Astérisque

GEBHARD BÖCKLE

Deformation rings for some mod 3 Galois representations of the absolute Galois group of Q_3

Astérisque, tome 330 (2010), p. 529-542

<http://www.numdam.org/item?id=AST_2010__330__529_0>

Astérisque
330, 2010, p. 529–542

DEFORMATION RINGS FOR SOME MOD 3 GALOIS REPRESENTATIONS OF THE ABSOLUTE GALOIS GROUP OF $\mathbf{Q}_3$

by

Gebhard Böckle

Abstract. — In this note we compute the (uni)versal deformation of two types of mod 3 Galois representations $\bar{\rho} : \mathrm{GL}(\overline{\mathbb{Q}_3}/\mathbb{Q}_3) \to \mathrm{GL}_2(\overline{\mathbb{F}_3})$. In the cases considered the (uni)versal ring is obstructed. Our main result is that the ring is still an integral domain. The result has consequences for the p-adic local Langlands correspondence: By work of Colmez and Kisin it allows one to deduce that benign crystalline points are Zariski dense in the universal space for $p = 3$. Thus the p-adic local Langlands correspondence [**4**] as well as the result [**6**] have no longer any exceptional cases for $p = 3$.

***Résumé* (Anneaux de déformation pour certaines représentations galoisiennes mod 3 du groupe de Galois absolu de $\mathbf{Q}_3$)**

Dans cette note, nous calculons la déformation (uni)verselle de deux types de représentations galoisiennes $\bar{\rho} : \mathrm{GL}(\overline{\mathbb{Q}_3}/\mathbb{Q}_3) \to \mathrm{GL}_2(\overline{\mathbb{F}_3})$. Dans les cas que nous considérons, l'anneau (uni)versel est obstrué. Notre résultat principal énonce que l'anneau reste intègre. Ce résultat a des conséquences pour la correspondance de Langlands p-adique locale : en utilisant les travaux de Colmez et de Kisin, il nous permet de déduire que les points crystallins bénins sont denses pour la topologie de Zariski, dans l'espace universel pour $p = 3$. Ainsi la correspondance de Langlands p-adique locale [**4**] ainsi que le résultat de [**6**] n'ont plus de cas exceptionnels pour $p = 3$.

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

$$\bar{\rho}\colon G_K \to \mathrm{GL}_2(\mathbb{F}_q)$$

of the absolute Galois group $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ of K.

2000 Mathematics Subject Classification. — 11F80, 11F85, 20F05, 11S37.
Key words and phrases. — Galois representation, local field, Demuškin group, universal deformation, p-adic local Langlands program.

To $\bar{\rho}$ we apply the deformation theory developed by Mazur [**9**]: Let 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 $\mathfrak{m}_R$. For $R \in \mathrm{CNL}_q$, a *lift* of $\bar{\rho}$ to R is a continuous representation $\rho : G_K \to \mathrm{GL}_2(R)$ such that $\bar{\rho} = \mathrm{GL}_2(\pi_R) \circ \rho$. 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 $\Gamma(R) := \mathrm{Ker}(\mathrm{GL}_2(\pi_R) : \mathrm{GL}_2(R) \to \mathrm{GL}_2(\mathbb{F}_q)) \subset \mathrm{GL}_2(R)$. Following Mazur one considers the functor which to any R in CNL_q associates the set of all deformations of $\bar{\rho}$ to R.

By [**9**] this functor always has a versal hull. The versal hull is a strict equivalence class of a lift $\rho_v : G_K \to \mathrm{GL}_2(R_v)$ 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 ρ_v with a $\mathbb{Z}_q$-algebra homomorphism $R_v \to R$ in CNL_q; (b) the composition of ρ_v with the canonical surjection $R_v \twoheadrightarrow R_v/(\mathfrak{m}_{R_v}^2, p)$ is universal for deformations to $\mathbb{F}_q[\varepsilon]/(\varepsilon^2)$. The versal hull is universal if $\dim_{\mathbb{F}_q} H^0(G_K, \mathrm{ad}) = 1$; here ad denotes the adjoint representation of G_K on the set of 2×2 matrices $M_2(\mathbb{F}_q)$ over $\mathbb{F}_q$, i.e., the composite of $\bar{\rho}$ with the conjugation action of $\mathrm{GL}_2(\mathbb{F}_q)$ on $M_2(\mathbb{F}_q)$.

