Compositio Mathematica **121:** 109–154, 2000.

Demuškin Groups with Group Actions and Applications to Deformations of Galois Representations

GEBHARD BÖCKLE
ETH Zürich, Departement Mathematik, HG G 66.4, Rämistrasse 101, CH8092 Zürich, Switzerland. e-mail: boeckle@math.ethz.ch

(Received: 24 December 1997; final version: 29 September 1998)

Abstract. We determine the universal deformation ring, in the sense of Mazur, of a residual representation $\bar{\rho}\colon G_K \to \mathrm{GL}_2(k)$, where k is a finite field of characteristic p and K is a local field of residue characteristic p. As one might hope for, but is not proven in the global case, the deformation ring is a complete intersection, flat over $W(k)$, with the exact number of equations given by the dimension of $H^2(G_K, \mathrm{ad}_{\bar{\rho}})$.

We then go on to determine the ordinary locus inside the deformation space and, using ideas of Mazur, apply this to compare the universal and the universal ordinary deformation spaces. Provided that the universal ring for ordinary deformations with fixed determinant is finite flat over $W(k)$, as was shown in many cases by Diamond, Fujiwara, Taylor–Wiles and Wiles, we show that the corresponding universal deformation ring – with no restriction of ordinariness or fixed determinant – is a complete intersection, finite flat over $W(k)$ of the dimension conjectured by Mazur, provided that the restriction of $\det(\bar{\rho})$ to the inertia subgroup is different from the inverse cyclotomic character.

Mathematics Subject Classifications (2000): Primary 11F33, 11S20, 20F05; Secondary 11F80, 11F85, 20G25.

Key words: Demuškin groups, G-equivariant presentations, Galois groups of local fields, Galois representations, deformation theory, ordinary deformations, modular forms.

1. Introduction

If one is given a representation $\bar{\rho}\colon G_K \to \mathrm{GL}_2(k)$, where K is a global field, k a finite field of characteristic $p > 2$, and G_K the absolute Galois group of K, and one tries to investigate deformations of this representation unramified outside a finite set of places, as in [Maz1], one finds that under some natural hypothesis, which are that the centraliser of $\mathrm{Im}(\bar{\rho})$ is precisely the set of homotheties, there is a universal deformation, and that the universal ring is a power series ring over $W(k)$, the ring of Witt vectors over k, modulo some relations that often come from the obstructions of the associated local deformation problems $\bar{\rho}_{\mathfrak{p}}\colon G_{K_{\mathfrak{p}}} \to \mathrm{GL}_2(k)$, where $\mathfrak{p}$ is a finite place of K. For this reason, we shall study here the local case rather thoroughly keeping possible applications to the global case in mind, e.g. Corollary 9.1.

In [Bos2] the problem of finding the universal deformation for $\bar{\rho}_{\mathfrak{p}}$ – or a smooth cover of it whose precise definition we shall give in Section 2 – was implicitly solved in the case where the image of $\bar{\rho}_{\mathfrak{p}}$ in $\mathrm{PGL}_2(k)$ contains elements of order prime to p and where the characteristic of the residue field of $K_{\mathfrak{p}}$ was different from p. The group theoretic problem involved was to consider a pro-p group with two generators and one relation. Furthermore, in [Bos1, §8] a special example was treated where the residue characteristic was equal to 3 and the pro-3 group involved was a Demuškin group on four generators. Yet the general problem was not pursued any further.

Here we will reconsider the problem of finding the universal deformation, or a smooth cover of it, in the local case where the relevant pro-p group is an arbitrary Demuškin group. We will mainly focus on the case that the image of $\bar{\rho}_{\mathfrak{p}}$ in $\mathrm{PGL}_2(k)$ contains an element of order prime to p, and only briefly discuss in the end the other case where our results are less explicit. The Demuškin group in question is the Galois group of the maximal pro-p Galois extension of $F_{\mathfrak{P}}$ where F corresponds to the inverse image under $\bar{\rho}$ of the p-Sylow subgroup of $\mathrm{Im}(\bar{\rho})$, and where $\mathfrak{P}$ is a prime in F above $\mathfrak{p}$. Further, we assume that $H^2(G_{K_{\mathfrak{p}}}, \mathrm{ad}_{\bar{\rho}}) \neq 0$ where $\mathrm{ad}_{\bar{\rho}}$ is the adjoint representation of $\mathrm{GL}_2(k)$ on $M_2(k)$ composed with $\bar{\rho}$, as otherwise there are no local obstructions, and hence the universal deformation ring is simply a power series ring over $W(k)$. We shall solve the problem of finding the universal deformation ring and determining the images of generators under the universal deformation modulo triple commutators completely, see Theorems 2.6 and 6.2. In all cases, the universal ring will be a complete intersection, flat over $W(k)$, and of the dimension that one might expect from the estimate given in Proposition 2 of [Maz1].

Next we shall calculate the ordinary locus of the deformation space we consider, see Corollary 7.4. This we apply to generalise [Maz2] to deformations over arbitrary global fields, not just $\mathbb{Q}$, and to more general residual representations, and, following an idea of [Maz3], we shall describe the consequences for the global universal deformation ring in light of recent results by Diamond, Fujiwara, Hida, Taylor and Wiles, as described in the abstract, see Corollary 9.8.

The organisation of the paper is as follows. In Section 2 we will define the universal deformation problem that we will study here. In the cases we consider, the image of $\bar{\rho}$ will be solvable, and so we will, following [Bos1, §6, §9], rewrite the problem in terms of G-equivariant homomorphisms from a pro-p Demuškin group to $\mathrm{GL}_2(R)$ satisfying some additional constraints, where R is a complete Noetherian local ring with residue field k. Then we will state a preliminary description of the universal deformation space, and give an outline of the steps necessary to obtain it.

In the next section we shall classify Demuškin groups with groups G of order prime to p acting on them and also morphisms from such groups into general pro-p groups. For the latter it is important to observe that, in a sense, it suffices to consider the relations modulo the third step of the lower q-central series, Proposition 3.8. For a similar result see [Win, Satz 2]. We will also address the natural question

if there is some kind of nice Demuškin relation for a nice set of generators compatible with the group action. For many cases we shall show that one cannot expect the usual relation. For $G = C_2$ however, we shall find a simple nice relation in terms of suitable generators.

Section 4 contains the relevant facts we need about the Hilbert pairing for local Galois groups, some general facts about symplectic spaces, of which the Hilbert pairing is a special example, and the explicit calculations of those pairings needed later on. In Section 5, we shall study closed pro-p subgroups H of $\mathrm{GL}_2(R)$, R complete, Noetherian, local with residue field k. Mainly we shall need some information about the first and second subquotient of the lower central series of H, in order to describe the Demuškin relation modulo the third step of the lower central series. Explicit calculations of Pink and an idea of Lazard, that the category of p-nilpotent p-groups is equivalent to that of p-nilpotent p-Lie algebras, facilitate the computations greatly. The subsequent section contains the precise description of the universal deformation spaces that we want to compute, and its proof.

In Section 7 we shall apply this description to find explicit equations describing the ordinary locus. The following section describes briefly the calculations and results in the case that the image of $\bar{\rho}$ in $\mathrm{PGL}_2(k)$ is a p-group.

In the last section we shall give some applications to global deformation problems. First we shall simplify and generalise an example given in [Bos1, §8]. Then – and this will occupy the major part of the last section – we shall use results by Diamond [Dia], Fujiwara [Fuji], Hida [Hida], Taylor and Wiles [TaWi] and Wiles [Wil], and an idea of Mazur, to tie together the global universal deformation space R^{univ} and the global universal ordinary deformation space with fixed determinant, $R^{\mathrm{ord},\det=\eta}$, for representations $\bar{\rho}\colon G_{M,S} \to \mathrm{GL}_2(k)$, M a totally real field, associated to an ordinary Hilbert modular form, S a finite set of places of M, containing all places above p and ∞. In all cases where they succeed in establishing an isomorphism between $R^{\mathrm{ord},\det=\eta}$ and a universal Hecke algebra $T^{\mathrm{ord},\det=\eta}$, it will follow that the universal ring is a complete intersection, flat over $W(k)$, of relative dimension $2[M:\mathbb{Q}]+1+\Delta_M$ over $W(k)$, Δ_M the defect to the Leopoldt conjecture at p for M, provided that the restriction of $\det(\bar{\rho})$ to the inertia subgroup of G_K is not the inverse cyclotomic character. For a slightly more general result, see Corollary 9.8. This is all confirming the conjectures of Mazur in [Maz1] regarding properties of the universal deformation space. Our results are consistent with the philosophy in [FoMa] that the intersection of the universal deformation ring and appropriate quotients of the local versal deformation rings at p should meet transversally.

Regarding our computations of deformations of local Galois representations, we should remark that if one could either carry out Lazard's correspondence explicitly with a good description of the resulting Lie algebra, or alternatively, if one could extend Pink's description, it might be possible to use the methods described here for representations into GL_n. An alternative approach might be to use Fontaine's (Φ,Γ)-modules, which describe arbitrary local Galois representations, in order to calculate the universal one. It might also be interesting to redo all of our calculations

in terms of (Φ, Γ)-modules, hoping that one can extend this analysis to crystalline or other types of deformations over rather general local fields.

We would like to thank N. Boston for some interesting discussions and for pointing out the calculations in [Pink] and Professor K. Wingberg for some helpful comments on presentations of Demuškin groups. Finally the referees deserve a lot of credit for many corrections and useful suggestions to improve the presentation.

2. Definition of the Deformation Problem

We start by recalling some notions concerning deformations of Galois representations. Let k be a finite field of characteristic $p > 2$, let K be any field, and $\bar{K}$ its separable closure. Let $\bar{\rho}: \mathrm{Gal}(\bar{K}/K) = G_K \to \mathrm{GL}_2(k)$ be a Galois representation, H the image of $\bar{\rho}$ inside $\mathrm{GL}_2(k)$ and L the Galois extension of K corresponding to H. The field L is called the splitting field of $\bar{\rho}$. By $G_L(p)$ we denote the maximal pro-p quotient of G_L, by $L(p)$ the corresponding pro-p extension of L. As $\mathrm{Gal}(\bar{K}/L)$ is characteristic, $L(p)$ is Galois over K. By $G_{\bar{\rho}}(p)$ we denote its Galois group over K, and so we have $1 \to G_L(p) \to G_{\bar{\rho}}(p) \to H \to 1$.

Let $\mathcal{C}$ be the category of complete Noetherian local rings $(R, \mathfrak{m})$ with residue field k and local ring homomorphisms which induce the identity on residue fields. If R is an object of $\mathcal{C}$, then it is a quotient of $W(k)[[T_1, \ldots, T_r]]$ for some r. For R in $\mathcal{C}$ we define $\Gamma_2(R) := \ker(\mathrm{GL}_2(R) \to \mathrm{GL}_2(k))$ and $\tilde{\Gamma}_2(R) \subset \mathrm{GL}_2(R)$ as the subgroup generated by $\Gamma_2(R)$ and the elements $\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$ for all $r \in R$.

Two lifts $\rho, \rho': G_K \to \mathrm{GL}_2(R)$ of $\bar{\rho}$ are called *strictly equivalent* if there is an $M \in \Gamma_2(R)$ such that $\rho = M\rho' M^{-1}$. A strict equivalence class of lifts of $\bar{\rho}$ to R is called a *deformation*. Let Π be a topologically finitely generated quotient of G_K through which $\bar{\rho}$ factors. We define the functor $\mathrm{Def}_\Pi: \mathcal{C} - - \to \mathit{Sets}$ by

$$\mathrm{Def}_\Pi(R) = \{\text{deformations of } \bar{\rho} \text{ to } R \text{ that factor through } \Pi\}.$$

THEOREM 2.1 ([Maz1]). *If the centraliser of $Im(\bar{\rho})$ is precisely the set of homotheties, then* Def_Π *is representable.*

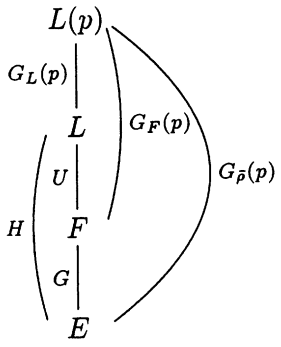
If $\mathrm{Im}(\bar{\rho})$ is solvable, one can carry out the following construction to replace Def in all relevant cases by a simpler functor. This is in particular satisfied, if K is a local field over $\mathbb{Q}_p$, or any $\mathbb{Q}_l$, and where $\Pi = G_{\bar{\rho}}(p)$. If H contains elements of order p, we can and will assume that H lies inside the set of upper triangular matrices. U will denote the set of unipotent elements of H. By the lemma of Schur-Zassenhaus, as U is a normal p-Sylow subgroup of H, we can pick a subgroup G of H of order prime to p, such that $U \rtimes G = H$.

We let F be the fixed field of U in L, and $G_F(p)$ the maximal pro-p quotient of G_F. As above we have a sequence $1 \to G_F(p) \to G_{\bar{\rho}}(p) \to G \to 1$ and also $1 \to G_L(p) \to G_F(p) \to U \to 1$. Finally we fix a lift of G to $\mathrm{GL}_2(W(k))$ and one

to $G_{\bar{\rho}}(p)$. They exist by the profinite version of Schur-Zassenhaus as $G_F(p)$ and $\tilde{\Gamma}_2(W(k))$ are pro-p groups. Via this lift, G can be viewed inside any matrix group $\mathrm{GL}_2(R)$, $R \in \mathcal{C}$ and thus acts via conjugation canonically on the latter.

We let $\{g_i : i \in \mathcal{I}\}$ denote a finite subset of $G_F(p)$ such that the elements $\bar{\rho}(g_i) = \begin{pmatrix} 1 & u_i \\ 0 & 1 \end{pmatrix}$ generate U as an H-module, where H acts by conjugation. We assume the u_i to be nonzero, so that $\mathcal{I}$ is empty if U is trivial. If $\mathcal{I}$ is non-empty, then we shall assume that $\mathcal{I} = \{1, \ldots, |\mathcal{I}|\}$. Furthermore, if $\mathcal{I}$ is non-empty, by conjugating $\bar{\rho}$ if necessary, we shall assume that that $u_1 = 1$. For each u_i we choose a lift $\hat{u}_i$ to $W(k)$, with the only requirement that $\hat{u}_1 = 1$. We shall also assume that k is large enough so that any element of $\mathrm{Im}(\bar{\rho})$ of order prime to p can be diagonalised. This can be done without loss of generality, and it simplifies the calculations in the dihedral case.

Henceforth, up to Section 8, we shall assume that the image of H in $\mathrm{PGL}_2(k)$ contains a non-trivial element of order prime to p. The following diagram summarises all relevant fields and Galois groups.



We now define the functor E_Π by

$$E_\Pi(R) := \{\alpha \in \mathrm{Hom}_G(G_F(p), \tilde{\Gamma}_2(R)) : \alpha(g_1) \text{ has (1,2) entry equal to 1 if } \mathcal{I} \neq \emptyset,$$
$$\alpha(g_i) \equiv \begin{pmatrix} 1 & u_i \\ 0 & 1 \end{pmatrix} \pmod{\mathfrak{m}} \text{ for all } i \in \mathcal{I}, \text{ and } \alpha \text{ factors through } \Pi\},$$

where the G action on $G_F(p)$ and $\mathrm{GL}_2(R)$ is described above. In particular if U is trivial, i.e. $G = H$, and if $\Pi = G_{\bar{\rho}}(p)$, then $E_\Pi(R) = \mathrm{Hom}_H(G_L(p), \Gamma_2(R))$.

Remark 2.2. If the image $\bar{G}$ of G in $\mathrm{PGL}_2(k)$ is trivial, but U is non-trivial, we define E_Π as above however we require that $\alpha(g_1)$ have both, its $(1,1)$-entry and its $(1,2)$-entry equal to one. We will use this functor in Section 8 where we briefly discuss the case where U is non-trivial, but $\bar{G}$ is trivial. There we will find that this is also a convenient choice for computing the ordinary quotient of the universal deformation

ring. If the image of H in $\mathrm{PGL}_2(k)$ is trivial alltogether, then $E_\Pi(R) = Hom(G_L(p), \Gamma_2(R))$.

The following proposition is easily derived from [Bos1, §6,9].

PROPOSITION 2.3. *The obvious morphism $E_\Pi \to \mathrm{Def}_\Pi$ is smooth, i.e. for any surjection $S \to R$ in $\mathcal{C}$, the morphism $E_\Pi(S) \to E_\Pi(R) \times_{\mathrm{Def}_\Pi(R)} \mathrm{Def}_\Pi(S)$ is surjective. It is an isomorphism if the centralizer of the image of H in $\mathrm{GL}_2(k)$ is the set of scalar matrices, i.e., if U is non-trivial or if the image of H in $\mathrm{PGL}_2(k)$ is dihedral (we assume $p > 2$). The induced map on tangent spaces $t_{E_\Pi} \to t_{\mathrm{Def}_\Pi}$ is always an isomorphism, where $t_{E_\Pi} = E_\Pi(k[\varepsilon]/(\varepsilon^2))$ and similarly for Def_Π. Furthermore E_Π is always representable – even if G is trivial, or both U and G are.*

Remark 2.4. The functor that one would like to study is the functor Def_Π. As already noted in [Maz1], unfortunately this functor is not always representable (it fails to be so, if the centralizer of the image of $\bar\rho$ is strictly larger than the group of scalar matrices). On the other hand, the functor which represents all lifts of $\bar\rho$ factoring through Π, we call it Lift_Π, is always representable. Usually the induced map on tangent spaces $t_{\mathrm{Lift}_\Pi} \to t_{\mathrm{Def}_\Pi}$ is only a surjection and not an isomorphism. The functor E_Π is a rigidified version of Lift_Π – it imposes some additional constraints on the lifts. What the above proposition says is that this rigidification is optimal in the sense that E_Π is still representable, while at the same time, one has an isomorphism of tangent spaces $t_{E_\Pi} \to t_{\mathrm{Def}_\Pi}$.

Remark 2.5. If we were to choose different g_i and $\hat u_i$ however keeping the condition $\hat u_1 = 1$, then the various functors E_Π would all be isomorphic. Thus we can fix this choice conveniently in the proofs to come.

Up to Section 8 we will assume that K is a local field of characteristic zero and residue characteristic p, i.e. a finite extension of $\mathbb{Q}_p$, and that $\Pi = G_{\bar\rho}(p)$. To alleviate the notation, we shall in the following omit the subscript Π.

Given $\bar\rho$, by $\bar\alpha$ we will denote the corresponding element in $E(k)$, by (α_E, R_E) the universal pair representing the functor E, and similarly by $(\rho_{\mathrm{Def}}, R_{\mathrm{Def}})$ a pair representing Def, if it is representable. We recall from the introduction, that $\mathrm{ad} = \mathrm{ad}_{\bar\rho}$ is the representation of $\mathrm{GL}_2(k)$ on $M_2(k)$ given by the conjugation operation, composed with $\bar\rho$. It can be regarded as a $k[G]$-module via $G \subset \mathrm{GL}_2(k)$. We define $h_i = \dim_k H^i(G_K, \mathrm{ad})$ for any non-negative integer i. We can now state our first main result.

THEOREM 2.6. *The ring R_E is isomorphic to $W(k)[[T_1, \ldots, T_{h_1}]]/I$ where the ideal I is generated by exactly h_2 relations, which are transversal, and described explicitly in Theorem 6.2. R_E is a complete intersection and flat over $W(k)$. Furthermore the universal homomorphism α_E can be described explicitly modulo triple commutators.*

Remark 2.7. Using Proposition 2.3 this theorem calculates the universal deformation $(\rho_{\mathrm{Def}}, R_{\mathrm{Def}})$ in all cases in which Def is representable. Also when starting with a global deformation problem that is representable, one can always – but not necessarily canonically – define a map from the global deformation functor to the local functor E_Π where Π is any given absolute local Galois group.

Remark 2.8. We are now about to embark on an outline of the proof. This outline will hopefully serve two purposes. On the one hand, it wants to give the reader an idea about the structure of the proof and the necessary steps to be carried out. We apologize that at this point not all the terms are properly defined. They will be while carrying out the program sketched. On the other hand, we shall at the end not repeat this sketch, but only fill in the necessary details. So for example before reading the proof of Theorem 6.2 it is advisable to first review this outline.

