors. The main result is that this ring is an integral domain. This has applications to the local Langlands conjecture. The computations are based on [Bö] but made more explicit.

1 Introduction

Let \( p \) be a prime, let \( \mathbb{Q}_p \) denote the completion of the field of rational numbers \( \mathbb{Q} \) under the \( p \)-adic norm and let \( K \supset \mathbb{Q}_p \) be a finite extension field. For \( q \) a power of \( p \) denote by \( \mathbb{F}_q \) the field of \( q \) elements and by \( \mathbb{Z}_q \) the ring of Witt vectors of \( \mathbb{F}_q \), so that \( \mathbb{Z}_q \) is the complete discrete valuation ring of characteristic zero with uniformizer \( p \) and residue field \( \mathbb{F}_q \). Consider a continuous representation \( \bar{\rho}: G_K \to \text{GL}_2(\mathbb{F}_q) \) of the absolute Galois group \( G_K := \text{Gal}(K_{sep}/K) \) of \( K \).

To \( \bar{\rho} \) we can apply the deformation theory developed by Mazur [Ma]: Let \( \text{CNL}_q \) denote the category of complete noetherian local \( \mathbb{Z}_q \)-algebras \( R \) with residue field \( \mathbb{F}_q \). The algebra structure yields a canonical surjective homomorphism \( \pi_R: R \to \mathbb{F}_q \) of \( \mathbb{Z}_q \)-algebras. Its kernel is the maximal ideal of \( R \) which we denote by \( m_R \). For \( R \in \text{CNL}_q \), a lift of \( \bar{\rho} \) to \( R \) is a continuous representation \( \rho: G_K \to \text{GL}_2(R) \) such that \( \bar{\rho} = \text{GL}_2(\pi_R) \circ \rho \). A deformation is a strict equivalence class of lifts where two lifts are strictly equivalent if they are in the same conjugacy class under conjugation by matrices in \( \Gamma(R) := \ker(\text{GL}_2(\pi_R) : \text{GL}_2(R) \to \text{GL}_2(\mathbb{F}_q)) \subset \text{GL}_2(R) \). Following Mazur one considers the functor which to any \( R \in \text{CNL}_q \) associates the set of all deformations of \( \bar{\rho} \) to \( R \).

By [Ma] this functor always has a versal hull. The versal hull is a strict equivalence class of a lift \( \rho_v: G_K \to \text{GL}_2(R_v) \) of \( \bar{\rho} \) which is characterized (up to isomorphism) by the following two properties: (a) any deformation to a ring \( R \) is obtained as the composite of \( \rho_v \) with a \( \mathbb{Z}_q \)-algebra homomorphism \( R_v \to R \) in \( \text{CNL}_q \); (b) the composition of \( \rho_v \) with the canonical surjection \( R_v \to R_v/(m^2_R, p) \) is universal for deformations to \( \mathbb{F}_q[\varepsilon]/(\varepsilon^2) \). Let \( \text{ad} \) denote the adjoint representation of \( G_K \) on the \( 2 \times 2 \) matrices \( M_2(\mathbb{F}_q) \), i.e., the composite of \( \bar{\rho} \) with the conjugation action of \( \text{GL}_2(\mathbb{F}_q) \) on \( M_2(\mathbb{F}_q) \). Then the versal hull is universal if \( \dim_{\mathbb{F}_q} H^0(G_K, \text{ad}) = 1 \).

In this note we shall explicitly compute the versal deformation rings for two (types of) \( \bar{\rho} \) in the case where \( K = \mathbb{Q}_3 \), and so from now on we specialize \( p \) to 3. For every \( n \in \mathbb{N} \) fix a primitive \( n \)-th
root of unity $\zeta_n \in \mathbb{Q}_5$. We define $\chi_3: G_{\mathbb{Q}_3} \rightarrow \mathbb{Z}/(3)^* \cong \mathbb{F}_3^*$ as the mod 3 cyclotomic character, so that $g\zeta_3 = \zeta_3^{\chi_3(g)}$ for $g \in G_{\mathbb{Q}_3}$. We also define characters $\omega_i: G_{\mathbb{Q}_3} \rightarrow \mathbb{F}_3^*$, $i = 1, 2$, by

$$\sigma \mapsto \omega_i(\sigma) = \frac{\sigma(a - \sqrt[3]{3})}{\sigma(a + \sqrt[3]{3})} \pmod{3\mathbb{Z}_3};$$

the fraction on the right is a primitive $(3^i - 1)$-th root of unity in $\mathbb{Z}_3$. The characters $\omega_i$ are totally and tamely ramified.

We shall study the following two (types of) residual mod 3 Galois representations $\bar{\rho}_i: \text{Gal}(\overline{\mathbb{Q}}_3/\mathbb{Q}_3) \rightarrow \text{GL}_2(\mathbb{F}_3)$: By $\bar{\rho}_1$ we denote a representation which is an extension of the trivial character by $\chi_3$, so that

$$\bar{\rho}_1: G_{\mathbb{Q}_3} \rightarrow \text{GL}_2(\mathbb{F}_q): \sigma \mapsto \begin{pmatrix} \chi_3(\sigma) & \beta(\sigma) \\ 0 & 1 \end{pmatrix}$$

for some power $q$ of 3; here $\sigma \mapsto \beta(\sigma)$ is a continuous 1-cocycle and the set of $\bar{\rho}_1$ up to isomorphism is in bijection with $H^1_{\text{cont}}(G_{\mathbb{Q}_3}, \mathbb{F}_q^3)$. If $0 = [\beta] \in H^1_{\text{cont}}(G_{\mathbb{Q}_3}, \mathbb{F}_q^3)$ we choose $\beta = 0$. From local Tate duality and the local Euler-Poincaré formula one deduces

$$\dim_{\mathbb{F}_q} H^1_{\text{cont}}(G_{\mathbb{Q}_3}, \mathbb{F}_q^3) = \dim \mathbb{F}_q^3 + \dim H^0_{\text{cont}}(G_{\mathbb{Q}_3}, \mathbb{F}_q^3) + \dim H^0_{\text{cont}}(G_{\mathbb{Q}_3}, (\mathbb{F}_q^3)^*(\chi_3)) = 1 + 0 + 1 = 2.$$

By $\bar{\rho}_2$ we denote the induced representation

$$\bar{\rho}_2 := \text{Ind}_{G_{\mathbb{Q}_3}}^{G_{\mathbb{Q}_3}} \omega_2^2: G_{\mathbb{Q}_3} \rightarrow \text{GL}_2(\mathbb{F}_3);$$

we remark that the image of $\bar{\rho}_2$ is a dihedral group of order 8 of which it is known that its irreducible degree 2 representation on $\mathbb{F}_3^*$ is defined over $\mathbb{F}_3$. To have a uniform notation for the coefficient fields for both $\bar{\rho}_i$, we take $q = 3$ for the representation $\bar{\rho}_2$.

