Mathematische Zeitschrift (2020) 295:1095–1142
https://doi.org/10.1007/s00209-019-02408-4

Mathematische Zeitschrift

Moderately ramified actions in positive characteristic

Dino Lorenzini[1] · Stefan Schröer[2]

Received: 8 May 2018 / Accepted: 19 July 2019 / Published online: 15 November 2019

Abstract
In characteristic 2 and dimension 2, wild $\mathbb{Z}/2\mathbb{Z}$-actions on $k[[u, v]]$ ramified precisely at the origin were classified by Artin, who showed in particular that they induce hypersurface singularities. We introduce in this article a new class of wild quotient singularities in any characteristic $p > 0$ and dimension $n \geq 2$ arising from certain non-linear actions of $\mathbb{Z}/p\mathbb{Z}$ on the formal power series ring $k[[u_1, \ldots, u_n]]$. These actions are ramified precisely at the origin, and their rings of invariants in dimension 2 are hypersurface singularities, with an equation of a form similar to the form found by Artin when $p = 2$. In higher dimension, the rings of invariants are not local complete intersection in general, but remain quasi-Gorenstein. We establish several structure results for such actions and their corresponding rings of invariants.

Mathematics Subject Classification 14B05 · 14J17 · 14L15 · 14E22 · 13B02

Contents

✉ Dino Lorenzini
lorenzin@uga.edu

Stefan Schröer
schroeer@math.uni-duesseldorf.de

[1] Department of Mathematics, University of Georgia, Athens, GA 30602, USA

[2] Mathematisches Institut, Heinrich-Heine-Universität, 40204 Düsseldorf, Germany

1 Introduction

Given a smooth quasi-projective algebraic variety X over a field k and a finite subgroup G of automorphisms of X, the quotient X/G exists, and a precise understanding of the singularities of X/G is often crucial in many problems in algebraic geometry, including in the geography of surfaces of general type, and in the study of the automorphisms of K3 surfaces and Enriques surfaces. The initial study of a quotient singularity on X/G is local, and consists in the analysis of the action of the isotropy subgroup of a point $x \in X$ on the completion of the regular local ring $\mathcal{O}_{X,x}$.

In characteristic zero, the action of a finite group G on the power series ring $A = k[[u_1, \ldots, u_n]]$ is always linearizable, an observation going back to Cartan [14]. The ring of invariants A^G has then good algebraic properties, such as being Cohen–Macaulay [24], and the singularity of Spec A^G is even rational [10,12]. Watanabe gave in [64] and [65] an explicit criterion for A^G to be Gorenstein.

When k has positive characteristic p and the order of G is divisible by p, an action of G on $k[[u_1, \ldots, u_n]]$ is called *wild*. Such actions are much more delicate to study. Most wild actions of G on $k[[u_1, \ldots, u_n]]$ are not linearizable, in which case the group G acts via true power series substitutions. The resulting rings A^G are usually not Cohen–Macaulay when $n \geq 3$ (Proposition 3.2). The elements of order p in the group $\mathrm{Aut}_k(k[[u_1, \ldots, u_n]])$ are completely understood only when $n = 1$ and k is finite [30,36]. In this article, we will focus on the geometric case where the action is ramified precisely at the origin (3.1). This type of wild action is never induced by a linear action on the variables (Lemma 3.3), and thus the large body of results in modular invariant theory is not immediately applicable to their study.

The starting point of our article is a result of Artin [4], who analyzed all wild actions of $G = \mathbb{Z}/2\mathbb{Z}$, ramified precisely at the origin, in dimension $n = 2$ when k is algebraically closed, and showed that

$$A^G = k[[x, y, z]]/(z^2 - abz - ya^2 + xb^2)$$

for some system of parameters $a, b \in k[[x, y]]$. In particular, this explicit description of A^G shows that it is a complete intersection and, hence, Gorenstein. Artin noted in [4] that it would be interesting to extend his result to wild $\mathbb{Z}/p\mathbb{Z}$-actions when $p > 2$. Peskin [46] subsequently described an explicit class of wild $\mathbb{Z}/3\mathbb{Z}$-actions ramified precisely at the origin with ring of invariants also described by an explicit equation when $n = 2$. In general, though, most wild $\mathbb{Z}/p\mathbb{Z}$-actions on $k[[u_1, u_2]]$ ramified precisely at the origin do not have Gorenstein rings of invariants (see Remark 9.5).

In this article, inspired by the work of Artin, we introduce a new class of wild $\mathbb{Z}/p\mathbb{Z}$-actions on $k[[u_1, \ldots, u_n]]$ ramified precisely at the origin, for all $n \geq 2$ and all primes p, whose rings of invariants are complete intersection when $n = 2$, and *quasi-Gorenstein* (Theorem 9.6) in general. Our main motivation for introducing these actions, in addition to their intrinsic interest as new explicit elements in the mysterious group of automorphisms of $k[[u_1, \ldots, u_n]]$, lies in the fact that already in dimension $n = 2$, we believe that this class of actions is rich enough to potentially solve two open problems concerning resolutions of singularities of $\mathbb{Z}/p\mathbb{Z}$-quotient singularities of surfaces: determine whether in the class of minimal resolutions of $\mathbb{Z}/p\mathbb{Z}$-quotient singularities, there is no bound on the number of vertices of valency at least 3 that the minimal resolution graph can have; and determine whether every power of p occurs as the determinant of the intersection matrix of a resolution of some $\mathbb{Z}/p\mathbb{Z}$-quotient singularity when $p > 2$. We address the latter problem in [35].

An analysis of Artin's arguments in [4] for $p = n = 2$ shows that it is possible to formulate five axiomatic conditions on a $\mathbb{Z}/p\mathbb{Z}$-action, such that any $\mathbb{Z}/p\mathbb{Z}$-action satisfying all five

of these axioms can be described in a particularly simple way, similar to the description obtained by Artin in the case $p = n = 2$. We call such $\mathbb{Z}/p\mathbb{Z}$-actions *moderately ramified*. As a byproduct, we also obtain a class of $(\mathbb{Z}/p\mathbb{Z})^{n-1}$-actions on $k[[u_1, \ldots, u_n]]$ whose rings of invariants are local complete intersections (Theorem 7.2).

Our new class of wild $\mathbb{Z}/p\mathbb{Z}$-actions can be described as follows. Start with an action of $G := \mathbb{Z}/p\mathbb{Z}$ on $A := k[[u_1, \ldots, u_n]]$ which is ramified precisely at the origin. We call $x_i := \prod_{\sigma \in G} \sigma(u_i)$ a norm element, and we show in Proposition 2.9 that it is always possible to find a regular system of parameters $u_1, \ldots, u_n$ in A such that A is finite of rank p^n over the *norm subring* $R := k[[x_1, \ldots, x_n]]$. Our axioms ensure that the ring A comes with a norm subring R such that $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ is Galois with elementary abelian Galois group H of order p^n, and that n distinguished subgroups $G_i^{\perp}$ of index p yield intermediate rings of invariants $R \subset A^{G_i^{\perp}} \subset A$ that result in a decomposition $A = A^{G_1^{\perp}} \otimes_R \ldots \otimes_R A^{G_n^{\perp}}$. Our description then relies on an analysis of the resulting schemes $Y_i := \mathrm{Spec}\, A^{G_i^{\perp}} \to S := \mathrm{Spec}\, R$ endowed with the natural action of $H/G_i^{\perp}$.

Extending to base schemes S of dimension bigger than one a construction of Raynaud [48], which was already further extended in dimension one by Romagny [53] to groups which are not necessarily finite and flat over S, we attach to the action of $H/G_i^{\perp}$ on Y_i a finite flat group scheme $\mathscr{G}_i/S$ and a natural action $\mathscr{G}_i \times_S Y_i \to Y_i$. In keeping with the terminology introduced by Romagny, we call the action $\mathscr{G}_i \times_S Y_i \to Y_i$ the *effective model* of the action of the constant group scheme $H/G_i^{\perp}$ on Y_i. Our final axiom imposes that Y_i/S be a torsor under the action of $\mathscr{G}_i/S$, for $i = 1, \ldots, n$. We then use the *Tate–Oort classification* of such group schemes $\mathscr{G}_i/S$ [62], and obtain explicit equations describing a moderately ramified G-action on A in Theorem 6.11.

Our terminology "moderately ramified G-action on A" refers to the fact that the ramification of the associated morphism $\mathrm{Spec}\, A \to \mathrm{Spec}\, A^H$ is "as small as possible". Moderately ramified actions are in some sense "as free as possible" outside ramification at the closed point. When $p = n = 2$, all five axioms are automatically satisfied when k is algebraically closed. For arbitrary $p \geq 2$, we obtain in dimension $n = 2$ a description in Theorem 7.7 of the ring of invariants A^G which generalizes Artin's description when $p = 2$ in [4].

In dimension $n > 2$, the ring A^G is never a complete intersection since it is known that this ring is not Cohen–Macaulay when the action is ramified precisely at the origin. Thus an explicit description of A^G by generators and relations is in general out of reach in higher dimensions. When $n = 3$, we are able to provide generators for A^G in Theorem 8.5 when the system of parameters associated with the G-action consists of polynomials rather than general power series. We are also able to provide a formula for the embedding dimension. Using methods from non-commutative algebra, we show for all $n \geq 2$ in Theorem 9.6 that A^G is quasi-Gorenstein, that is, that the dualizing module K_{A^G} is trivial in the class group $\mathrm{Cl}(A^G)$.

The paper is organized as follows. In Sect. 2 we study general properties of norm subrings R inside $A = k[[u_1, \ldots, u_n]]$. Section 3 focuses on wild G-actions on A that are ramified precisely at the origin, and presents a criterion for the extension $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ to be Galois in terms of the extension $\mathrm{Frac}(A^G)/\mathrm{Frac}(R)$. The proof of this criterion uses results on fundamental groups. Section 4 deals with extensions of group schemes and torsors, and proves the existence of the effective model of a group action over higher-dimensional bases. These concepts are further developed explicitly in dimension 1 in Sect. 5. Section 6 introduces the central notion of moderately ramified action and the main structure results for such action. In Sect. 7 we study various auxiliary invariant rings that are attached to moderately ramified actions. We treat the case $n = 3$ in Sect. 8, where we present a set of generators for the ring A^G

for certain moderately ramified actions. We show that the canonical class $[K_{A^G}] \in \mathrm{Cl}(A^G)$ is trivial in Sect. 9.

2 Norm subrings

Let A denote a complete local noetherian ring that is regular, of dimension $n \geq 1$, and with maximal ideal $\mathfrak{m}_A$. Recall that a field of representatives for A is a subfield k of A such that the composition $k \subset A \to A/\mathfrak{m}_A$ is an isomorphism of fields. When $A/\mathfrak{m}_A$ is perfect, such a subfield is unique. We will always in this article assume that A contains a field, and we fix a field of representatives $k \subset A$ and regard it as ground field. A set of n elements $x_1, \ldots, x_n \in A$ which generate an $\mathfrak{m}_A$-primary ideal in A is called *system of parameters*. The following facts are well-known.