Proof (Outline). From the definition of E it is clear that we need to analyze the G-equivariant homomorphisms from $G_F(p)$ to $\tilde{\Gamma}_2(R)$ that agree with $\bar{\alpha}$ modulo $\mathfrak{m}$ and satisfy some further condition if U is non-trivial.

If $G_F(p)$ is free, it follows by Lemma 3.2 that one can lift the decomposition $\oplus V_i$ of the Frattini quotient of $G_F(p)$ into irreducible $\mathbf{F}_p[G]$-modules, to a corresponding free product decomposition of $G_F(p)$ with free pro-p factors P_i where the P_i carry a G action and the Frattini quotient of P_i equals V_i. For each P_i one can choose a single G-generator x_i, i.e. an element of P_i whose G orbit generates P_i topologically. In particular this means that $\mathbf{F}_p[G]\bar{x}_i = V_i$. The shape of the action on x_i implies a certain shape for possible images A_i in $\tilde{\Gamma}_2(R)$. By freeness of the P_i there are no further constraints on the images, and so every choice of A_i gives a homomorphism and vice versa. Finally one has to consider possibly some other constraints coming from E, like x_1 mapping to $\begin{pmatrix} * & 1 \\ * & * \end{pmatrix}$ if U is non-trivial. So we will need to know the G-module structure of $G_F(p)$ which will be recalled in Theorem 4.1, and we will need some lemmas about good choices of images that will be provided in Lemma 5.3. The calculation is rather straightforward.

If $G_F(p)$ is not free, then it is known to be a Demuškin group, i.e., a group with a single relation that is determined by the torsion part $\mathbb{Z}/(p^n)$ of the abelianisation of $G_F(p)$ and the cohomology pairing $H^1(G_F, \mathbb{Z}/(p)) \times H^1(G_F, \mathbb{Z}/(p)) \to H^2(G_F, \mathbb{Z}/(p))$, or equivalently by giving a so-called Demuškin relation in the second part of the lower q-central series of a minimal free hull of $G_F(p)$. The number $q = p^n$ is the number of p-power roots of unity contained in F. This will be recalled in Theorem 4.1.

As in the previous case, one can pick G-generators x_i that correspond to the pieces of the decomposition $\oplus V_i$ of the Frattini quotient into irreducible $\mathbf{F}_p[G]$-modules. One can even find subgroups P_i inside $G_F(p)$ as above, by the remark after Lemma 3.2. Yet we also have a relation. Hence an arbitrary assignment of A_i's as above will not necessarily define a homomorphism from the Demuškin group we consider.

Hence we need conditions on the choices of the A_i under which the image of the Demuškin relation is the identity. If we choose nice x_i w.r.t. the G action, it seems rather hopeless to find a nice form for the Demuškin relation in them, and thus for the relation in the A_i that has to be satisfied (Proposition 3.6) while on the contrary if we choose the x_i so that the relation is nice, we lose all control over the shapes of the A_i.

The way out of this dilemma is the following observation formalized in Proposition 3.8. If the A_i satisfy the Demuškin relation modulo the third step of the lower q-central series of the subgroup generated by all A_i, then one can find an element r in the second step $\mathcal{F}^{(2,q)}$ of the lower q-central series of a free pro-p group $\mathcal{F}$ with the right number of generators that has the shape of a Demuškin relation and that is mapped to the identity under $x_i \mapsto A_i$. This can all be done G-equivariantly, and one has a classification of Demuškin groups with a G action – where the order of G is prime to p – which says that this Demuškin group is isomorphic to the original one (Theorem 3.4). One can interpret this as follows. One can G-equivariantly replace the x_i by x_i' that agree with the x_i in the Frattini quotient such that the map $x_i' \mapsto A_i$ is a well-defined homomorphism. As we only want to construct a universal, i.e. a sufficiently general, homomorphism (α_E, R_E), controlling homomorphisms up to this degree will suffice. Essentially the original problem is thus reduced to a calculation modulo triple and higher commutators which can be carried out. That this calculation is indeed sufficient will be checked at the end – c.f. the last paragraph of this overview for the method used to accomplish this.

To perform the above calculation, we first need to understand the Demuškin relation in $\mathcal{F}$ modulo $\mathcal{F}^{(3,q)}$ for a free group $\mathcal{F}$ mapping G-equivariantly to $G_F(p)$ with the same number of generators, i.e. we need to understand the Hilbert pairing. The results will be recalled in Theorem 4.2. In Section 4.2, we shall also recall some general facts on symplectic modules and determine the relevant hyperbolic pairings explicitly, i.e. G-equivariant pairings, for G cyclic or dihedral, between absolutely irreducible $k'[G]$-modules, k' the minimal field over $\mathbf{F}_p$ so that a given $\mathbf{F}_p[G]$ representation decomposes into absolutely irreducible components.

The next step is to understand P modulo $P^{(3,q)}$ for P a closed subgroup of $\tilde{\Gamma}_2(R)$. Again in general this is quite hard despite some encouraging results by Pink (Theorem 5.4) but due to the shape of the A_i given in Lemma 5.3, it is sufficient to do this for certain subgroups. For those the results of Pink do allow a simple calculation. At this point there is another idea, of Lazard, that comes into play. It says that there is a rather simple equivalence between p-nilpotent p-groups and p-nilpotent p-Lie algebras. As $p > 2$ this applies to our situation modulo third and higher commutators. Therefore it will be enough to express the relation on the side of Lie algebras and to compute its image in Lie algebras which is exactly what can be achieved using Pink's calculation. (Strictly speaking, Lazard's results are not really needed, as the results of Pink do contain all correspondences we shall use, but it was a major guideline before being aware of Pink's results.) The advantage in working with Lie algebras is that now the image of subgroups generated by certain

A_i has naturally a $W(k)$ scalar multiplication – obviously it isn't necessarily free over $W(k)$. This happens exactly when working with a $W(k)$-structure is preferable, i.e. when the splitting field of V_i is not $\mathbf{F}_p$, but a finite extension inside k. Thus one only needs a description of pairings over the splitting field. This will all be explained in Section 5.

Having done all this, one has an explicit form for a relation among the A_i modulo some third and higher commutators. This determines an explicit ring A/I over which the relation among the A_i is satisfied (Theorem 6.2). Our preparations imply that there is a G-equivariant map in E_Π from G_K to $\mathrm{GL}_2(A/I)$. For the induced map from the universal ring R_E to A/I, one first verifies that it induces an isomorphism on mod p tangent spaces, and hence that it is surjective, and then, using Lemma 6.4, that it is injective as well. Thus the ring A/I we constructed is identified with the universal ring R_E. □

3. Demuškin Groups with Group Actions

By D we will always denote a pro-p group that is a Demuškin group. We assume throughout that $p > 2$. Being a Demuškin group is characterized by the following three properties.

(i) $n = \dim_{\mathbf{F}_p} H^1(D, \mathbb{Z}/(p)) < \infty$.
(ii) $\dim_{\mathbf{F}_p} H^2(D, \mathbb{Z}/(p)) = 1$.
(iii) The cup product pairing $H^1(D, \mathbb{Z}/(p)) \times H^1(D, \mathbb{Z}/(p)) \to H^2(D, \mathbb{Z}/(p))$ is an alternating non-degenerate bilinear form.

This implies that D has n generators and one relation and so its abelianisation $D/[D, D]$ must be isomorphic to $\mathbb{Z}_p^{n-1} \times \mathbb{Z}_p/(q)$ where q is a power of p, possibly $p^\infty = 0$, that is uniquely determined by D. As $p > 2$ it is well known that n and q characterize D completely, [Dem1, Dem2, Lab].

Our first aim will be to extend this to the case where we have a group G of order prime to p acting on D. So in the following let G be such a group. The action of G on D induces an action on $H^i(D, \mathbb{Z}/(p^l))$ for all natural numbers i, l, and this action is compatible with the cup product pairing, e.g. [MacL, p. 351].

We denote for any pro-p group P its Frattini subgroup, i.e. the topological closure of $P^p[P, P]$, by $\Phi(P)$, and its Frattini quotient, i.e. $P/\Phi(P)$, by $\bar{P}$. Concerning the action of G on D, we quote the following Lemma from [Bos1, §2].

LEMMA 3.1. *Given two actions of G on the pro-p group P such that the actions on the Frattini quotient $\bar{P}$ agree, then the actions agree up to an inner automorphism of P.*

Furthermore, if an action of G on $\bar{P}$ is given, i.e. a homomorphism from G to $\mathrm{Aut}(\bar{P})$, and if the image of G under this homomorphism is in the image of $\mathrm{Aut}(P) \to \mathrm{Aut}(\bar{P})$, then there exists up to conjugation a unique G operation on P extending the one on $\bar{P}$.

As a consequence, the action of G on D is already uniquely determined, up to an inner automorphism, by the action on the Frattini quotient $\bar{D}$. Furthermore, $H^1(D, \mathbb{Z}/(p)) = Hom(\bar{D}, \mathbb{Z}/(p))$, and thus this action is also determined by the action of G on $H^1(D, \mathbb{Z}/(p))$. This suggests that in fact any Demuškin group with a group action corresponds to a bilinear pairing with a group action and an invariant q and vice versa, which will be shown below.

Let χ^{-1} be the character by which G acts on $H^2(D, \mathbb{Z}/(p))$. As is well known $H^2(D, \mathbb{Z}/(p)) \cong Hom(\mathcal{R}/[\mathcal{R}, \mathcal{F}], \mathbb{Z}/(p))$ if

$$1 \to \mathcal{R} \to \mathcal{F} \to D \to 1 \tag{1}$$

is a presentation of D where $\mathcal{F}$ a free pro-p group with n generators. As is shown in the proof of [Bos1, Lemma 2.5], one can assume this sequence to be compatible with the G operation. So G acts on $\mathcal{R}/([\mathcal{F}, \mathcal{R}]\mathcal{R}^p) \cong \mathbb{Z}/(p)$ via χ. As $\mathcal{R}$ is one-generated as a normal subgroup, by which we mean that there is an element r of $\mathcal{F}$ whose normal topologically closed hull is $\mathcal{R}$, $\mathcal{R}/[\mathcal{R}, \mathcal{F}] \cong \mathbb{Z}_p$. By Lemma 3.1, the G action on it is given as the lift of χ to $\mathbb{Z}_p^*$ via the Teichmüller character, which will also be denoted by χ.

In the case that $q \neq 0$, we consider the G-equivariant sequence

$$1 \to \mathcal{R}/[\mathcal{R}, \mathcal{F}] \cong \mathbb{Z}_p \to \mathcal{F}^{ab} = \mathcal{F}/[\mathcal{F}, \mathcal{F}] \cong \mathbb{Z}_p^n \to D/[D, D] \cong \mathbb{Z}_p^{n-1} \times \mathbb{Z}_p/(q) \to 1$$

that can be obtained as the inverse limit of the inflation-restriction sequence associated to the sequence (1) with coefficients $\mathbb{Z}/(p^l)$, l going to ∞. Using the decomposition of the projective $\mathbb{Z}_p[G]$-module $\mathcal{F}^{ab}$ into irreducible summands, one may assume that $\mathcal{R}/[\mathcal{R}, \mathcal{F}]$ maps into exactly one of them with index q. Thus the action of G on the torsion part $\mathbb{Z}/(q)$, that has to be fixed by G, is also given by χ.

To prove the main result of this section, we need the following group theoretical lemma which is a slight generalisation of a result of [Bos1, §2].

LEMMA 3.2. *Given $\mathcal{F}$, a finitely generated free pro-p group with an action of G, and a decomposition $\mathcal{F}/(\mathcal{F}^q[\mathcal{F}, \mathcal{F}]) \cong A_1 \oplus A_2$ where the A_i are projective $\mathbb{Z}_p/(q)[G]$-modules, then $\mathcal{F} \cong \mathcal{F}_1 * \mathcal{F}_2$ where the $\mathcal{F}_i$ are free pro-p groups carrying a G action such that $\mathcal{F}_i/(\mathcal{F}_i^q[\mathcal{F}_i, \mathcal{F}_i]) \cong A_i$.*

In particular, if $\mathcal{F}/(\mathcal{F}^q[\mathcal{F}, \mathcal{F}])$ has a free one-dimensional G invariant subgroup generated by an element $\bar{r}$, i.e., G acts on $\bar{r}$ by a character χ, then there is a lift r of it in $\mathcal{F}$ on which G acts by (the Teichmüller lift of) χ.

Proof. This is a simple modification of the proof of [Bos1, Lemma 2.4]. The key observation is that

$$\mathrm{Aut}(\mathcal{F}) \to \mathrm{Aut}(\mathcal{F}/(\mathcal{F}^q[\mathcal{F}, \mathcal{F}])) \cong \mathrm{GL}_m(\mathbb{Z}_p/(q)),$$

where m is the rank of $\mathcal{F}$, is surjective. This holds, as the image clearly contains all permutation matrices and also all invertible upper or lower triangular matrices, and hence by Bruhat decomposition all elements of $\mathrm{GL}_m(\mathbb{Z}_p/(q))$. So given A_i,

we choose a free pro-p group $\mathcal{F}_i$ with the same number of generators as A_i. The G action is given by a homomorphism to $\mathrm{Aut}(A_i)$. By the lemma of Schur-Zassenhaus this lifts to an action on $\mathcal{F}_i$. Finally by Lemma 3.1, the group $\mathcal{F}_1 * \mathcal{F}_2$ is isomorphic to $\mathcal{F}$ as they have isomorphic Frattini quotients. □

Remark 3.3. If $\mathcal{F}$ in the above lemma is not free, then as in [Bos1, Lemma 2.4] one can still find subgroups $\mathcal{F}_i$, $i = 1, 2$ with the desired quotients $\mathcal{F}_i/(\mathcal{F}_i^q[\mathcal{F}_i, \mathcal{F}_i])$, but one cannot expect $\mathcal{F}$ to be their free product any more.

The following is the main result of this section – remember $p > 2$.

THEOREM 3.4. *Let D be any Demuškin group with n generators and invariant q. If a group G of order prime to p acts on D, and we denote by V the $\mathbf{F}_p[G]$-module $H^1(D, \mathbb{Z}/(p))$ and by T the module $H^2(D, \mathbb{Z}/(p))$, then $V \times V \to T$ is a G-equivariant non-degenerate alternating bilinear form, and the action of G on the torsion subgroup of D^{ab}, which is as a group isomorphic to $\mathbb{Z}/(q)$, is given by the (Teichmüller lift of the) character χ, if χ^{-1} describes the action on T.*

Conversely, assume we are given some G-equivariant non-degenerate alternating bilinear form $\kappa : V \times V \to T$ and a number q which is either a power of p or zero (which we think of as p^∞). If $q \neq 0$, we assume that $\mathbf{F}_p^{triv}$ is a direct summand of V. Then there exists a Demuškin group D with an action of G such that this bilinear form is the one given by $H^1(D, \mathbb{Z}/(p)) \otimes H^1(D, \mathbb{Z}/(p)) \to H^2(D, \mathbb{Z}/(p))$. Furthermore this group D is unique up to isomorphism of pro-p groups with G action.

Proof. We only have to show existence and uniqueness, given the bilinear form. We shall first show the existence. By Lemma 3.1 we choose a free $\mathbb{Z}_p[G]$-module V_∞ whose Frattini quotient is isomorphic to V. Again by the same lemma we choose a free pro-p group $\mathcal{F}$ with a G action, such that the Frattini quotient $\bar{\mathcal{F}}$ of $\mathcal{F}$ is isomorphic to $Hom(V, \mathbb{Z}/(p))$ as an $\mathbf{F}_p[G]$-module. By Lemma 3.1 we shall assume that $\mathcal{F}^{ab} \cong Hom(V_\infty, \mathbb{Z}_p)$ as $\mathbb{Z}_p[G]$-modules. We now identify $Hom(\mathcal{F}^{ab}, \mathbb{Z}_p)$ and V_∞. As G is of order prime to p it is well known that the Grothendieck group of free $\mathbb{Z}_p$-modules with G action is isomorphic to that of $\mathbf{F}_p$ vector spaces with G action. So the bilinear form κ considered as an element of $Hom_G(V \wedge V, \mathbf{F}_p^{\chi^{-1}})$ can be lifted to a G-equivariant non-degenerate alternating bilinear form $V_\infty \times V_\infty \to \mathbb{Z}_p^{\chi^{-1}}$. Dually we find a G-equivariant map $\phi : \mathbb{Z}_p^{\chi} \to \mathcal{F}^{ab} \wedge \mathcal{F}^{ab}$. By V_m, $\mathcal{F}_m^{ab}$, ϕ_m etc., we denote $V_\infty/(m)$, $\mathcal{F}^{ab}/(m)$, $\phi/(m)$, etc. We also note that the character χ always appears when we are 'on the side of groups', e.g. as the action of G on $\mathcal{R}/[\mathcal{F}, \mathcal{R}]\mathcal{R}^q$ or on the part of $\mathcal{F}_q^{ab}$ which corresponds via class field theory to p-power roots of unity, while the character χ^{-1} appears on the corresponding dual 'cohomological side', e.g. as the action on $H^2(D, \mathbb{Z}/(q))$ or on a certain piece of $H^1(D, \mathbb{Z}/(q))$.

Let $\mathcal{F}^{(i,q)}$ denote the i-th step of the lower q-central series, i.e. $\mathcal{F}^{(0,q)} = \mathcal{F}$ and $\mathcal{F}^{(i,q)} = [\mathcal{F}^{(i,q)}, \mathcal{F}](\mathcal{F}^{(i,q)})^q$. All the $\mathcal{F}^{(i,q)}$ are normal G invariant subgroups of F. It is not hard to see that $\mathcal{F}^{(2,q)}/\mathcal{F}^{(3,q)} \cong \mathcal{F}_q^{ab} \oplus (\mathcal{F}_q^{ab} \wedge \mathcal{F}_q^{ab})$ as $\mathbb{Z}_p/(q)[G]$-modules,

if $q \neq 0$, where the first copy is generated by the q-th power elements and the second by commutators. If $q = 0$, then $\mathcal{F}^{(2,q)}/\mathcal{F}^{(3,q)} \cong \mathcal{F}^{ab} \wedge \mathcal{F}^{ab}$. If $q \neq 0$, by assumption V contains a G invariant element. So we can decompose $V_\infty = \mathbb{Z}_p^{triv} \oplus \mathbb{Z}_p^{\chi^{-1}} \oplus M$ where the restriction of the given bilinear form to both, $\mathbb{Z}_p^{triv} \oplus \mathbb{Z}_p^{\chi^{-1}}$ and M, is non-degenerate. Let x, y be generators of $\mathbb{Z}_p^{\chi}$. We define the element $\bar{r}$ in $\mathcal{F}^{(2,q)}/\mathcal{F}^{(3,q)}$ as

$$\bar{r} = x \pmod q \oplus \phi_q(y \pmod q) \in \mathcal{F}_q^{ab} \oplus (\mathcal{F}_q^{ab} \wedge \mathcal{F}_q^{ab})$$

If $q = 0$, we define $\bar{r} = \phi_q(y \pmod q)$. By construction, G acts on the element $\bar{r}$ via the character χ. We shall now construct a lift r of $\bar{r}$ to $\mathcal{F}$ on which G acts again by χ.

As a characteristic subgroup of $\mathcal{F}$, $\mathcal{F}^{(2,q)}$ carries a G operation, and hence we can decompose

$$\mathcal{F}^{(2,q)}/(\mathcal{F}^{(2,q)^q}[\mathcal{F}^{(2,q)}, \mathcal{F}^{(2,q)}]) \cong \mathbb{Z}_p^{\chi}/(q) \oplus N$$

provided $q \neq 0$, where $\mathbb{Z}_p^{\chi}/(q)$ is generated by $\bar{r}$ and N is a projective $\mathbb{Z}_p/(q)[G]$-module. By the Lemma 3.2 we find a lift r of $\bar{r}$ in $\mathcal{F}^{(2,q)}$ on which G acts by χ. In the case that $q = 0$, we can, again by the Lemma 3.2, find elements $r_{p^s} \in \mathcal{F}^{(2,p^s)}$ for all $s \in \mathbb{N}$ such that G acts on them via χ and such that they are congruent to $\bar{r}$ modulo $\mathcal{F}^{(2,p^s)}$. We take any element

$$r \in C := \bigcap_{t \in \mathbb{N}} \Big(\text{closure}\{r_{p^s} : s \geqslant t\} \Big).$$

As the intersection of non-empty closed subsets in the compact group $\mathcal{F}$, the set C is non-empty. Since the set of $x \in \mathcal{F}$ satisfying $gx = x^{\chi(g)}$ is closed, all elements in C satisfy this relation. Finally the sets involved in forming the intersection of C lie in $\bar{r}\mathcal{F}^{(2,p^t)} \pmod{\mathcal{F}^{(3,0)}}$. Hence r is a lift of $\bar{r}$ as desired.