Let $\rho_i: G_{\mathbb{Q}_3} \rightarrow \text{GL}_2(R_i)$ denote the versal hull of $\bar{\rho}_i$. One easily verifies that it is universal if either $i = 2$ or if $i = 1$ and $[\beta] \neq 0$. The main result of this article is an explicit computation of $R_i$ which leads to the following result:

**MainThm**

**Theorem 1.1** The ring $R_i$ is an integral domain. Moreover $R_i$ is a local complete intersection, flat over $\mathbb{Z}_q$ and of relative dimension $4 + \dim H^0(G_{\mathbb{Q}_3}, \text{ad})$.

The proof follows closely that of the main result [Bö, Theorem 2.6]. The new assertion made, in comparison with [Bö], is that the rings $R_i$ for the two cases at hand are integral domains. This implies that the $\text{Spf}(R_i[\frac{1}{3}])$ are reduced and irreducible.

We now survey the present article. In Section 2 Mazur’s deformation functor for the $\bar{\rho}_i$ considered here is identified as a functor describing sets of equivariant homomorphisms from the pro-3 completion $P$ of the absolute Galois group of an extension of $\mathbb{Q}_3$ determined by $\bar{\rho}_i$ to a pro-3 Sylow subgroup of $\text{GL}_2(R)$ – the idea to consider functors of equivariant homomorphisms goes back to Boston, e.g. [Bo]. The group $P$ is a Demuškin group which carries an action of $\text{Im}(\bar{\rho})$ modulo its normal 3-Sylow subgroup $U$. In Section 3, we recall the main results on such groups.

Compared to the results in [Bö] there are two improvements. In Section 2 the Demuškin group $P$ arises from an extension of $\mathbb{Q}_3$ that is possibly of a smaller degree than in [Bö]. This facilitates the computations related to $D_2$. In Section 3 we are able to give an explicit presentation of $P$ in terms of topological generators and one relation $r$ where on the generators and thus also on $r$ the action of $\text{Im}(\bar{\rho})/U$ is also given explicitly! For $\bar{\rho}_1$ this was indicated in [Bö, Example 3.7]. For $\bar{\rho}_2$ this is new and
rather simple – but it was not noticed in [Bö]. The explicit form of $r$ will in Sections 4 and 5 allow the explicit computation of the versal deformations $\rho_i$. The Rings $R_i$ are given as the quotient of a power series ring over $\mathbb{Z}_q$ by ideals whose generators can in principle be given explicitly. However the actual generators we find are too complicated to write down. Instead, using a computer algebra package, we can give truncated power series to sufficient high precision to prove the above theorem.

2 A functor of equivariant homomorphisms

For a field $k$ let $k^\text{sep}$ denote a fixed separable closure. We defines $P_k$ as the pro-3 completion of $G_k := \text{Gal}(k^\text{sep}/k)$. This is a quotient of $G_k$ be a closed normal subgroup. The fixed field of this subgroup inside $k^\text{sep}$ we denote by $\mathbb{Q}$.

We introduce various extension fields of $\mathbb{Q}_3$ inside $\mathbb{Q}_3$ and Galois groups – they depend on $\bar{\rho}$ but we omit this dependency in the notation. The splitting field of $\bar{\rho}$ is $L := G_{\mathbb{Q}_3}^{Ker(\bar{\rho})}$. The group $H := \text{Gal}(L/\mathbb{Q}_3)$ has a unique 3-Sylow subgroup denoted $U$ – it is trivial for $\bar{\rho}_2$. For $\bar{\rho}_1$ the fixed field $L$ is $E := \mathbb{Q}_3(\zeta_3)$ and we write $G := \text{Gal}(E/\mathbb{Q}_3)$. Since $U$ is a pro-3 group one has $E(3) = L(3)$. For $\bar{\rho}_2$ we define $L_0 := G_{\mathbb{Q}_3}^{Ker(\text{ad})}$ as the splitting field of the representation $\text{ad}$ and we set $C := \text{Gal}(L/L_0)$ and $G := \text{Gal}(L_0/\mathbb{Q}_3)$. For the convenience of the reader, we display the situations for both $\bar{\rho}_i$ in the following diagrams:

In the diagram for $\bar{\rho}_1$ the group $G$ is isomorphic to a cyclic group of order 2, say $G = \{1, \sigma\}$. The group $U$ is of order 1, 3 or 9 as can be deduced from $\dim \mathbb{F}_q H^1(G_{\mathbb{Q}_3}, \mathbb{F}_3^*) = 2$. If $U$ is non-trivial, we denote by $u \in U$ a non-trivial element. By conjugating $\bar{\rho}_1$ suitable, we may then assume that $\bar{\rho}_1(u) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. In [Bo], §2 a profinite version of the Lemma of Schur-Zassenhaus is proved. It implies that $\text{Gal}(L(3)/\mathbb{Q}_3)$ is isomorphic to a semi-direct product $P_E \rtimes G$. We thus fix a lift of the generator $\sigma$ of $\text{Gal}(E/\mathbb{Q}_3)$ to $\text{Gal}(L(3)/\mathbb{Q}_3)$ of order 2. By the results in [Bo] any two such lifts are conjugate by an inner automorphism.

In the diagram for $\bar{\rho}_2$ the group $H$ is a dihedral group of order 8 and its quotient $G$ is a Klein 4-group. Because $P_{L_0}$ is a pro-3 group and the index $[L : L_0]$ is 2, one has $L \cap L_0(3) = L_0$ and thus $\text{Gal}(LL_0(3)/L_0)$ is isomorphic to the product $P_{L_0} \times C$. Again by the profinite Schur-Zassenhaus lemma, we have $\text{Gal}(LL_0(3)/\mathbb{Q}_3) \cong P_{L_0} \rtimes H$ where the subgroup $C \subset H$ acts trivially on $P_{L_0}$. As above we fix a splitting of $\text{Gal}(LL_0(3)/\mathbb{Q}_3) \rightarrow H$ and note that any two such differ by an inner automorphism.

Define $U_2(\mathbb{F}_q) \subset \text{GL}_2(\mathbb{F}_q)$ as the subgroup of upper triangular matrices with 1’s on the diagonal.
and define for any \( R \in \text{CNL}_q \) the group \( \tilde{\Gamma}(R) \) as \( \text{GL}_2(\pi_R)^{-1}(U_2(\mathbb{F}_q)) \), so that:

\[
\Gamma(R) = \text{GL}_2(\pi_R)^{-1}(\{1\}) \subset \tilde{\Gamma}(R) \subset \text{GL}_2(R).
\]

The groups \( \Gamma(R) \) and \( \tilde{\Gamma}(R) \) are pro-3 groups. It follows from [Bo, §6.9] that any lift \( \rho: G_{\mathbb{Q}_3} \to \text{GL}_2(R) \) of \( \tilde{\rho}_i \) contains \( \text{Gal}(\overline{\mathbb{Q}_3}/L(3)) \) in its kernel. But for \( \tilde{\rho}_2 \) slightly more is true.\(^3\)

**Lemma 2.1** Any lift \( \rho: G_{\mathbb{Q}_3} \to \text{GL}_2(R) \) of \( \tilde{\rho}_2 \) contains \( \text{Gal}(\overline{\mathbb{Q}_3}/LL_0(3)) \) in its kernel.