Lemma 2.1 *If $x_1, \ldots, x_n \in A$ is a system of parameters, then the ensuing homomorphism of complete local k-algebras $R := k[[x_1, \ldots, x_n]] \to A$ is finite and flat. Its degree is the length of $A/(x_1, \ldots, x_n)A$.*

Proof The ring A, viewed as an R-module is finite, according to [68, Corollary 2 and Remark on page 293]. Since R is regular and A is Cohen–Macaulay, the R-module A is free of finite rank, by [57, Proposition 22, page IV-37]. This rank is the vector space dimension of $A/(x_1, \ldots, x_n)A$ over $k = R/(x_1, \ldots, x_n)$, which coincides with the length of $A/(x_1, \ldots, x_n)A$. □

A set of n elements $u_1, \ldots, u_n$ in A which generate $\mathfrak{m}_A$ is called a *regular system of parameters*. The resulting homomorphism $k[[u_1, \ldots, u_n]] \to A$ is then bijective.

Let $G \subset \mathrm{Aut}(A)$ be a finite group of automorphisms such that k lies in the ring of invariants A^G. Clearly, $\mathfrak{m}_A \cap A^G$ is a maximal ideal with residue field k. It follows from [41, Théorème 2], that A^G is a complete *noetherian* local ring and that A is an A^G-module of finite type. Choose a regular system of parameters $u_1, \ldots, u_n \in A$, and consider the *norm elements*

$$x_i := N_{A/A^G}(u_i) = \prod_{\sigma \in G} \sigma(u_i), \quad 1 \leq i \leq n.$$

These elements are obviously G-invariant, and we can consider the complete local k-subalgebra $R \subset A^G$ generated by $x_1, \ldots, x_n$. Let us call R a *norm subring* of A. The ring extensions $R \subset A^G \subset A$ play a crucial role in this article. In this section, we determine under what conditions the extension $R \subset A$ is finite.

Definition 2.2 A regular system of parameters $u_1, \ldots, u_n \in A$ is called *weakly admissible* (resp. *admissible*) with respect to the G-action if, for each $(\sigma_1, \ldots, \sigma_n) \in G^n$, the elements $\sigma_1(u_1), \ldots, \sigma_n(u_n) \in A$ form a system of parameters (resp., form a regular system of parameters).

The main justification for introducing this notion is the following result:

Proposition 2.3 *Let $u_1, \ldots, u_n$ be a regular system of parameters of A. Then the associated norm elements $x_1, \ldots, x_n$ form a system of parameters in A if and only if the elements $u_1, \ldots, u_n$ are weakly admissible with respect to the action of G. If the above equivalent conditions hold, then the homomorphism of k-algebras $k[[x_1, \ldots, x_n]] \to A$ is finite and flat of degree at least $|G|^n$, with equality when the regular system is admissible.*

Proof Let $g := |G|$. Choose an enumeration $\sigma_1, \ldots, \sigma_g$ of the elements of G such that $\sigma_1 := e$ is the neutral element. Define $f_{i,j} := \sigma_j(u_i)$, with $1 \leq j \leq g$ and $1 \leq i \leq n$. In particular, $f_{i,1} = u_i$ and $x_i = \prod_{j=1}^{g} f_{i,j}$. Let $X := \mathrm{Spec}(A)$ and consider the closed subsets $V(f_{i,j}) \subset X$. Clearly,

$$V(x_1, \ldots, x_n) = \bigcap_{i=1}^{n} \left(\bigcup_{j=1}^{g} V(f_{i,j}) \right).$$

Let $J := \{1, \ldots, g\}$. Using the distributive properties of $\cap$ and $\cup$, we find that

$$V(x_1, \ldots, x_n) = \bigcup_{(j_1,\ldots,j_n)\in J^n} \left(\bigcap_{i=1}^{n} V(f_{i,j_i}) \right) = \bigcup_{(j_1,\ldots,j_n)\in J^n} V(f_{1,j_1}, \ldots, f_{n,j_n}). \quad (2.4)$$

If the elements $x_1, \ldots, x_n \in A$ form a system of parameters, then $V(x_1, \ldots, x_n)$ contains only the closed point and, thus, each $V(f_{1,j_1}, \ldots, f_{n,j_n})$ consists only of the closed point. Hence, for each tuple $(j_1, \ldots, j_n)$, the elements $f_{i,j_1}, \ldots, f_{i,j_n} \in A$ form a system of parameters. In other words, the elements $u_1, \ldots, u_n \in A$ are weakly admissible. Conversely, when the elements $u_1, \ldots, u_n \in A$ are weakly admissible, it immediately follows from (2.4) that the elements $x_1, \ldots, x_n \in A$ form a system of parameters.

Now suppose that the regular system of parameters $u_1, \ldots, u_n \in A$ is weakly admissible, such that the associated norm elements $x_1, \ldots, x_n$ form a system of parameters in A. According to Lemma 2.1, the ring A is a finite and flat module over $R = k[[x_1, \ldots, x_n]]$. To determine its rank, we need to compute the length of A/I, where $I := (x_1, \ldots, x_n)A$. We now establish the inequality $\mathrm{length}(A/I) \geq g^n$ using general facts on the *Hilbert–Samuel multiplicity* $e(I, A)$ of I. Since we assume that the elements $u_1, \ldots, u_n \in A$ are weakly admissible, the ideal $I \subset A$ is generated by a system of parameters. Since the ring A is Cohen–Macaulay, the formula $\mathrm{length}(A/I) = e(I, A)$ holds [5, Proposition 5.9]. For any $\mathfrak{m}_A$-primary ideal $J \subset A$, we have $e(J^s, A) = s^n e(J, A)$ [40, page 108]. Applying this to $J := \mathfrak{m}_A^g$ and using the fact that $e(\mathfrak{m}_A, A) = 1$ since A is regular, we find that $e(J, A) = g^n$. Finally, the inclusion $I \subset J$ gives $e(I, A) \geq e(J, A)$ [40, page 109], and the desired inequality follows.

Finally, assume that the regular system of parameters $u_1, \ldots, u_n \in A$ is admissible. To proceed, it is convenient to consider the slightly more general situation where we omit the precise definition of the element $f_{i,j}$, and keep only the following hypothesis: for each element $(j_1, \ldots, j_n) \in J^n$, the elements $f_{1,j_1}, \ldots, f_{n,j_n}$ form a regular system of parameters of A. In particular, $f_{i,j} \in \mathfrak{m}_A \backslash \mathfrak{m}_A^2$ for each $i \in [1, n]$ and $j \in [1, g]$. Letting $u_i := f_{i,1}$, we find that $u_1, \ldots, u_n$ form a regular system of parameters of A.

For each $\ell \in [1, n]$ and $r \in [1, g]$, define $g_{\ell,r} := \prod_{j=1}^{r} f_{\ell,j}$, and denote as previously $x_\ell := g_{\ell,g}$. When $2 \leq \ell \leq n-1$, consider the ideal

$$I_{\ell,r} := (x_1, \ldots, x_{\ell-1}, g_{\ell,r}, u_{\ell+1}, \ldots, u_n) \subset A.$$

Define similarly the ideals $I_{1,r} = (g_{1,r}, u_2, \ldots, u_n)$ and $I_{n,r} = (x_1, \ldots, x_{n-1}, g_{n,r})$ for each $r \in [1, g]$. With respect to the lexicographic ordering on the set of all pairs (ℓ, r) in $[1, n] \times [1, g]$, the gn ideals $I_{\ell,r}$ form a decreasing sequence

$$I_{\ell,r} = (x_1, \ldots, x_{\ell-1}, g_{\ell,r}, u_{\ell+1}, \ldots, u_n) \supseteq (x_1, \ldots, x_{\ell-1}, g_{\ell,r+1}, u_{\ell+1}, \ldots, u_n) = I_{\ell,r+1}$$

between $I_{1,1} = (u_1, \ldots, u_n)$ and $I_{n,g} = (x_1, \ldots, x_n)$. Note that this sequence of ideals contains the repetitions $I_{\ell,g} = I_{\ell+1,1}$.

Since the module $I_{\ell,r}/I_{\ell,r+1}$ is generated by $g_{\ell,r}$, and because $g_{\ell,r+1} = g_{\ell,r} f_{\ell,r+1}$, we find that $I_{\ell,r}/I_{\ell,r+1}$ is annihilated by

$$J_{\ell,r+1} := (x_1, \ldots, x_{\ell-1}, f_{\ell,r+1}, u_{\ell+1}, \ldots, u_n).$$

It follows that $\mathrm{length}(A/J_{\ell,r+1}) \geq \mathrm{length}(I_{\ell,r}/I_{\ell,r+1})$. We claim that

$$\mathrm{length}(A/J_{\ell,r+1}) \leq g^{\ell-1}$$

for all $r \in [0, g-1]$ and $\ell \in [1, n]$. Assuming this claim, we find the upper bound

$$\begin{aligned} \mathrm{length}(A/(x_1, \ldots, x_n)) &= 1 + \sum\nolimits_{\ell=1}^{n} \sum\nolimits_{r=1}^{g-1} \mathrm{length}(I_{\ell,r}/I_{\ell,r+1}) \\ &\leq 1 + \sum\nolimits_{\ell=1}^{n} (g-1) g^{\ell-1} = g^n. \end{aligned} \tag{2.5}$$

To verify the claim, we proceed by induction on $n = \dim(A)$. Assume that $n = 1$. By construction, $J_{1,r+1} = (f_{1,r+1})$. By hypothesis, $f_{1,r+1} \in \mathfrak{m}_A \backslash \mathfrak{m}_A^2$. Hence, $f_{1,r+1}$ is a uniformizer and $A/(f_{1,r+1})$ has length one, as desired.

Assume now that $n > 1$, and that the assertion holds for $n-1$. Since $f_{\ell,r+1}$ is part of a regular system of parameters, we find that the ring $\overline{A} := A/(f_{\ell,r+1})$ is a complete regular local ring of dimension $n-1$. When $a \in A$, denote by $\overline{a}$ its class in $\overline{A}$. When $2 \leq \ell \leq n-1$, we have

$$\mathrm{length}(A/J_{\ell,r+1}) = \mathrm{length}(\overline{A}/(\overline{x}_1, \ldots, \overline{x}_{\ell-1}, \overline{u}_{\ell+1}, \ldots, \overline{u}_n)). \tag{2.6}$$

Similarly, $A/J_{1,r+1}$ and $\overline{A}/(\overline{u}_2, \ldots, \overline{u}_n))$ have the same length, and $A/J_{n,r+1}$ and $\overline{A}/(\overline{x}_1, \ldots, \overline{x}_{n-1})$ also have same length. We now observe that we can apply our induction hypothesis to bound the right-hand side of (2.6). Indeed, the set of elements $\overline{f}_{i,r} \in \overline{A}$ with $i \in [1, n]$ and $i \neq \ell$, and with $r \in [1, g]$, inherits the property that every sequence $\overline{f}_{1,j_1}, \ldots, \overline{f}_{n,j_n}$ of $n-1$ elements (where no term $\overline{f}_{\ell,j_\ell}$ appears) is a regular system of parameters in $\overline{A}$. In case $\ell < n$, we can view $\overline{u}_{\ell+1}$ as $\overline{f}_{\ell+1,1}$ and conclude by induction. In the boundary case $\ell = n$, it suffices to show that $\mathrm{length}(\overline{A}/(\overline{x}_1, \ldots, \overline{x}_{n-1}) \leq g^{n-1}$. To prove this inequality we use the argument in (2.5) and use induction to justify each inequality found in that argument. □

Recall that a G-action on $A = k[[u_1, \ldots, u_n]]$ is called *linear* if each $\sigma \in G$ acts as a substitution of variables $u_j \mapsto \sum_{i=1}^{n} \lambda_{ij}^{\sigma} u_i$ for some linear representation $G \to \mathrm{GL}_n(k)$, $\sigma \mapsto (\lambda_{ij}^{\sigma})$. For instance, the $\mathbb{Z}/2\mathbb{Z}$-action on $k[[u, v]]$ which permutes u and v is linear, and our next lemma implies that u, v is not weakly admissible for this action.