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 $n \in \mathbb{N}$ we fix a primitive n-th root of unity $\zeta_n \in \overline{\mathbb{Q}_3}$. We define $\chi_3 : G_{\mathbb{Q}_3} \to \mathbb{Z}/(3)^* \cong \mathbb{F}_3^*$ 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 $\omega_i : G_{\mathbb{Q}_{3^i}} \to \mathbb{F}_{3^i}^*$, $i = 1, 2$, by

$$\sigma \mapsto \omega_i(\sigma) \equiv \frac{\sigma(\sqrt[3^i-1]{3})}{\sqrt[3^i-1]{3}} \pmod{3\,\mathbb{Z}_{3^i}};$$

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

We shall study the following two (types of) residual mod 3 Galois representations $\bar{\rho}_i : \mathrm{Gal}(\overline{\mathbb{Q}_3}/\mathbb{Q}_3) \to \mathrm{GL}_2(\overline{\mathbb{F}_3})$: By $\bar{\rho}_1$ we denote a representation which is an extension of the trivial character by χ_3, so that

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

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 $H^1_{\mathrm{cont}}(G_{\mathbb{Q}_3}, \mathbb{F}_q^{\chi_3})$. If $0 = [\beta] \in H^1_{\mathrm{cont}}(G_{\mathbb{Q}_3}, \mathbb{F}_q^{\chi_3})$ we choose $\beta = 0$. From local Tate duality and the local Euler-Poincaré formula, cf. [**10**, §3], one deduces

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

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

$$\bar{\rho}_2 := \mathrm{Ind}_{G_{\mathbb{Q}_9}}^{G_{\mathbb{Q}_3}} \omega_2^2 \colon G_{\mathbb{Q}_3} \to \mathrm{GL}_2(\mathbb{F}_3);$$

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

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 $4 + \dim H^0(G_{\mathbb{Q}_3}, \mathrm{ad})$.*

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

By [**6**, Cor. 1.3.6], the $\bar{\rho}_i$ considered here are precisely those 2-dimensional representations of $G_{\mathbb{Q}_3}$ over a finite extension of $\mathbb{F}_3$ for which Mazur's deformation functor is obstructed, i.e., for which $H^2(G_{\mathbb{Q}_3}, \mathrm{ad}) \neq 0$. Thus Theorem 1.1 holds for the (uni)versal deformation rings of all such residual representations. Moreover one can easily adapt the (methods of the) present article to study deformation functors for deformations having a fixed determinant ψ as in [**6**]. The corresponding (uni)versal deformation ring satisfies all assertions of Theorem 1.1 except that its relative dimension is $3 + \dim H^0(G_{\mathbb{Q}_3}, \mathrm{ad}^0)$.

Since $\mathrm{Spec}\, R_i[1/3]$ is irreducible, [**3**, § 6] or [**6**, Cor. 1.3.4] imply that trianguline or benign crystalline points are Zarisiki dense in it—as well as the analogous result for deformations with a fixed determinant (note that [**6**, Cor. 2.3.7] only needs cases of the present note in which $\dim H^0(G_{\mathbb{Q}_3}, \mathrm{ad}^0) = 0$, i.e., those in which R_i is universal). By this, the p-adic local Langlands correspondence [**4**, in part. Thme. II.3.3] and the result [**6**, Thms. 0.1 and 0.3] have no longer any exceptional cases for $p = 3$.

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 $\mathrm{GL}_2(R)$—the idea to consider functors of equivariant homomorphisms goes back to Boston, e.g. [**2**]. The group P is a Demuškin group which carries an action of $\mathrm{Im}(\bar{\rho})$ modulo its normal 3-Sylow subgroup U. In Section 3, we recall the main results on such groups.

Compared to the results in [**1**] 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 [**1**] or [**2**]. This facilitates the computations related to $\bar{\rho}_2$. 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 $\mathrm{Im}(\bar{\rho})/U$ is also

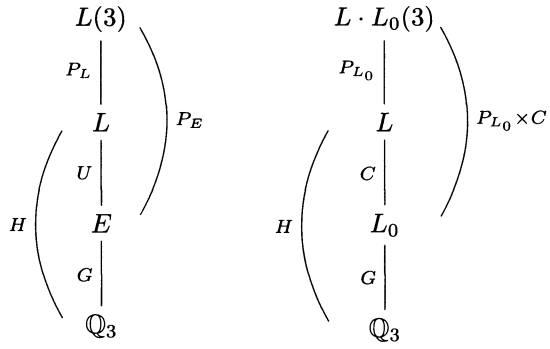
given explicitly! For $\bar{\rho}_1$ this was indicated in [**1**, Example 3.7]. For $\bar{\rho}_2$ this is new and rather simple—but it was not noticed in [**1**]. The explicit form of r will in Sections 4 and 5 allow the explicit computation of the versal deformations ρ_i. The Rings R_i are given as 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 Theorem 1.1.