We define D to be the quotient of $\mathcal{F}$ by the closed normal subgroup generated by r. As the subgroup spanned by r is invariant under G, the normal subgroup generated by it is invariant, too, and thus D carries an action by G. By Proposition 3 in [Lab], which calculates the bilinear form $H^1(D, \mathbb{Z}/(p)) \otimes H^1(D, \mathbb{Z}/(p)) \to H^2(D, \mathbb{Z}/(p))$ explicitly, one can verify that it agrees with $\kappa : V \times V \to T$ if we choose $\bar{r}$ as above.

Finally we have to show uniqueness. Here we use again Lemma 3.1. As we know already that as pro-p groups two Demuškin groups with same invariants n and q are isomorphic, and that by assumption we have isomorphic actions of G on the Frattini quotient of D, any two such groups have to be isomorphic, the isomorphism being given by an inner automorphism – after having identified the abstract groups in such a way that the Frattini quotients agree as $\mathbf{F}_p[G]$-modules. □

Remark 3.5. The construction in the proof of Theorem 3.4 did not provide us with nice generators of the Demuškin group, that are in some way compatible with the

action of G and for which the relation, or even the relation modulo $\mathcal{F}^{(3,q)}$ has the usual form of a Demuškin relation, as we assumed nothing particular for the element $\bar{r}$. For general groups G we do not think that one is even able to choose nice generators, respecting the G operation in some way. But even if one can choose such generators, for the relation the best one should expect is a relation that has a nice expression in terms of the generators and the desired action of G via χ modulo $\mathcal{F}^{(3,q)}$.

For example, if G acts as a permutation group on the Frattini quotient a choice of nice generators is possible. Another case is when G is Abelian, and the exponent of G divides $p-1$. Then the Frattini quotient decomposes as the direct sum of one-dimensional representations. So by Lemma 3.2 we can lift their generators to generators of D on which G acts by the corresponding characters. In this case, the pairing is also simple to express with respect to these generators – more about pairings in the next section – and so one can achieve the usual Demuškin relation modulo $\mathcal{F}^{(3,q)}$. The following proposition shows that this is all that one can expect. Obviously everything just remarked only depends on the fact that the Frattini quotient decomposes into one-dimensional characters, so it is not really necessary that G is abelian of exponent dividing $p-1$.

If the Frattini quotient decomposes into absolutely irreducible $\mathbf{F}_p[G]$-modules, i.e., $\mathbf{F}_p$ serves as the splitting field for all occurring representations, then one can also expect reasonable generators for D.

We would like to thank Prof. Wingberg for showing some scepticism regarding the existence of a nice form of the relation in terms of nice generators. This led to the following.

PROPOSITION 3.6. *Let G be Abelian of exponent dividing $p-1$. Let D be a Demuškin group of rank $s \geqslant 4$ with non-trivial G action. Then it is not possible to find a presentation of D with generators x_i, $i = 1, \ldots, n$, on which G acts via characters $\chi_i : G \to \mathbb{Z}_p^*$ and a single relation of the form $r = x_1^q[x_1, x_2] \ldots [x_{n-1}, x_n]$.*

Proof. We assume that we have given such a presentation. Let χ be the dual of the Teichmüller lift of the character by which G acts on $H^2(D, \mathbb{Z}/(p))$. Then we must clearly have $\chi_i \chi_{i+1} = \chi$ for i odd between one and n. Let $\mathcal{R}$ be the closed normal subgroup generated by r. As G acts on D, $\mathcal{R}$ must be stable under G. In particular it must contain r^σ for all $\sigma \in G$.

We will work inside $\tilde{\mathcal{F}}$ which will denote the quotient of $\mathcal{F}$ by the closed, G-stable subgroup $[[\mathcal{F}, \mathcal{F}], [\mathcal{F}, \mathcal{F}]][[[\mathcal{F}, \mathcal{F}], \mathcal{F}], \mathcal{F}]\mathcal{F}^p$. The images of $r, \mathcal{R}$ in $\tilde{\mathcal{F}}$ will be $\tilde{r}, \tilde{\mathcal{R}}$. To simplify notation we will not add the tilde to the x_i. We have the following exact sequence $1 \to \Phi(\tilde{\mathcal{F}}) \to \tilde{\mathcal{F}} \to \bar{\mathcal{F}} \to 1$, where $\bar{\mathcal{F}}$ as well as $\Phi(\tilde{\mathcal{F}})$ are elementary p-abelian. It is easy to see that we can take the elements

$$[x_i, x_j] \text{ for } i < j \quad \text{and} \quad [[x_i, x_j]x_k] \text{ for } i < j, i \leqslant k$$

as a basis for $\Phi(\tilde{\mathcal{F}})$, by using the Jacobi rule on general commutators $[[x_i, x_j], x_k]$.

Furthermore $\tilde{\mathcal{R}}$ has as a basis the elements

$$\tilde{r}, [\tilde{r}, x_1], \ldots, [\tilde{r}, x_n].$$

It is clear that modulo $[[\mathcal{F}, \mathcal{F}], \mathcal{F}]$ we have $r^\sigma \equiv r^{\chi(\sigma)}$. So let $a_\sigma = r^\sigma r^{-\chi(\sigma)}$. Then a_σ is inside the subgroup of $\Phi(\tilde{\mathcal{F}})$ generated by triple commutators $[[x_i, x_j], x_k]$. One calculates

$$\begin{aligned} a_\sigma &= \prod_{\substack{i=1 \\ i \text{ odd}}}^{n} [x_i^{\chi_i(\sigma)}, x_{i+1}^{\chi_{i+1}(\sigma)}][x_i, x_{i+1}]^{-\chi(\sigma)} \\ &= \left(\prod_{\substack{i=1 \\ i \text{ odd}}}^{n} [[x_i, x_{i+1}], x_i]^{\frac{\chi_i(\sigma)-1}{2}} [[x_i, x_{i+1}], x_{i+1}]^{\frac{\chi_{i+1}(\sigma)-1}{2}} \right)^{-\chi(\sigma)} \end{aligned}$$

Furthermore it is easy to see that the elements

$$[[x_i, x_{i+1}], x_k], \quad i = 1, \ldots, s \text{ odd}, k = 1, \ldots, s$$

are linearly independent. Using the Jacobi identity, the basis of $\tilde{\mathcal{R}}$ and the expression for a_σ it follows that a_σ lies in $\tilde{\mathcal{R}}$ if and only if all $\chi_i(\sigma) = 1$. As σ was arbitrary, this can only happen if G acts trivially, contrary to our assumption. □

EXAMPLE 3.7. Finally if $G \cong C_2 = \{e, \sigma\}$, there is a reasonable relation that replaces the usual Demuškin relation. We will use the notation from above, in particular that G acts on x_i via χ_i. For i odd we define $\tau([x_i, x_{i+1}])$ by

$$\tau([x_i, x_{i+1}]) = \begin{cases} [x_i^{\chi_i(\sigma)}, x_{i+1}^{\chi_{i+1}(\sigma)}] & \text{if } \chi \text{ is trivial,} \\ [x_{i+1}^{\chi_{i+1}(\sigma)}, x_i^{\chi_i(\sigma)}] & \text{else.} \end{cases}$$

We define

$$r = x_1^q \prod_{\substack{i=1 \\ i \text{ odd}}}^{n} [x_i, x_{i+1}] \prod_{\substack{i=n \\ i \text{ odd}}}^{1} \tau([x_i, x_{i+1}]) x_1^q$$

where the notation means that the entries in the first product are listed by increasing, those in the second be decreasing order. One can then directly check that $r^\sigma = r^{\chi(\sigma)}$. So one found a reasonably nice substitute for the usual Demuškin relation, as now clearly $\mathcal{F}/(r)$, the quotient by the closed normal subgroup generated by r, is a Demuškin group with the desired action of G and invariants s, q. A similar symmetric expression can be given for G cyclic in the case $\chi = triv$.

Next we shall consider homomorphisms from Demuškin groups to arbitrary pro-p groups. Given a group by generators and relations, one can define a homomorphism from it into another group by freely mapping the generators, provided all the relations are satisfied in the other group. For a Demuškin group we will establish

the existence of a homomorphism given on generators under weaker assumptions provided we are allowed to replace the originally chosen generators of the Demuškin group by new ones, that have the same images in the Frattini quotient as the old ones, while keeping the same images. Similar results in this direction were obtained by Wingberg in [Win, Satz 2] using some results of Jakovlev. We formulate the following proposition which will later facilitate explicit calculations.

PROPOSITION 3.8. *Let D be a Demuškin group with an action of a group G. We assume that we are given a G-equivariant presentation of D by $1 \to \mathcal{R} \to \mathcal{F} \to D \to 1$ where $\mathcal{F}$ is a free pro-p group with the same number of generators as D, i.e. the same Frattini quotient. Let $\mathcal{F}^{(i,q)}$ be the lower q-central series as defined in the previous paragraph. Let P be some pro-p group with an action of G. Let r be an element of $\mathcal{F}$ whose normal topologically closed hull is $\mathcal{R}$, and on which G acts by a character. If we have a homomorphism α from $\mathcal{F}$ to P, such that the image of $\alpha(r) \in \alpha(\mathcal{F}^{(3,q)})$, or in other words, $\alpha(r)$ is the identity in $\alpha(\mathcal{F})/\alpha(\mathcal{F}^{(3,q)})$, then there exists a homomorphism from D to P that agrees with α modulo $\alpha(\mathcal{F}^{(2,q)})$. More precisely, if we pick free generators x_i of $\mathcal{F}$ and images α_i in P such that the so defined α satisfies $\alpha(r) \in (\alpha(\mathcal{F}))^{(3,q)}$ then we can find free generators x_i' of $\mathcal{F}$ that agree with the x_i modulo $\mathcal{F}^{(2,q)}$, such that α' defined by $x_i' \mapsto \alpha_i$ defines a homomorphism $D \to P$.*

Proof. First we suppose $q > 0$. Let N_i be the normal subgroup of $\mathcal{F}$ that is the composite of $\mathcal{F}^{(i,q)}$ and $\ker(\alpha)$. Thus N_i is a finitely generated free pro-p group. Furthermore $N_i/(N_i^q[N_i, N_i])$ contains an element such that the subgroup generated by it is stabilised by G. So by Lemma 3.2 the subgroup N_i contains an element r_i on which G acts by a character and which agrees with r modulo $\mathcal{F}^{(i,q)}$. By a compactness argument as used in the proof of Theorem 3.4 one can find $r' \in \ker(\alpha)$ with the same property. In particular it agrees with r modulo $\mathcal{F}^{(3,q)}$. If $q = 0$ one can use induction over p^i powers and again compactness to obtain such an element. As in the proof of Theorem 3.4, one sees that $\mathcal{F}/(r')$ is a Demuškin group D' isomorphic to D. Finally as r' is in the Kernel of α, a map from D' to P is induced. As D and D' agree modulo $D^{(3,q)}$, this homomorphism considered as one on D agrees with α modulo $D^{(3,q)}$. The way the isomorphism between D and D' can be realized is by replacing the originally chosen generators x_i of $\mathcal{F}$ by x_i' as described at the end of the statement of the proposition. □

For some purposes it is easier to work with the Lie algebra associated to the lower q-central series of a pro-p-group. We will only use the filtration $\mathcal{F}^{(i,0)}$. The following is known from [Laz].

PROPOSITION 3.9. *Let $C_i(P) = P^{(i,0)}$ for some pro-p group P and $C_i(L)$ be the Lie ideal of a p-Lie algebra generated by i fold commutators. Then there is an equivalence between the category of p-Lie algebras L for which $C_p(L) = 0$ and the category of pro-p groups P for which $C_p(P) = 0$. Given L one can define the associated pro-p group in the following way. The elements are the same as those of L and the product of two*

elements is given by the Campbell–Hausdorff formula. For $p > 2$ this equivalence exists in particular between the subcategories of the above categories where $C_3 = 0$. Then the pro-p group associated to a Lie algebra L has the composition law $X \circ Y = X + Y + [X, Y]$.

4. The Hilbert Pairing and *G*-Equivariant Pairings

For any field E, let $\mu_{p^n}(E)$ denote the set of p^n-th roots of unity contained in E. The following theorem is a well-known consequence of the results of Demuškin as stated in [Lab], and the G-module structure of $G_F(p)^{ab}$ as determined by Iwasawa, [Iwa], as G has order prime to p. As usual, F/K is a Galois extension of local fields of order prime to p. We note that $H^i(G_F(p), \mathbb{Z}/(p)) \cong H^i(G_F, \mathbb{Z}/(p))$ for all $i \in \mathbb{N}$.

THEOREM 4.1. *If $\mu_p(F) = \{1\}$, then $G_F(p)$ is a free pro-p group of rank $1 + [F : \mathbb{Q}_p]$ and its Frattini quotient is as an $\mathbf{F}_p[G]$-module isomorphic to $\mathbf{F}_p^{triv} \oplus \mathbf{F}_p[G]^s$, where $G = \mathrm{Gal}(F/K)$ and $s = [K : \mathbb{Q}_p]$.*

On the other hand, if $\mu_p(F) \neq \{1\}$, the pairing

$$H^1(G_F, \mathbb{Z}/(p)) \times H^1(G_F, \mathbb{Z}/(p)) \to H^2(G_F, \mathbb{Z}/(p)) \cong Hom(\mathbb{Z}/(p), \mu_p), \tag{2}$$

induced from the cup-product pairing, is a non-degenerate alternating G-equivariant pairing, the Hilbert symbol. Moreover $G_F(p)$ is a Demuškin group with invariants $n = n(G_F(p)) = \dim_{\mathbf{F}_p} H^1(G_F, \mathbb{Z}/(p))$ and $q = q(G_F(p))$, the number of p power roots of unity in F, and the Frattini quotient of $G_F(p)$ is isomorphic to $\mathbf{F}_p^{triv} \oplus \mu_p(F) \oplus \mathbf{F}_p[G]^s$ as a G-module, where G acts on $\mu_p(F)$ and $s = [K : \mathbb{Q}_p]$. Finally, the above pairing is still alternating, non-degenerate G-equivariant between free $\mathbb{Z}/(q)$-modules, if one uses $\mathbb{Z}/(q)$ coefficients.

Next we recall from [Koch, Sätze 6, 9 and 10] the main result about the $G = \mathrm{Gal}(F/K)$-structure of the above pairing (2).

THEOREM 4.2. *Let χ be the cyclotomic character on $\lim_{\leftarrow} \mu_{p^n}(\bar{K}) \cong \mathbb{Z}_p$. Then one can decompose $H^1(G_F, \mathbb{Z}/(p))$ as an $\mathbf{F}_p[G]$-module as*

$$H^1(G_F, \mathbb{Z}/(p)) \cong \mathbf{F}_p^{\chi^{-1}} \oplus \mathbf{F}_p^{triv} \oplus U \oplus V,$$

where $\mathbf{F}_p^{\chi^{-1}}$ is paired with $\mathbf{F}_p^{triv}$, U is paired with V, and the pairing between all other pairs is trivial. It follows in particular that $H^1(G_F, \mathbb{Z}/(p))$ is hyperbolic under the above pairing, i.e., the direct sum of two pairwise isotropic $\mathbf{F}_p[G]$-modules.

As the categories of $\mathbf{F}_p[G]$-modules and of projective $\mathbb{Z}/(q)[G]$-modules are equivalent, as p does not divide the order of G, it is not hard to see that the previous

theorem generalises to the pairing

$$H^1(G_F, \mathbb{Z}/(q)) \times H^1(G_F, \mathbb{Z}/(q)) \to H^2(G_F, \mathbb{Z}/(q)) \cong Hom(\mathbb{Z}/(q), \mu_q),$$

where now one has to use four projective $\mathbb{Z}/(q)[G]$-modules. Also there are more general results known by work of Jakovlev, Jannsen and Wingberg, [JaWi, Win] and the references therein.

We now recall several basic properties of non-degenerate alternating G-equivariant bilinear forms $\kappa : X \times X \to T$ of $\mathbf{F}_p[G]$-modules, where T is a one-dimensional $\mathbf{F}_p$ vector space with its action given by the character χ^{-1}. This will then be applied to $X = H^1(G_F, \mathbb{Z}/(q))$ and $T = H^2(G_F, \mathbb{Z}/(q))$. We shall keep in mind that the X, in which we are interested, is hyperbolic.

Clearly we can decompose X into irreducible $\mathbf{F}_p[G]$-modules. As the pairing is non-degenerate, given an irreducible submodule V, by Schur's lemma, there must be an irreducible V' such that $V' \cong V^* \otimes T$, and the pairing restricted to $V + V'$ and its complement is non-degenerate. If X is hyperbolic, we can arrange things so that the sum $V + V'$ is always direct, even if $V \cong V'$ which could happen in general.

PROPOSITION 4.3. *Let k be a finite field over $\mathbf{F}_p$ and X a finite dimensional $k[G]$-module that carries an alternating non-degenerate bilinear form $\kappa : X \times X \to T$ compatible with the G action where T is, as a vector space, isomorphic to k. Then one can decompose*

$$X = V_1 \oplus \ldots \oplus V_l \oplus V_1' \oplus \ldots \oplus V_l' \oplus W_1 \oplus \ldots \oplus W_m,$$

where the V_i, V_i', W_j are irreducible $k[G]$-modules, $V_i' \cong V_i^* \otimes T$ for $i = 1, \ldots, l$, $W_j \cong W_j^* \otimes T$ for $j = 1, \ldots, m$, the pairing κ sets up a perfect duality between V_i and V_i', and between W_j with itself, and is trivial between all other pairs.

If in addition X is hyperbolic we can assume that $m = 0$.

In fact such a decomposition exists over any ring R in which $|G|$ is a unit provided X, T are projective over $R[G]$. The modules in the decomposition will be irreducible projective $R[G]$-modules. This applies to $R = \mathbb{Z}/(q)$ or $W(k)/(q)$.

PROPOSITION 4.4. *Given two irreducible $k[G]$-modules V, V' and a one-dimensional $k[G]$-module T, such that $V' \cong V^* \otimes T$, there exists a bilinear non-degenerate alternating pairing on $V \oplus V'$. If V and V' are not isomorphic, then it is unique up to multiplication by an element in $\mathrm{Aut}_G(V)$, the splitting field of V. Thus if V is absolutely irreducible, it is unique up to multiplication by an element in k^*.*

Proof. By Schur's lemma $Hom(V', V^* \otimes T)$ is a skew field finite over k, and by Frobenius' theorem it must be a finite extension of k, in fact the splitting field of V, or V' which is the same. Given a non-zero homomorphism α in this set, which

thus must be an isomorphism, one can define the form

$$\kappa : V \oplus V' \times V \oplus V' \to T : ((v, v'), (w, w')) \to \alpha(v')(w) - \alpha(w')(v)$$

Non-degeneracy and skew-symmetry are obvious. If V and V' are not isomorphic, given a pairing, one can define a homomorphism α by $\alpha(v')(v) = \kappa((0, v'), (v, 0))$, and in fact all non-degenerate pairings must arise in this way. The other claims are now obvious. □

The last fact we want to recall is how bilinear forms behave under base change.

PROPOSITION 4.5. *Let X and T be $k[G]$-modules where T has dimension one over k. We assume that X is either irreducible, or the sum of two irreducibles V, V' such that $V^* \otimes T \cong V'$. Let k' be the splitting field of X – this makes sense under the above assumptions. Given an alternating non-degenerate, i.e. non-zero, bilinear form $X \times X \to T$, and a decomposition*

$$X \otimes k' \cong Y \oplus Y^1 \oplus \ldots \oplus Y^{n-1}$$

where Y is either irreducible, or the sum of two irreducibles W, W' and the superscript i means that one applies the ith power of the Frobenius automorphism σ of k' over k to the matrices giving the representation Y, then the pairing can clearly be extended and there are the following possibilities.