**Proof:** The image of \( C \) under \( \tilde{\rho}_2 \) is the set \( \{\pm 1\} \) where \( 1 \) is the identity matrix in \( \text{GL}_2(\mathbb{F}_q) \). If we denote by 12 the same matrix in \( \text{GL}_2(R) \) it follows that

\[
\text{GL}_2(\pi_R)^{-1}(\{\pm 1\}) \cong \Gamma(R) \times \{\pm 1\} \subset \text{GL}_2(R).
\]

By the profinite Schur-Zassenhaus lemma any element of order 2 in \( \text{GL}_2(\pi_R)^{-1}(\{\pm 1\}) \) is conjugate to \(-1\) and hence equal to \(-1\) since this element is central. By the same lemma \( \rho(\text{Gal}(\overline{\mathbb{Q}_3}/L_0)) \subset \text{GL}_2(\pi_R)^{-1}(\{\pm 1\}) \) is a semidirect product of a group of order 2 and a pro-\( p \) group. Up to strict equivalence we may assume that the group of order 2 is generated by the central element \(-1 \in \text{GL}_2(R)\). Hence \( \rho(\text{Gal}(\overline{\mathbb{Q}_3}/L_0)) \) is a product of a pro-3 group with \( \{\pm 1\} \). In particular, the pro-3 group is the Galois group of a Galois extension of \( L_0 \), and thus of a subextension of \( L_0(3) \).

We now define functors \( EH_i: \text{CNL}_q \to \text{Sets} \) of equivariant homomorphisms corresponding to the \( \tilde{\rho}_i \) as follows: To \( R \in \text{CNL}_q \) we associate

\[
EH_1(R) := \{ \alpha \in \text{Hom}_{G,\text{cont}}(P_E, \tilde{\Gamma}(R)) \mid \alpha \text{ mod } m_R = \tilde{\rho}_1|_{G_E} \text{ and } \rho(u) = \left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right) \text{ if } U \neq 0 \}
\]

if \( i = 1 \), and we associate \( EH_2(R) := \text{Hom}_{H,\text{cont}}(P_{L_0}, \Gamma(R)) \) if \( i = 2 \). Again by Schur-Zassenhaus, if \( i = 1 \) we fix a homomorphism \( \lambda_1: \text{Gal}(E/\mathbb{Q}_3) \to \text{GL}_2(\mathbb{Z}_q) \) whose mod 3 reduction is the composite of \( \tilde{\rho}_1 \) with a splitting of \( \text{Gal}(L/\mathbb{Q}_3) \to \text{Gal}(E/\mathbb{Q}_3) \), and if \( i = 2 \) a homomorphism \( \lambda_2: \text{Gal}(L/\mathbb{Q}_3) \to \text{GL}_2(\mathbb{Z}_3) \) which is a lift of \( \tilde{\rho}_2 \). The following is a variant of [Bö, Prop. 2.3]; its proof is left to the reader who may consult [Bo, §6.9].

**Proposition 2.2** The functors \( EH_i \) are representable. Let \( (\tilde{R}_i, \tilde{\alpha}_i) \) denote a universal pair and define the continuous representation \( \tilde{\rho}_i: G_{\mathbb{Q}_3} \to \text{GL}_2(\tilde{R}_i) \) by

\[
\tilde{\rho}_i((h, g)) := \alpha_i(h)\lambda_i(g)
\]

for \((h, g) \) in \( P_E \rtimes G \cong \text{Gal}(L(3)/\mathbb{Q}_3) \) or in \( P_{L_0} \rtimes H \cong \text{Gal}(LL_0(3)/\mathbb{Q}_3) \), respectively. Then the strict equivalence class of \((\tilde{R}_i, \tilde{\rho}_i)\) is a versal hull of \( \tilde{\rho}_i \).

### 3 Demuškin groups with group actions

The fields \( E \) and \( L_0 \) both contain a primitive third root of unity \( \zeta_3 \). By [La] it follows that the pro-3 groups \( P_E \) and \( P_{L_0} \), respectively, are Demuškin groups. We briefly recall some relevant notions from [La] on Demuškin groups, where the prime \( p \) is specialized to 3:

A pro-3 Demuškin group is a pro-3 group \( D \) such that the following properties are satisfied:

(a) \( n := \text{dim}_{\mathbb{F}_3} H^1(D, \mathbb{F}_3) < \infty \).
(b) \( \dim_{F_3} H^2(D, F_3) = 1 \).

(c) The cup product pairing \( H^1(D, F_3) \times H^1(D, F_3) \to H^2(D, F_3) \) is an alternating non-degenerate bilinear form.

By (a) the group \( D \) is topologically generated by \( n \) but no fewer elements. By (b) the group \( D \) has a presentation as a pro-3 group with \( n \) generators and one relation. By (c) the number \( n \) is even. It follows that the abelianization \( D^{ab} = D/[D, D] \) is a quotient of \( \mathbb{Z}_3^n \) by a pro-cyclic subgroup. Hence \( D^{ab} \cong \mathbb{Z}_3^{n-1} \times \mathbb{Z}_3/(Q) \) for a unique \( Q \in 3^n \cup \{0\} \). Using that all non-degenerate alternating bilinear form on a vector space are isomorphic, one can show that the invariants \( Q \) and \( n \) completely classify Demuškin groups up to isomorphism, cf. [La].