Lemma 2.7 *Suppose that the G-action on $A = k[[u_1, \ldots, u_n]]$ is linear. If there is an element $\sigma \in G$ whose matrix (λ_{ij}^{σ}) has a zero on the diagonal, then the regular system of parameters $u_1, \ldots, u_n \in A$ is not weakly admissible with respect to the action of G.*

Proof After reordering the $u_1, \ldots, u_n \in A$, we may assume that the non-zero diagonal entry is $\lambda_{11}^{\sigma} = 0$. For the tuple $(\sigma, e, \ldots, e) \in G^n$, where $e \in G$ denotes the neutral element, the resulting elements $\sigma(u_1), u_2, \ldots, u_n \in A$ do not form a system of parameters, because they generate the ideal $(u_2, \ldots, u_n) \subset A$. □

Any regular system of parameters $u_1, \ldots, u_n \in A$ induces a basis $\overline{u}_1, \ldots, \overline{u}_n$ of the cotangent space $\mathfrak{m}_A/\mathfrak{m}_A^2$. Fixing this basis of $\mathfrak{m}_A/\mathfrak{m}_A^2$, we obtain an induced linear representation $G \to \mathrm{GL}(\mathfrak{m}_A/\mathfrak{m}_A^2) = \mathrm{GL}_n(k)$.

Lemma 2.8 *Let $u_1, \ldots, u_n \in A$ be a regular system of parameters with induced linear representation $G \to \mathrm{GL}(\mathfrak{m}_A/\mathfrak{m}_A^2) = \mathrm{GL}_n(k)$. If the image of G is contained in the Borel subgroup of upper triangular matrices, then $u_1, \ldots, u_n$ is admissible with respect to the action of G.*

Proof Given $(\sigma_1, \ldots, \sigma_n) \in G^n$, we need to show that the elements $\sigma_1(u_1), \ldots, \sigma_n(u_n)$ form a regular system of parameters of A. For this, it suffices to show that the images $\overline{\sigma_1(u_1)}, \ldots, \overline{\sigma_n(u_n)}$ in $\mathfrak{m}_A/\mathfrak{m}_A^2$ form a basis. That they form a basis is clear from the assumption that each σ_i induces in the basis $\overline{u}_1, \ldots, \overline{u}_n$ a matrix which is upper triangular. □

Note in particular that it follows from Lemma 2.8 that if the induced representation of G on the cotangent space is trivial, then any regular system of parameters is automatically admissible.

Proposition 2.9 *If the ring A has characteristic $p > 0$ and the group G is a finite p-group, then A contains an admissible regular system of parameters.*

Proof Let $u_1, \ldots, u_n$ be any regular system of parameters of A with induced linear representation $G \to \mathrm{GL}(\mathfrak{m}_A/\mathfrak{m}_A^2) = \mathrm{GL}_n(k)$. Since G is a finite p-group, it is possible to change basis in $\mathfrak{m}_A/\mathfrak{m}_A^2$ so that in the new basis, every element in the image of G is an upper triangular matrix whose diagonal coefficients are all 1 [59, Proposition 26 on page 64]. The proposition then follows from Lemma 2.8. □

3 Actions ramified precisely at the origin

Let A be a complete local noetherian ring that is regular, of dimension $n \geq 2$, and characteristic $p > 0$, with maximal ideal $\mathfrak{m}_A$ and field of representatives k. Let G be a finite cyclic group of order p, and assume that A is endowed with a faithful action of G so that k lies in the ring of invariants A^G. For each prime ideal $\mathfrak{p} \subset A$, we write $I_\mathfrak{p} \subset G$ for the inertia subgroup consisting of all $\sigma \in G$ with $\sigma(\mathfrak{p}) = \mathfrak{p}$ and such that the induced morphism $\overline{\sigma} : A/\mathfrak{p} \to A/\mathfrak{p}$ is the identity.

3.1 We say that the G-action is *ramified precisely at the origin* if $I_{\mathfrak{m}_A} = G$ and $I_\mathfrak{p} = \{\mathrm{id}\}$ for every non-maximal prime ideal $\mathfrak{p}$.

We discuss in this section several algebraic properties of the ring of invariants A^G and of the field extension $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ induced by a norm subring $R \subset A$. Let us start by recalling the following well-known facts.

Proposition 3.2 *Suppose that the G-action on A is ramified precisely at the origin.*

(i) *The ring of invariants A^G is a complete local noetherian domain that is normal, with $\dim(A^G) = n$ and $\mathrm{depth}(A^G) = 2$.*
(ii) *The ring extension $A^G \subset A$ is local, finite of degree p, but not flat. The induced map on residue fields is an isomorphism.*
(iii) *The singular locus of $\mathrm{Spec}(A^G)$ consists of the closed point $\mathfrak{m}_{A^G}$. The morphism $\mathrm{Spec}(A)\backslash\{\mathfrak{m}_A\} \to \mathrm{Spec}(A^G)\backslash\{\mathfrak{m}_{A^G}\}$ is a G-torsor.*

Proof It is standard that A^G is an integrally closed domain, and that the ring extension $A^G \subset A$ is integral. In light of the Going-Up Theorem, the ring A^G must be local, the ring extension $A^G \subset A$ is local, and $\dim(A^G) = \dim(A)$.

Let us show that A^G is noetherian (see also [41, Théorème 2]). According to Proposition 2.9, there exists a regular system of parameters $u_1, \ldots, u_n \in A$ that is admissible with respect to the G-action. Let $R = k[[x_1, \ldots, x_n]]$ be the resulting norm subring. Then the extension $R \subset A$ if finite of degree p^n (Proposition 2.3). It follows that A^G is also a finitely generated R-module and, hence, A^G is noetherian.

Now that we know that A^G is noetherian, Proposition 2 and Proposition 4 in [16] show that A^G has depth 2 (see also [15, 2.4], or [46, Corollary 1.6]). Since A is complete, the completion B of A^G with respect to its maximal ideal maps to A, and the image of B in A is A^G. Thus, A^G is complete since it is the image of a complete ring. This completes the proof of (i).

By our overall assumption we have $k \subset A^G$, so the inclusion $A^G \subset A$ has trivial residue field extension. If A^G is regular, then A would be flat over A^G [40, Theorem 23.1]. But then the Zariski–Nagata Theorem on the Purity of the Branch Locus [2, Chapter VI, Theorem 6.8] would imply that the branch locus is pure of codimension 1, which would contradict our hypothesis that $A^G \subset A$ is ramified precisely at the origin. Hence, the ring A^G is not regular, and it follows from [20, IV.6.5.1 (i)], that $A^G \subset A$ is not flat. This shows (ii). Part (iii) follows from [49, Exposé V, Proposition 2.6]. □

The following lemma will be used in 6.15.

Lemma 3.3 *Suppose that the G-action on A is ramified precisely at the origin. Then no element $v \in \mathfrak{m}_A \setminus \mathfrak{m}_A^2$ is G-invariant. In particular, the action of G on A is not linear.*

Proof Suppose that there exists $v \in \mathfrak{m}_A \setminus \mathfrak{m}_A^2$ which is G-invariant. Extend v to a regular system of parameters $u_1, \ldots, u_n$ of A, with $u_1 = v$. Let σ denote a generator of G, and consider the ideal $\mathfrak{a} \subset A$ generated by the elements $\sigma(u_i) - u_i$, $i = 1, \ldots, n$. Since any prime ideal $\mathfrak{p}$ of A which contains $\mathfrak{a}$ is such that $I_{\mathfrak{p}} \neq (0)$, we find that $V(\mathfrak{a}) = \{\mathfrak{m}_A\}$. In particular, $\dim(A/\mathfrak{a}) = 0$. On the other hand, by construction, the ideal $\mathfrak{a}$ is generated by at most $n - 1$ elements because $\sigma(u_1) - u_1 = 0$. Thus, since $\dim(A) = n$, we find that $\dim(A/\mathfrak{a}) > 0$, a contradiction.

It follows that an action of G on A which is ramified precisely at the origin is *never* linear, because a matrix of order p always has an eigenvector for the eigenvalue $\lambda = 1$ in characteristic p. Note that this statement about non-linearity was noted already in [46, Proposition 2.1]. □

Our next theorem is used in Proposition 6.20.

Theorem 3.4 *Assume that the G-action on A is ramified precisely at the origin.*

(i) *Choose a regular system of parameters $u_1, \ldots, u_n \in A$ which is admissible with respect to the G-action, and consider the corresponding norm subring $R = k[[x_1, \ldots, x_n]]$. Then the extension* $\mathrm{Frac}(A^G)/\mathrm{Frac}(R)$ *is not purely inseparable.*

(ii) *Assume that the field k has no Galois extension of degree p. Then any k-automorphism $\varphi : A^G \to A^G$ extends to an automorphism $\varphi' : A \to A$. Furthermore, if A^G contains a subring R such that the extension $R \subset A^G$ is finite and* $\mathrm{Frac}(A^G)/\mathrm{Frac}(R)$ *is Galois, then the extension* $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ *is Galois as well.*

Proof (i) Consider the local schemes $X := \mathrm{Spec}(A)$, $Y := \mathrm{Spec}(A^G)$, and $S := \mathrm{Spec}(R)$, and write $U \subset X$, $V \subset Y$, and $W \subset S$ for the complements of their closed points. Suppose that $\mathrm{Frac}(R) \subset \mathrm{Frac}(A^G)$ is purely inseparable, so that the finite morphism $Y \to S$ is a universal homeomorphism. According to [49, Exposé IX, Theorem 4.10], the étale covering $U \to V$

would be the base-change of an étale covering $W' \to W$. The latter is the restriction of some étale covering $S' \to S$ by the Zariski–Nagata Purity Theorem. Consequently, $U \to V$ is the restriction of some étale covering $Y' \to Y$. Since the schemes X and Y' are normal, both restriction maps $\Gamma(Y', \mathscr{O}_{Y'}) \to \Gamma(U, \mathscr{O}_U) \leftarrow \Gamma(X, \mathscr{O}_X)$ are bijective, whence $Y' = X$, contradicting the fact that $X \to Y$ is not étale.