Acknowledgements. — I would like to thank very much P. Colmez for bringing the problem that led to this note to my attention and moreover to allow me to publish it in present the volume dedicated to J.-M. Fontaine. The author was supported by a grant of the Deutsche Forschungsgemeinschaft within the SFB/TR 45.

2. A functor of equivariant homomorphisms

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

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



for $\bar{\rho}_1$ for $\bar{\rho}_2$

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 $\dim_{\mathbb{F}_3} H^1(G_{\mathbb{Q}_3}, \mathbb{F}_3^{\chi_3}) = 2$. 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 $\bar{\rho}_1(u) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. In [**2**, §2] a profinite version of the Lemma of Schur-Zassenhaus is stated. It implies that $\mathrm{Gal}(L(3)/\mathbb{Q}_3)$ is isomorphic to a semi-direct product $P_E \rtimes G$. We thus fix a lift of the generator σ of $\mathrm{Gal}(E/\mathbb{Q}_3)$ to $\mathrm{Gal}(L(3)/\mathbb{Q}_3)$ of order 2. By the quoted Schur-Zassenhaus lemma 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 $\mathrm{Gal}(LL_0(3)/L_0)$ is isomorphic to the product $P_{L_0} \times C$. Again by the profinite Schur-Zassenhaus lemma, we have $\mathrm{Gal}(LL_0(3)/\mathbb{Q}_3) \cong P_{L_0} \rtimes H$ where the subgroup $C \subset H$ acts trivially on P_{L_0}. As above we fix a splitting of $\mathrm{Gal}(LL_0(3)/\mathbb{Q}_3) \to H$ and note that any two such differ by an inner automorphism.

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

$$\Gamma(R) = \mathrm{GL}_2(\pi_R)^{-1}(\{1\}) \subset \tilde{\Gamma}(R) \subset \mathrm{GL}_2(R).$$

The groups $\Gamma(R)$ and $\tilde{\Gamma}(R)$ are pro-3 groups. It follows from [**2**, §6.9] that any lift $\rho\colon G_{\mathbb{Q}_3} \to \mathrm{GL}_2(R)$ of $\bar{\rho}_i$ contains $\mathrm{Gal}(\overline{\mathbb{Q}_3}/L(3))$ in its kernel. But for $\bar{\rho}_2$ slightly more is true.

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

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

$$\mathrm{GL}_2(\pi_R)^{-1}(\{\pm 1_2\}) \cong \Gamma(R) \times \{\pm 1_2\} \subset \mathrm{GL}_2(R).$$

By the profinite Schur-Zassenhaus lemma any element of order 2 in $\mathrm{GL}_2(\pi_R)^{-1}(\{\pm 1_2\})$ is conjugate to -1_2 and hence equal to -1_2 since this element is central. By the same lemma $\rho(\mathrm{Gal}(\overline{\mathbb{Q}_3}/L_0)) \subset \mathrm{GL}_2(\pi_R)^{-1}(\{\pm 1_2\})$ 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 $-1_2 \in \mathrm{GL}_2(R)$. Hence $\rho(\mathrm{Gal}(\overline{\mathbb{Q}_3}/L_0))$ is a product of a pro-3 group with $\{\pm 1_2\}$. 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 $\mathrm{EH}_i\colon \mathrm{CNL}_q \to \mathbf{Sets}$ of equivariant homomorphisms corresponding to the $\bar{\rho}_i$ as follows: To $R \in \mathrm{CNL}_q$ we associate

$$\mathrm{EH}_1(R) := \left\{ \alpha \in \mathrm{Hom}_{G,\mathrm{cont}}\left(P_E, \tilde{\Gamma}(R)\right) \,\middle|\, \alpha \mod \mathfrak{m}_R = \bar{\rho}_1|_{G_E} \text{ and } \alpha(u) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \text{ if } U \neq 0 \right\}$$

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

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

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

3. Demuškin groups with group actions

The fields E and L_0 both contain ζ_3. By [**8**] it follows that the pro-3 groups P_E and P_{L_0}, respectively, are Demuškin groups. We briefly recall some relevant notions form [**8**] 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) $n := \dim_{\mathbb{F}_3} H^1(D, \mathbb{F}_3) < \infty$.
(b) $\dim_{\mathbb{F}_3} H^2(D, \mathbb{F}_3) = 1$.
(c) The cup product pairing $H^1(D, \mathbb{F}_3) \times H^1(D, \mathbb{F}_3) \to H^2(D, \mathbb{F}_3)$ 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 $D^{\mathrm{ab}} = D/[D,D]$ is a quotient of $\mathbb{Z}_3^n$ by a pro-cyclic subgroup. Hence $D^{\mathrm{ab}} \cong \mathbb{Z}_3^{n-1} \times \mathbb{Z}_3/(Q)$ for a unique $Q \in 3^{\mathbb{N}} \cup \{0\}$. Using that (in characteristic different from 2) all non-degenerate alternating bilinear forms on a vector space are isomorphic, one can show that the invariants Q and n completely classify Demuškin groups up to isomorphism, cf. [**8**].