To give the construction of a Demuškin group for a given pairing and a given \( Q \), we first recall the definition of the lower \( Q \)-central series of a pro-\( p \) group \( P \): One sets \( P^{(0)} := P \) and defines recursively \( P^{(i+1)} := [P^{(i)}, P^{(i)}]/(P^{(i)})Q \) for \( i \geq 0 \), where \( [P^{(i)}, P^{(i)}]/(P^{(i)})Q \) is the topological closure of the subgroup of \( P^{(i)} \) generated by all \( Q \)-powers and all commutators. Let now \( n \in \mathbb{N} \) be even, \( V \) a vector space over \( F_3 \) and \( b : V \times V \to F_3 \) is a non-degenerate alternating bilinear form. Let \( F_n \) be a free pro-\( p \) group on \( n \) generators \( \hat{x}_1, \ldots, \hat{x}_n \). Define \( \chi_i : F_n \to F_3 \) to be the homomorphism with \( \chi_i(\hat{x}_j) = \delta_{i,j} \). Then \( \{\chi_i\}_{i=1,\ldots,n} \) is a basis of \( \text{Hom}(F_n, F_3) = H^1(F_n, F_3) \) over \( F_3 \). We choose an isomorphism \( V \cong \text{Hom}(F_n, F_3) \), so that \( b \) induces a pairing on \( H^1(F_n, F_3) \). Let \( r \in F_n \) be an element in \( F_n^{(1)} \) such that

\[
    r \equiv x_1^Q \prod_{1 \leq i < j \leq n} [\hat{x}_i, \hat{x}_j]^{b(\chi_i, \chi_j)} \pmod{P^{(2)}}
\]

and let \( N \) be the closed normal hull of the subgroup of \( F_n \) generated by \( r \). Then \( F_n/N \) is a Demuškin group with invariants \( n \) and \( Q \) and whose alternating pairing on \( H^1(F_n, F_3) \) is the one induced from \( b \).

We now add the structure of an action of a finite group \( G \) of order prime to \( p = 3 \) to a pro-3-Demuškin group. Observe that all \( F_3[G] \)-modules are self-dual, as follows from character theory since \( 3 / \#G \). The following is the specialization of [Bô, Theorem 3.4] to \( p = 3 \).

**Theorem 3.1** Let \( G \) be a finite group of order prime to 3. If \( G \) acts on a pro-3 Demuškin group \( D \), then \( D \rtimes G \) is determined up to isomorphism by the invariants \( n \) and \( Q \) of \( D \) and the action of \( G \) on \( H^1(D, F_3) \). The cup product pairing

\[
    \cup : H^1(D, F_3) \times H^1(D, F_3) \to H^2(D, F_3) \cong F_3
\]

is \( G \)-equivariant.

Conversely suppose that \( V \) and \( T \) are finite modules over \( F_3[G] \) with \( \dim_{F_3} T = 1 \) and \( H^0(G, V) \neq 0 \) and that \( b : V \times V \to T \) is a non-degenerate alternating \( G \)-equivariant pairing. Then for any \( Q \) there exists a Demuškin group \( D \) with invariants \( n = \dim V \) and \( Q \) and such that the \( F_3[G] \)-module \( H^1(D, F_3) \) is isomorphic to \( V \). In this case there is a \( G \)-equivariant isomorphism between \( b \) and the pairing \( \cup \).

Let \( K \) be in \( \{E, L_0\} \). Since \( \zeta_3 \) lies in \( K \), a result of Demuškin, cf. [La], shows that \( P_K \) is a Demuškin group. The invariant \( Q \) is 3 since \( \zeta_3 \notin K \). By [Iw], the isomorphism type of \( V^* \cong P_K/P^{(1)}_K \) as a \( G = \text{Gal}(K/Q_3) \)-module is \( F_3[G] \oplus F_3 \oplus F^{x_3} \), where \( F_3 \) without a superscript denotes the trivial \( G \)-module of dimension 1. The \( G \)-module structure of \( T = H^2(G_K, F_3) \) is easily identified with \( F^{x_3} \), so that in a topological presentation of \( P_K \) the action of \( G \) on a suitable generator of the relation ideal is given by \( \chi_3 \).
A constraint on the pairing (and the only one) is given by [Ko, Sätze 6, 9, 10]: The $F_3[G]$-module $P_K/P_{K}^{(1)}$ is isomorphic to a direct sum $(F_3 \oplus U) \oplus (F_3^3 \oplus V)$ such that the duals of the two summands are maximal isotropic subspaces under the cup product pairing. This means that one can decompose the $G$-module $H^1(G_K, F_3)$ in irreducible summands, such that each summand is paired with exactly one other summand, but no summand is paired with itself. Any two alternating pairings satisfying this constraint and having the same underlying $F_3[G]$-module and the same target $T$ are isomorphic. Based on this, we now construct explicit models of the $P_K$.

Suppose first that $\bar{\rho} = \bar{\rho}_1$. Recall that $\sigma$ is a generator of $G = \Gal(E/F_3)$ (of order 2). On the free pro-3 group $F_4$ on 4 topological generators $x_1, \ldots, x_4$ consider the following well-defined action by $G$:

$$\sigma(x_1) = x_1^{-1}, \quad \sigma(x_2) = x_2, \quad \sigma(x_3) = x_3^{-1}, \quad \sigma(x_4) = x_4.$$

Define $r_0 := x_1^3[x_1, x_2][x_3, x_4]$. This corresponds to the standard relation for the standard alternating form on $F_3^4$ -- according to the definition of our action, this form is $G$-equivariant. We have

$$\sigma(r_0) = x_1^{-3}[x_1^{-1}, x_2][x_3^{-1}, x_4], \quad \text{and} \quad r_0^{-1} = [x_4, x_3][x_2, x_1][x_3^{-3} \equiv \sigma(r_0) \pmod{F_4^{(2)}}];$$

here we use that $F_4^{(1)}/F_4^{(2)}$ is abelian and that $[g^{-1}h] = g^{-1}h^{-1}g = h^{-1}g^{-1} = [h, g] \pmod{F_4^{(2)}}$.

If $N_0 \subset F_4$ denotes the closed normal subgroup generated by $r_0$, then $F_4/N_0$ is a Demuškin group; however it is not clear that action of $G$ preserves $N_0$, i.e. that the quotient carries an action of $G$.

To remedy this, we define

$$r := r_0\sigma(r_0)^{-1} = x_1^3[x_1, x_2][x_3, x_4][x_4, x_3^{-1}][x_2, x_1^{-1}]x_1^3$$

and denote by $N_4 \subset F_4$ the closed normal subgroup generated by $r$. Since $r \equiv r_0^2 \pmod{F_4^{(2)}}$, the quotient $F_4/N_4$ is a Demuškin group. But furthermore we have $\sigma(r) = \sigma(r_0)r_0^{-1} = (r)^{-1}$. Therefore $N_4$ is preserved under the action of $G$. By the Theorem 3.1 and the above observations on $Q$ and on the $G$-module structure of $P_E/P_{E}^{(2)}$, we have shown:

**Lemma 3.2** The pro-3 group $F_4/N_4$ is as a group with $G$-action isomorphic to $P_E$.

Suppose now that $\bar{\rho} = \bar{\rho}_2$. Then $H := \Gal(L_0/Q_3)$ is a dihedral group of order 8. It has a presentation $H = \langle \varrho, \sigma \mid \varrho^4 = \sigma^2 = \varrho \sigma \varrho \sigma = 1 \rangle$ where $\varrho, \sigma$ act as follows on $L = Q_3(\zeta_4, \sqrt[3]{3})$:

$$\varrho(\zeta_4) = \zeta_4, \quad \varrho(\sqrt[3]{3}) = \zeta_4 \sqrt[3]{3}, \quad \sigma(\zeta_4) = -\zeta_4, \quad \sigma(\sqrt[3]{3}) = \sqrt[3]{3}.$$