(ii) In order to extend $\varphi : A^G \to A^G$ to A, let $\tau : V \to V$ be the morphism induced by φ. Define the scheme $\tau^*(U)$ by requiring that the following diagram be Cartesian:

$$\begin{array}{ccc} \tau^*(U) & \longrightarrow & U \\ \downarrow & & \downarrow \\ V & \xrightarrow[\tau]{} & V. \end{array}$$

Our task is to show the existence of a V-isomorphism $U \to \tau^*(U)$. Composing this isomorphism with the given morphism $\tau^*(U) \to U$ produces an extension of the morphism τ, giving the desired automorphism φ' of $A = \Gamma(U, \mathscr{O}_U)$.

Choose a separable closure $\mathrm{Frac}(A^G) \subset \Omega$. In turn, we get a geometric point $b : \mathrm{Spec}(\Omega) \to V$. Recall that the algebraic fundamental group $\pi_1(V, b)$ is defined as the group of automorphisms for the fiber functor $(\mathrm{Cov}/V) \to (\mathrm{Set})$ that sends a finite étale $V' \to V$ to the underlying set of the base-change $V' \otimes_V \Omega$. Here (Cov/V) denotes the category of all finite étale V-schemes, which thus becomes equivalent to the category of finite sets endowed with a continuous action of $\pi_1(V, b)$ [49, Exposé V, Section 7]. By abuse of notation, we also write $\pi_1(V, \Omega)$ for the fundamental group with respect to the base-point $b : \mathrm{Spec}(\Omega) \to V$.

Up to isomorphism, the two finite étale G-coverings $U_1 = U$ and $U_2 = \tau^*(U)$ correspond to the finite set G, endowed with actions via group homomorphisms $h_i : \pi_1(V, \Omega) \to G$ for $i = 1, 2$. Let $H_i \subset \pi_1(V, \Omega)$ be their kernels. The task is to show that the two actions on G are isomorphic, in other words, that $H_1 = H_2$. To proceed, choose a lifting of the geometric point $b : \mathrm{Spec}(\Omega) \to V$ along $U_i \to V$. This gives an identification $H_i = \pi_1(U_i, \Omega)$. Clearly, $\Gamma(U_i, \mathscr{O}_{U_i})$ is a complete local noetherian ring that is regular. Let X_i be its spectrum. The commutative diagram

$$\begin{array}{ccc} U_i & \longrightarrow & V \\ \downarrow & & \downarrow \\ X_i & \longrightarrow & \mathrm{Spec}(k) \end{array}$$

induces a commutative diagram of fundamental groups

$$\begin{array}{ccc} \pi_1(U_i, \Omega) & \longrightarrow & \pi_1(V, \Omega) \\ \downarrow & & \downarrow \\ \pi_1(X_i, \Omega) & \longrightarrow & \pi_1(k, \Omega). \end{array}$$

The map on the left is bijective, because X_i is regular and $X_i \smallsetminus U_i$ has codimension two [49, Exposé X, Corollary 3.3]. The lower map is bijective as well, because X_i is local henselian [49, Exposé X, Théorème 2.1]. It follows that the kernel $N \subset \pi_1(V, \Omega)$ for the map on the right is isomorphic to G, and that both $H_i = \pi_1(U_i, \Omega)$ are sections for $\pi_1(V, \Omega) \to \pi_1(k, \Omega)$. Any two sections differ by a homomorphism $\pi_1(k, \Omega) \to N$. The latter must be zero, by assumption on the field k. In turn, $H_1 = H_2$.

Now suppose that $R \subset A^G$ is finite and $\mathrm{Frac}(R) \subset \mathrm{Frac}(A^G)$ is Galois, say of degree $d \geq 1$. To check that $\mathrm{Frac}(R) \subset \mathrm{Frac}(A)$ is Galois, it suffices to extend each $\mathrm{Frac}(R)$-

automorphism $\varphi : \mathrm{Frac}(A^G) \to \mathrm{Frac}(A^G)$ to an automorphism $\varphi' : \mathrm{Frac}(A) \to \mathrm{Frac}(A)$. Indeed, the group H of automorphisms of $\mathrm{Frac}(A)$ over $\mathrm{Frac}(R)$ then contains at least dp elements, obtained as products of extension φ' and $\sigma \in G$. Since $[\mathrm{Frac}(A) : \mathrm{Frac}(R)] = dp$, we find that $\mathrm{Frac}(R) \subset \mathrm{Frac}(A)$ is Galois. The desired extensions φ' do exist, because then the morphism φ extends to the integral closure A^G of R with respect to $R \subset A^G$, and thus to A. □

Remark 3.5 (i) We do not know whether the conclusion of Theorem 3.4 (ii) holds without the additional hypothesis on the field of representatives k.

(ii) We do not know of an example of an action of $G = \mathbb{Z}/p\mathbb{Z}$ on $A = k[[u_1, \ldots, u_n]]$ ramified precisely at the origin where $\mathrm{Frac}(A^G)/\mathrm{Frac}(R)$ is not separable. When the action is not ramified precisely at the origin, it is easy to find examples where $\mathrm{Frac}(A^G)/\mathrm{Frac}(R)$ is not separable. Indeed, if $\sigma(u_i) = u_i$, then $u_i \in A^G$ and $x_i := \mathrm{Norm}(u_i) = u_i^p \in R$.

4 The effective model of a group action

Let $R := k[[x_1, \ldots, x_n]]$, and let $L/\mathrm{Frac}(R)$ be a Galois extension of degree p. Let B denote the integral closure of R in L. It is natural to wonder what conditions can be imposed on the Galois extension $L/\mathrm{Frac}(R)$ to guarantee that the ring B is simple, say $B \simeq R[u]/(f(u))$ for some easily described $f(u) \in R[u]$. To give an answer to this question that will be useful in 6.8 in our study of normal forms of $\mathbb{Z}/p\mathbb{Z}$-actions on $A = k[[u_1, \ldots, u_n]]$, we introduce below the notion of effective model of a group action.

Let G denote the Galois group of $L/\mathrm{Frac}(R)$. Clearly, G also acts on B. Letting $S = \mathrm{Spec}\, R$ and $Y := \mathrm{Spec}\, B$, we obtain an action of the constant group scheme G_S/S on Y/S. Assume now that Y/S is flat. Then, associated with this action on Y/S is a uniquely defined group scheme $\mathcal{G}/S$ with an S-action $\mathcal{G} \times_S Y \to Y$. The group scheme $\mathcal{G}/S$ is called *the effective model of the action of G on Y*. It was considered first by Raynaud in [48, Proposition 1.2.1], in cases where R is a discrete valuation ring. This theory was extended, still in the case where R is a discrete valuation ring, to cases where G_S is not constant, and even not finite over S, in [52] and [53]. In the case where G_S is constant, some cases where the base scheme S is not of dimension 1 are considered in [1, 2.2]. The main result in this section is Theorem 4.3 below, which proves the existence of the effective model when G_S/S is constant but the base S is not necessarily of dimension 1.

Fix a noetherian base scheme S and some prime number $p > 0$. Let $Y \to S$ be a finite flat morphism of degree p. Denote by $\mathrm{Aut}(Y/S)$ the group of S-automorphisms of Y. Consider the group-valued functor $\mathrm{Aut}_{Y/S}$, with $\mathrm{Aut}_{Y/S}(T) := \mathrm{Aut}(Y_T/T)$ for any S-scheme T. Using the existence of Hilbert schemes [19, 221-19], such functor is shown to be representable, by a scheme denoted $\mathrm{Aut}_{Y/S}/S$. In our situation, we will need to use the fact that the structure morphism $\mathrm{Aut}_{Y/S} \to S$ is affine. For convenience, we recall a proof of this fact below. This proof can be easily modified to also give a proof of the existence of $\mathrm{Aut}_{Y/S}/S$.

Lemma 4.1 *The structure morphism $\mathrm{Aut}_{Y/S} \to S$ is affine.*

Proof The question is local in S, so it suffices to treat the case where the schemes $S = \mathrm{Spec}(R)$ and $Y = \mathrm{Spec}(B)$ are affine. Furthermore, we may assume that B admits a basis $b_1, \ldots, b_p \in B$ as R-module, and that $b_1 = 1_B$. Let $\underline{\mathrm{GL}}(B) = \underline{\mathrm{GL}}_{p,R}$ be the group scheme of R-linear automorphisms. Its underlying scheme is the spectrum of the localization $R[T_{ij}]_{\det}$, where $T_{11}, \ldots, T_{pp}$ are p^2 indeterminates and $\det = \det(T_{ij})$ is the determinant of the matrix $(T_{ij})_{1 \le i,j \le p}$. We have a canonical monomorphism $\mathrm{Aut}_{Y/S} \subset \underline{\mathrm{GL}}_{p,R}$. To show that

the scheme $\mathrm{Aut}_{Y/S} \to S$ is affine, it suffices to show that the monomorphism is a closed embedding.

Let $\tau = (\tau_{ij})$ be an R-linear map $B \to B$. Write $\mu : B \otimes B \to B$ for the algebra multiplication, with $\mu(b_i \otimes b_j) = \sum \mu_{kij} b_k$. Then the linear map τ is an algebra homomorphism if and only if $\mu \circ (\tau \otimes \tau) = \tau \circ \mu$ and $\tau(b_1) = b_1$. The latter means $\tau_{21} = \ldots = \tau_{p1} = 0$. As to the former condition, we have $(\mu \circ (\tau \otimes \tau))\,(b_i \otimes b_j) = \sum_k (\sum_{r,s} \tau_{ri}\tau_{sj}\mu_{krs}) b_k$ and $(\tau \circ \mu)\,(b_i \otimes b_j) = \sum_k (\sum_t \mu_{ijt}\tau_{kt}) b_k$. Comparing coefficients gives $\sum_{r,s} \tau_{ri}\tau_{sj}\mu_{krs} = \sum_t \mu_{ijt}\tau_{kt}$ for all $1 \le k \le n$. Replacing the scalars τ_{ri} by the indeterminates T_{ij}, we obtain equations that define a closed subscheme inside $\underline{\mathrm{GL}}_{p,R}$. Applying the above computations over arbitrary R-algebras R', we infer that this closed subscheme represents the functor $\mathrm{Aut}_{Y/S}$. □

Let now G be an abstract group of order p acting on Y via S-automorphisms. In other words, G is endowed with a group homomorphism $G \to \mathrm{Aut}_S(Y/S)$. The quotient scheme Y/G exist, and *we assume that the structure map $Y/G \to S$ is an isomorphism*. Write G_S/S for the constant group scheme associated to G. The action of G on Y/S yields a natural homomorphism of group schemes

$$f : G_S \to \mathrm{Aut}_{Y/S}\,. \tag{4.2}$$

Since $\mathrm{Aut}_{X/S} \to S$ is separated and $G_S \to S$ is proper, the morphism $G_S \to \mathrm{Aut}_{Y/S}$ is proper, and its schematic image $f(G_S) \subset \mathrm{Aut}_{Y/S}$ is finite over S (use [20, Chapter II, Corollary 5.4.3]).