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 $P^{(i+1)} := (P^{(i)})^Q [P^{(i)}, P]$, for $i \geq 0$, as the topological closure of the subgroup of $P^{(i)}$ generated by all Q-powers and all commutators with one of the arguments in $P^{(i)}$. Let now $n \in \mathbb{N}$ be even, V a vector space over $\mathbb{F}_3$ of dimension n and $b : V \times V \to \mathbb{F}_3$ a non-degenerate alternating bilinear form. Let F_n be a free pro-p group on n generators $x_1, \ldots, x_n$. Define $\chi_i \colon F_n \to \mathbb{F}_3$ to be the homomorphism with $\chi_i(x_j) = \delta_{i,j}$. Then $\{\chi_i\}_{i=1,\ldots,n}$ is a basis of $\mathrm{Hom}(F_n, \mathbb{F}_3) = H^1(F_n, \mathbb{F}_3)$ over $\mathbb{F}_3$. We choose an isomorphism $V \cong \mathrm{Hom}(F_n, \mathbb{F}_3)$, so that b induces a pairing on $H^1(F_n, \mathbb{F}_3)$. Let $r \in F_n$ be an element in $F_n^{(1)}$ such that

$$r \equiv x_1^Q \prod_{1 \leq i < j \leq n} [x_i, x_j]^{b(\chi_i, \chi_j)} \pmod{F_n^{(2)}}$$

and let N be the closed normal hull of the subgroup of F_n generated by r. By verifying conditions (a)–(c) above, one can show that F_n/N is a Demuškin group with invariants n and Q and whose alternating pairing on $H^1(F_n, \mathbb{F}_3)$ is the one induced from the blinear form b, cf. [**8**, § 3].

We now add the structure of an action of a finite group G of order prime to 3 to a pro 3-Demuškin group. Observe that all $\mathbb{F}_3[G]$-modules are self-dual, as follows from character theory since $3 \nmid \#G$. The following is the specialization of [**1**, 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 $H^1(D, \mathbb{F}_3)$. The cup product pairing*

$$\cup\colon H^1(D,\mathbb{F}_3) \times H^1(D,\mathbb{F}_3) \to H^2(D,\mathbb{F}_3) \cong \mathbb{F}_3 \tag{1}$$

is G-equivariant.

Conversely suppose that V and T are finite modules over $\mathbb{F}_3[G]$ with $\dim_{\mathbb{F}_3} T = 1$ 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 $Q \in 3^{\mathbb{N}} \cup \{0\}$ there exists a Demuškin group D with invariants $n = \dim V$ and Q such that the $\mathbb{F}_3[G]$-module $H^1(D,\mathbb{F}_3)$ is isomorphic to V. In this case there is a G-equivariant isomorphism between b and the pairing (1).

As recalled above, for $K \in \{E, L_0\}$ the group P_K is a pro-3 Demuškin group. The invariant Q is 3 since $\zeta_9 \notin K$. By [**5**], the isomorphism type of $V^* \cong P_K/P_K^{(1)}$ as a $G = \mathrm{Gal}(K/\mathbb{Q}_3)$-module is $\mathbb{F}_3[G] \oplus \mathbb{F}_3 \oplus \mathbb{F}_3^{\chi_3}$, where $\mathbb{F}_3$ without a superscript denotes the trivial G-module of dimension 1. The G-module structure of $T = H^2(G_K, \mathbb{F}_3)$ is easily identified with $\mathbb{F}^{\chi_3^{-1}}$, so that in a topological presentation of P_K the action of G on a suitable generator of the normal subgroup of relations is via χ_3.

A constraint on the pairing in Theorem 3.1 (and the only one) for Demuškin groups D of the form P_k, k a local field, is given by [**7**, Sätze 6, 9, 10]: The $\mathbb{F}_3[G]$-module $P_K/P_K^{(1)}$ is isomorphic to a direct sum $(\mathbb{F}_3 \oplus U) \oplus (\mathbb{F}_3^{\chi_3} \oplus V)$ 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 $H^1(G_K, \mathbb{F}_3)$ into 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 $\mathbb{F}_3[G]$-module and the same target T are isomorphic. Based on this, we now construct explicit models for the groups P_K:

Suppose first that $\bar{\rho} = \bar{\rho}_1$. Recall that $G = \mathrm{Gal}(E/\mathbb{Q}_3) = \{1, \sigma\}$. On the free pro-3 group F_4 on 4 topological generators $x_1, \ldots, x_4$ consider the following 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 $\mathbb{F}_3^4$—according to the definition of our action, this form is G-equivariant. We have

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

here we use that $F_4^{(1)}/F_4^{(2)}$ is abelian and that $[g^{-1}, h] = g^{-1}hgh^{-1} \equiv hgh^{-1}g^{-1} = [h, g] \pmod{F_4^{(2)}}$. 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 by [**1**, Prop. 3.6] the subgroup N_0 is not preserved under G. To remedy this, following [**1**, Example 3.7] 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 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 $H := \mathrm{Gal}(L/\mathbb{Q}_3)$ 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 ϱ, σ act as follows on $L = \mathbb{Q}_3(\zeta_4, \sqrt[4]{3})$:

$$\varrho(\zeta_4) = \zeta_4, \quad \varrho(\sqrt[4]{3}) = \zeta_4\sqrt[4]{3}, \quad \sigma(\zeta_4) = -\zeta_4, \quad \sigma(\sqrt[4]{3}) = \sqrt[4]{3}.$$

The quotient $G := \mathrm{Gal}(L_0/\mathbb{Q}_3)$ of H is a Klein 4-group. By $\bar\varrho$ and $\bar\sigma$ we denote the restrictions of ϱ and σ to $L_0 = \mathbb{Q}_3(\zeta_4, \sqrt{3})$, 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 $\zeta_3 = 1/2(-1 + \zeta_4\sqrt{3})$, we have

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

The irreducible $\mathbb{F}_3[G]$-modules are $\mathbb{F}_3$, $\mathbb{F}_3^{\chi_3}$, $\mathbb{F}_3^{\omega_1}$, $\mathbb{F}_3^{\chi_3\omega_1}$. Thus

$$P_{L_0}/P_{L_0}^{(1)} \cong \mathbb{F}_3^{\chi_3} \oplus \mathbb{F}_3 \oplus \mathbb{F}_3^{\chi_3} \oplus \mathbb{F}_3 \oplus \mathbb{F}_3^{\omega_1} \oplus \mathbb{F}_3^{\omega_1\chi_3}$$

as an $\mathbb{F}_3[G]$-module. On the duals of $\mathbb{F}_3 \oplus \mathbb{F}_3^{\chi_3}$ and $\mathbb{F}_3^{\omega_1} \oplus \mathbb{F}_3^{\omega_1\chi_3}$ 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 $\omega_1(\bar\sigma) = \chi_3\omega_1(\bar\varrho) = 1$.

Let now F_6 be the free pro-3 group on topological generators $x_1, \ldots, x_6$. The following table describes an 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:

(2)

	x_1	x_2	x_3	x_4	x_5	x_6
$\bar\varrho$	x_1^{-1}	x_2	x_3^{-1}	x_4	x_5^{-1}	x_6
$\bar\sigma$	x_1^{-1}	x_2	x_3^{-1}	x_4	x_5	x_6^{-1}

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

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

As before, by [**1**, Prop. 3.6] this cannot work. We define $r_1 := r_0\bar\sigma(r_0^{-1})$ and

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

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

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

and

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

Hence 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 Demuškin group:

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

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

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 in the residually reducible case

To prove Theorem 1.1, we determine $\mathrm{EH}_1(R) \subset \mathrm{Hom}_{G,\mathrm{cont}}(P_E, \tilde{\Gamma}(R))$ for any ring $R \in \mathrm{CNL}_q$. By Lemma 3.2 we may use the pro-3 group F_4/N_4 with its G-action from Lemma 3.2 as a model for P_E.

Let α be in $\mathrm{EH}_1(R)$ and denote by $A_i \in \tilde{\Gamma}(R) \subset \mathrm{GL}_2(R)$ the image of $x_i \in F_4$, $i = 1,\dots,4$, under α. We assume (without loss of generality) that $\gamma_1(\sigma) = s := \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}_q)$. Then the G-equivariance of α 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

$$A_1 = \begin{pmatrix} \sqrt{1+bc} & b \\ c & \sqrt{1+bc} \end{pmatrix}, \; A_2 = \sqrt{1+a}\begin{pmatrix} \sqrt{1+d} & 0 \\ 0 & \sqrt{1+d}^{-1} \end{pmatrix},$$

$$A_3 = \begin{pmatrix} \sqrt{1+b'c'} & b' \\ c' & \sqrt{1+b'c'} \end{pmatrix}, \; A_4 = \sqrt{1+a'}\begin{pmatrix} \sqrt{1+d'} & 0 \\ 0 & \sqrt{1+d'}^{-1} \end{pmatrix};$$