The quotient $G := \Gal(L_0/Q_3)$ of $H$ is a Klein 4-group. By $\bar{\varrho}$ and $\bar{\sigma}$ we denote the restrictions of $\varrho$ and $\sigma$ to $L_0 = Q_3(\zeta_4, \sqrt[3]{3})$, so that $G = \langle \bar{\varrho}, \bar{\sigma} \mid \bar{\varrho}^2 = \bar{\sigma}^2 = \bar{\varrho} \bar{\sigma} \bar{\varrho} \bar{\sigma} = 1 \rangle$. Choosing $\zeta_3 = 1/2(-1 + \zeta_4 \sqrt[3]{3})$, we have

$$\bar{\varrho}(\zeta_4) = \zeta_4, \quad \bar{\varrho}(\sqrt[3]{3}) = -\sqrt[3]{3}, \quad \bar{\sigma}(\zeta_4) = \zeta_3^{-1}, \quad \bar{\sigma}(\sqrt[3]{3}) = \sqrt[3]{3}, \quad \bar{\sigma}(\zeta_3) = \zeta_3^{-1}.$$ 

The irreducible $F_3[G]$-modules are $F_3, F_3^{\chi_3}, F_3^{\omega_3}, F_3^{\chi_3 \omega_3}$. Thus

$$P_{L_0}/P_{L_0}^{(1)} \cong F_3^{\chi_3} \oplus F_3 \oplus F_3^{\chi_3} \oplus F_3^{\omega_3} \oplus F_3^{\omega_3 \chi_3} \oplus F_3^{3 \chi_3} \oplus F_3^{\omega_3 \chi_3}$$

as an $F_3[G]$-module. On the duals of $F_3^{\chi_3} \oplus F_3^{\chi_3}$ and $F_3^{\omega_3} \oplus F_3^{3 \chi_3}$ we have the obvious alternating pairing. We note that $\chi_3(\bar{\varrho}) = \chi_3(\bar{\sigma}) = \omega_1(\bar{\varrho}) = \chi_3 \omega_1(\bar{\sigma}) = -1$ and $\omega_1(\bar{\sigma}) = \chi_3 \omega_1(\bar{\varrho}) = 1$. 

---

**DemGpForF**
Let now $F_6$ be the free pro-3 group on generators $x_1, \ldots, x_6$. The following table describes a well-defined action of $G$ on $F_6$ such that $F_6/F_6^{(1)} \cong P_{L_0}/P_{L_0}^{(1)}$ as an $\mathbb{F}_3[G]$-module:

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$x_3$</th>
<th>$x_4$</th>
<th>$x_5$</th>
<th>$x_6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\bar{\sigma}$</td>
<td>$x_1^{-1}$</td>
<td>$x_2^{-1}$</td>
<td>$x_3^{-1}$</td>
<td>$x_4^{-1}$</td>
<td>$x_5^{-1}$</td>
</tr>
<tr>
<td>$\sigma$</td>
<td>$x_1^{-1}$</td>
<td>$x_2^{-1}$</td>
<td>$x_3^{-1}$</td>
<td>$x_4^{-1}$</td>
<td>$x_5^{-1}$</td>
</tr>
</tbody>
</table>

A first attempt for a relation describing $P_{L_0}$ might be

$$r_0 := x_3^3[x_1,x_2][x_3,x_4][x_5,x_6].$$

However, by [Bö, Prop. 3.6] the closed normal subgroup $N_6$ generated by $r_0$ is not preserved under the action of $G$. We define $r_1 := r_0\bar{\sigma}(r_0^{-1})$ and

$$r := r_1\bar{\sigma}\bar{\sigma}(r_1) = r_0\bar{\sigma}(r_0^{-1})\bar{\sigma}(r_0)\bar{\sigma}(r_0^{-1}).$$

Then $\bar{\sigma}(r_1) = r_1^{-1}$ and from $\bar{\sigma}\bar{\sigma} = \bar{\sigma}\bar{\sigma}$ one deduces

$$\bar{\sigma}(r) = r_1^{-1}\bar{\sigma}\bar{\sigma}(r_1^{-1}) = r_1^{-1}\bar{\sigma}\bar{\sigma}(r_0^{-1})r_1^{-1}r_1 = r_1^{-1}(r^{-1})r_1$$

and

$$\bar{\sigma}(r) = \bar{\sigma}(r_1)\bar{\sigma}(r_1) = \bar{\sigma}\bar{\sigma}(r_1^{-1})r_1^{-1} = (r_1\bar{\sigma}\bar{\sigma}(r_1))^{-1} = r^{-1}.$$

We deduce that the closed normal subgroup $N_6$ of $F_6$ generated by $r$ is preserved under the action of $G$. The following computations modulo $F_6^{(2)}$ show that the quotient $F_6/N_6$ is a Demushkin group:

$$a^3[b,c] \equiv [b,c]a^3 \pmod{F_6^{(2)}}, \quad [b,c]^{-1} = [c,b] \equiv [b^{-1},c] \pmod{F_6^{(2)}},$$

$$\bar{\sigma}(r_0) \equiv r_0^{-1} \pmod{F_6^{(2)}}, \quad r_1 \equiv r_0^2 \pmod{F_6^{(2)}}, \quad \bar{\sigma}(r_0) \equiv r_0 \pmod{F_6^{(2)}},$$

and thus $r \equiv r_0^4 \pmod{F_6^{(2)}}$. Again by Theorem 3.1 and the above remarks on $Q$ and on the $G$-module structure of $P_{L_0}/P_{L_0}^{(2)}$, we have shown:

**Lemma 3.3** The pro-3 group $F_6/N_6$ is as a group with $G$-action isomorphic to $P_{L_0}$.

### 4 Proof of the main theorem for $\bar{\rho}_1$

We now compute the subset $\text{EH}_1(R) \subset \text{Hom}_{G,\text{cont}}(P_E, \breve{\Gamma}(R))$ for any ring $R \in \text{CNL}_q$ where we use $F_4/N_4$ from Lemma 3.2 as a model for $P_E$ with $G$-action.