Let $s \in S$ be any point, and consider the natural morphism $\mathrm{Spec}\,\mathscr{O}_{S,s} \to S$. We denote by $f(G_S) \otimes \mathscr{O}_{S,s}$ the base change of $f(G_S) \to S$ by $\mathrm{Spec}\,\mathscr{O}_{S,s} \to S$. Both the construction of $\mathrm{Aut}_{Y/S}$ and of the schematic closure of $f(G_S)$ commute with the base change by $\mathrm{Spec}\,\mathscr{O}_{S,s} \to S$. Let now $s \in S$ be a regular point of codimension 1, so that $\mathscr{O}_{S,s}$ is a discrete valuation ring. We are in a position to apply a theorem of Romagny [53, Theorem 4.3.4] to obtain that the scheme $f(G_S) \otimes \mathscr{O}_{S,s}$ is in fact a subgroup scheme of the group scheme $\mathrm{Aut}_{Y/S} \otimes \mathscr{O}_{S,s}$. The group scheme $f(G_S) \otimes \mathscr{O}_{S,s}$ over $\mathrm{Spec}\,\mathscr{O}_{S,s}$ is called the *effective model* for the G-action at the point $s \in S$. Our next theorem slightly extends this result. Note that Theorem 4.3.4 in [53] is stated for group schemes $\mathcal{G} \to \mathrm{Spec}\,\mathscr{O}_{S,s}$ that need not be finite. The hypothesis in Theorem 4.3.4 that $\mathcal{G}/\mathrm{Spec}\,\mathscr{O}_{S,s}$ is universally affinely dominant (see [53, 3.1.1]) is automatically satisfied in our situation where we require $\mathcal{G} \to \mathrm{Spec}\,\mathscr{O}_{S,s}$ to be finite and flat. The same is true for the hypothesis that $\mathcal{G} \to \mathrm{Spec}\,\mathscr{O}_{S,s}$ is pure (see [53, 2.1.1 and 2.1.3]).

Let $\zeta \in \mathbb{Z}_p$ denote a primitive $(p-1)$-th root of unity, and define Λ_p to be the subring $\mathbb{Z}[\zeta, 1/p(p-1)] \cap \mathbb{Z}_p$ of $\mathbb{Q}_p$. Note that all schemes $S \to \mathrm{Spec}\,\mathbb{F}_p$ of characteristic p are in fact schemes over $\mathrm{Spec}\,\Lambda_p$ in a unique way, after composing with the natural homomorphism $\Lambda_p \subset \mathbb{Z}_p \to \mathbb{F}_p$.

Theorem 4.3 *Let $p > 0$ be prime. Let S be a noetherian locally factorial scheme over Λ_p. Keep the above notation. In particular, let $Y \to S$ be a finite flat morphism of degree p. Let G be an abstract group of order p acting on Y via S-automorphisms. Then there is a finite flat S-group scheme $\mathscr{G}$ of degree p and a S-homomorphism $h : \mathscr{G} \to \mathrm{Aut}_{Y/S}$ such that, given any point $s \in S$ of codimension at most* 1*, the base change of h over* $\mathrm{Spec}(\mathscr{O}_{S,s})$*, $\mathscr{G} \otimes \mathscr{O}_{S,s} \to \mathrm{Aut}_{Y/S} \otimes \mathscr{O}_{S,s}$, induces an isomorphism of* $\mathrm{Spec}(\mathscr{O}_{S,s})$*-group schemes*

$$\mathscr{G} \otimes \mathscr{O}_{S,s} \longrightarrow f(G_S) \otimes \mathscr{O}_{S,s}.$$

The pair $(\mathscr{G}, h)$ is unique up to unique isomorphism. Moreover, Y/S is a torsor for the $\mathscr{G}$-action if and only if the fiber $Y \otimes k(s)$ is a torsor for the action of $\mathscr{G} \otimes \kappa(s)$ for each point $s \in S$ of codimension at most 1*.*

Extending Romagny's terminology, we call the finite flat S-group scheme $\mathscr{G}$, together with its action on Y, the *effective model* for the G-action on Y. The proof of Theorem 4.3 is postponed to 4.13. We start with several preliminary propositions.

Lemma 4.4 *Let S be a noetherian scheme. Let $U \subset S$ be a dense open subscheme which contains all points of S which do not satisfy Serre's Condition (S_1). Let $G_1 \to S$ and $G_2 \to S$ be two finite and flat morphisms. Let $\varphi : G_1 \to G_2$ and $\psi : G_1 \to G_2$ be two S-morphisms such that $\varphi_{|U}$ and $\psi_{|U}$ are equal as morphisms from $G_1 \times_S U$ to $G_2 \times_S U$. Then $\varphi = \psi$.*

Proof The equality can be checked locally on the base. Thus we may assume that $S = \operatorname{Spec} R$ is affine, in which case $G_i = \operatorname{Spec}(A_i)$ for some R-algebra A_i which are free of finite rank as R-module, and the two given morphisms corresponds to morphisms $\varphi^*, \psi^* : A_2 \to A_1$ of R-algebras. Since S is noetherian, the set $\operatorname{Ass}(R)$ is finite. Thus the Prime Avoidance Lemma lets us find $f \in R$ such that $\operatorname{Ass}(R)$ is contained in the special open set $D(f)$ of S, and such that $D(f) \subseteq U$. Then $f \in R$ is regular [20, Chapter IV, Corollary 3.1.9]. Since A_1/R and A_2/R are free, the localization map

$$\operatorname{Hom}_R(A_2, A_1) \longrightarrow \operatorname{Hom}_R(A_2, A_1)_f = \operatorname{Hom}_{R_f}((A_2)_f, (A_1)_f)$$

is injective. It follows that $\varphi^* = \psi^*$. □

Let (FFG/S) denote the category of finite flat group schemes over S.

Proposition 4.5 *Let S be a noetherian scheme. Let $U \subset S$ be a dense open subscheme and consider the restriction functor $(FFG/S) \to (FFG/U)$.*

(i) *If U contains all points of S which do not satisfy Serre's Condition (S_1), then the restriction functor is faithful.*
(ii) *If U contains all points of S which have codimension at most 1 and all points which do not satisfy Serre's condition (S_2), then the restriction functor is full.*

Proof (i) Follows immediately from Lemma 4.4.

(ii) Let G_1, G_2 be two finite flat group schemes over S, and $\varphi_U : (G_1)_U \to (G_2)_U$ be a homomorphism over U. We have to extend it to S. Since S is noetherian, there is a maximal open subset over which φ_U extends. It suffices to treat the case where $U \subset S$ itself is maximal. Seeking a contradiction, we assume $U \neq S$ and choose a generic point s in the closed subset $S \smallsetminus U$. One easily sees that if $(\varphi_U)_{U \cap \operatorname{Spec}(\mathscr{O}_{S,s})}$ extends over $\operatorname{Spec}(\mathscr{O}_{S,s})$, then it extends to some φ_V over some open neighborhood V of $s \in S$. Using (i), we may shrink V so that φ_U and φ_V coincide on the overlap $U \cap V$. Hence, φ_U extends to $U \cup V$, which is a contradiction. This reduces us to the case where $S = \operatorname{Spec}(R)$ is local, and $U \subset S$ is the complement of the closed point $s \in S$. Then $G_i = \operatorname{Spec}(A_i)$ for some Hopf R-algebra A_i, such that the underlying R-modules are free of finite rank. The morphism φ that we seek corresponds to an R-linear Hopf algebra map $A_2 \to A_1$. Consider the free R-module $M = \operatorname{Hom}_R(A_2, A_1)$ of finite rank and the corresponding coherent sheaf $\mathscr{M}$. The long exact sequence of local cohomology yields

$$\Gamma_s(S, \mathscr{M}) \longrightarrow \Gamma(S, \mathscr{M}) \longrightarrow \Gamma(U, \mathscr{M}) \longrightarrow H^1_s(S, \mathscr{M}). \tag{4.6}$$

By assumption, the local ring R has depth ≥ 2. Whence the outer terms vanish, and the homomorphism of Hopf algebras φ_U extends to a homomorphism of R-modules $\varphi : A_2 \to A_1$. Arguing in the same way as for Lemma 4.4, one sees that the morphism φ is compatible with the Hopf structures. □

Proposition 4.7 *Let S be a noetherian scheme. Let $\mathscr{G}$ be a finite flat S-group scheme, and let Y be a finite flat S-scheme. Assume that there exists an open subscheme U of S such that Y_U is endowed with a U-group scheme action $\mu_U : \mathscr{G}_U \times_U Y_U \to Y_U$ of $\mathscr{G}_U$. If U contains all points of S that are of codimension at most 1 and all points of S which do not satisfy Serre's Condition (S_2), then the given U-group scheme action μ_U extends to a unique S-group scheme action $\mu : \mathscr{G} \times_S Y \to Y$ of $\mathscr{G}$ on Y.*

Proof As in the proof for Proposition 4.5, it suffices to treat the case that $S = \mathrm{Spec}(R)$ is local, and $U \subset S$ is the complement of the closed point. Then $Y = \mathrm{Spec}(B)$ and $\mathscr{G} = \mathrm{Spec}(A)$ are given by R-algebras that are free of finite rank as R-modules. The desired group scheme action $\mu : \mathscr{G} \times Y \to Y$ corresponds to a linear map $B \to A \otimes_R B$ satisfying certain axioms. Consider the free R-module $M = \mathrm{Hom}_R(B, A \otimes_R B)$; arguing with a short exact sequence in local cohomology like (4.6), we see that the desired homomorphism exists. The uniqueness of the extension follows from Lemma 4.4. □

Proposition 4.8 *Let S be a noetherian scheme. Let $\mathscr{G}$ be a finite flat S-group scheme, and let Y be a finite flat S-scheme endowed with a S-group scheme action $\mu : \mathscr{G} \times_S Y \to Y$. If for each point $s \in S$ of codimension at most 1, the fiber $Y \otimes \kappa(s)$ is a torsor over $\mathscr{G} \otimes \kappa(s)$, then Y is a $\mathscr{G}$-torsor.*

Proof We have to show that the canonical map $\mu \times \mathrm{pr}_2 : \mathscr{G} \times_S Y \to Y \times_S Y$ is an isomorphism. The question is local, so we may assume that $S = \mathrm{Spec}(R)$ is the spectrum of a local ring, and write $Y = \mathrm{Spec}(B)$ and $\mathscr{G} = \mathrm{Spec}(A)$. Let $f : B \otimes_R B \to A \otimes_R B$ be the resulting map between free modules of finite rank, and consider its determinant $\det(f) \in R$. Suppose the latter is not a unit, and choose a minimal prime ideal $\mathfrak{p} \subset R$ annihilating $R/\det(f)R$. Replacing R by the localization $R_{\mathfrak{p}}$, we arrive at the situation that $\det(f)$ is invertible precisely outside the closed point $s \in S = \mathrm{Spec}(R)$. By Krull's Principal Ideal Theorem, the point $s \in S$ is of codimension at most 1. By assumption, the class of $\det(f)$ in $\kappa(s)$ is nonzero, contradiction. □

Remark 4.9 The above propositions might be known to the experts, but we did not find an appropriate reference for them in the literature. Lemme 2 in [42], stated without proof, asserts that the restriction functor induces an equivalence of categories between the category of torsors under $\mathscr{G}/S$ and the category of torsors under $\mathscr{G}_U/U$, for any dense open set U of a regular noetherian scheme S which contains all points of codimension 1 in S. This statement is proved in [38, 3.1].