here $a, a', c, c', d, d' \in \mathfrak{m}_R$ and $b, b' \in R$—whether b or b' lie in $\mathfrak{m}_R$ depends on $\bar{\rho}_1$. The image of the explicit relation r under the homomorphism $F_4 \to \tilde{\Gamma}(R)$ induced by α 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 $\bar{\sigma}(\_)^{-1}$, so that $B = \left(\begin{smallmatrix} \sqrt{1+UV} & U \\ V & \sqrt{1+UV} \end{smallmatrix}\right)$ for suitable $U, V \in \mathfrak{m}_R$ which are formal expressions in b, b', c, c', d, d'. Conversely, given any 4-tuple of matrices $A_1, \dots, A_4$ 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 $\bar{\rho}_1(x_1), \bar{\rho}_1(x_3)$, respectively. Then this 4-tuple determines a G-equivariant homomorphism $\alpha \in \mathrm{EH}_1(R)$ if and only if the $(1,2)$- and $(2,1)$-entries of B, as defined above, are zero. (By the invariance of B under $\bar{\sigma}(\_)^{-1}$ 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 $\bar{\sigma}(\_)^{-1}$, 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 β in the definition of $\bar{\rho}_1$, we shall divide the analysis of the functor EH_1 into three cases. By the inflation-restriction sequence and the isomorphism $P_E \cong F_4/N_4$ one has

$$H^1(G_{\mathbb{Q}_3}, \mathbb{F}_q^{\chi_3}) = \mathrm{Hom}_{\mathrm{Gal}(E/\mathbb{Q}_3)}(G_E, \mathbb{F}_q^{\chi_3}) = \mathrm{Hom}_G(F_4/N_4, \mathbb{F}_q^{\chi_3}).$$

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

(a) $\beta(x_1) \neq 0$: Here we choose $u = x_1$, so that $b = 1$ for the functor EH_1. We write $b' = \tau(b' \mod \mathfrak{m}_R) + \delta'_b$ where τ is the Teichmüller lift composed with the tautological algebra homomorphism $\mathbb{Z}_q \to R$ and δ'_b is an element of $\mathfrak{m}_R$.
(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* EH_1 *is represented by the pair* $(\tilde{R}, \tilde{\alpha})$ *which is given as follows (according to the above three cases):*

(a) $\tilde{R} = \mathbb{Z}_q[[a, a', \delta'_b, c, c', d, d']]/(B_1(1,2) - B_2(1,2), B_1(2,1) - B_2(2,1))$ *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 *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* $F_4/N_4 \to \tilde{\Gamma}(R)$ *defined by mapping* x_i *to* A_i *with* A_i *as above.*

To prove Theorem 1.1 for $\bar{\rho}_1$, 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 $\underline{r}(c, b', c', d')$. One verifies

$$\underline{r}(c, \delta_b', c', d') \equiv c^2 + 2c'd' + \beta(x_3)'cd' \pmod{(3, (c, \delta_b', c', d')^2)}.$$

Independently of $\beta(x_3)$, the polynomial $c^2 + 2c'd' + \beta(x_3)'cd'$ is irreducible in $\overline{\mathbb{F}_3}[c, c', d']$. Therefore also $\underline{r} \in \mathbb{Z}_q[[a, a', \delta_b', c, c', d']]$ is irreducible which proves that $\tilde{R} = \mathbb{Z}_q[[a, a', \delta_b', c, c', d']]/(\underline{r})$ is an integral domain.

Throughout the formal computations for case (a) one has to be aware that b' is not a variable in the maximal ideal. This makes the computations more difficult than in the 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 $\underline{r}'(b, c, c', d)$ and one verifies

$$-\underline{r}'(c, b', c', d') \equiv 3c - 2cd + 3bc' + c^2b + cd^2 - bc'd \pmod{(3, b, c, c', d)^4}.$$

The factorization $-\underline{r}'(c, b', c', d') \equiv 3c - 2cd = c(3 - 2d) \pmod{(3, b, c, c', d)^3}$ of $\underline{r}'$ is the unique one modulo $\mathfrak{m}^3$ where $\mathfrak{m}$ 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 $\mathfrak{m}^4$ and hence $\underline{r}'$ is irreducible. Again we deduce that $\tilde{R} = \mathbb{Z}_q[[a, a', b, c, c', d']]/(\underline{r}')$ is an integral domain.