If X is reducible, we can choose W, W' inside Y so that the restriction of the base changed pairing to $Y \cong W \oplus W'$ is perfect and pairs W with W'. Also in this case, the bilinear form on Y^i is simply σ^i applied to the bilinear form on Y.

If X is irreducible there are two possible cases. Either Y is paired with $Y^{n/2}$, in which case n has to be even and then the bilinear form on $Y^i \oplus Y^{i+n/2}$ is given by σ^i applied to the bilinear form on $Y \oplus Y^{n/2}$.

Or Y is paired with itself, and the pairing on Y^i is given by applying σ^i to the pairing $Y \times Y \to T \otimes k'$.

As a consequence, for X irreducible, a non-degenerate alternating pairing $X \times X \to T$ exists if and only if over the splitting field k' there exists a non-trivial homomorphism $Y \wedge Y \to T$ or alternatively $Y^* \otimes T \cong Y^{n/2}$. In either case the number of such pairings is the cardinality of the units of $k' = End_G(V)$.

Proof. The proof for the case that X is reducible is rather simple and similar to the other case and will thus be omitted. So from now we assume that X is irreducible.

Let τ be the G-equivariant linear transformation that gives the isomorphism $X \otimes k' \cong \bigoplus_{i=0}^{n-1} Y^i$, and let A denote a matrix representing the bilinear pairing on X, and hence on $X \otimes k'$, too. We choose a k'-basis B of $Y = Y^0 = Y^n$, and take for Y^i the basis obtained from it by i-fold application of the Frobenius automorphism σ. Let A' be the matrix giving the pairing on $\bigoplus_{i=0}^{n-1} Y^i$ and denote by τ^t the transpose of τ. From our special choice of basis we find

$$A' = \tau^{-t} A \tau \quad \text{and} \quad \tau\sigma = P\tau$$

where P is the permutation matrix $P = (\delta_{i,i+n})_{i=1,\ldots,n\dim Y}$ ($\delta_{i,j}$ is the Kronecker delta function), and we regard the indices modulo $n\dim Y$. Let $A'_{i,j}$ denote the $\dim Y \times \dim Y$ submatrix of A' which describes the pairing between Y^i and Y^j. As A is invariant under σ, it follows that $A'_{i,j} = (A'_{i-1,j-1})^\sigma$. Thus, if Y is paired with Y^i, i.e. $A'_{0,i}$ is non-degenerate, then by the above $A'_{n-i,0}$ is non-degenerate, and Y^{n-i} is paired with Y. Hence $Y^{n-i} \cong Y^i$, as Y^i and Y^j can only be paired if $Y^i \cong (Y^j)^* \otimes T$. But the Y^i are pairwise non-isomorphic, as k' is the splitting field and X is irreducible, and it follows that Y can only be paired with itself or with $Y^{n/2}$. The statements about the bilinear form on the other pairs is now clear by repeated application of the Frobenius automorphism. □

We will now analyze the relevant modules for the later calculations. So far we know the abstract module structure of $H^1(G_F, \mathbb{Z}/(p))$ as an $\mathbf{F}_p[G]$-module, and that the cup-product pairing is non-degenerate, G-equivariant and hyperbolic. By the above it follows, that for the sum of two irreducible paired pieces, over the splitting field of them, the pairing is determined up to a non-zero scalar. This will suffice for our purposes to find an explicit expression for 'the' Demuškin relation modulo third and higher commutators.

In the notation of Proposition 3.8, we simply want to find an element in $\mathcal{F}$ on which G acts by a character, whose normal topological closure generates $\mathcal{R}$, and which we can describe explicitly modulo triple commutators. The element modulo $\mathcal{F}^{(3,q)}$ shall be $\bar{r}$. In the notation of Theorem 3.4, we found

$$\mathcal{F}^{(2,q)}/\mathcal{F}^{(3,q)} \cong \mathcal{F}_q^{ab} \wedge \mathcal{F}_q^{ab} \oplus \mathcal{F}_q^{ab},$$

where the first summand is generated by q-th powers and the second by commutators. Correspondingly, we shall write $\bar{r} = \bar{r}' + \bar{r}''$, so that $\bar{r}'$ is a linear combination of commutators. From the construction in the proof of Theorem 3.4, it follows that G will act on both $\bar{r}'$ and $\bar{r}''$ via a character, and furthermore that $\bar{r}'$ can be recovered from the cup product pairing as follows.

It is the image of any generator of T^* under the map $\kappa^* \in Hom(T^*, \Lambda^2(X^*))$, where κ, X and T are as defined two paragraphs below Theorem 4.2, and we identify $\Lambda^2(X^*)$ with $\mathcal{F}_q^{ab} \wedge \mathcal{F}_q^{ab}$. We observe that by Schur's lemma, if we assume a decomposition as in Proposition 4.3, κ^* factors via $\sum_i \Lambda^2(V_i^* \oplus V_i'^*)$. So we can write $\bar{r}' = \sum_i r_i$ (to alleviate the notation, we shall not use the notation $\bar{r}'_i$ for the individual components, but simply r_i). By Proposition 4.4, the r_i are unique up to scalars in the splitting field of V_i. So if we determine the r_i individually, we shall know $\bar{r}'$ up to scalars for each r_i. A more careful analysis using the results quoted from [Koch] might explicitly describe those scalars, but as they are not needed in the applications we have in mind, we did not carry out this analysis. To summarize:

LEMMA 4.6. *If $0 \neq \bar{r}'$ is in the image of κ^*, and if we chose for all i some $r_i \neq 0$ in the image of $T^* \to \Lambda^2(V_i^* \oplus V_i'^*)$, both maps coming from dualizing the pairing, then there exist elements ε_i in the splitting field of each V_i such that $\bar{r}' = \sum_i \varepsilon_i r_i$ over*

the splitting field of X, or appropriately understood via the action of the various splitting fields on the various modules $V_i^* \oplus V_i'^*$.

LEMMA 4.7. *Let $G = C_n$ be cyclic or $G = D_n$ be dihedral of order prime to p. Let T be a one-dimensional $k[G]$-module, where the action of G is given by α. In the dihedral case, α necessarily has to have order dividing two. Let V, V' be absolutely irreducible $k[G]$-modules with a hyperbolic G-equivariant alternating non-degenerate pairing $\otimes^2(V \oplus V') \to T$. By r we shall denote an element in $\Lambda^2(V^* \oplus V'^*)$ as the elements r_i described above. The element $[x, y] \in \Lambda^2(V^* \oplus V'^*)$ shall denote the image of the element $x \otimes y + y \otimes x \in \otimes^2(V^* \oplus V'^*)$, $x \in V^*, y \in V'^*$, projected to $\Lambda^2(V^* \oplus V'^*)$. Then*

(i) *If $V \cong k^{\psi}$ for a character ψ, then $V' \cong k^{\alpha\psi^{-1}}$ and in terms of basis elements v, v' of V^*, V'^* in $(V^* \oplus V'^*)^2$, r is given by $[v, v']$ up to a non-zero scalar. Note that in the dihedral case all characters have order one or two, and there are two of them, if n is odd, and four, if n is even.*

(ii) *If G is dihedral and $V \cong \mathrm{Ind}_{C_n}^{D_n} k^{\psi}$ for a character ψ of C_n of order unequal two, then $V' \cong V$. If we pick a basis v, w, resp. v', w', of V^*, resp. V'^*, so that C_n acts via the characters ψ, ψ^{-1} on the v's and w's, respectively, and so that a fixed element of order two not inside C_n acts by interchanging v's and w's, then, up to a non-zero scalar, r is given by $[v, w'] + [w, v']$ if α is trivial, and it is given by $[v, w'] - [w, v']$ if α is of order two, trivial on C_n.*

Analogous results hold, if we replace all the above modules by projective $\mathbb{Z}/(q)[G]$-modules.

We omit the more or less obvious proof.

5. Closed Subgroups of $\mathrm{GL}_2(R)$ and Special Matrices

We shall start by describing the basic matrices that will occur as images of the Demuškin group with the G action that we consider. As described in Section 2, the image of G in $\mathrm{PGL}_2(k)$ is non-trivial and either cyclic or dihedral.

We shall first fix some notation which we shall use until the end of Section 7. If G is cyclic, let ψ be the Teichmüller lift to $W(k)^*$ of the character by which G acts on the $(1, 2)$ entry of $\mathrm{GL}_2(k)$. Then $\mathrm{ad}_{\bar{\rho}}|_G \cong (k^{triv})^2 \oplus k^{\psi} \oplus k^{\psi^{-1}}$

If the image of G in $\mathrm{PGL}_2(k)$ is dihedral, isomorphic to D_n, we shall assume that C_n is inside the diagonal matrices. Note that for D_2 this requires a choice that we will make once and for all. Then $\mathrm{ad}_{\bar{\rho}} \cong k^{triv} \oplus k^{\phi} \oplus \mathrm{Ind}_{C_n}^{D_n} k^{\psi}$. where ϕ is the unique non-trivial character that is trivial on C_n, and ψ is the character from above, once the action is restricted to C_n. If $n \neq 2$, then $\mathrm{Ind}_{C_n}^{D_n} k^{\psi}$ is irreducible. Else we can write it as $k^{\psi'} \oplus k^{\psi''}$ where ψ' and ψ'' are the characters trivial on the third and fourth

matrix, respectively, of the following description of $D_2 \subset \mathrm{PGL}_2(W(k))$ given by

$$\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\right\}.$$

Further let χ be the character of G_K by which it acts on the p power roots of unity inside F. It factors through G and we shall denote the corresponding character of G again by χ.

DEFINITION 5.1. For any finite field k and any n, and for projective $W(k)/(p^n)[G]$-modules X, Y, we define $(X, Y)_G = \dim_k Hom_{k[G]}(X/(p), Y/(p))$. X and Y will be called relatively prime, if $Hom_{k[G]}(X, Y) = 0$, or equivalently $(X, Y)_G = 0$. In fact it is not necessary that X, Y are defined over the same field. One could simply base change them to a common larger field and take the definitions there.

LEMMA 5.2. *Let P be a pro-p group with an action of G and a filtration P_i such that the subquotients are $\mathbf{F}_p[G]$-modules. Let Q be another pro-p group with G action. Assume that the Frattini quotient $\bar{Q}$ is relatively prime to all subquotients of $\{P_i\}$, then $Hom_G(Q, P)$ is trivial, i.e. consists only of the map sending all of Q to $\{1\} \subset P$.*

The proof uses the prime-to-adjoint principle as in [Bos1, §2], or [Boe1, Lemma 2.4.4].

The above lemma applies to $P \subset \mathrm{GL}_2(R)$ for any $R \in \mathcal{C}$ and our usual G where one has the obvious filtration by powers of $\mathfrak{m}$, so that all subquotients are sums of submodules of $\mathrm{ad}_{\bar{\rho}}$.

As described in the outline of the proof of Theorem 2.6, using the remark after Lemma 3.2, we can find closed subgroups P_i, $i = 0, \ldots, m$, inside $G_F(p)$ such that their Frattini quotients $\bar{P}_i$ are irreducible, the $\bar{P}_i$ inject into $\bar{G}_F(p)$ and the sum of the $\bar{P}_i$ is direct, summing up to $\bar{G}_F(p)$. Hence by the Burnside basis theorem the P_i generate $G_F(p)$. By the results of the previous sections we can arrange so that the $\bar{P}_i$ are paired with $\bar{P}_{m-i}$ where $m+1$ is the number of irreducible summands of $\bar{G}_F(p)$ – hence m is odd. We shall now describe images of nicely chosen $x_i \in P_i$ under a homomorphism α to a matrix group. We fix the following notation.

$$D(a, b) = \begin{pmatrix}a & 0\\ 0 & d\end{pmatrix}, \qquad S(b, c) = \begin{pmatrix}\sqrt{1+bc} & b\\ c & \sqrt{1+bc}\end{pmatrix}.$$

Note that $S(b, 0)$ and $S(0, c)$ are upper and lower triangular, resp., with entry one along the diagonal.

LEMMA 5.3. *Given i and $\alpha \in Hom_G(P_i, \mathrm{GL}_2(R))$, we can pick an x_i in P_i with non-zero image in $\bar{P}_i$ whose image in $\mathrm{GL}_2(R)$ is as follows.*

(i) *If $\bar{P}_i$ is relatively prime to* ad*, then $\alpha(x_i) = D(1, 1)$.*

(ii) *If* $\bar{P}_i \cong \mathbf{F}_p^{triv}$, *then* $\alpha(x_i) = \sqrt{1+a_i}\, D(\sqrt{1+d_i}, \sqrt{1+d_i}^{-1})$ *for some* $a_i, d_i \in \mathfrak{m}$, *and* $a_i = d_i$ *if* G *is dihedral.*

(iii) *If* G *is cyclic and* $\bar{P}_i \otimes k$ *contains* k^{ψ} *or* $k^{\psi^{-1}}$, *but not both (in particular we exclude* $\psi = \psi^{-1}$*) then* $\alpha(x_i) = S(b_i + \hat{u}_i, 0)$ *or* $\alpha(x_i) = S(0, c_i)$ *with* $b_i, c_i \in \mathfrak{m}$, *resp.*

(iv) *If* G *is cyclic and* $\bar{P}_i \otimes k$ *contains* k^{ψ} *and* $k^{\psi^{-1}}$ *(this includes* $\psi = \psi^{-1}$*) then* $\alpha(x_i) = S(b_i + \hat{u}_i, c_i)$ *with* $b_i, c_i \in \mathfrak{m}$.

(v) *If* G *is dihedral with* $n > 2$ *and* $\bar{P}_i \otimes k$ *contains* $\mathrm{Ind}_{C_n}^{D_n} k^{\psi}$, *then* $\alpha(x_i) = S(b_i, b_i)$ *with* $b_i \in \mathfrak{m}$.

(vi) *If* $G \cong D_2$ *and* $\bar{P}_i \otimes k$ *equals* $k^{\psi'}$ *or* $k^{\psi''}$, *then* $\alpha(x_i) = S(b_i, b_i)$ *or* $\alpha(x_i) = S(b_i, -b_i)$, *respectively, with* $b_i \in \mathfrak{m}$.

(vii) *If* G *is dihedral and* $\bar{P}_i \otimes k \cong k^{\phi}$, *then* $\alpha(x_i) = D(\sqrt{1+d_i}, \sqrt{1+d_i}^{-1})$ *with* $b \in \mathfrak{m}$.

The images of the x_i *determine* α *completely as each* P_i *is topologically generated by the* G *orbit of* x_i. *To see the latter, one uses the Burnside basis theorem and the irreducibility of the* $\bar{P}_i$ *which implies that* $\bar{P}_i$ *is generated over* $\mathbf{F}_p$ *by the* G *orbit of* $\bar{x}_i$. *As* $\bar{P}_i$ *is not necessarily absolutely irreducible, only irreducible, we have to use at several instances the word contains instead of equals.*

For the proof we need the following theorem from [Pink]. Let $\theta : \mathrm{SL}_2(R) \to \mathfrak{sl}_{2,R}$ denote the map sending x to $x - \mathrm{tr}(x)/2 \cdot \mathrm{Id}$, where $\mathfrak{sl}_{2,R}$ is the set of two-by-two matrices of trace zero considered in a natural way as a Lie algebra over R.

THEOREM 5.4. *There is a canonical one-to-one correspondence between all closed pro-p subgroups of* $\Omega \subset \mathrm{SL}_2(R)$ *and the following pairs* (L, Δ)*: First,* L *should be a closed additive subgroup of* $sl_{2,R}$ *satisfying*

(i) $\bigcap_n L^n = \{0\}$,
(ii) $[L, L] \subset L$, *and*
(iii) $\mathrm{tr}(L \cdot L) \cdot L \subset L$.

These three conditions imply that the formula

$$\bar{x} * \bar{y} := \overline{y\sqrt{1 + \mathrm{tr}(x^2)/2} + x\sqrt{1 + \mathrm{tr}(y^2)/2}}$$

is a well-defined composition law on the set $L/[L, L]$ *making it into an abelian pro-p group with identity* $\bar{0}$. *Then* Δ *should be a closed subgroup of* $(L/[L, L], *)$ *such that the additive group* $L/[L, L]$ *is topologically generated by the subset* Δ.

Furthermore given Ω, L *is the closed additive subgroup of* $\mathfrak{sl}_{2,R}$ *generated by* $\theta(\Omega)$ *and* Δ *its image under* θ *in* $L/[L, L]$. *Also, for* $n \geqslant 2$ *one has* $L_n/L_{n+1} \cong C_n(\Omega)/C_{n+1}(\Omega)$ *via* θ *for the n-th subquotient of the lower central series, where* L_n *is an abbreviation for* $C_n(L)$. *The inverse to* θ *on those subquotients, we will denote by* Θ. *Explicitly,* Θ *is given by*

$$\Theta : L \to \Omega : x \mapsto x + \mathrm{Id}\sqrt{1 + \mathrm{tr}(x^2)/2}.$$

To describe $C_1(\Omega)/C_2(\Omega) = \Delta$ *one needs the structure defined by* $*$ *on* L_1/L_2 *and in*

general there is an inclusion of Δ *into it. Finally, for* $x, y \in \Omega$ *one has* $[\theta(x), \theta(y)] = \theta([x, y])$ *modulo* L_3 *where the right pair of brackets is formed in* Ω*, the left in the Lie algebra.*

Proof of Lemma 5.3. In all but cases (iii), (iv) and (v), one can either appeal to prime-to-adjointness, Lemma 5.2, or $\bar{P}_i$ is absolutely irreducible and one-dimensional and one can apply Lemma 3.2 to obtain a generator x_i as in that lemma. This determines the shape of the image completely.

In case (v) one can also apply Lemma 3.2 to obtain a generator x_i on which $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, a special lift of the C_2 quotient in $\mathrm{PGL}_2(W(k))$, acts trivially. By considering the determinant representation, the shape of $\alpha(x_i)$ must be as described above.

Case (iii) can be handled by a simple induction argument via the filtration on $\mathrm{GL}_2(R)$ given by

$$\left\{ \begin{pmatrix} 1+a & b \\ c & 1+d \end{pmatrix} : a, c, d \in \mathfrak{m}^{n+1} \right\}_n$$

and refinements, or its transpose, and using prime-to-adjointness. In case (iv), if n is even, then we pick x_i for the action of $D_2 \subset D_n$.

There remains the case (iv) when n is odd. Using the determinant representation and prime-to-adjointness, it is clear that $\mathrm{Im}(\alpha)$ lies in $\mathrm{SL}_2(R)$. Now we can apply the structure theorem on closed pro-p subgroups of $\mathrm{SL}_2(R)$ quoted above. We shall use the notation from there.

Let (L, Δ) be the pair consisting of a Lie algebra L inside $\mathfrak{sl}_{2,R}$ and $\Delta \subset (L_1/L_2, *)$ a closed subgroup. Let z_i be any element in P_i non-zero in the Frattini quotient. Let $g \in C_n$ be a generator. Then $y_i = z_i(z_i^g)^{-1}$ is also such an element. By explicit calculation one finds that the difference between $[\theta(\alpha(z_i)), \theta(\alpha((z_i^g)^{-1}))] \in L_2$ and $\theta(y_i) \in L$ is of the form $\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$. This is clearly in L and as we modified the element $\theta(y_i)$ with image in Δ modulo L_2 by an element in L_2, the modified element will be in $\theta(\mathrm{Im}(\alpha))$. We take as x_i the corresponding element in $\mathrm{Im}(\alpha)$. It is easy to see that, under the θ correspondence, $S(b, c)$ corresponds to $\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}$. □

Remarks 5.5. We want to make a few comments on the matrices that appear as images.