4.10 Denote by (FFG^p/S) the full subcategory of (FFG/S) consisting of all finite flat S-group schemes of degree p. According to [62, Theorem 1], such group schemes G/S take as values commutative groups annihilated by p. To apply further results of [62], we assume now that the base scheme S is a scheme over $\mathrm{Spec}\,\Lambda_p$.

Certain elements $w_i \in \Lambda_p$, $1 \le i \le p$ are introduced in [62] on page 9, with the property that $w_i \equiv i!$ modulo p. When $S \to \mathrm{Spec}\,\Lambda_p$ is given, we also denote by w_i the image of w_i in $\Gamma(S, \mathscr{O}_S)$. Consider now triples $(\mathscr{L}, \alpha, \beta)$, where $\mathscr{L}$ is an invertible sheaf on the scheme S, endowed with global sections $\alpha \in \Gamma(S, \mathscr{L}^{\otimes(p-1)})$ and $\beta \in \Gamma(S, \mathscr{L}^{\otimes(1-p)})$ so that $\alpha \otimes \beta = w_p$. Here the equality is obtained after identifying in the natural way $\mathscr{L}^{\otimes(p-1)} \otimes \mathscr{L}^{\otimes(1-p)}$ with $\mathscr{O}_S$.

An abelian sheaf $\mathscr{G}^{\mathscr{L}}_{\alpha,\beta}$, annihilated by p, is associated to such triple $(\mathscr{L}, \alpha, \beta)$ as follows. For any T/S, let

$$\mathscr{G}^{\mathscr{L}}_{\alpha,\beta}(T) := \left\{ x \in \Gamma(T, \mathscr{L} \otimes_{\mathscr{O}_S} \mathscr{O}_T) \mid x^{\otimes p} = \alpha \otimes x \right\},$$

and the group law is given by the formula

$$x \star x' := x + x' + \frac{\beta}{w_{p-1}} D_p(x \otimes 1, 1 \otimes x'),$$

where D_p is a certain polynomial in two variables described in [62, page 14]. It satisfies $D_p(X_1, X_2) \equiv \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} X_1^i X_2^{p-i}$ modulo p. The sheaf $\mathscr{G}_{\alpha,\beta}^{\mathscr{L}}$ is representable by a finite flat S-group scheme of degree p, denoted by the same letter $\mathscr{G}_{\alpha,\beta}^{\mathscr{L}}$. We can assemble a category (Trp/S) whose objects are triples $(\mathscr{L}, \alpha, \beta)$ as above, and whose morphisms are homomorphisms between invertible sheaves respecting the sections. According to [62, Theorem 2], we have:

Proposition 4.11 *The functor $(Trp/S) \to (FFG^p/S)$, given by $(\mathscr{L}, \alpha, \beta) \mapsto \mathscr{G}_{\alpha,\beta}^{\mathscr{L}}$, is essentially surjective.*

From this one deduces:

Proposition 4.12 *Suppose that S is a locally factorial scheme over Λ_p, and let $U \subset S$ be an open subscheme containing all points of codimension at most* 1. *Then the restriction functor $(FFG^p/S) \to (FFG^p/U)$ is an equivalence of categories.*

Proof The restriction functor is fully faithful by Proposition 4.5, and we have to check that it is essentially surjective. In light of Proposition 4.11, it suffices to extend an invertible sheaf $\mathscr{L}_U$ and the sections $\alpha_U, \beta_U \in \Gamma(U, \mathscr{L}_U)$ corresponding to a triple in (Trp/U) to a triple in (Trp/S). Write $\mathscr{L}_U = \mathscr{O}_U(D_U)$ for some Cartier divisor D_U. Since S is locally factorial, we can view D_U as a Weil divisor and write it as a difference $D_U = A_U - B_U$ of effective Weil divisors. Denote by A and B the closures in S of A_U and B_U. These Weil divisors over S correspond to invertible sheaves, giving the desired extension of the invertible sheaf $\mathscr{O}_U(D_U)$. The sections are extended as in the proof of Proposition 4.5. □

4.13 *Proof of Theorem* 4.3. Since S is a disjoint union of integral schemes, it suffices to prove the theorem when S is irreducible. Let $f : G_S \to \mathrm{Aut}_{Y/S}$ be the morphism introduced in (4.2). Let $f(G_S) \subseteq \mathrm{Aut}_{Y/S}$ denote the schematic image, which is finite over S. According to [20, Chapter IV, Theorem 11.1.1], the set $W \subset f(G_S)$ of all points where the morphism $f(G_S) \to S$ is flat is open. Let V' be the complement in S of the image under f of the closed set $f(G_S) \smallsetminus W$. Since f is finite, V' is open. Then the induced map $f(G_S)_{V'} \to V'$ is flat. Consider now

$$V := \left\{ s \in S \mid f(G_S) \otimes_{\mathscr{O}_S} \mathscr{O}_{S,s} \subset \mathrm{Aut}_{Y/S} \otimes_{\mathscr{O}_S} \mathscr{O}_{S,s} \text{ is a subgroup scheme} \right\}.$$

We claim that V is open in S, and that $f(G_S)_V$ is a subgroup scheme of $(\mathrm{Aut}_{Y/S})_V$. This is a local question, and we may assume that $S = \mathrm{Spec}(R)$ is affine, with $f(G_S) = \mathrm{Spec}(A)$ and $\mathrm{Aut}_{Y/S} = \mathrm{Spec}(B)$ (we use here the fact noted in Lemma 4.1 that $\mathrm{Aut}_{Y/S} \to S$ is affine). Write $A = B/I$, and let $\mathfrak{p} \subset R$ be the prime ideal corresponding to a point $s \in V$. The comultiplication map $B \to B \otimes B \to A \otimes A$ factorizes over $A = B/I$ when localized at $\mathfrak{p}$. Since I is finitely generated, there is an element $a \in R \smallsetminus \mathfrak{p}$ so that the map factorizes when inverting a. Then $\mathrm{Spec}(R_a) \subset S$ defines an open neighborhood over which the group law for $\mathrm{Aut}_{Y/S}$ defines a composition $f(G_S) \times f(G_S) \to f(G_S)$. In a similar way one construct an open neighborhood over which the inversion map for $\mathrm{Aut}_{Y/S}$ maps $f(G_S)$ to itself. Summing up, $V \subset S$ is open.

Now consider the open subset $U := V \cap V'$ of S. Define $\mathscr{G}_U := f(G_S)_U$. Then the structure morphism $\mathscr{G}_U \to U$ is finite and flat, and the inclusion $\mathscr{G}_U \subset (\mathrm{Aut}_{Y/S})_U$ is a

subgroup scheme, necessarily closed. We claim that $\mathscr{G}_U \to U$ has degree p. Since U is integral, it suffices to check this over the generic point $\eta \in U$. By construction of the effective model, $\mathscr{G}_\eta = G$ is the constant group of order p.

According to Romagny's result [53, Theorem A], U contains each point $s \in S$ of codimension one. Using Proposition 4.12, we extend $\mathscr{G}_U$ to a finite flat group scheme $\mathscr{G}$ over S. The canonical inclusion $\mathscr{G}_U \subset \operatorname{Aut} Y/S_U$ gives an action on Y_U. By Proposition 4.7, this action extends to an action of $\mathscr{G}$ on Y. This shows the existence of $\mathscr{G}$ and $h : \mathscr{G} \to \operatorname{Aut}_{Y/S}$.

The uniqueness also follows from Propositions 4.12 and 4.7, because for any other $\mathscr{G}'$ and $h' : \mathscr{G} \to \operatorname{Aut}_{Y/S}$ as in the assertion, there is an open subset $U_0 \subset U$ containing all points of codimension one with $\mathscr{G}'|U_0 = f(G_S)|U_0$. If the fibers Y_s are $\mathscr{G}_s$-torsors for each point $s \in S$ of codimension one, then Y is a $\mathscr{G}$-torsor, by Proposition 4.7. □

Now let R be a noetherian domain of characteristic $p > 0$ and write $S := \operatorname{Spec}(R)$. Fix some elements $a, b \in R$ with $a \neq 0$, and consider the R-algebra

$$B := R[u]/(u^p - a^{p-1}u - b),$$

endowed with the automorphism $u \mapsto u + a$ of order p. This automorphism induces an action of $G = \mathbb{Z}/p\mathbb{Z}$ on the S-scheme $Y := \operatorname{Spec}(B)$. Let $\mathscr{G}/S$ denote the group scheme $\mathscr{G}_{a,0} = \operatorname{Spec} R[z]/(z^p - a^{p-1}z)$ in the Tate–Oort classification.

Lemma 4.14 *There is a natural S-action $\mathscr{G} \times_S Y \to Y$ of $\mathscr{G}/S$ on Y/S such that Y/S is a torsor under $\mathscr{G}/S$. Moreover, any torsor Z/S under $\mathscr{G}/S$ is isomorphic to a torsor of the form Y/S.*

Proof Indeed, the p-polynomial $P(z) = z^p - a^{p-1}z$ defines an isogeny of the additive group scheme, and yields a short exact sequence

$$0 \longrightarrow \mathscr{G} \longrightarrow \mathbb{G}_{a,S} \xrightarrow{P} \mathbb{G}_{a,S} \longrightarrow 0$$

in the fppf-topology. In turn, we get a long exact sequence

$$H^0(S, \mathscr{O}_S) \xrightarrow{P} H^0(S, \mathscr{O}_S) \xrightarrow{\delta} H^1(S, \mathscr{G}) \longrightarrow H^1(S, \mathbb{G}_{a,S}) \longrightarrow H^1(S, \mathbb{G}_{a,S}). \tag{4.15}$$

The element $b \in R = H^0(S, \mathscr{O}_S)$ yields, via the coboundary map δ, a $\mathscr{G}$-torsor. According to [18, Chapter III, Definition 3.1.3], the torsor is defined as the fiber for the $\mathscr{G}$-torsor $P : \mathbb{G}_a \to \mathbb{G}_a$ over the section $b : S \to \mathbb{G}_a$. We thus see that Y is the $\mathscr{G}$-torsor coming from $b \in R$ via the coboundary map. The group scheme action $\mathscr{G} \times_S Y \to Y$ is just induced by the addition in $\mathbb{G}_a$, hence given by the homomorphism $u \mapsto z + u$.