Case (c). — Now b, b' lie in the maximal ideal $S := \mathbb{Z}_q[[a, a', b, b', c, c', d, d']]$ and one verifies

$$\underline{r}_1 := B_1(1,2) - B_2(1,2) \equiv bd + b'd' \pmod{(3, (b, b', c, c', d, d')^2)},$$

$$\underline{r}_2 := B_1(2,1) - B_2(2,1) \equiv cd + c'd' \pmod{(3, (b, b', c, c', d, d')^2)}.$$

We claim that $\bar{R} := S/(3, \underline{r}_1, \underline{r}_2)$ is an integral domain of Krull dimension 6. Assuming the claim for the moment, the following argument shows that $\tilde{R} = S/(\underline{r}_1, \underline{r}_2)$ is an integral domain: Consider the graded ring $\mathrm{gr}_{3\tilde{R}}(\tilde{R}) := \oplus_{n \geq 0} 3^n \tilde{R}/3^{n+1}\tilde{R}$. As $\dim S - \dim \bar{R} = 3$, the sequence 3, $\underline{r}_1$, $\underline{r}_2$ is regular, and so the element $3 \in \tilde{R} = R/(\underline{r}_1, \underline{r}_2)$ is a non-zero-divisor. Hence $\mathrm{gr}_{3\tilde{R}}(\tilde{R})$ is the polynomial ring $\bar{R}[X]$. By the claim this is an integral domain. But if the associated graded ring (of the ideal $3\tilde{R}$) is an integral domain, then so is $\tilde{R}$. It also follows that $\tilde{R}$ is a complete intersection of relative dimension 6 over $\mathbb{Z}_q$.

To prove the claim, we define $\bar{\mathfrak{n}}$ as the maximal ideal of $\bar{S} := \mathbb{F}_q[[a, a', b, b', c, c', d, d']]$ and $\bar{\mathfrak{m}}$ as the maximal ideal of $\bar{R}$. There is an obvious surjection between graded rings

$$\mathbb{F}_q[a, a', b, b', c, c', d, d'] \cong \mathrm{gr}_{\bar{\mathfrak{n}}}(\bar{S}) \to \mathrm{gr}_{\bar{\mathfrak{m}}}(\bar{R})$$

and one verifies that its kernel is generated by the "initial terms" of the reductions of $\underline{r}_1$, $\underline{r}_2$ modulo 3, i.e. by $bd + b'd'$ and $cd + c'd'$. It will suffice to show that $\mathbb{F}_q[a, a', b, b', c, c', d, d']/(bd + b'd', cd + c'd')$ is an integral domain of dimension 6: If this is proved $\mathrm{gr}_{\bar{\mathfrak{m}}}(\bar{R})$ and thus also $\bar{R}$ will have dimension 6 and will be an integral domain. Finally, to see that $\mathbb{F}_q[a, a', b, b', c, c', d, d']/(bd + b'd', cd + c'd')$ is an integral domain of the asserted dimension observe that $\mathbb{F}_q[b, b', c, c', d, d']/(bd + b'd', cd + c'd')$ is an integral domain of Krull dimension 4 since it is a subring of

$$\mathbb{F}_q[b^{\pm 1}, c^{\pm 1}, d^{\pm 1}, b'^{\pm 1}, c'^{\pm 1}, d'^{\pm 1}]/(\tfrac{b}{b'} + \tfrac{d'}{d}, \tfrac{c}{c'} + \tfrac{d'}{d}) \cong \mathbb{F}_q[b^{\pm 1}, c^{\pm 1}, d^{\pm 1}, b'^{\pm 1}]$$

under the obvious monomorphism and since both rings have the same fraction fields.

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

Theorem 4.2. — *Under the hypotheses of Theorem 4.1, in all three cases (a)–(c) 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 the main theorem for the residually dihedral case

Finally we investigate the functor EH_2. Using the model F_6/N_6 for P_{L_0} from Lemma 3.3, for any $R \in \mathrm{CNL}_q$ we have $\mathrm{EH}_2(R) = \mathrm{Hom}_{G,\mathrm{cont}}(F_6/N_6, \Gamma(R))$. To further compute this, we make the following choice for the lift λ_2 of H to $\mathrm{GL}_2(\mathbb{Z}_3)$: We take $\lambda_2(\rho) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $\lambda_2(\sigma) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

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

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

One deduces

$$A_1 = \left(\begin{smallmatrix} \sqrt{1+d} & 0 \\ 0 & \sqrt{1+d}^{-1} \end{smallmatrix}\right), A_2 = (1+a)\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), A_3 = \left(\begin{smallmatrix} \sqrt{1+d'} & 0 \\ 0 & \sqrt{1+d'}^{-1} \end{smallmatrix}\right),$$
$$A_4 = (1+a')\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), A_5 = \left(\begin{smallmatrix} \sqrt{1+b^2} & b \\ b & \sqrt{1+b^2} \end{smallmatrix}\right), A_6 = \left(\begin{smallmatrix} \sqrt{1-c^2} & -c \\ c & \sqrt{1-c^2} \end{smallmatrix}\right);$$