Let $\alpha$ be in $\text{EH}_1(R)$ and denote by $A_i \in \breve{\Gamma}(R) \subset \text{GL}_2(R)$ the image of $x_i \in F_4$, $i = 1, \ldots, 4$, under $\alpha$. Writing $s := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, the $G$-equivariance of $\alpha$ yields $sA_1s^{-1} = A_1^{-1}$, $sA_2s^{-1} = A_2$, $sA_3s^{-1} = A_3^{-1}$ and $sA_4s^{-1} = A_4$. One deduces

$$A_1 = \begin{pmatrix} \sqrt{1+a} & b \\ c & \sqrt{1+bc} \end{pmatrix}, \quad A_2 = \sqrt{1+a}\begin{pmatrix} \sqrt{1+d} & 0 \\ 0 & \sqrt{1+ad} \end{pmatrix}, \quad A_3 = \begin{pmatrix} \sqrt{1+b'} & 0 \\ c' & \sqrt{1+b'c'} \end{pmatrix}, \quad A_4 = \sqrt{1+a'}\begin{pmatrix} \sqrt{1+d'} & 0 \\ 0 & \sqrt{1+ad'} \end{pmatrix},$$

here $a, d, a', d', b, c, b, c' \in R$ and with the possible exception of $b, b'$ they lie in $m_R$. For $b$ and $b'$ this depends on $\bar{\rho}_1$. The image of the explicit relation $r$ under the homomorphism $F_4 \to \breve{\Gamma}(R)$ induced by $\alpha$ is

$$B := A_1^3[A_1, A_2][A_3, A_4][A_4, A_3^{-1}][A_2, A_1^{-1}]A_1^3.$$
One verifies that this expression is invariant under $\tilde{\sigma}(\_)^{-1}$; it is thus of the form $B = \left( \frac{\sqrt{1+UV}}{V} \right)^{U}$ for suitable $U \in R$ and $V \in \mathfrak{m}_R$, which are formal expressions in $b, c, b', c', d, d'$. Conversely, given any 4-tuple of matrices $A_1, \ldots , A_4$ of the above shape with $a, a', c, c', d, d' \in \mathfrak{m}_R$ and $b, b' \in R$ such that $b, b' \mod \mathfrak{m}_R$ agree with $\tilde{\rho}_1(x_1), \tilde{\rho}_1(x_3)$, respectively. Then this 4-tuple determines a $G$-equivariant homomorphism $\alpha \in \text{EH}_1(R)$ if and only if the $(1, 2)$- and $(2, 1)$-entries of $B$, as defined above, are zero. (By the invariance of $B$ under $\tilde{\sigma}(\_)^{-1}$ it then follows that $B = 1$.)

To simplify the computation we define $B_1 := [A_2, A_1]A_1^{-6}[A_1^{-1}, A_2]$ and $B_2 := [A_3, A_4][A_4, A_3^{-1}]$. Then $B = 1$ is equivalent to $B_1 = B_2$. Since the matrices $B_1$ and $B_2$ are again invariant under $\tilde{\sigma}(\_)^{-1}$, the equality $B_1 = B_2$ is equivalent to the equality $B_1(1, 2) = B_2(1, 2)$ of the $(1, 2)$-entries of these matrices and the equality $B_1(2, 1) = B_2(2, 1)$ of their $(2, 1)$-entries. By explicit computation, e.g., by a computer-algebra package, one can show that $B_1(1, 2) − B_2(1, 2)$ and $B_1(2, 1) − B_2(2, 1)$ lie in $\mathfrak{m}_R$ (even though $b$ and $b'$ may be units of $R$). We note that $B_1$ is a formal expression in $b, c, d$ and $B_2$ in $b', c', d'$.

Depending on the 1-cocycle $\beta$ in the definition of $\tilde{\rho}_1$, we shall divide the analysis of the functor $\text{EH}_1$ into three cases. By the inflation-restriction sequence and the isomorphism $P_E \cong F_4/N$ one has

$$H^1(G_{\mathbb{Q}_q}, \mathbb{F}^{\times 3}_q) = \text{Hom}_{\text{Gal}(E/\mathbb{Q}_q)}(G_E, \mathbb{F}^{\times 3}_q) = \text{Hom}_G(F_4/N, \mathbb{F}^{\times 3}_q).$$

By $\beta$ we also denote the $G$-equivariant homomorphism induced by $\beta$. We distinguish the following cases

(a) $\beta(x_1) \neq 0$: Here we choose $u = x_1$, so that $b = 1$ for the functor $\text{EH}_1$. We write $b' = \tau(b' \mod \mathfrak{m}_R) + \delta'_b$ where $\tau$ is the Teichmüller lift composed with the tautological algebra homomorphism $\mathbb{Z}_q \to R$ and $\delta'_b$ lies in $\mathfrak{m}_R$.

(b) $\beta(x_3) \neq 0 = \beta(x_1)$: We choose $u = x_3$, so that $b' = 1$ and $b \in \mathfrak{m}_R$.

(c) $\beta = 0$: Then $U = \{1\}$ and so $b, b' \in \mathfrak{m}_R$.

**Theorem 4.1** The functor $\text{EH}_1$ is represented by the pair $(\tilde{R}, \tilde{\alpha})$ which is given as follows (according to the above three cases):

(a) $\tilde{R} = \mathbb{Z}_q[[a, a', \delta'_a, c, c', d, d']]/(B_1(1, 2) − B_2(1, 2), B_1(2, 1) − B_2(2, 1))$ where we regard $B_1(1, 2) − B_2(1, 2)$ and $B_1(2, 1) − B_2(2, 1)$ as formal expressions in the indeterminates $a, a', b, b', c, c', d, d'$ in which we replace $b$ by 1 and $b'$ by $\tau(b' \mod \mathfrak{m}_R) + \delta'_b$.

(b) $\tilde{R} = \mathbb{Z}_q[[a, a', b, c, c', d, d']]/(B_1(1, 2) − B_2(1, 2), B_1(2, 1) − B_2(2, 1))$ where we regard $B_1(1, 2) − B_2(1, 2)$ and $B_1(2, 1) − B_2(2, 1)$ as formal expressions in the indeterminates $a, a', b, b', c, c', d, d'$ in which we replace $b'$ by 1.

(c) $\tilde{R} = \mathbb{Z}_q[[a, a', b, b', c, c', d, d']]/(B_1(1, 2) − B_2(1, 2), B_1(2, 1) − B_2(2, 1))$ where we regard $B_1(1, 2) − B_2(1, 2)$ and $B_1(2, 1) − B_2(2, 1)$ as formal expressions in the indeterminates $a, a', b, b', c, c', d, d'$.

In all cases $\tilde{\alpha}$ is the homomorphism $F_4/N \to \tilde{\Gamma}(R)$ defined by mapping $x_i$ to $A_i$ with $A_i$ as above.