The etale cohomology group $H^1(S, \mathbb{G}_{a,S})$ is isomorphic to the coherent sheaf cohomology group $H^1(S, \mathscr{O}_S)$, and since S is affine, this latter group is trivial. Hence, since torsors under $\mathscr{G}$ are in bijection with the elements of $H^1(S, \mathscr{G})$, any torsor Z/S under $\mathscr{G}/S$ is isomorphic to a torsor of the form Y/S. □

Proposition 4.16 *Suppose that R is a locally factorial noetherian domain of characteristic $p > 0$. Then $\mathscr{G}/S$ and the S-action $\mathscr{G} \times_S Y \to Y$ in Lemma 4.14 is the effective model for the action of $G = \mathbb{Z}/p\mathbb{Z}$ on Y/S.*

Proof Since the $\mathscr{G}$-action on the torsor Y is faithful, the canonical map $\mathscr{G} \to \operatorname{Aut}_{Y/S}$ is a monomorphism. The structure morphism $\mathscr{G} \to S$ is finite, and $\operatorname{Aut}_{Y/S} \to S$ is affine (Lemma 4.1). It follows that $\mathscr{G} \to \operatorname{Aut}_{Y/S}$ is proper, hence a closed embedding by [20,

Chapter IV, Proposition 18.12.6]. Being flat, the morphism $\mathscr{G} \to S$ has the going-down property, hence the generic fiber $\mathscr{G}_\eta$ is dense in $\mathscr{G}$. By assumption, the scheme $S = \mathrm{Spec}(R)$ is normal, whence contains no embedded component, and the same holds for $\mathscr{G}$, because it is the spectrum of $R[z]/(z^p - a^{p-1}z)$, whose underlying R-module is free. It follows that $G = \mathscr{G}_\eta$ is schematically dense in $\mathscr{G}$.

Our assumption that S is locally factorial and Theorem 4.3 show that the effective model for the G-action exists. Theorem 4.3 also shows that the closed subscheme $\mathscr{G}$ of $\mathrm{Aut}_{Y/S}$ is the effective model if we show that when S has dimension 1, then $\mathscr{G}$ is equal to the schematic image $\mathscr{G}' := f(G_S)$ of the canonical homomorphism $f : G_S \to \mathrm{Aut}_{Y/S}$. Since G_S is reduced and $G_\eta \subset G_S$ is dense, the same properties hold for $\mathscr{G}'$. Both $\mathscr{G}$ and $\mathscr{G}'$ are the closures of their generic fibers inside $\mathrm{Aut}_{Y/S}$. Hence, $\mathscr{G} = \mathscr{G}'$. □

5 Wild actions in dimension one

We further discuss in this section the notion of effective model for a group action in the case where the base scheme S has dimension 1. The main result of this section is Theorem 5.1.

Let $A := k[[u]]$ be a formal power series ring over a field k of characteristic $p > 0$. Let $\sigma : A \to A$ be a k-linear automorphism of order p, generating a cyclic group $G \subset \mathrm{Aut}_k(A)$ of order p. Let $x := N_{A/A^G}(u) = \prod_{\sigma \in G} \sigma(u)$ be the norm element of the uniformizer $u \in A$. It is obviously invariant under the action of G, so that $k[[x]] \subset A^G$. Samuel's Theorem [56] ensures that this canonical inclusion $k[[x]] \subset A^G$ is an equality.

Since the field k contains only $\zeta = 1$ as p-th root of unity, we find that $\sigma(u) = u +$ (higher order terms). It is standard to define the *ramification break* of the action as the largest integer $m > 0$ such that the induced action of σ on $A/\mathfrak{m}_A^{m+1}$ is trivial. In particular, $\sigma(u) = u + u^{m+1}$(unit), and $m > 0$ completely determines the higher ramification groups $G = G_1 = G_2 = \cdots = G_m \supsetneq G_{m+1} = (0)$.

Let now $Y := \mathrm{Spec}\, A$ and $S := \mathrm{Spec}\, A^G$. Using the G-action on A, we associate an action of the constant group scheme G_S on Y, given by the morphism $G_S \times_S Y \to Y$ corresponding to the ring homomorphism $A \to A \otimes_{A^G} A^G[s]/(s^p - s)$ defined by

$$a \longmapsto \sum_{i=0}^{p-1} \left(\sigma^i(a) \otimes \prod_{j \in \mathbb{F}_p,\ j \neq \bar{i}} \frac{(s-j)}{(\bar{i}-j)} \right).$$

Consider now the effective model $\mathscr{G}/S$ for the action of G_S on Y, as recalled in Sect. 4. Since $\dim(S) = 1$, the existence of the effective model is proved already in [53, Theorem 4.3.4], where one finds that $\mathscr{G}/S$ is a finite flat group scheme of degree p with an S-action $\mathscr{G} \times_S Y \to Y$. It is natural to ask when Y/S is a torsor for this action. The answer to this question is given in our next theorem, which is the main result of this section.

Theorem 5.1 *Keep the above notation. Let $\mathscr{G}/S$ be the effective model for the action of G_S on Y. The following are equivalent:*

(i) *The scheme Y/S is a torsor for the action of $\mathscr{G}/S$.*
(ii) *The integer $m+1$ is divisible by p.*
(iii) *There exists a uniformizer $u \in A$ and an invariant element $a \in A^G$ such that $\sigma(u) = u + a$.*

Let $\rho := (m+1)(p-1)/p$. When these equivalent conditions are satisfied, the group scheme $\mathscr{G}$ is isomorphic to the group scheme $\mathscr{G}_{x^\rho,0}$ in the Tate–Oort classification [62].

Note that in characteristic $p = 2$, the equivalent conditions in Theorem 5.1 automatically hold, because the ramification break m is known to be always odd in this case (the proof of this fact is recalled in Lemma 5.5). Theorem 5.1 illustrates the fact that the geometric condition *Y/S is a torsor for the action of $\mathscr{G}/S$* implies an interesting condition on the equation defining the automorphism σ. When the three equivalent conditions in Theorem 5.1 are satisfied, we call the action of G on A *moderately ramified*. We consider the case where $\dim(A) > 1$ in Definition 6.10 and impose an analogous geometric condition (MR5) in our general definition of moderately ramified action. The proof of Theorem 5.1 is postponed to 5.6. We start by reviewing the relevant parts of the Tate–Oort classification [62].

5.2 Let R be any ring of characteristic $p > 0$, with $\mathrm{Pic}(R) = 0$. Set $S := \mathrm{Spec}\, R$. The Tate–Oort classification [62], which we already discussed in 4.10, now takes the following simpler form: a group scheme $\mathscr{G}/S$ whose structure sheaf is locally free of rank p is isomorphic to $\mathscr{G}_{\alpha,\beta} := \mathrm{Spec}(R[T]/(T^p - \alpha T))$ for some elements $\alpha, \beta \in R$ with $\alpha\beta = 0$. As abelian sheaves,

$$\mathscr{G}_{\alpha,\beta}(T) := \left\{ s \in \Gamma(T, \mathscr{O}_T) \mid s^p = \alpha s \right\},$$

with group law given by the formula $s \star s' = s + s' + \beta \sum_{i=1}^{p-1} \frac{1}{i!(p-i)!} s^i s'^{p-i}$. Moreover, two group schemes $\mathscr{G}_{\alpha,\beta}/S$ and $\mathscr{G}_{\alpha',\beta'}/S$ are isomorphic if and only if there exists $\epsilon \in R^\times$ such that $\alpha' = \epsilon^{p-1}\alpha$ and $\beta' = \epsilon^{1-p}\beta$.

Proposition 5.3 *Suppose that R is a domain. Then the generic fiber of $\mathscr{G}_{\alpha,\beta}$ is étale if and only if $\alpha \neq 0$ and $\beta = 0$. Assume in addition that R is normal. Then the generic fiber of $\mathscr{G}_{\alpha,\beta}$ is constant if and only if $\beta = 0$ and $\alpha = a^{p-1}$ for some non-zero $a \in R$.*

Proof Taking the derivative of $T^p - \alpha T$, we see that α defines the locus where the structure morphism $\mathscr{G}_{\alpha,\beta} \to \mathrm{Spec}(R)$ is not smooth. Suppose that the generic fiber of $\mathscr{G}_{\alpha,\beta}$ is étale. Then $\alpha \neq 0$. Since R is a domain, the condition $\alpha\beta = 0$ ensures $\beta = 0$. The converse is also clear.

Now assume that R is normal. Suppose that $\alpha = a^{p-1}$ for some non-zero $a \in R$. Then we have a factorization $T^p - \alpha T = \prod_{i=0}^{p-1}(T - ia)$. The roots ia are pairwise different. Thus the generic fiber of $\mathscr{G}_{\alpha,\beta}$ must be constant. Conversely, suppose that $\mathscr{G}_{\alpha,\beta}$ is generically constant. Then the polynomial $T^p - \alpha T$ is separable, and its roots are contained in the field of fractions $F = \mathrm{Frac}(R)$. In particular, there is a non-zero element $a \in F$ with $a^{p-1} = \alpha$. Again it follows that $\beta = 0$. Since R is normal, we already have $a \in R$. □

Corollary 5.4 *Let $\mathscr{G}/S$ be a finite flat group scheme of degree p that is generically constant. Then $\mathscr{G}/S$ is isomorphic to $\mathscr{G}_{x^{r(p-1)},0}/S$ for some unique integer $r \geq 0$.*

Proof According to Proposition 5.3, the group scheme $\mathscr{G}$ is isomorphic to $\mathscr{G}_{\alpha,0}$ for some power series of the form $\alpha = a^{p-1}$ with $a \in R$. Write $\alpha = \epsilon \cdot x^e$ for some unit $\epsilon \in R$ and some exponent $e \geq 0$. Taking valuations of both sides, we see that $e = (p-1)r$ for some r, so x^e, and whence the unit ϵ, are $(p-1)$-th powers. Since α is unique up to invertible $(p-1)$-th powers, we may assume $\alpha = x^{r(p-1)}$, so that

$$\mathscr{G} = \mathscr{G}_{x^{r(p-1)},0} = \mathrm{Spec}\, R[s]/(s^p - x^{r(p-1)}s).$$

The integer $r \geq 0$ is unique, because it is the length of the intersection, inside the scheme $\mathscr{G}$, of the zero-section (defined by $s = 0$) and any non-zero section (defined by $s = ix^r$ for some $i \in \mathbb{F}_p^\times$). □

We now return to the initial set-up of this section where $A = k[[u]]$ and $R = A^G = k[[x]]$. Recall that since $\mathrm{Frac}(A)/\mathrm{Frac}(A^G)$ is a Galois extension of degree p, we can find $z \in \mathrm{Frac}(A)$, a power series $f(x) = \sum_{i=0}^{\infty} \lambda_i x^i \in k[[x]]^\times$, and an integer μ, such that $\mathrm{Frac}(A) = \mathrm{Frac}(A^G)(z)$ and z satisfies the Artin–Schreier equation $z^p - z = x^{-\mu} f(x)$. Since the extension A/A^G is totally ramified, we find that $\mu > 0$. It is well-known that there exists such z with μ coprime to p. Indeed, write $\mu = pr - i$ for some uniquely defined non-negative integers r and $0 \leq i < p$. The ring A contains the element $s := zx^r$, which satisfies the equation $s^p - x^{r(p-1)}s = x^i f(x)$. If $i = 0$, then the residue field of A contains the class of s, and since the residue field extension is trivial, we find that λ_0 is a p-th power modulo (x), say $\lambda_0 = \ell^p$ for some $\ell \in k$. It follows that we can consider $z' := z + \ell/x^r$, which satisfies $z'^p - z' = x^{-\mu} f(x) - \lambda_0/x^\mu + \ell/x^r$. After possibly finitely many similar steps, we obtain a generator z for $\mathrm{Frac}(A)$ whose associated integer $\mu > 0$ is coprime to p. The following lemma is well-known, and the notation introduced in its proof will be used in 5.6.