(i) Matrices of the type $S(b, c)$ seem to have appeared in [Bos2] for the first time in this context. There, it was remarked on the fact that the matrix coefficients of their powers are related to cyclotomic polynomials. In fact it is also possible to write down explicit power series that express those coefficients. If we denote

by b_n, c_n the power series in b, c defined by

$$S(b, c)^n = S(b_n, c_n)$$

then one has the explicit expressions

$$b_n(b, c) = bg_n(bc) \quad c_n(b, c) = cg_n(bc) \quad \sqrt{1 + b_n c_n} = f_n(bc),$$

where $f_n(x) = \sum_k a_{n,k} x^k$ and $g_n(x) = \sum_k b_{n,k} x^k$ with

$$a_{n,k} = 1(2k)! \prod_{j=0}^{k-1} (n^2 - (2j)^2) \quad \text{and} \quad b_{n,k} = n(2k+1)! \prod_{j=0}^{k-1} (n^2 - (2j+1)^2).$$

For example $g_3(x) = 3 + 4x$.

(ii) All the matrices that are involved in the description of the images of D_2 generate abelian subgroups of $\mathrm{GL}_2(R)$. This can be checked by explicit calculation. A more conceptual way to see this is to use the exponential and logarithm maps for $R = \mathbb{Z}_p[[b]]$ after tensoring this with $\mathbb{Q}_p$. There it is clear that the images under the logarithm are of a shape that always commute with each other, so that after applying the exponential map the elements will still commute. For example if we take $S(b, -b)$, its logarithm is of the shape $\begin{pmatrix} 0 & \beta \\ -\beta & 0 \end{pmatrix}$. As all commutators between matrices of this shape are zero, their exponentials form a commuting family.

A second application of the above theorem of Pink will be on the closed image generated by P_i and P_{m-i} in $\mathrm{GL}_2(R)$. First we make a few definitions. In all but cases (iii), (iv) and (v), we define $k_1 = k_0 = \mathbf{F}_p$. In those cases we define k_1 to be the minimal extension of $\mathbf{F}_p$ over which ψ is defined. In case (iii) and in case (v), if $\bar{P}_i|_{C_n}$ is reducible, we define $k_0 = k_1$. In the remaining cases we define k_0 as the unique subfield of k_1 such that $[k_1 : k_0] = 2$. This field exists as the irreducibility of $\bar{P}_i|_{C_n}$ implies that $\psi^{-1} = \psi^{\sigma^n}$ for some integer n, where σ is the Frobenius automorphism. Hence $k_1 = \mathbf{F}_{p^{2n}}$.

LEMMA 5.6. *We keep the assumptions of the previous lemma and assume that the x_i are chosen accordingly. We define the Lie algebra L as the image under θ of the closed subgroup generated by the images of the G orbits of x_i and x_{m-i}.*

Then L_1/L_2 and L_2/L_3 carry naturally $W(k_1)$-module structures. The Lie bracket is compatible with the $W(k_0)$-structure. If x_i falls into one of the cases (iii), (iv) or (v), one has $(L_1/L_2, *) = (L_1/L_2, +)$. Also in the cases where $k_1 \neq k_0$, the Lie bracket extends naturally to a Lie bracket

$$(L_1/L_2, +) \otimes_{W(k_0)} W(k_1) \times (L_1/L_2, +) \otimes_{W(k_0)} W(k_1) \to (L_2/L_3, +).$$

Furthermore, if r_i is the Demuškin relation restricted to P_iP_{m-i}, as defined above Lemma 4.6, one has the following expression for $\theta(\alpha(r_i))$ in L_2/L_3 where ε_i is a unit scalar of $W(k)$, up to possibly interchanging i and $m-i$.

(A) *If $\bar{P}_i \cong \mathbf{F}_p^{triv}$, $\bar{P}_{m-i} \cong \mathbf{F}_p^{\chi}$, $\chi^2 \neq 1$, then $\theta(\alpha(r_i)) = \varepsilon_i b_{m-i} d_i \sqrt{1+d_i}^{-1} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ if $\chi = \psi$ and $\theta(\alpha(r_i)) = \varepsilon_i c_{m-i} d_i \sqrt{1+d_i}^{-1} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ if $\chi = \psi^{-1}$.*

(B) *If $\bar{P}_i \cong \mathbf{F}_p^{triv}$, $\bar{P}_{m-i} \cong \mathbf{F}_p^{\chi}$, χ has order two, $\chi = \psi$ and G is not dihedral, then*

$$\theta(\alpha(r_i)) = \varepsilon_i \frac{d_{m-i}}{\sqrt{1+d_{m-i}}} \begin{pmatrix} 0 & b_i \\ c_i & 0 \end{pmatrix}.$$

(C) *If G is cyclic, χ is trivial, and $\bar{P}_i \otimes k$ contains k^{ψ}, but not $k^{\psi^{-1}}$, and so $\bar{P}_{m-i}$ contains $k^{\psi^{-1}}$, then $\theta(\alpha(r_i)) = \varepsilon_i c_{m-i} b_i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.*

(D) *If G is cyclic and $\bar{P}_i \otimes k$ contains both k^{ψ} and $k^{\psi^{-1}}$, and if χ is trivial, then*

$$\theta(\alpha(r_i)) = (\varepsilon_{m-i} b_i c_{m-i} - \varepsilon_i b_{m-i} c_i) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

(E) *If G is dihedral with image D_2 in $\mathrm{PGL}_2(k)$, and if $\chi = \psi'\psi''$, and hence χ is of order two, and $\bar{P}_i \cong k^{\psi'}$, or if G is dihedral, $\chi = \phi$ and $\bar{P}_i \otimes k$ contains $\mathrm{Ind}_{C_n}^{D_n} k^{\psi}$, then $\theta(\alpha(r_i)) = \varepsilon_i b_i b_{m-i} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.*

(F) *In all other cases $\theta(\alpha(r_i)) = 1$.*

Proof. The first half is obvious unless we are in one of the three special cases, as pro-p groups always admit exponentiation by elements of $\mathbb{Z}_p$. In the three special cases, we first show $(L_1/L_2, *) \cong (L_1/L_2, +)$. This we will carry out only for x_i belonging to case (iii). The other two cases are analogous. Note first that if $\bar{P}_i \otimes k$ contains k^{ψ} and $k^{\psi^{-1}}$, then the same is true for $\bar{P}_{m-i} \otimes k$.

L is the smallest topologically closed Lie algebra containing $\alpha(x_i)$ and $\alpha(x_{m-i})$ which is closed under the G operation – via conjugation. In particular L_1/L_2 contains all G conjugates of $\alpha(x_i)$ and $\alpha(x_{m-i})$. Using $\mathbb{Z}_p$ linear combinations of the set $[\theta(\alpha(x_i)), \theta(\alpha(x_i^g))]_{g \in G}$ one finds that the $W(k_1)$ span of $b_i c_i \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ lies inside L_2 and similarly that of $b_{m-i} c_{m-i} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. By calculating commutators between these matrices and $\theta(\alpha(x_i^g))$ or $\theta(\alpha(x_{m-i}^g))$, one sees that all matrices $b_i^2 c_i^2 \alpha(x_{m-i}^g)$ and $b_{m-i}^2 c_{m-i}^2 \alpha(x_i^g)$ are in L_2. Thus from the definition of $*$ and using series expansions it follows that $x * y = x + y$ in L_1/L_2.

Next $\mathbb{Z}_p\{\psi(g) : g \in G\} = W(k_1)$ and $\psi(g)^{-1} = \sigma^n(\psi(g))$, and so we can define for $x \in W(k_1)$

$$xS(b_i, c_i) = S(xb_i, \sigma^n(x)c_i).$$

This way we define a $W(k_1)$-module structure. But the Lie bracket from L_1/L_2 to L_2/L_3 is only $W(k_0)$ linear, as can be seen from

$$[a\theta(S(b, c)), a'\theta(S(b', c'))] = (\sigma^n(a')abc' - \sigma^n(a)a'b'c)D(1, -1).$$

Moreover the above calculation shows that L_2/L_3 does have a $W(k)$-structure, so in particular a $W(k_1)$-structure. Finally using the explicit basis

$$\left\{\begin{pmatrix} 0 & b_i \\ c_i & 0 \end{pmatrix}, \begin{pmatrix} 0 & \psi(g)b_i \\ \psi(g^{-1})c_i & 0 \end{pmatrix}, \begin{pmatrix} 0 & b_{m-i} \\ c_{m-i} & 0 \end{pmatrix}, \begin{pmatrix} 0 & \psi(g)b_{m-i} \\ \psi(g^{-1})c_{m-1} & 0 \end{pmatrix}\right\}$$

of L_1/L_2, one can see that Lie bracket of $L_1/L_2 \otimes_{W(k_0)} W(k_1)$ has its image naturally in L_2/L_3.

It remains to calculate the expression $\theta(\alpha(r_i))$. Again, all but the three special cases are obvious. We will give a full proof for x_i belonging to case (iii). Using Theorem 5.4 and Proposition 3.9, we can work with the associated Lie algebras. By the above, L_1/L_2 has a $W(k_0)$-structure, but for purposes of calculating Lie brackets, we can assume a $W(k_1)$-structure. Morally we then have one copy of $W(k_1)^{\psi}$, $W(k_1)^{\psi^{-1}}$ $W(k_1)^{\chi\psi}$, $W(k_1)^{\chi\psi^{-1}}$ and a Lie bracket that respects the G action, 'morally' meaning, that one could have torsion, depending on $a_i, a_{m-i}, b_i, b_{m-i}$.

If the pairing on $W = P_i^{ab} \oplus P_{m-i}^{ab}$ is given by the matrix $A = (a_{l,l'})$ with respect to some basis $\{y_{i,l}\} \cup \{y_{m-i,l'}\}$, then

$$r_i = \sum_{l,l'} a_{l,l'}[y_{i,l}, y_{m-i,l'}] \in \Lambda^2 W.$$

Under tensoring with $W(k_1)$, α extends uniquely to a map between $W(k_1)$ Lie algebras

$$(W \oplus \Lambda^2 W) \otimes W(k_1) \to L_1/L_2 \otimes_{W(k_0)} W(k_1) \oplus L_2/L_3.$$

The space $W \otimes W(k)$ decomposes into one-dimensional eigenspaces for certain characters of G, and the G-equivariant pairing on individual pieces was calculated in Lemma 4.7. If we pick an appropriate basis $\{z_{i,l}\} \cup \{z_{m-i,l'}\}$ respecting the eigenspaces, then there are units ε_l such that

$$r_i = \sum_l \varepsilon_l[z_{i,l}, z_{m-i,l}],$$

where the product of the characters for $z_{i,l}$ and for $z_{m-i,l}$ is χ. The image contains only components with an action by the four aforementioned characters. It follows that $\theta(\alpha(r_i))$ has the shape given in the lemma. □

Remark 5.7. It might appear surprising at first, that there is no relation in the dihedral case, if χ is trivial and $\bar{P}_i \otimes k$ contains $\mathrm{Ind}_{C_n}^{D_n} k^{\psi}$, as there is a non-trivial

pairing. But the reason is rather simple. Clearly, as χ is trivial, the action of G on r_i must be trivial modulo $C_3(\mathrm{Im}(\alpha))$. But we also know that the image of r_i must have determinant one, while on the other hand, in the dihedral case the image on which G acts trivially are the homotheties. From there it is clear that the image of r_i must be trivial.

Alternatively one could break up the deformations into deformations of the determinant and deformations with image inside $SL_2(R)$. In the dihedral case with χ being trivial, it is easy to calculate that there are no obstructions for $SL_2(R)$-valued deformations. This is an alternative reason why $\theta(\alpha(r_i)) = 1$ in this case.

6. The Proofs and Precise Statements

We first list, using local Tate duality and the Euler–Poincaré characteristic (see [Mil, Ch. 1, §2]), the cohomological conditions that should govern the relations describing R_E.

LEMMA 6.1. If $\mu_p(L) = \{1\}$, *then* $H^2(G_K, \mathrm{ad}_{\bar{\rho}}) = 0$. *Else we obtain the following for* h_2, *the k dimension of* $H^2(G_K, \mathrm{ad}_{\bar{\rho}}) \cong (Hom(\mathrm{ad}_{\bar{\rho}}, \mathbf{F}_p)^U \otimes \mu_p(L))^G$.

- *If U is trivial and G is abelian, then*

$$(\mathrm{ad}_{\bar{\rho}} \otimes \mu_p(L))^G \cong ((k^{\chi})^2 \oplus k^{\chi\psi} \oplus k^{\chi\psi^{-1}})^G.$$

  (i) *If* χ *acts trivially, then* $h_2 = 2$.
  (ii) *If* $\chi = \psi$ *and the order of* ψ *is two, then* $h_2 = 2$.
  (iii) *If* $\chi = \psi$ *or* $\chi = \psi^{-1}$ *and* $\psi \neq \psi^{-1}$, *then* $h_2 = 1$.
  (iv) *In all other cases,* $h_2 = 0$.

- *If U is trivial and G is not abelian, then*

$$(\mathrm{ad}_{\bar{\rho}} \otimes \mu_p(L))^G \cong ((k^{\chi}) \oplus k^{\chi\phi} \oplus Ind_{C_n}^{D_n} k^{\psi} \otimes k^{\chi})^G.$$

  (v) *If* χ *is trivial, then* $h_2 = 1$.
  (vi) *If* $\chi = \phi$, *then* $h_2 = 1$.
  (vii) *In all other cases* $h_2 = 0$.

- *If U is non-trivial, then*

$$((\mathrm{ad}_{\bar{\rho}})^U \otimes \mu_p(L))^G \cong (k^{\chi} \oplus k^{\psi^{-1}\chi})^G.$$

  (vii) *If* χ *is trivial, then* $h_2 = 1$.
  (ix) *If* $\chi = \psi$, *then* $h_2 = 1$.
  (x) *In all other cases* $h_2 = 0$.

Furthermore $h_1 = 4[K : \mathbb{Q}_p] + \dim_k H^0(G_K, \mathrm{ad}) + h_2$.

We are now in a position to completely determine the universal deformation (R_E, α_E) in all the cases considered here. In Section 5, we calculated the shapes

of all the r_i, that appear. We only have to piece together these expressions to calculate the Demuškin relation modulo $C_3(\mathrm{Im}(\alpha))$ and then construct a representation using Proposition 3.8, which we will then show is the universal one.

We shall continue to use the notation from the previous section and we shall assume that the x_i are chosen as in Lemma 5.3. We shall always assume that $P_0 \cong \mathbb{Z}_p^{\chi}$ and $P_m \cong \mathbb{Z}_p^{triv}$ correspond via duality to $\mathbf{F}_p^{\chi^{-1}}$ and $\mathbf{F}_p^{triv}$ in Theorem 4.2. In particular, x_0 modulo $[G_F(p), G_F(p)]$ is the q torsion element of the abelianisation. If U is non-trivial, we shall take for the g_i, as defined after Theorem 2.1, the elements x_i. If $\bar{\rho}(x_0) \neq I$, then we take $g_1 = x_0$, else we shall assume that $g_1 = x_1$ by a suitable permutation of the indices i – without permuting however $i = 0, m$. For the choices of the $\hat{u}_i$ we also refer to the definitions after Theorem 2.1.

We remark that if we define $s = [K : \mathbb{Q}_p]$, then

$$(\bar{G}_F(p), \mathbf{F}_p^{triv})_G = s + 1 + \delta_K = (\bar{G}_F(p), \mathbf{F}_p^{\chi})_G,$$
$$(\bar{G}_F(p), k^{\tau})_G = s \text{ for any non-trivial character } \tau \neq \chi \text{ of G},$$
$$(\bar{G}_F(p), \mathrm{Ind}_{C_n}^{D_n} k^{\psi})_G = s \text{ if G surjects onto Dn when mapped to PGL2(k)},$$

where δ_k is one if K contains p-th roots of unity and zero else.

THEOREM 6.2. *Let A be the power series ring over $W(k)$ where the indeterminates are exactly the a_i, b_i, c_i, d_i that occur in the expressions for all the $\alpha(x_i)$. Then there exist*

(A) *x_i' which satisfy $x_i' \equiv x_i$ modulo $G_F(p)^{(2,q)}$,*
(B) *an ideal I inside A as described below,*
(C) *and a representation $\alpha' \in E(A/I)$ such that $\alpha'(x_i') = \alpha(x_i)$ where by $\alpha(x_i)$ we mean the formal expressions given in Lemma 5.3.*

The functor represented by $Hom(A/I, \_)$ has the same tangent space as the functor E and in fact they are isomorphic, i.e. $(\alpha', A/I) \cong (\alpha, R_E)$. For the definition of I we will use the cases (i) *to* (vii)*, as described in the previous lemma. The cases* (i) *to* (iv) *will be used for all cases where G is cyclic, so also in the cases where U is non-trivial.*

The description of I is as follows. In cases (i) *to* (iv)*, below, we only list the ideal for trivial U. If U is non-trivial and $g_1 = x_0$, one has to add the variable b_0 to the ideal, and if $g_1 = x_1$, one has to add the variable b_1 to it. Also an expression like $\sum b_i$ means that we sum over all the b_i that exist as variables.*

(i) $I = ((1 + a_0)^q - 1, \sum_i \varepsilon_i c_i (\hat{u}_{m-i} + b_{m-i}) - ((1 + d_0)^q - 1)(1 + d_0)^{-q/2})$.

(ii) $$I = \Big(\sum_i \varepsilon_i (\hat{u}_i + b_i) d_{m-i} (1 + d_{m-i})^{-1/2} - (\hat{u}_0 + b_0) g_q((\hat{u}_0 + b_0)c_0), \sum_i \varepsilon_i c_i d_{m-i} (1 + d_{m-i})^{-1/2} - c_0 g_q((\hat{u}_0 + b_0)c_0) \Big).$$

(iii) $I = (\sum \varepsilon_i d_i (1+d_i)^{-1/2}(\hat{u}_{m-i} + b_{m-i}) - q(\hat{u}_0 + b_0))$ if $\chi = \psi$, *and*
$I = (\sum \varepsilon_i d_i (1+d_i)^{-1/2} c_{m-i} - q c_0)$ if $\chi = \psi^{-1}$.

(iv) $I = (0)$.

(v) $I = ((1+a_0)^q - 1)$.

(vi) $I = (\sum \varepsilon_i b_i b_{m-i} - ((1+d_0)^q - 1)(1+d_0)^{-q/2})$

(vii) $I = (0)$.

Remarks 6.3.

(i) As described in [Mazl, §1.6], by computing the cup-product $H^1(G_K, \mathrm{ad}) \times H^1(G_K, \mathrm{ad}) \to H^2(G_K, \mathrm{ad})$, one could recover the quadratic parts of the relations generating I. If U is trivial, then this can be carried out following the calculations in [Lab]. Apart from the quadratic part there is in some cases a qth power part. This seems unaccessible using cohomological methods.

(ii) In the cases where U is non-trivial, one has to observe, that one or two of the equations in I can be used to eliminate variables of A. This is in agreement with the fact, that for cases (viii) to (x) the number of variables of A is one or two larger than the dimension h_1 of $H^1(G_K, \mathrm{ad})$. After eliminating those variables, the number of equations needed to generate the resulting ideal I' is exactly h_2.

(iii) From the description of R_E, given in the theorem, it follows that R_E is a complete intersection which is flat over $W(k)$.

(iv) The ε_i are still units in $W(k)$, but not necessarily the same as in Lemma 5.6. Furthermore, by replacing the matrix entries b_i, c_i or d_i by $\varepsilon_i^{-1} b_i$, $\varepsilon_i^{-1} c_i$ or $\varepsilon_i d_i$, respectively, one could eliminate the ε_i in the relations for I. Furthermore by a change of variables one could replace the expressions $d_i \sqrt{1+d_i}^{-1/2}$ simply by d_i. Both operations however do complicate the images of the x_i modulo triple and higher commutators.

(v) Finally we note that the equations we find are different from, but necessarily equivalent to those, that one would find by a direct calculation using

$$x_0^q [x_0, x_1] \ldots [x_{m-1}, x_m] = 1.$$

Again this is not the true relation of our Demuškin group, but just an approximation good enough to determine the universal deformation ring. The reason for this discrepancy is simply that we used Theorem 5.4 to calculate the commutators in a linearised form. In many cases one could indeed calculate the above expression directly, for example in all non-dihedral cases where χ is of order greater than two.

Proof. To derive the relation(s) in I, we rewrite the Demuškin relation modulo $C_3(\mathrm{Im}(\alpha))$ as

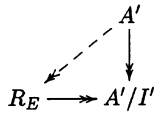
$$\sum_i \theta(\alpha(r_i)) \equiv \theta(\alpha(x_0)^q).$$

We note that this is equivalent to equating θ^{-1} of the left hand side to $\alpha(x_0)^q$ inside $\mathrm{Im}(\alpha)/C_3(\mathrm{Im}(\alpha))$.