To prove Theorem 1.1 for $\tilde{\rho}_1$, we need to study the differences $B_1(1, 2) − B_2(1, 2)$ and $B_1(2, 1) − B_2(2, 1)$ generating the relation ideal of $\tilde{R}$ in greater detail. Unfortunately the explicit expressions for these differences are rather lengthy. To analyze them, we used a computer-algebra package – all assertions we make in the following regarding these expressions were obtained in this way. We analyze the three cases separately.
Case (a): Substituting $b = 1$ in $B_1(1, 2) - B_2(1, 2)$, we find
\[ B_1(1, 2) - B_2(1, 2) \equiv c - d - \beta(x_3)d' \pmod{(3, (c, c', d, d')^2)), \]
and thus we can solve for $d$. Since $B_1(1, 2) - B_2(1, 2)$ is a quadratic polynomial in $d$, this can be done explicitly. Precisely one of the two solutions obtained by replacing $\sqrt{1 + x}$ by its standard Taylor series expansion is the correct one. This solution for $d$ can be substituted in $B_1(2, 1) - B_2(2, 1)$ yielding a single relation $r(c, b', c', d')$. One verifies
\[ r(c, b', c', d') \equiv c^2 + 2c' d' + \beta(x_3)c'd' \pmod{(3, (c, c', d, d')^2)). \]
Independently of $\beta(x_3)$, the polynomial $c^2 + 2c'd' + \beta(x_3)c'd'$ is irreducible in $\mathbb{F}_q[c, c', d']$. Therefore also $r \in \mathbb{Z}_q[[a, a', \delta', c, c', d']]$ is irreducible which proves that $\bar{R} = \mathbb{Z}_q[[a, a', \delta', c, c', d']]/r$ is an integral domain.
Throughout the formal computations for case (a) one has to be aware that $\bar{R}$ is not a variable in the maximal ideal. This makes the computations more difficult than in then remaining cases.

Case (b): Substituting $b' = 1$ in $B_1(1, 2) - B_2(1, 2)$ and noting that $b$ now is a formal variable, we find
\[ B_1(1, 2) - B_2(1, 2) \equiv -d' \pmod{(3, (b, c, c', d, d')^2)) \]
so that we can solve for $d'$. Again $B_1(1, 2) - B_2(1, 2)$ is a quadratic polynomial in $d'$, and so one can solve for $d'$ explicitly. Substituting the Taylor series expansion for $d'$ into $B_1(2, 1) - B_2(2, 1)$ yields a single relation $r'(b, c, c', d)$ and one verifies
\[ -r'(b, c, c', d') \equiv 3c - 2cd + 3bc' + c^2b + cd^2 - bc'd \pmod{(3, b, c, c', d)^4}). \]
Note that $-r'(b, c, c', d') \equiv 3c - 2cd = c(3 - 2d) \pmod{(3, b, c, c', d)^3)$ is the unique factorization of $r'$ modulo $m^3$ where $m$ is the maximal ideal of $\mathbb{Z}_q[[b, c, c', d]]$. One can now verify that this factorization is not liftable to a factorization modulo $m^4$ and hence $r'$ is irreducible. Again we deduce that $\bar{R} = \mathbb{Z}_q[[a, a', b, c, c', d']]/r'$ is an integral domain.

Case (c): Now $b, b'$ lie in the maximal ideal $R := \mathbb{Z}_q[[a, a', b, b', c, c', d, d']]$ and one verifies
\[ r_1 := B_1(1, 2) - B_2(1, 2) \equiv bd + b'd' \pmod{(3, (b, b', c, c', d, d')^2)), \]
\[ r_2 := B_1(2, 1) - B_2(2, 1) \equiv cd + c'd' \pmod{(3, (b, b', c, c', d, d')^2)). \]
The first observation is that $\mathbb{Z}[b, b', c, c', d, d']/(bd + b'd', cd + c'd')$ is an integral domain since it is a subring of $\mathbb{Z}[b^{\pm 1}, c^{\pm 1}, d^{\pm 1}, b'^{\pm 1}, c'^{\pm 1}, d'^{\pm 1})/(b^2 + d'^2, c + d^2) \equiv \mathbb{Z}[b, c, d, b', c', d']$ under the obvious homomorphism. Replacing $\mathbb{Z}$ by $\mathbb{F}_q$ the same assertion holds. Thus if we could show that replacing $r_1$ and $r_2$ by their quadratic reductions (modulo 3), then the following claim would (essentially) finish the proof:

Claim If $\bar{R}/(3)$ is an integral domain then so is $\tilde{R}$: Suppose
\[ fg = h_1 r_1 + h_2 r_2 \in \mathbb{Z}_q[[a, a', b, b', c, c', d, d']] \]
for $f, g$ not in the ideal $(r_1, r_2)$. Let $n, m \in \mathbb{N}_0$ be such that $f \in 3^m R \setminus p^{m+1} R$ and $g \in p^n R \setminus 3^{n+1} R$. If $f^{3^{-m}}$ reduces to zero in $\bar{R}/(p, r_1, r_2)$, then we replace $f$ by $f - f_m$ for some $f_m \in (r_1, r_2)$ such that the new $f$ lies in $3^{m+1} R$. Since $f$ does not lie in $(r_1, r_2)$ and $R$ is 3-adically complete, after a finite
number of iterations, we may assume that $3^{-m}f$ does not reduce to zero in $R/(3,\Gamma_1,\Gamma_2)$. The same argument applies to $g$, and thus without loss of generality, we may assume that $f$ and $g$ themselves reduce to non-zero elements in $R/(3,\Gamma_1,\Gamma_2)$. Since $R/(3,\Gamma_1,\Gamma_2)$ is an integral domain, the product of the reductions is non-zero. This contradicts (3) and thus proves the claim.

We now work toward simplifying the $\Gamma_*$. Let $\tilde{R} := R/3R = \mathbb{F}_q[[a,a',b,b',c,c',d,d']]$ with maximal ideal $\tilde{m}$ and let $f$ be the ideal in $\tilde{R}$ generated by the classes of $\Gamma_1$ and $\Gamma_2$, so that $\tilde{R}/(\Gamma_1,\Gamma_2) = \tilde{R}/I$. For any $f \in \tilde{R}$ we define

$$\text{ht } f := \text{sup}\{n \in \mathbb{N} \mid \exists h \in \tilde{m}^n, h \equiv f \pmod{I}\} \in \mathbb{N}_0 \cup \{\infty\}.$$  

Using the fact that $\tilde{R}$ is $\tilde{m}$-adically complete, one shows that $\text{ht } f = \infty$ if and only if $f$ lies in $\tilde{I}$. Suppose $f \in \tilde{R} \setminus \tilde{I}$ and that $h$ is chosen so that $h \equiv f \pmod{I}$ and $h \in \tilde{m}^{\text{ht } f}$. This implies that the image of $h$ in the graded ring $\bigoplus_{i=0}^{\infty} \tilde{m}^i/\tilde{m}^{i+1} \cong \mathbb{F}_q[b, b', c, c', d, d']$ does not lie in the ideal $(bd + b'd', cd + c'd')$ and in fact this is an alternative way to characterization of $\text{ht } f$. We have already observed that the ideal $(bd + b'd', cd + c'd')$ is a prime ideal in the graded ring. From this one easily deduces that the function $f \mapsto \text{ht } f$ satisfies $\text{ht}(fg) = \text{ht } f + \text{ht } g$. In turn, this property of $\text{ht}$ implies that $\tilde{R}/\tilde{I}$ is an integral domain.