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 α is $A_1^3[A_5, A_6]$. It follows that the image of the relation $r = 1$ under the homomorphism $F_6 \to \Gamma(R)$ induced by α is $B = B_1 B_2 \stackrel{!}{=} 1$ where

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

Since $B_1 = \alpha(r_1)$ and $B_2 = \alpha(\bar{\sigma}\bar{\varrho}(r_1))$ the matrices B_i are invariant under $\bar{\sigma}(\_)^{-1}$ and the matrix B_2 is obtained from B_1 by conjugation by $t := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. The invariance under $\bar{\sigma}(\_)^{-1}$ implies that in any case B_1 is of the form $\left(\begin{smallmatrix} 1+U & -V \\ V & (1-V^2)/(1+U) \end{smallmatrix}\right)$ for $U, V \in \mathfrak{m}_R$ which are expressions in terms of b, c, d. The condition $r \stackrel{!}{=} 1$ turns under α into the condition $B_1^{-1} = tB_1t^{-1}$ in $\mathrm{GL}_2(R)$. 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_6.

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* b,c,d. *The homomorphism* $\tilde{\alpha}: F_6/N_6 \to \Gamma(R)$ *is defined by mapping* x_i *to* A_i *with* A_i *as above.*

To prove Theorem 1.1 for $\bar{\rho}_2$, 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:

$$\begin{pmatrix} (1+d)^3\left(1+8b^2c^2(1-c^2)+4bc\sqrt{(1+b^2)(1-c^2)(1+4b^2c^2)}\right) & -4b^2c(1+2c^2+4b^2c^2)\sqrt{(1-c^2)} \\ 4b^2c(1+2c^2+4b^2c^2)\sqrt{(1-c^2)} & (1+d)^3\left(1+8b^2c^2(1-c^2)-4bc\sqrt{(1+b^2)(1-c^2)}(1+4b^2c^2)\right) \end{pmatrix}$$

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

$$\underline{r} := (1+d)^6\left(1+8b^2c^2(1-c^2)+4bc\sqrt{(1+b^2)(1-c^2)}(1+4b^2c^2)\right)-\left(1+8b^2c^2(1-c^2)-4bc\sqrt{(1+b^2)(1-c^2)}(1+4b^2c^2)\right).$$

Modulo $(3,\mathfrak{m}^4)$ for $\mathfrak{m}$ the maximal ideal of $\mathbb{Z}_3[[a,a',b,c,d,d']]$ we find $\underline{r}\equiv -bc-d^3$. Therefore the image of $\underline{r}$ in $\mathbb{F}_3[[a,a',b,c,d,d']]$ is irreducible and so is $\underline{r}$. It follows that $\mathbb{Z}_3[[a,a',b,c,d,d']]//(\underline{r})$ 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 $\bar{\rho}_2$.

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

[1] G. Böckle – "Demuškin groups with group actions and applications to deformations of Galois representations", *Compositio Math.* **121** (2000), p. 109–154.

[2] N. Boston – "Explicit deformation of Galois representations", *Invent. Math.* **103** (1991), p. 181–196.

[3] P. Colmez – "Représentations triangulines de dimension 2", *Astérisque* **319** (2008), p. 213–258.

[4] ———, "Représentations de $\mathrm{GL}_2(\mathbf{Q}_p)$ et (φ,Γ)-modules", this volume.

[5] K. Iwasawa – "On Galois groups of local fields", *Trans. Amer. Math. Soc.* **80** (1955), p. 448–469.

[6] M. Kisin – "Deformations of $G_{\mathbf{Q}_p}$ and $\mathrm{GL}_2(\mathbf{Q}_p)$ representations", this volume.

[7] H. Koch – "Über Darstellungsräume und die Struktur der multiplikativen Gruppe eines p-adischen Zahlkörpers", *Math. Nachr.* **26** (1963), p. 67–100.

[8] J. P. Labute – "Classification of Demushkin groups", *Canad. J. Math.* **19** (1967), p. 106–132.

[9] B. Mazur – "Deforming Galois representations", in *Galois groups over* $\mathbf{Q}$ *(Berkeley, CA, 1987)*, Math. Sci. Res. Inst. Publ., vol. 16, Springer, 1989, p. 385–437.

[10] L. C. WASHINGTON – "Galois cohomology", in *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, Springer, 1997, p. 101–120.

G. BÖCKLE, Fakultät für Mathematik, Universität Duisburg-Essen, 45117 Essen, Germany
E-mail : gebhard.boeckle@uni-due.de