In all cases, but $\psi = \chi^{-1} \neq 1$ and $\chi^2 = 1$, it is obvious how to calculate $\alpha(x_0)^q$. In the remaining case we use the functions f_n from Remark 5.5. Then by Proposition 3.8, there is a deformation $\alpha' \in E(A/I)$ with the properties (A) to (C). The statement about the tangent spaces is obvious from the construction.

It remains to show that $(\alpha', A/I)$ is isomorphic to the universal deformation (α_E, R_E). By universality of the latter, there exists a map $R_E \to A/I$ mapping α_E to α'. As the tangent spaces are isomorphic, it follows that the map is surjective.

In the case where U is non-trivial, let A' be the ring A with the superfluous variables eliminated, i.e. with $b_0 = 0$ if $g_1 = x_0$, or $b_1 = 0$ if $g_1 = x_1$, and possibly one more variable eliminated. In the other cases one simply takes $A' = A$. Let I' by the resulting ideal. So then the number of topological generators of A' is exactly h_1. From the smoothness of A' and the completeness of R_E it follows that we can find a surjective lift as indicated in the following diagram.



So we can now think of R_E as a quotient of A' by an ideal J that is contained in I'. Let $\mathfrak{n}'$ be the ideal generated by q and all the remaining variables. Then clearly $I' \subset \mathfrak{n}'^2$.

Now let (α, R) be an arbitrary deformation, with $\mathfrak{n}$ the ideal corresponding to $\mathfrak{n}'$ and where we chose generators according to Lemma 5.3. If U is trivial, then one easily finds that the third step of the Frattini filtration of $\mathrm{Im}(\alpha)$ is contained in the set of matrices that are the identity modulo $\mathfrak{n}^3$. If U is non-trivial, then one has to be a bit more careful. One can show easily that the fourth step of the Frattini quotient is inside the set of matrices

$$M = \left\{ \begin{pmatrix} 1+\alpha & \beta \\ \gamma & 1+\delta \end{pmatrix} : \alpha, \beta, \delta \in \mathfrak{n}^2, \gamma \in \mathfrak{n}^3 \right\}.$$

The possible remainders of the third step of the Frattini filtration modulo M are of the type

$$((\hat{u}_i + b_i)c_j - (\hat{u}_j + b_j)c_i) \begin{pmatrix} 0 & \hat{u}_k + b_k \\ c_k & 0 \end{pmatrix}$$

Also the equations where we eliminate an element after setting $b_0 = 0$ or $b_1 = 0$, resp., come from the $(1, 2)$-entry of the relation matrix written above. So after the elimination there remains at most one equation, and this equation is an explicit expression in products of c_i's and d_j's up to sums of unknown expressions in

$$((\hat{u}_i + b_i)c_j - (\hat{u}_j + b_j)c_i)c_k$$

modulo $\mathfrak{n}^3$. By the following lemma the proof is complete, independently of the shape of U. □

LEMMA 6.4. *Let* $(R, \mathfrak{m})$ *be a complete Noetherian regular local ring and* $\mathfrak{n}$ *an ideal that contains a power of* $\mathfrak{m}$. *Let* $\mathrm{gr}_{\mathfrak{n}}(R)$ *be the associated graded ring. Let* $F_1, \ldots, F_t$ *be functions in* $\mathfrak{n}^k - \mathfrak{n}^{k+1}$ *that are linearly independent in* $\mathfrak{n}^k/\mathfrak{n}^k\mathfrak{m}$ *over* $R/\mathfrak{m}$. *Let* $G_1, \ldots, G_{t'}$ *be functions such that* $F_i \cong G_i$ $(mod\ \mathfrak{n}^k\mathfrak{m})$ *for* $i = 1, \ldots, t$, *and assume that the ideal* $(G_1, \ldots, G_{t'})$ *is contained in* $(F_1, \ldots, F_t)$, *then the ideals are equal.*

Proof. By the containment of the ideals there are $\lambda_{i,j} \in R$ such that $G_i = \sum_j \lambda_{i,j} F_j$. By the linear independence of the F_j modulo $\mathfrak{n}^k\mathfrak{m}$, and the fact that $F_j \equiv G_j (mod\ \mathfrak{n}^k\mathfrak{m})$ it follows that the square matrix $(\lambda_{i,j})_{i,j=1,\ldots,t}$ is invertible modulo $\mathfrak{m}$ and hence invertible over R. Therefore the F_j are in the ideal generated by the G_i. □

Remark 6.5. It is important that we know the precise shape of the relations in the construction of the above deformation, and not just relations up to $\mathfrak{n}^3$, for example! Only this allows us to conclude that $I' \supset J$, and only then the lemma on the rings is true. The lemma cannot apply in cases where one ring is $\mathbb{Z}_p[[T]]/(qT)$ and the other is $\mathbb{Z}_p[[T]]/((1+T)^q - 1)$, even though modulo $\mathfrak{n}^3$ the expressions of the relations agree, because the ideals (qT) and $((1+T)^q - 1)$ are not contained in each other. □

7. The Ordinary Locus

We now apply the methods of the previous sections to identify the ordinary locus of a local representation, and eventually to obtain some information on the ordinary locus of global representations. We follow the definition of ordinary as given in [Maz2]. We note that the definition of ordinary as given in [Dia] or [Wil] corresponds to co-ordinary in [Maz2]. In particular the transition between the two, which can be achieved by a simple twist by the character $\det(\bar{\rho})^{-1}$, changes the determinant to its inverse. So whenever later on we will refer to the determinant of $\bar{\rho}$ in [Dia] or [Wil] one has to be aware of this.

Let I_K be the inertia group of G_K. A two-dimensional representation $\rho_0 : G_K \to \mathrm{GL}_2(R)$ for $R \in \mathcal{C}$ is called ordinary, if for R^2, given a G_K-module structure via the class of ρ_0, the R-submodule of I_K invariants is a free R-module of rank one and a direct summand of R^2, in the sense of R-modules, and the same for any quotient of R. Equivalently one could say that, with respect to a suitable basis of R^2, ρ_0 has the property that

$$\rho_0|_{I_K} \subset \{\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} : x \in R, y \in R^*\}$$

and that $\rho_0(I_K)$ contains either an element of finite order prime to p, or an element $\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix}$ where x is a unit in R. In particular, if $\bar{\rho}$ is ordinary, H cannot be dihedral.

We define the analogous notion for the functor E. We now assume that $\bar{\alpha}$ is ordinary, and that G has non-trivial image in $\mathrm{PGL}_2(k)$, and is mapped under $\bar{\alpha}$ to diagonal matrices, as explained in Section 2, so that the image of $\bar{\alpha}$ is as described in the previous section. We define the functor E^{ord} as

$$E^{ord}(R) = \{\alpha \in E(R) : \alpha|_{I_K} \text{ has (1,1)-entry 1 and (2,1)-entry 0}\}.$$

In Theorem 6.2, we determined the shape of R_E very precisely. However so far, we did not care about possibly choosing the P_i so that the closed normal of all but one of them equals I_K. In fact we used a Demuškin relation that in many cases is too simple to guarantee the above. Until now, we only took into account the non-degenerate alternating pairing on $H^1(G_L, \mathbb{Z}/(p))$ and the choice of an element in our presentation that generates the torsion subgroup of G_L^{ab} (all assuming that $\zeta_p \in L$). Now we also have to incorporate I_K. This is why we need the following refined versions of Propositions 3.4 and 3.8. (We present them here and not in Section 3, as their proofs and statements involve tools and notions from Sections 4 and 5.)

PROPOSITION 7.1. *Let D be a Demuškin group as in Theorem 3.4 with an action of G (we assume that we have the same assumptions and use the same notation as in Theorem 3.4 and its proof). Suppose we have a G-equivariant surjection $\pi : D \to \Gamma$, where Γ is isomorphic to $\mathbb{Z}_p$ with trivial G action, and suppose that the $\mathbb{Z}_p[G]$-module D^{ab} contains at least two copies of $\mathbb{Z}_p^{triv}$ as summands, and that $q > 0$. Then we can find a G-equivariant presentation*

$$1 \to \mathcal{R} \to \mathcal{F} \overset{pr}{\to} D \to 1 \tag{3}$$

such that:

(i) $\bar{\mathcal{F}} \cong \bar{D}$ *under pr.*

(ii) $\mathcal{F}$ *is the free pro-p product of subgroups $\mathcal{F}(i)$, $i = 0, \ldots, m$, where the $\mathcal{F}(i)$ are closed under the action of G, and the $\bar{\mathcal{F}}(i)$ are irreducible $\mathbf{F}_p[G]$-modules. By the last requirement, m is uniquely determined.*

(iii) $\mathcal{F}(0) \cong \mathcal{F}(1) \cong \mathbb{Z}_p^{\chi}$ *and* $\mathcal{F}(m) \cong \mathcal{F}(m-1) \cong \mathbb{Z}_p^{triv}$. *By x_i we denote a topological generator of $\mathcal{F}(i)$ for $i = 0, 1, m-1, m$.*

(iv) *Under the perfect pairing*

$$\begin{aligned}\kappa : (\mathcal{F}_q^{ab})^* \times (\mathcal{F}_q^{ab})^* &\cong H^1(D, \mathbb{Z}/(q)) \times H^1(D, \mathbb{Z}/(q)) \\ &\to H^2(D, \mathbb{Z}/(q)) \cong \mathbb{Z}/(q)^{\chi^{-1}},\end{aligned}$$

$(\mathcal{F}(0)_q^{ab})^*$ is paired with $(\mathcal{F}(m)_q^{ab})^*$, $(\mathcal{F}(1)_q^{ab})^*$ is paired with $(\mathcal{F}(m-1)_q^{ab})^*$, and each $(\mathcal{F}(i)_q^{ab})^*$ is either paired with itself, or a unique $(\mathcal{F}(j)_q^{ab})^*$ where $2 \leqslant i, j \leqslant m-2$.

(v) *The image of $*_{i=2}^{m} \mathcal{F}(i)$ under pr in D^{ab} is a free $\mathbb{Z}_p$-module of rank $n-2$, that of $\mathcal{F}(0) * \mathcal{F}(1)$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}/(q)$. If t is a fixed generator of D_{tors}^{ab}, the torsion subgroup of D^{ab}, then there exist a, b in $\mathbb{Z}$, unique modulo q, such that the image of $x_0^a x_1^b$ under pr in D^{ab} equals t. Furthermore $(a, b) = \mathbb{Z}$.*

(vi) *There is an element r in $\mathcal{R}$ on which G acts via χ, and whose topologically closed normal hull is $\mathcal{R}$, such that*

$$r = \tilde{r}r', \tilde{r} = x_0^{aq}x_1^{bq}[x_0, x_m][x_1, x_m - 1]\tilde{\phi}_q(x)$$

where r' is in $\mathcal{F}^{(3,q)} \cap \mathcal{F}^{(2,0)}$, and $\tilde{\phi}_q$ is the composite of the map $\phi_q : \mathbb{Z}/(q)^\chi \to \mathcal{F}_q^{ab} \times \mathcal{F}_q^{ab}$ from the proof of Theorem 3.4 with the map

$$\tilde{}: \bigwedge^2 \mathcal{F}_q^{ab} \twoheadrightarrow \bigwedge^2 \left(\bigoplus_{i=2}^{m-2} \mathcal{F}(i)_q^{ab} \right),$$

and x is a generator of $\mathbb{Z}/(q)^\chi$. In a less technical language, $\tilde{\phi}_q(x)$ is simply the product of all partial Demuškin relations that come from the pairings among the $(\mathcal{F}(i)_q^{ab})^*$ for $2 \leqslant i \leqslant m-2$ Also G acts on the image of $\tilde{r}$ in the abelian group $\mathcal{F}^{(2,q)}/(\mathcal{F}^{(3,q)} \cap \mathcal{F}^{(2,0)})$ via χ.

Conversely if one has a group with such a presentation it is clearly a Demuškin group with an action of G (by the proof of Theorem 3.4) that comes with a distinguished quotient isomorphic to Γ, where the kernel of this quotient map is the image in D of the closed normal hull of $*_{i=0}^{m-1} \mathcal{F}(i)$.

Proof. We can assume that we have a G-equivariant presentation (3) satisfying (i). We need to study $\mathcal{F}_q^{ab} \cong D_q^{ab}$. Let $\hat{t}$ be an element of $\mathcal{F}$ mapping to $t \in D^{ab}$ on which G acts via χ (this uses Lemma 3.2). We choose $x_m \in \mathcal{F}$ on which G acts trivially and which maps under $pr \circ \pi$ to a generator of Γ. We use s, t for the images of x_m and $\hat{t}$ in $\mathcal{F}_q^{ab}$, and let ξ_s denote the map from $\mathcal{F}_q^{ab}$ to $\Gamma/(q)$ induced from π.

For a free submodule V of $(\mathcal{F}_q^{ab})^*$ we denote by $V^\perp$ the free submodule of $(\mathcal{F}_q^{ab})^*$ that is annihilated by all elements of V under the alternating pairing κ. As the pairing is perfect, it is not hard to prove that $V^\perp$ is again free, and of complementary dimension to V, i.e. $\dim V/(p) + \dim V^\perp/(p) = \dim \mathcal{F}_p^{ab}$. This will be the property of a perfect pairing that we will need most often below. For an element e of $\mathcal{F}_q^{ab}$ that is nonzero in $\mathcal{F}_p^{ab}$, we denote by $\ker(e)$ the free submodule of $(\mathcal{F}_q^{ab})^*$ of maps that vanish on e. (There are two natural dualities we have to deal with.)

We first observe that $V_2 := \langle \xi_s \rangle^\perp \cap \ker(s)$ is a free submodule of $\mathcal{F}_q^{ab}$ of codimension two. Otherwise $(q/p)\langle \xi_s \rangle^\perp \subset \ker(s)$, and so $(q/p)\xi_s(s) = 0$, a contradiction.

As $\ker(s)$ is free over $\mathbb{Z}/(q)$, closed under the action of G, and of codimension one, it follows that $\ker(s)^\perp$ is free of dimension one and closed under the action of G. By ξ_s' we denote a generator of it. It is easy to see that $\langle \xi_s' \rangle^\perp = \ker(s)$. It follows that $\kappa(\xi_s, \xi_s')$ must be a unit, and so we may choose ξ_s' so that this unit is one. Furthermore κ induces a non-degenerate pairing on V_2, because we have $V_2 = \langle \xi_s \rangle^\perp \cap \langle \xi_s' \rangle^\perp$.

Now we look at $\ker(t) \cap V_2$. It is closed under the action of G, and modulo p it has codimension at most one. Thus it is always possible to find a free $\mathbb{Z}/(q)$ submodule V_3 inside $\ker(t) \cap V_2$ of codimension one in V_2, which is closed under the action of G, and so that it has a complement inside V_2 on which G acts via the character χ^{-1} (this uses that $D^{ab}/(p)$ contains at least two copies of $\mathbf{F}_p^{triv}$ and therefore of $\mathbf{F}_p^\chi$).

By ξ_t we denote a generator of this complement, and as before, we construct an element ξ_t' inside V_2 such that $\langle \xi_t' \rangle^{\perp} = V_3$ (inside V_2), and $\kappa(\xi_t, \xi_t') = 1$. We let V_4 be the complement in V_2 of ξ_t' and ξ_t. As before κ restricted to V_4 is non-degenerate and closed under the action of G.

By Proposition 4.3, we can decompose V_4 into projective irreducible $\mathbb{Z}/(q)[G]$-modules, $V_4 = \oplus_{i=2}^{m-2} W_i$, such that under κ each W_i is paired with a unique W_j. We define $W_0 = \langle \xi_s' \rangle$, $W_1 = \langle \xi_t' \rangle$, $W_{m-1} = \langle \xi_t \rangle$, and $W_m = \langle \xi_s \rangle$. Thus $\mathcal{F}_q^{ab} \cong \oplus_{i=0}^{m} W_i^*$, where by our construction $W_m^* = \langle s \rangle$ and $t \in W_0^* \oplus W_1^*$.

We now use Lemma 3.2 to choose a lifting of this decomposition to $\mathcal{F}$. As the elements x_i we take lifts of generators of the W_i^* for $i = 0, 1, m-1, m$. It is then immediate that conditions (i) to (v) are satisfied. One checks that the kernel of $\mathcal{F}^{ab} \to D^{ab}$ is generated by $\tilde{r}$, and as in the proof of Theorem 3.4, that $\tilde{r}$ also generates the kernel of $\mathcal{F}/\mathcal{F}^{(3,q)} \to D/D^{(3,q)}$. From this (vi) follows. Finally one can again appeal to the proof of Theorem 3.4 to see that any group D with a presentation (3) satisfying the conditions (i) to (vi), is a Demuškin group with an action of G. From the properties of the presentation in (3), one deduces the existence of a distinguished G-equivariant quotient isomorphic to Γ. □

Remark 7.2. If D above is the pro-p completion of the absolute Galois group of a local field of characteristic zero and residue characteristic p, then the constants a, b above can be determined, e.g. as in [Koch, §10.3]. (There the variables α_0 and α_1 can be chosen so that G acts via χ on them, and hence the G action poses no problems here.)

The following is a refinement of Proposition 3.8 to the above situation.

PROPOSITION 7.3. *Let D be a Demuškin group with an action of a group G. We assume that we are given a G-equivariant presentation of D as in the previous proposition, and so, in particular, G has a distinguished G-equivariant quotient Γ. Let P be some pro-p group with an action of G. Let r and $\tilde{r}$ be as above. If we have a homomorphism α from $\mathcal{F}$ to P, such that $\alpha(\tilde{r}) \in \alpha(\mathcal{F}^{(3,q)} \cap \mathcal{F}^{(2,0)})$, then there exists a homomorphism α' from D to P with image $\alpha(\mathcal{F})$ that agrees with α modulo $\alpha(\mathcal{F}^{(3,q)} \cap \mathcal{F}^{(2,0)})$. In particular, the image under α' of the kernel of $D \to \Gamma$ and the image under α of the kernel of $\mathcal{F} \to \Gamma$ agree.*

This time we omit the proof, as it is a simple variation of the proof of Proposition 3.8.

With the above tools at hand, it is now clear, how to obtain a description of R_E^{ord} as a quotient of R_E. We first have to recalculate the relations generating the ideal I of A/I using the above refined Demuškin relation $\tilde{r}$. (We only need this in cases (i) to (iii) in the notation of Lemma 6.1.) Then we have to see what further equations we must impose to cut out R_E^{ord} from R_E. For this, we need the previous proposition which gives us a precise description of the image of the inertia group.

To fix the notation, we take for the subgroups P_i the images of the $\mathcal{F}(i)$ after choosing a presentation for $D = G_F(p)$ as in Proposition 7.1 - assuming that

$\zeta_p \in F$. We choose the x_i for $i = 2, \ldots, m-2$ as we did in Section 5, and the element $g_1 \in G_F(p)$ is chosen as follows (provided U is non-trivial). If $\bar{\rho}(x_0) \neq 1$, then we take $g_1 = x_0$, else, if $\bar{\rho}(x_1) \neq 1$, we take $g_1 = x_1$. If neither case applies, and if U is non-trivial, we assume that the $\mathcal{F}(i)$ $(2 \leqslant i \leqslant m-2)$ are ordered in such a way that $\bar{\rho}(x_2)$ is non-trivial, and then we take $g_1 = x_2$. With respect to the above presentation of $G_F(p)$ and choices of x_i, one can now calculate the following equations, i.e. generators of I, by the same method as in Section 6. We use the cases as in the previous section and obtain.