We have thus shown the following theorem, which due to Proposition 2.2 and Theorem 4.1 immediately implies Theorem 1.1 for $\tilde{\rho}_1$.

**Theorem 4.2** Under the hypotheses of Theorem 4.1, in all three cases the ring $\tilde{R}$ is an integral domain, which is flat over $\mathbb{Z}_q$, a complete intersection and of relative dimension $5$ in the first two cases and $6$ in the last case.

## 5 Proof of main theorem for $\tilde{\rho}_2$

Finally we investigate the functor $EH_2$. Using the model $F_6/N$ for $P_{L_0}$ from Lemma 3.3, for any $R \in \text{CNL}_q$ we have $EH_2(R) = \text{Hom}_{G,\text{cont}}(F_6/N_0, \Gamma(R))$. To further compute this, we make the following choice for the lift $\lambda_2$ of $H$ to $\text{GL}_2(\mathbb{Z}_3)$: We take $\lambda_2(\rho) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\lambda_2(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Let $\alpha$ be in $EH_2(R)$ and denote by $A_i \in \Gamma(R) \subset \text{GL}_2(R)$ the image of $x_i \in F_6$, $i = 1, \ldots, 6$, under $\alpha$. Using Table (2), the $G$-equivariance of $\alpha$ yields

$$\lambda_2(\rho)A_1\lambda_2(\rho)^{-1} = A_1^{-1}, \lambda_2(\sigma)A_1\lambda_2(\sigma)^{-1} = A_1^{-1}, \lambda_2(\rho)A_2\lambda_2(\rho)^{-1} = A_2, \lambda_2(\sigma)A_2\lambda_2(\sigma)^{-1} = A_2 \text{ etc.}$$

One deduces

$$A_1 = \begin{pmatrix} \sqrt{1+d} & 0 \\ 0 & \sqrt{1+d^{-1}} \end{pmatrix}, A_2 = (1+a)\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A_3 = \begin{pmatrix} \sqrt{1+d} & 0 \\ 0 & \sqrt{1+d^{-1}} \end{pmatrix}, A_4 = (1+a')\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$  

$$A_5 = \begin{pmatrix} \sqrt{1+b^2} & b' \\ b & \sqrt{1+b'^2} \end{pmatrix}, A_6 = \begin{pmatrix} \sqrt{1-c'^2} & -c \\ c & \sqrt{1-c'^2} \end{pmatrix};$$

for $a, a', b, c, d, d' \in \mathfrak{m}_R$. Using that the images of $x_1, \ldots, x_4$ commute, the image of $r_0$ under $\alpha$ is $A_2[A_5, A_6]$. It follows that the image of the relation $r = 1$ under the homomorphism $\alpha$ is $B = B_1B_2 = 1$ where

$$B_1 := A_2^3[A_5, A_6][A_6, A_5^{-1}]A_1^3, \quad B_2 := A_2^3[A_5^{-1}, A_6^{-1}][A_6^{-1}, A_5]A_1^3.$$  

Since $B_1 = \alpha(r_1)$ and $B_2 = \alpha(\bar{\sigma}\bar{\rho}(r_1))$ the matrices $B_i$ are invariant under $\bar{\sigma}(\bar{\rho})^{-1}$ and the matrix $B_2$ is obtained from $B_1$ by conjugation by $t := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The invariance under $\bar{\sigma}(\bar{\rho})^{-1}$ implies that
in any case $B_1$ is of the form \( \left( \frac{1+U}{V}, \frac{1-V}{1+U} \right) \) for $U, V \in \mathfrak{m}_R$ which are expressions in terms of $a, a', b, c, d, d'$. The condition $r = 1$ turns under $\alpha$ into the condition $B_1^{-1} = tB_1t$ in $GL_2(R)$. This is equivalent to a single condition on $B_1$, namely that $1 + U = (1 - V^2)/(1 + U)$, i.e. that the $(1, 1)$-entry $B_1(1, 1)$ and the $(2, 2)$-entry $B_1(2, 2)$ of $B_1$ must agree. Conversely, any homomorphism $F_6 \to \Gamma(R)$ for which the image of $r_1$ is a matrix $B_1$ with $B_1(1, 1) = B_1(2, 2)$ factors via $F_6/N_0$.

**Theorem 5.1** The functor $EH_2$ is represented by the pair $(\tilde{R}, \tilde{\alpha})$ defined as follows:

\[
\tilde{R} := \mathbb{Z}_3[[a, a', b, c, d, d']]/(B_1(1, 1) - B_1(2, 2))
\]

where we regard $B_1(1, 1) - B_1(2, 2)$ as formal expressions in the indeterminates $a, a', b, c, d, d'$. The homomorphism $\tilde{\alpha} : F_3/N \to \tilde{\Gamma}(\tilde{R})$ is defined by mapping $x_i$ to $A_i$ with $A_i$ as above.

To prove Theorem 1.1 for $\tilde{r}_2$, it remains to make $B_1(1, 1) - B_1(2, 2)$ explicit. Since it fits this page, we simply display the formally calculated matrix $B_1$:

\[
\begin{pmatrix}
(1+d)(1+8b^2c'(1-c^2)+4bc\sqrt{(1+b^2)(1-c^2)}) & -4b^2c(1-2c^2)\sqrt{1-c^2} \\
4b^2c(1-2c^2)\sqrt{1-c^2} & (1+d)^2((1+8b^2c^2(1-c^2)-4bc\sqrt{(1+b^2)(1-c^2)})
\end{pmatrix}
\]

The vanishing of $B_1(1, 1) - B_1(2, 2)$ is thus equivalent to that of

\[
r := (1+d)^2(1+8b^2c(1-c^2)+4bc\sqrt{(1+b^2)(1-c^2)}) - ((1+8b^2c^2(1-c^2)-4bc\sqrt{(1+b^2)(1-c^2)})
\]

Modulo $(3, m^4)$ for $m$ the maximal ideal of $\mathbb{Z}_3[[a, a', b, c, d, d']]$ we find \( r \equiv -bc - d^3 \). Therefore the image of $r$ in $F_3[[a, a', b, c, d, d']]$ is irreducible and so is $\tilde{r}$. It follows that $\mathbb{Z}_3[[a, a', b, c, d, d']]/(r)$ is an integral domain. All other assertions of the following theorem are simple to verify. Due to Proposition 2.2 and Theorem 5.1 the theorem immediately implies Theorem 1.1 for $\tilde{r}_2$.

**Theorem 5.2** The ring $\tilde{R}$ in Theorem 5.1 is an integral domain, which is flat over $\mathbb{Z}_q$, a complete intersection and of relative dimension 5.

**References**