(i)
$$I = \Bigg(\sum_i \varepsilon_i c_i(\hat{u}_{m-i} + b_{m-i}) - (1+d_0)^{aq}(1+d_1)^{bq} + \\ + (1+d_0)^{-aq}(1+d_1)^{-bq}, (1+a_0)^{aq}(1+a_1)^{bq} - 1 \Bigg).$$

(ii)
$$I = \Bigg(\sum_i \varepsilon_i(\hat{u}_i + b_i) d_{m-i}(1+d_{m-i})^{-1/2} - \\ - (\hat{u}_0 + b_0) g_{aq}((\hat{u}_0 + b_0)c_0) - (\hat{u}_1 + b_1) g_{bq}((\hat{u}_1 + b_1)c_1), \\ \sum_i \varepsilon_i c_i d_{m-i}(1+d_{m-i})^{-1/2} - c_0 g_{aq}((\hat{u}_0 + b_0)c_0) - c_1 g_{bq}((\hat{u}_1 + b_1)c_1) \Bigg).$$

(iii)
$$I = \Bigg(\sum \varepsilon_i d_i (1+d_i)^{-1/2}(\hat{u}_{m-i} + b_{m-i}) - q(a\hat{u}_0 + ab_0 + b\hat{u}_1 + bb_1) \Bigg) \text{ if } \chi = \psi,$$
$$I = \Bigg(\sum \varepsilon_i d_i (1+d_i)^{-1/2} c_{m-i} - q(ac_0 + bc_1) \Bigg) \text{ if } \chi = \psi^{-1}.$$

As in the previous section we assume that $\hat{u}_1 = 1$, and the corresponding $b_i = 0$. So in all cases where U is non-trivial, this allows to eliminate one variables using one of the equations.

To find the equations in the case $\chi = \psi$, we used that one can use the square of $\tilde{r}$ as a relation where the order of the individual components is rather arbitrary. Thus we can use $x_0^{aq} x_1^{2bq} x_0^{aq}$ as a part of that relation. When writing θ of the corresponding matrix, one can simplify this expression by peeling off parts that belong the triple and higher commutator parts in the Lie algebra that one considers. This simplifies the equations considerably.

To obtain the ordinary quotient, we have to set all the $c_i = 0$, and have to impose the equations $(1+a_i)(1+d_i) = 1$ for all variables but $i = m$. The number of those equations can be read of from the little table right above Theorem 6.2. Sometimes one of the equations is already implied by imposing all but this equation. We summarise this in the following corollary.

COROLLARY 7.4. *The functor E^{ord} is representable, and the corresponding universal ring R_E^{ord} is isomorphic to the quotient of A/I by the ideal $(c_i, a_j + d_j + a_j d_j \; j \neq m)$.*

In particular, we mod out by exactly $2s$ *equations if* $\chi \neq \psi^{-1}$, *triv or* $\chi = triv$ *and* U *is non-trivial, and by* $2s+1$ *equations otherwise. Furthermore,* R_E^{ord} *is a complete intersection, flat over* $W(k)$ *of relative dimension* $d_{ord} = \dim H^0\ (G_K, \mathrm{ad}) + 2[K : \mathbb{Q}_p]$, *and with* $d_{ord} + \delta_K + \delta_{\chi=\psi}$ *topological generators over* $W(k)$.

We define $\delta_{K,\bar{\rho}}$ to be one if $\chi = \psi^{-1} \neq triv$ and zero otherwise. Thus, unless U is trivial and $\chi = triv$, $2s + \delta_{K,\bar{\rho}}$ is precisely the number of equations needed to cut out R_E^{ord} from R_E. The reason for this will become somewhat clearer after part (ii) of the remark below.

Remarks 7.5.

(i) We note that the number of equations needed to cut out R_E^{ord} as a quotient of R_E is exactly the loss of dimension in the tangent space of the respective rings modulo p. So the number of equations is in all cases as small as possible. However the Krull dimension decreases in all cases only by $2s$ Furthermore one can directly verify our results on the size of tangent spaces modulo p by purely cohomological methods, as for example done in [Wil] in special cases. In cases where R_E^{ord} is known to be smooth, this purely cohomological method suffices to calculate the number of equations, yet in general it doesn't.

(ii) In cases where R_E^{ord} is cut out by $2s+1$ equations from R_E, it seems tempting to try to find a quotient of R_E that has the same Krull dimension as R_E^{ord}, surjects onto the latter, is cut out by $2s$ equations and has an interpretation as a universal ring representing a naturally defined subfunctor of E. So far we were unable to provide a 'geometric' condition describing such a subfunctor in cases where $\psi^{-1} = \chi \neq triv$. (This is the case where $\delta_{K,\bar{\rho}} = 1$.)
If $\chi = triv$ one could use the subfunctor describing deformations such that the image of the deformation is of Borel type and that the action on the $(1,1)$-entry is trivial on a chosen maximal torsion free subgroup of the image of I_F inside $G_F^{ab}(p)$. One can check that this corresponds to a quotient Q of R_E that is cut out by $2s$ equations, and that R_E^{ord} is a quotient of Q by an equation $d = 0$ where the variable d satisfies an equation $(1+d)^q = 1$ in Q, and that Q is flat over $W(k)$. The issue of having only to mod out by $2s$ equations to obtain R_E^{ord} from R_E will become important in the last section.

(iii) If we let $\eta : G_K \to \mathcal{O}^*$, for $\mathcal{O} \in \mathcal{C}$, be such that $\eta(\mathrm{mod}\ \mathfrak{m}_{\mathcal{O}}) = \det(\bar{\rho})$, we can define E^{η} and $E^{ord,\eta}$ as the subfunctors defined over $\mathcal{C}_{\mathcal{O}}$ where one assumes that $\det(\rho) = \eta$. Then one can show easily that those functors are representable and, as in the previous corollary, that the universal ring $R_E^{ord,\eta}$ is obtained from R_E^{η} by dividing out $2s + \delta_{K,\bar{\rho}}$ equations, and furthermore that $R_E^{ord,\eta}$ is a complete intersection, flat over $W(k)$ of relative dimension $d_{ord,\eta} = \dim H^0(G_K, \mathrm{ad}^0) + [K : \mathbb{Q}_p]$, and with $d_{ord,\eta} + \delta_{\chi=\psi}$ topological generators over $W(k)$.
One way to see this is to notice that by twisting with one-dimensional characters, the problem can be reduced to considering maps into $\mathrm{SL}_2(R)$ instead of $\mathrm{GL}_2(R)$ and then everything can be adapted to this case.

8. The Case Where No Prime-to-p Group Acts

Here we want to embark on a short discussion of the case where $\bar{G}$ is trivial. The functor E_Π that we shall consider is the functor described in Remark 2.2 with $\Pi = G_K(p)$. If U is trivial, it is simply the functor of homomorphisms from Π to $\Gamma_2(R)$. We still assume that K is a local field as in Section 2. Relevant for determining the ordinary locus inside the whole space is only the case where U is non-trivial.

In this section, we shall not carry out all the details. We only set up the notation, explain the steps one needs to carry out and present fairly explicit equations from which the theorem at the end of this section will follow readily. We shall consider only the case where $\zeta_p \in K$, so that $G_K(p)$ is a Demuškin group. As $\bar{G}$ is trivial there is no group action that simplifies the shapes of the images of generators of G_F.

We can and will assume that G itself is trivial. To justify this assumption, we remark that the triviality of $\bar{G}$ implies that the image of G comes to lie in the set of scalar matrices, and so one can replace $\bar{\rho}$ by a twist for which G is trivial. On the level of universal deformation spaces such a twist gives an isomorphism. Furthermore if $\bar{\rho}$ is ordinary, then the same holds for the twist, which must then be a twist by an unramified character, and so there is also an isomorphism of the corresponding ordinary universal deformation spaces.

We use the notation as in Proposition 7.1 and remark, that all the references to G can simply be ignored, that all the $\mathcal{F}(i)$ are isomorphic to $\mathbb{Z}_p$, that for each i we pick any generator x_i of each $\mathcal{F}(i)$, and that the relation we need to consider is

$$\tilde{r} = x_0^{aq} x_1^{bq} [x_0, x_m][x_1, x_m - 1][x_2, x_{m-2}] \dots [x_{(m-1)/2}, x_{(m+1)/2}].$$

(This is the Demuškin relation, as given for example in [Koch, §10.3].) The image of x_i we represent as a matrix $\sqrt{1+e_i}M_i$ where $M_i = \begin{pmatrix} a_i & \hat{u}_i + b_i \\ c_i & d_i \end{pmatrix}$ is of determinant one. One now introduces a new variable $z_i = a_i - d_i$. Because of our condition on the determinant it is possible to express a_i and d_i in terms of $\hat{u}_i + b_i$, c_i and z_i. We take these three together with e_i as independent variables. We also let $\delta_i = (\hat{u}_i + b_i)c_i + z_i^2$.

Again the calculus of Pink will be crucial. Using Cayley–Hamilton, one can show that $\theta(M_i^n) = g_n(\delta_i)\theta(M_i)$, g_n the function from Remark 5.5. We remark that $g_{nm}(\delta_i) = g_m(\delta_i g_n(\delta_i)^2) g_n(\delta_i)$, and modulo p, $g_{p^i}(\delta_i) = \delta_i^{(p^i-1)/2}$, and $g_n(\delta_i)$ is a unit whenever n is a unit in $\mathbb{Z}_p$.

When setting up the equation corresponding to $\tilde{r}$ in the Lie algebra defined by Pink, the use of a symmetric expression for the image of $x_0^{aq} x_1^{bq}$ modulo the image of $\mathcal{F}^{(3,q)} \cap \mathcal{F}^{(2,0)}$ simplifies the matrix relation significantly. One needs to check that this can indeed be done modulo L_3. With these simplifications one obtains two relations that give four equations for the universal deformation space, namely

$(1+e_0)^{aq}(1+e_1)^{bq}=1$, and

$$\sum_i \begin{pmatrix} (\hat{u}_i+b_i)c_{m-i}-(\hat{u}_{m-i}+b_{m-i})c_i & 2z_i(\hat{u}_{m-i}+b_{m-i})-2z_{m-i}(\hat{u}_i+b_i) \\ 2c_iz_{m-i}-2c_{m-i}z_i & c_i(\hat{u}_{m-i}+b_{m-i})-c_{m-i}(\hat{u}_i+b_i) \end{pmatrix}$$
$$= \sqrt{1+\delta_0 g_{aq}(\delta_0)^2}\, g_{bq}(\delta_1)\begin{pmatrix} z_1 & \hat{u}_1+b_1 \\ c_1 & -z_1 \end{pmatrix} + \sqrt{1+\delta_1 g_{bq}(\delta_1)^2}\, g_{aq}(\delta_0)\begin{pmatrix} z_0 & \hat{u}_0+b_0 \\ c_0 & -z_0 \end{pmatrix}$$

Modulo p, the expression $g_{aq}(\delta_0)$ can be written as $\delta_0^{(q-1)/2} g_a(\delta_0)^q$. From this one can see that the universal ring R_E is flat over $W(k)$ of relative dimension $h_1-h_2=4[K:\mathbb{Q}_p]+h_0$.

It is now obvious how to describe the ordinary locus and the number of equations needed to cut it out. If the analysis is carried out properly one obtains the following result that holds trivially if K does not contain ζ_p.

THEOREM 8.1. *If we are given $\bar{\rho}: G_K \to \mathrm{GL}_2(k)$, K a local field of residue characteristic p, and if the image of $\bar{\rho}$ in $\mathrm{PGL}_2(k)$ is a p-group, then the universal space R_E is a complete intersection, flat over $W(k)$ of relative dimension $4[K:\mathbb{Q}]+h_0$.*

If further $\bar{\rho}$ is ordinary, then R_E^{ord} is a quotient of R_E by exactly $2([K:\mathbb{Q}]+\delta_K)$ equations, and the same is true for $R_{E,\mathcal{O}}^{ord,\eta}$ as a quotient of $R_{E,\mathcal{O}}^{\eta}$, if we have a given determinant $\eta: G_K \to \mathcal{O}$ that agrees modulo p with $\det(\bar{\rho})$. Also, all the universal rings above are complete intersection and flat over $W(k)$.

In this case we define $\delta_{K,\bar{\rho}}=\delta_K$. In the same way as in part (ii) of Remark 7.5, one can show that R_E has a reasonably defined quotient which is a complete intersection, flat over $W(k)$, we call it Q, cut out by $2s+\delta_{K,\bar{\rho}}$ equations such that R_E^{ord} is a quotient of Q by an equation $d=0$ where modulo p, the expression d satisfies $d^q=0$ in Q (and so $R_E/(p)$ and $Q/(p)$ have the same reduced quotients.) This explains the choice of $\delta_{K,\bar{\rho}}$.

We also mention that, when computing the equations for the ordinary quotient, there is one particular case, the case when x_m maps to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ under $\bar{\rho}$, when it is more convenient to work with a different description as given in Remark 2.2. Then it is better to rigidify Lift_Π by requiring that $\rho(x_m)=\begin{pmatrix} * & 1 \\ * & * \end{pmatrix}$ and in addition $\rho(x_i)=\begin{pmatrix} 1 & * \\ * & * \end{pmatrix}$ for some $i \neq m$.

9. Applications to the Structure of Global Deformation Rings

We shall now apply the above results to the global situation. For the proper definitions see [Maz1, Maz2].

In the following, we let M be a number field. $S_p=\{\mathfrak{p}_i : i=1,\ldots,t\}$ will denote the set of places of M above p. S will denote a finite set of places of M, containing all places above p and above ∞, $G_{M,S}$ the Galois group of the maximal Galois extension of M, unramified outside S. Exceptionally, we shall denote by $G_{M,\{p,\infty\}}$ the Galois group $G_{M,S}$ with S the set of all places of M above p and ∞.

We present as a first application of Theorem 6.2 a generalisation of an example in [Bos1, 8.1] – in fact the proof as presented there contains a small oversight, as, in the notation from loc. cit., $(W_2, \mathrm{ad}) = 1$ and not zero as claimed there. So the argument there would need to be modified.

COROLLARY 9.1. *Given $\bar{\rho} : G_{\mathbb{Q},S} \to \mathrm{GL}_2(k)$ an odd, absolutely irreducible Galois representation with splitting field L over $\mathbb{Q}$ where S is a finite set of places of $\mathbb{Q}$ containing p and ∞. In particular, the global universal deformation ring R_S of the global deformation problem in the sense of [Maz1] for deformations unramified outside S exists. Assume the following conditions.*

(i) $\bar{\rho}_{|G_{\mathbb{Q}_p}} \sim \begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}$ *such that $\chi_1\chi_2^{-1} = \chi$ is the mod p cyclotomic character, where $G_{\mathbb{Q}_p}$ is some (any) chosen decomposition group of p inside $G_{\mathbb{Q},S}$.*

(ii) $H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathrm{ad}) = 0$ (this holds for example if $\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbf{F}_p)$, if $\mathrm{Gal}(L/\mathbb{Q}) \supset \mathrm{SL}_2(k)$ and $p > 5$, or if $\bar{\rho}$ is tame).

(iii) p does not divide the class group of $L(\zeta_p)$ – or, weaker, the semisimplification of the class group of $L(\zeta_p)$ as an $\mathbf{F}_p[\mathrm{Gal}(L(\zeta_p)/\mathbb{Q})]$-module admits no non-trivial map to $\mathrm{ad}_{\bar{\rho}}$ or $\mathrm{ad}^0_{\bar{\rho}}(1)$.

(iv) As an $\mathbf{F}_p[\mathrm{Gal}(L/\mathbb{Q})]$-module, the cokernel of $\mu_p(L) \to \bigoplus_{\mathfrak{q}|l \in S-\{p,\infty\}} \mu_p(L_\mathfrak{q})$ admits no non-trivial map to $\mathrm{ad}_{\bar{\rho}}$.

If $p = 3$, then R_S is isomorphic to $W(k)[[X_1, \ldots, X_5]]/I$ where the ideal I has the following description. There are variables $U_1, \ldots, U_6$ in the ideal $(X_1, \ldots, X_5)$, the images of a set of coordinates of the local at p deformation problem, such that

$$I = (U_1U_3 + U_4U_6 - U_4(3 + 4U_4U_5),\ U_2U_3 + U_5U_6 - U_5(3 + 4U_4U_5)).$$

If $p > 3$, then

$$R_S \cong W(k)[[X_1, \ldots, X_4]]/(U_1U_2 + U_4(U_3 - q))$$

where again $U_1, \ldots, U_4$ are images of a set of coordinates of the local at p deformation problem.

If we suppose further that $\zeta_p \in L$, or that there is a complex conjugation c of $\mathrm{Gal}(L/\mathbb{Q})$ which lies inside $\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)$ for some place $\mathfrak{p}$ of L above p such that c acts non-trivially on $\mathbb{Q}_p(\zeta_p)$ (by assumption (i) $L_\mathfrak{p}$ contains ζ_p), then the following identifications can be made. If $p = 3$, and if the image of $\bar{\rho}$ is conjugate to a subgroup of $\mathrm{GL}_2(\mathbf{F}_3)$, or if $\bar{\rho}$ is tame, then we can choose $X_4 = U_4$ and $X_5 = U_5$. If $p > 3$ and $\bar{\rho}$ is tame, then we can choose $X_2 = U_2$ and $X_4 = U_4$.

Proof. Conditions (iv) and (ii) together with the part of (iii) referring to $\mathrm{ad}_{\bar{\rho}}$ imply that

$$H^2(G_{\mathbb{Q},S}, \mathrm{ad}) \to H^2(G_{\mathbb{Q}_p}, \mathrm{ad})$$

is an isomorphism (this follows from the Poitou-Tate sequence, e.g. [Boe2, §6]). From [Boe2, §5], it follows that the only relations necessary in a minimal presen-

tation of R_S are those coming from the local deformation problem at p. (In the tame case any references to [Boe2] are unnecessary; one can always use the methods provided in [Bos1].) From Theorem 6.2 we can then read off the explicit shape of the relations given above where the U_i are images of coordinates of the deformation problem at p. If necessary we can also make a change of variables $U_i\sqrt{1+U_i}^{-1/2} \mapsto U_i$. This establishes the first part of the corollary. It remains to verify that in the special cases we can identify the variables as described in the proposition. (As in [Bos1], one can only hope to identify some of the local variables.)

Let R_p denote the (versal) deformation ring of the local at p deformation problem. Then there is a canonical map from R_p to R_S. If $\mathfrak{m}_A$ denotes the maximal ideal of a local ring A, we need to study the induced map

$$\mathfrak{m}_{R_p}/(p, \mathfrak{m}_{R_p}^2) \to \mathfrak{m}_{R_S}/(p, \mathfrak{m}_{R_S}^2),$$

or equivalently its dual map $H^1(G_{\mathbb{Q},S}, \mathrm{ad}) \to H^1(G_{\mathbb{Q}_p}, \mathrm{ad})$. For this we consider the following diagram where the rows are inflation-restriction sequences.

$$\begin{array}{ccccccc} 0 \to & H^1(G_{\mathbb{Q},S}, \mathrm{ad}^0) & \to & Hom_{\mathrm{Gal}(L/\mathbb{Q})}(G_{L,S}, \mathrm{ad}^0) & \to 0 \\ & \alpha\downarrow & & \beta\downarrow & \\ 0 \to & H^1(G_{\mathbb{Q}_p}, \mathrm{ad}^0) & \to & Hom_{\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)}(G_{L_\mathfrak{p}}, \mathrm{ad}^0) & \to 0 \end{array}$$

The four outer zeros in the diagram follow from assumptions (i) and (iii) together with the tameness of $\bar{\rho}$, or the property that $\mathrm{Im}(\bar{\rho})$ is inside $\mathrm{GL}_2(\mathbf{F}_3)$. α is injective by assumption (iii). We want to study β. The structure of $G_{L_\mathfrak{p}}^{ab}/(p)$ as a Galois module was given in Section 4 to be

$$\mathbf{F}_p \oplus \mathbf{F}_p^\chi \oplus \mathbf{F}_p[\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)].$$

By assumptions (iii) and (iv), invoking the methods from [Bos1], in particular the results from §3 of loc.cit., β surjects onto the quotient $Hom_{\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)}(\mathbf{F}_p^\chi, \mathrm{ad}^0)$ of $Hom_{\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)}(G_{L_\mathfrak{p}}, \mathrm{ad}^0)$. Thus we can choose the images in R_S of the corresponding local variables to be basis elements of $\mathfrak{m}_{R_S}/(p, \mathfrak{m}_{R_S}^2)$. In the case $p = 3$, this achieves what we wanted. For $p > 3$ it allows us to choose $X_4 = U_4$. In the tame case if $p > 3$, one can actually show that β surjects onto $Hom_{\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)}((\mathbf{F}_p^\chi)^2, \mathrm{ad}^0)$, where the second copy of $\mathbf{F}_p^\chi$ is a summand of $\mathbf{F}_p[\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)]$. This uses that there is a complex conjugation that acts non-trivially on $\mathbb{Q}_p(\zeta_p)$. Thus the choice $X_2 = U_2$ is justified. (The names of the global variables to which we assign local ones are arbitrary, as we did not fix a choice of the global variables at the beginning.) □

Remark 9.2. The problem with identifying local and global variables in the case that $\bar{\rho}$ is not tame is that there isn't necessarily a zero at the right end of the top row (but the group $H^2(\mathrm{Gal}(L/\mathbb{Q}), \mathrm{ad}^0)$). Thus it could happen that the part of $Hom_{\mathrm{Gal}(L/\mathbb{Q})}(G_{L,S}, \mathrm{ad}^0)$ that surjects onto $Hom_{\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)}(\mathbf{F}_p^\chi, \mathrm{ad}^0)$ maps non-trivially to $H^2(\mathrm{Gal}(L/\mathbb{Q}), \mathrm{ad})$. It seems very difficult to study when this happens.

The next goal is a generalisation of the Main Proposition of [Maz2] from which we shall then derive results on the universal deformation spaces with no restrictions at the place p.

Let $\bar{\rho} : G_{M,S} \to \mathrm{GL}_2(k)$ be a Galois representation such that the centraliser of $\mathrm{Im}(\bar{\rho})$ inside $\mathrm{GL}_2(k)$ is the set of homotheties. $\eta : G_M \to \mathcal{O}^*$ will denote a character extending $\det(\bar{\rho})$ for some fixed $\mathcal{O} \in \mathcal{C}$ finite over $W(k)$. The splitting field of $\bar{\rho}$ will be the field corresponding to the kernel of $\bar{\rho}$. We suppose that $\bar{\rho}$ is ordinary at all primes in $\Sigma = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} \subset S_p$, $r \leqslant t$, i.e., the restriction of $\bar{\rho}$ to the local Galois groups $G_{M_{\mathfrak{p}_i}}$ are ordinary in the above sense for $i = 1, \ldots, r$. Let $s_i = [M_{\mathfrak{p}_i} : \mathbb{Q}_p]$ and $\delta_i = \delta_{M_{\mathfrak{p}_i}, \bar{\rho}}$, which was defined in the previous two sections. From now on, h_i is used for the k-dimension of $H^i(G_{M,S}, \mathrm{ad})$.

We shall define several universal deformation problems, which are easily seen to be representable. $(\rho_{S,\mathcal{O}}, R_{S,\mathcal{O}})$ will be a universal couple representing all deformations of $\bar{\rho}$ to rings in $\mathcal{C}_{\mathcal{O}}$, unramified outside S. If $\mathcal{O} = W(k)$, $\mathcal{O}$ will be omitted in the notation. Note that $R_{S,\mathcal{O}} = R_S \otimes_{W(k)} \mathcal{O}$ whenever R_S is defined, and $\mathcal{O}$ is finite flat over $W(k)$. The superscript $\Sigma{-}ord$ will mean that the deformations are supposed to be ordinary at all $\mathfrak{p}_i \in \Sigma$, the superscript η, that the determinant of the deformations is fixed to be η, and several superscripts separated by commas shall mean that all the conditions listed are supposed to be verified. We obtain immediately from the results in Section 8.

COROLLARY 9.3. *If all the conditions on M and $\bar{\rho}$ listed above are satisfied, then $(\rho_S^{\Sigma-ord}, R_S^{\Sigma-ord})$ is a quotient of (ρ_S, R_S) obtained by dividing R_S by at most $\sum_{i=1}^{r} 2s_i + \delta_i$ equations. The same holds for $(\rho_{S,\mathcal{O}}^{\Sigma-ord,\eta}, R_{S,\mathcal{O}}^{\Sigma-ord,\eta})$ as a quotient of $(\rho_{S,\mathcal{O}}^{\eta}, R_{S,\mathcal{O}}^{\eta})$.*

Remark 9.4. If we specialise this to the situation $M = \mathbb{Q}$ and S any set of places containing $\{\infty, p\}$ as in [Maz2], then R_S^{ord} is a quotient of R_S by at most two equations, provided that $\chi_1^{-1}\chi_2 \neq \chi$ if $\bar{\rho}$ is given by $g \mapsto \begin{pmatrix} \chi_1(g) & a(g) \\ 0 & \chi_2(g) \end{pmatrix}$. This is certainly satisfied if $\det(\bar{\rho}) \neq \chi$ if restricted to the inertia group at p. So Corollary 9.3 strengthens the Main Proposition of [Maz2].

We will now discuss the consequences for (ρ_S, R_S) if we know certain ring-theoretic properties of $R_{S,\mathcal{O}}^{\Sigma-ord,\eta}$. The rings for which such properties have been established recently are the rings $R_{S,\mathcal{O}}^{S_p-ord,\eta}$ where M is totally real and satisfies some further assumptions stated below.

LEMMA 9.5. *Let $\mathcal{O}$ be a finite flat local $W(k)$-algebra in $\mathcal{C}$, and so for $\mathcal{O}$-modules, flatness over $\mathcal{O}$ and over $W(k)$ is equivalent. Let $R, R' \in \mathcal{C}_{\mathcal{O}}$, and suppose we are given surjections $S = \mathcal{O}[[x_1, \ldots, x_n]] \to R' \to R$ where R is finite flat over $\mathcal{O}$, the kernel of $S \to R'$ is an ideal generated by m equations, and that of $R' \to R$ by l so that $l + m \leqslant n$. Then $l + m = n$, R, R' are complete intersections, and R' is flat over $\mathcal{O}$ of relative dimension l.*

Furthermore, if R' is obtained by base change from $W(k)$ to $\mathcal{O}$ from a quotient R_0 of $W(k)[[x_1, \ldots, x_n]]$, cut out by at most m equations, then R_0 itself is a complete intersection, flat over $W(k)$ of relative dimension l over $W(k)$.

Proof. The prove of the first part is straightforward, as the quotient of a ring of dimension $n+1$ by s equations has dimension greater or equal to $n+1-s$. If the top ring is smooth, and the quotient ring has dimension equal to $n+1-s$, then the quotient ring is a complete intersection. Regarding the flatness, let $f_1, \ldots, f_m$ be elements of S generating the kernel of $S \to R'$, and let $f_{m+1}, \ldots, f_n$ be lifts to S of elements of R' spanning the kernel of $R' \to R$. Then by flatness of R over $W(k)$, the elements $f_1, \ldots, f_n, p$ form a regular sequence. As S is local, any subsequence of any reordering is a regular sequence, in particular $f_1, \ldots, f_m, p$. The statement about R_0 is also straightforward. □

From now on we shall assume that M is totally real. For R we will take the ring $R^{\eta}_{S,\mathcal{O}}$, and for R' the ring $R^{S_p-ord,\eta}_{S,\mathcal{O}}$ where we assume that there exists an ordinary Hilbert modular eigenform f whose associated p-adic representation $\rho_{f,p} : G_M \to \mathrm{GL}_2(\mathcal{O})$ takes values in $\mathcal{O}$, or equivalently such that all the Hecke eigenvalues of f are in $\mathcal{O}$, where $\mathcal{O} \in \mathcal{C}$ is a discrete valuation ring, finite over $W(k)$. Also we shall assume that $\bar{\rho}$ is such that the deformation functor is representable.

By [Maz1, Prop. 2], it is known that $R_S/(p)$ is a quotient of $k[[x_1, ..., x_{h_1}]]$ by at most h_2 equations. In fact as is noted in [Boe2], one can check that Mazur's argument also shows that R_S is a quotient of $W(k)[[x_1, \ldots, x_{h_1}]]$ by at most h_2 equations.

For $R^{S_p-ord,\eta}_{S,\mathcal{O}}$ it has been established in many cases that it is finite flat over $\mathcal{O}$, by constructing an explicit isomorphism to a certain universal Hecke algebra. We now state several sufficient sets of conditions under which the structure of $R^{S_p-ord,\eta}_{S,\mathcal{O}}$ is known. References are [Dia], [TaWi], [Wil] for the first part and [Fuji] for the second.

THEOREM 9.6. *If $M = \mathbb{Q}$, and if $\bar{\rho}$ is absolutely irreducible if restricted to $G_{\mathbb{Q}(\zeta_p)}$, modular and p-ordinary, then for any finite set S, $R^{p-ord,\eta}_{S,\mathcal{O}}$ is finite flat over $\mathcal{O}$, where $\mathcal{O}$ is determined as described above by a cusp form that gives rise to $\bar{\rho}$.*

If M is totally real, linearly disjoint from $\mathbb{Q}(\zeta_p)$, unramified over $\mathbb{Q}$ at all places above p, if p is prime to the class number of M and if $\bar{\rho}$ is absolutely irreducible if restricted to $G_{M(\zeta_p)}$, p-ordinary, has a minimal modular lifting, and is unramified outside p and infinity, then $R^{p-ord,\eta}_{(p,\infty),\mathcal{O}}$ is finite flat over $\mathcal{O}$, $\mathcal{O}$ associated to a Hilbert modular cusp form as above.

The results of Fujiwara are stronger than we quote them in the second part above. But we only use the above as an example to demonstrate the general method, that we learned from [Maz3], that leads to Corollary 9.8 below.

LEMMA 9.7. *Suppose $R \in \mathcal{C}$ and $y \in R$ is an element satisfying an equation $g(y) \in W(k)[y]$ such that $R/(p, y)$ is finite and $g(y) \equiv y^l \pmod{p}$ for some integer l,*

and suppose that one has an surjection $\mathcal{O}[[x_1, \ldots, x_n]] \to R$ *whose kernel is generated by at most n elements* $f_1, \ldots, f_n$, *where* $\mathcal{O}/W(k)$ *is finite flat. Then R is a complete intersection, finite flat over* $W(k)$.

By induction it is obvious that the statement also holds if we mod out by several variables y_i *all subject to analogous conditions to the y above.*

Proof. In $R/(p)$ the image $\bar{y}$ of y satisfies $\bar{y}^l = 0$. So $(R/(p))_{red} \cong (R/(p, y))_{red}$. This implies that $R/(p)$ is zero dimensional. Hence $f_1, \ldots, f_n, p$ form a regular sequence. But then $R \cong \mathcal{O}[[x_1, \ldots, x_n]]/(f_1, \ldots, f_n)$ is a complete intersection, flat over $W(k)$ and hence finite over it, as it has relative dimension zero. □

COROLLARY 9.8. *We assume that* M, $\bar{\rho}$, S *are as in the previous theorem, in particular* $S = S_p \cup \{\text{infinite places}\}$, *if* $M \neq \mathbb{Q}$, *and that* Σ *is any subset of* S_p. *Further we assume that there exists a totally even* k^**-valued character* ξ *of M such that* $\delta_i = 0$ *for all primes* $\mathfrak{p}_i$ *in M dividing p for the residual representation* $\bar{\rho} \otimes \xi$. *Then* R_S *and* $R^{\eta}_{S,\mathcal{O}}$ *are complete intersections, flat over* $W(k)$ *of relative dimension* $2[M : \mathbb{Q}] + 1 + \delta_M$, $2[M : \mathbb{Q}]$, *resp. If* ξ *is trivial, then also* $R^{\Sigma-ord,\eta}_{S,\mathcal{O}}$ *is a complete intersections, flat over* $W(k)$, *and of relative dimension* $2\sum_{i:\mathfrak{p}_i \notin \Sigma} s_i$. *Finally for* $M = \mathbb{Q}$ *our condition on the vanishing of the* δ_i *for some twist of* $\bar{\rho}$ *is equivalent to the condition that the restriction of* $\bar{\rho}$ *to a decomposition group at p is neither peu ramifié nor très ramifié in the sense of Serre ([Ser]).*

The proof in the case of fixed determinant η is an immediate consequence of the Theorem 9.6 using Corollary 9.3 and Lemmas 9.5 and 9.7. (It also uses that twisting $\bar{\rho}$ by a character induces isomorphisms of the corresponding universal rings R_S and $R^{\eta}_{S,\mathcal{O}}$, where η will be different for the twisted representation.)

To obtain the results without having to fix the determinant, one can use the following isomorphism, which holds in fact also for the associated deformation spaces, $R_{S,\mathcal{O}} \cong R^{\eta}_{S,\mathcal{O}} \hat{\otimes} \mathbb{Z}[[\Gamma_S]]$ where Γ_S is the maximal abelian outside S unramified extension of M. This can be found in [Hida] or [Boe2].

Remarks 9.9.

(i) Similar results on $R^{\Sigma-ord}_{S,\mathcal{O}}$ can be derived from results obtained by Hida in [Hida].

(ii) One can prove that R_S and R^{η}_S are complete intersections, flat over $W(k)$ and of the dimension predicted by Mazur, by reasoning as above, also in the following cases.

   (a) Suppose $M = \mathbb{Q}$, $\bar{\rho}$ restricted to the decomposition subgroup at p is associated to a finite flat group scheme over $\mathbb{Z}_p$, $\bar{\rho}$ is modular and S is finite.
   This can be seen as follows. By work of Ramakrishna, see [Ram], the local universal deformation ring associated to finite flat deformations with fixed determinant is isomorphic to $\mathbb{Z}_p[[x]]$, and the local deformation ring R^{η} for deformations with fixed determinant is isomorphic to $\mathbb{Z}_p[[x_1, x_2, x_3]]$. So the former is a quotient of the latter by two equations. Now one can conclude as above using the results by Wiles and Diamond in [Wil] and [Dia].

(b) Suppose M is arbitrary totally real and satisfies all the conditions of Theorem 9.6 but the condition of p-ordinariness. Instead we require that the restriction of $\bar{\rho}$ to the inertia groups at primes above p is either flat or ordinary and satisfies $\delta_i = 0$ at all ordinary places (so some of the places can be of one type and some of the other). Then one can use [Fuji] and [Ram] to conclude. It is conceivable that this also works, if one uses the weaker assumptions considered in [Con] instead of flatness at the primes $\mathfrak{p}_i$.

(iii) It seems rather unfortunate, that, as we mentioned in Remark 7.5 (ii), we do not have a geometric condition at the place p replacing ordinariness, in the cases when $\bar{\rho}$ restricted to p is peu or très ramifié, and such that the quotient corresponding to this condition is cut out by precisely $2s$ equations. Then for $M = \mathbb{Q}$, one could try to investigate in the global case if deformations satisfying this condition at p and having fixed determinant are represented by a universal ring that is finite flat over $W(k)$.

(iv) Let S_0 be the union of the set of places where $\bar{\rho}$ ramifies and the set of all places above p and infinity. It can be shown, see [Boe1], that if the minimal universal ring, i.e. the one where one has as little freedom as possible for the deformations at all places away from p, is finite flat over $W(k)$, then the ring R_{S_0} has the same property.

Deriving results on $R_{S'}$ from R_S, if S' contains S, seems in general rather difficult. The only primes that one could add, we believe, are the primes of the type used by Wiles as auxiliary primes, as those are the only unramified primes where the local equation does only depend on the local ramification group.

So enlarging the set S of primes where ramification is allowed should always be first treated for the 'small' deformation spaces, i.e. with ordinariness restrictions and fixed determinant, or with a flatness condition at p, as there one has good control over the universal deformation by comparing it with corresponding Hecke algebras. Then raising of the level can usually be achieved by some criteria of Lenstra and Wiles. Only afterwards one can apply our methods to remove the constraints at places above p.

(v) It could be hoped that our results might help answering the following question. Is the set of modular points, i.e. elements of $\mathrm{Spec}(R_S)$ that correspond to modular forms, Zariski dense in it? Is there a universal Hecke algebra that is isomorphic to the universal deformation space R_S? There has been some progress by Gouvêa and Mazur [GoMa] for $M = \mathbb{Q}$, in special cases. They show the density using some results of Coleman, and they construct a candidate of a p-adic Hecke algebra. In fact Coleman's results seems to provide a way to fill up Zariski dense three-dimensional neighbourhoods of a modular point of $R_S[1/p]$. By our results, $\mathrm{Spec}(R_S[1/p])$ has dimension three in many cases, and so one could hope that this would help in the density question. This requires that one have at least one modular point. Regarding the isomorphism with the p-adic Hecke algebra, again it might be important to know that R_S has relative dimension three. We plan to further discuss this in a future publication.

References

[Boe1] Böckle, G.: Explicit universal deformations of even Galois representations, Accepted by *Math. Nachr.*

[Boe2] Böckle, G.: A local-to-global principle for deformations of Galois representations, *J. Reine Angew. Math.* **509** (1999), 199–236.

[Bos1] Boston, N.: Explicit deformations of Galois representations, *Invent. Math.* **103** (1990), 181–196.

[Bos2] Boston, N.: Families of Galois representations – Increasing the ramification, *Duke Math. J.* **66** (3) (1992), 357–367.

[Con] Conrad, B.: Ramified deformation problems, *Duke Math. J.* **97** (3) (1999), 439–513.

[Dia] Diamond, F.: On deformation rings and Hecke rings, *Ann. of Math.* **144** (1996), 137–166.

[Dem1] Demuškin, S.: On the maximal p-extension of a local field (Russian), *Izv. Akad. Nauk, USSR. Math. Ser.* **25** (1961), 329–346.

[Dem2] Demuškin, S.: On 2-extensions of a local field (Russian), *Sibirsk. Mat. Z.* **4** (1963), 951–955.

[FoMa] Fontaine, J.-M. and Mazur, B.: Geometric Galois representations, in: J. Coates (ed.), *Elliptic Curves, Modular Forms and Fermat's Last Theorem*, International Press, Cambridge.

[Fuji] Fujiwara, K.: Deformation rings and Hecke algebras in the totally real case, Preprint, 9 July, 1996.

[GoMa] Gouvêa, F. and Mazur, B.: On the density of modular representations, In: *Computational Perspectives on Number Theory* (*Chicago; IL, 1998*), AMS/IP Stud. Adv. Math. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 127–142.

[Hida] Hida, H.: Adjoint modular Selmer groups of several variables over totally real fields, Note of lectures given at Université de Paris-Nord, 17 June, 1997.

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

[JaWi] Jannsen, U. and Wingberg, K.: Die Struktur der absoluten Galoisgruppe p-adischer Zahlkörper, *Invent. Math.* **70** (1982), 71–98.

[Koch] Koch, H.: Über Darstellungssäume und die Struktur der multiplikativen Gruppe eines p-adischen Zahlkörpers, *Math. Nachr.* **29** (1965), 77–111.

[Lab] Labute, J.: Classification of Demuškin groups, *Canad. J. Math.* **19** (1967) 106–132.

[Laz] Lazard, M.: Sur les groupes nilpotents et les anneaux de Lie, *Ann. Ecole Sup. Norm* **71** (1954), 101–190.

[MacL] MacLane, S.: *Homology*, Grundlehren Math. Wiss. 114, Springer-Verlag, New York, 1975.

[Maz1] Mazur, B.: Deforming Galois representations, in *Galois Groups over* $\mathbb{Q}$, Springer-Verlag, New York, 1987.

[Maz2] Mazur, B.: Two-dimensional p-adic Galois representations unramified away from p, *Compositio Math.* **74** (1990), 115–133.

[Maz3] Mazur, B.: An 'infinite fern' in the universal deformation space of Galois representations, *Proc. Journées Arithméthiques*, Barcelona, 1995.

[Mil] Milne, J. S.: *Arithmetic Duality Theorems*, Perspect. Math. 1, Academic Press, Boston, MA, 1986.

[Pink] R. Pink, Classification of pro-p subgroups of SL_2 over a p-adic ring, where p is an odd prime, *Compositio Math.* **88** (1993), 251–264.

[Ram] Ramakrishna, R.: On a variation of Mazur's deformation functor, *Compositio Math.* **87** (1993), 269–286.

[Ser] Serre, J.-P.: Sur les représentations modulaires de degré 2 de Gal($\bar{\mathbb{Q}}/\mathbb{Q}$), *Duke Math. J.* **54** (1987), 179–230.

[TaWi] Taylor, R. and Wiles, A.: Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* **141** (1995), 553–572.

[Wil] Wiles, A.: Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* **142** (1995), 443–551.

[Win] Wingberg, K.: Der Eindeutigkeitssatz für Demuškinformationen, *Invent. Math.* **70** (1982), 99–113.