Lemma 5.5 *Write as above* $\mathrm{Frac}(A) = \mathrm{Frac}(A^G)(z)$ *such that* z *satisfies the Artin–Schreier equation* $z^p - z = x^{-\mu} f(x)$ *with* $\mu > 0$ *coprime to* p. *Then* $\mu = m$.

Proof Write $\mu = pr - i$ with $0 < i < p$. Let $0 < c < p$ be the unique integer such that ci is congruent to 1 modulo p, and let $d := (ci - 1)/p$, so that $ci - dp = 1$. The element $s = zx^r \in \mathrm{Frac}(A)$ satisfies the integral equation

$$s^p - x^{r(p-1)}s = x^i f(x).$$

Recall that $A = k[[u]]$, so that $\mathrm{ord}_u(s) = \mathrm{ord}_u(z) + pr = -\mu + pr = i$. Consequently, the element s^c/x^d has valuation $\mathrm{ord}_u(s^c/x^d) = ci - pd = 1$. Thus the element s^c/x^d is a uniformizer in A, and hence $k[[s^c/x^d]] = A$. The group action $z \mapsto z + 1$ sends s to $s + x^r$. To determine the ramification break m, it remains to compute the valuation of

$$\frac{(s + x^r)^c}{x^d} - \frac{s^c}{x^d} = \sum_{n=0}^{c-1} \binom{c}{n} s^n x^{r(c-n)-d},$$

and we leave this computation to the reader. □

5.6 *Proof of Theorem* 5.1. The implication (iii)⇒(ii) is immediate: Suppose that $\sigma(u) = u + a$ for some invariant a. Then $m + 1 := \mathrm{val}_u(\sigma(u) - u) = \mathrm{val}_u(a)$, and the latter is a multiple of p since $A^G \subset A$ has degree p.

(ii)⇒(i): Suppose that $m = pr - 1$. As above, we can find $z \in \mathrm{Frac}(A)$ and a power series $f(x) = \sum_{i=0}^{\infty} \lambda_i x^i \in k[[x]]^\times$ such that $\mathrm{Frac}(A) = \mathrm{Frac}(A^G)(z)$ and z satisfies the Artin–Schreier equation $z^p - z = x^{-m} f(x)$. With the notation from the proof of Lemma 5.5, we have $i = c = 1$ and $d = 0$, and we see that $s := zx^r \in A$ is a uniformizer, satisfying the equation

$$s^p - x^{r(p-1)}s - xf(x) = 0.$$

Moreover, the G-action is given by $s \mapsto s + x^r$. In light of the exact sequence (4.15), the scheme $Y = \mathrm{Spec}(A)$ is a torsor for the group scheme $\mathscr{G}_{x^{r(p-1)},0}$. By Proposition 4.16, the group scheme $\mathscr{G}_{x^{r(p-1)},0}$ and its associated action on Y is the effective model for the action of G on Y.

(i)⇒(iii): Suppose that Y is a $\mathscr{G}$-torsor. Corollary 5.4 shows that since $\mathscr{G}/S$ is a finite flat group scheme of degree p that is generically constant, then it is isomorphic to $\mathscr{G}_{x^{r(p-1)},0}/S$ for some unique integer $r \geq 0$. The case $r = 0$ is impossible, for then the closed fiber of $\mathscr{G}$ is

étale, whereas the closed fiber of $Y \to S$ is non-reduced. Since Y is a $\mathscr{G}$-torsor, Lemma 4.14 allows us to write that

$$A = k[[x]][s]/(s^p - x^{r(p-1)}s - g(x))$$

for some power series $g(x) \in k[[x]]$. The induced G-action is given by $s \mapsto s + x^r$. Using the hypothesis that A is formally smooth over k, we infer that the partial derivative of $s^p - x^{r(p-1)}s - g(x)$ with respect to x is a unit, and we deduce from the Implicit Function Theorem that one may express x as a formal power series in s. In turn, the canonical map $k[[s]] \to A$ is bijective. Setting $u = s$ and $a = x^r$, we see that (iii) holds. □

We can generalize the last statement of Theorem 5.1 as follows.

Proposition 5.7 *Let G and A be as at the beginning of this section. In particular, $A^G = R = k[[x]]$, $Y = \operatorname{Spec} A$, and $S = \operatorname{Spec} k[[x]]$. Let $m > 0$ be the ramification break, and write $m + 1 = pr + i$ with some unique integers $r \geq 0$ and $0 \leq i < p$. Then the effective model $\mathscr{G}/S$ of the action of the constant group scheme G_S on Y is isomorphic to $\mathscr{G}_{x^{r(p-1)},0}/S$.*

Proof According to Corollary 5.4, the effective model of the G-action is of the form

$$\mathscr{G} = \mathscr{G}_{x^{\ell(p-1)},0} = \operatorname{Spec} R[s]/(s^p - x^{\ell(p-1)}s)$$

for some integer $\ell \geq 1$. We have to prove that $\ell = r$. In the group scheme $\mathscr{G}_{x^{\ell(p-1)},0}/S$, the zero-section is given by the ideal (s). Let P denote the section defined by the ideal $(s - x^\ell)$. By definition of the effective model when $\dim(S) = 1$ (see proof of Theorem 4.3 in 4.13), we have a closed immersion $\mathscr{G} = \mathscr{G}_{x^{\ell(p-1)},0} \subset \underline{\mathrm{GL}}_S(\mathscr{O}_Y)$. Thus the section P gives an S-automorphism $P_0 : Y \to Y$, and this automorphism becomes the identity after tensoring with $R/\mathfrak{m}_R^\ell$, but is not the identity when tensoring with $R/\mathfrak{m}_R^{\ell+1}$.

Consider now the morphism $G_S \to \mathscr{G}$. Since this morphism is an isomorphism after tensoring with $\operatorname{Frac}(R)$, we find that $P \in \mathscr{G}(S)$ lifts to a generator of $G_S(S)$. By definition of the ramification break $m \geq 0$, any generator of $G_S(S)$ corresponds to an automorphism $Y \to Y$ such that this automorphism becomes the identity after tensoring with $A/\mathfrak{m}_A^{m+1}$ over A, but is not the identity when tensoring with $A/\mathfrak{m}_A^{m+2}$. It follows that this automorphism becomes the identity after tensoring with $R/\mathfrak{m}_R^r$ over R, but is not the identity when tensoring with $R/\mathfrak{m}_R^{r+1}$. Applying this to the automorphism P_0 shows that $\ell = r$. □

6 Moderately ramified actions

Let A be a complete local noetherian ring that is regular, of dimension $n \geq 2$ and characteristic $p > 0$, with maximal ideal $\mathfrak{m}_A$ and field of representatives k. Let G be a finite cyclic group of order p, and assume that A is endowed with a faithful action of G ramified precisely at the origin (3.1), such that $k \subset A^G$. Choose an admissible regular system of parameters $u_1, \ldots, u_n \in A$ with respect to the G-action (Proposition 2.9). Write as before $x_i := N_{A/A^G}(u_i)$, $i = 1, \ldots, n$, for the norm elements, and consider the norm subring $R := k[[x_1, \ldots, x_n]]$ of $A = k[[u_1, \ldots, u_n]]$. The ring extension $R \subset A$ is flat and finite of degree p^n (Proposition 2.3).

In this section, we introduce *five cumulative assumptions* on the G-action and on the choice of parameters, which ensure that the ramification in $\operatorname{Spec}(A) \to \operatorname{Spec}(R)$ is "as small and simple as possible". This will lead to the notion of *moderately ramified* G-action in Definition 6.10, for which we shall obtain structure results in Theorems 6.11 and 6.19.

We show in Proposition 6.20 that when $n = 2$ and $p = 2$, and k has no separable quadratic extensions, then every G-action that is ramified precisely at the origin is moderately ramified. The first condition on the G-action that we want to consider is:

(MR 1) *The field extension* $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ *is Galois.*

As we note in Theorem 3.4, this condition often reduces to checking that the smaller extension $\mathrm{Frac}(A^G)/\mathrm{Frac}(R)$ is Galois. Assuming from now on that (MR 1) holds, we write H for the Galois group of $\mathrm{Frac}(A)/\mathrm{Frac}(R)$, which has order p^n and contains G. Given $\mathfrak{p} \in \mathrm{Spec}\, A$, the notation $I_{\mathfrak{p}}$ always refers in this section to the inertia group inside H.

Proposition 6.1 *If* (MR 1) holds, then the Galois group H is generated by the inertia subgroups $I_{\mathfrak{p}} \subset H$, where $\mathfrak{p}$ runs through the height one prime ideals in A.

Proof Consider the subgroup $H' \subset H$ generated by the inertia subgroups $I_{\mathfrak{p}}$ for all height one prime ideals $\mathfrak{p}$ of A. Set $R' := A^{H'}$ and consider the morphism $\mathrm{Spec}\, R' \to \mathrm{Spec}\, R$. Seeking a contradiction, we assume $H' \neq H$, so that $R' \neq R$. Let $\mathfrak{q} \subset R$ be a prime ideal of height one. Then there exists a prime ideal $\mathfrak{p} \subset A$ of height one such that $\mathfrak{q} = R \cap \mathfrak{p}$. It follows that the morphism $\mathrm{Spec}\, R' \to \mathrm{Spec}\, R$ is unramified over $\mathfrak{q}$. On the other hand, the morphism is ramified at the maximal ideal of R', because the morphism is finite and the residue field extension at the maximal ideal is trivial. Since R' is normal and R is regular and the morphism is finite, we can apply the Zariski–Nagata Purity Theorem to $\mathrm{Spec}\, R' \to \mathrm{Spec}\, R$ and find that the non-empty branch locus is pure of codimension one in $\mathrm{Spec}\, R$. This is a contradiction. □

A similar argument appears in [58, Théorème 2'], and we discuss this result further in Remark 6.21. The next condition ensures that the inertia groups for the quotient map $\mathrm{Spec}(A) \to \mathrm{Spec}(R)$ are as small and uniform as possible:

(MR 2) *The inertia group* $I_{\mathfrak{p}}$ *of every ramified prime ideal* $\mathfrak{p} \subset A$ *of height one is cyclic of order* p, *and normal in* H.

Our next lemma shows that this condition is automatic in dimension two.

Lemma 6.2 *If* (MR 1) *holds and* $n = 2$, *then Condition* (MR 2) *also holds, and* H *is elementary abelian of order* p^2.

Proof When $n = 2$, we find that $|H| = p^2$ and so H is abelian. By the Zariski–Nagata Purity Theorem applied to the ramified morphism $\mathrm{Spec}\, A \to \mathrm{Spec}\, R$, there is at least one prime ideal $\mathfrak{p}$ of height one in A whose inertia group $I_{\mathfrak{p}} \subset H$ is non-trivial. The group $I_{\mathfrak{p}}$ cannot be the whole group H, otherwise the morphism $\mathrm{Spec}\, A \to \mathrm{Spec}\, A^G$ is ramified at $\mathfrak{p}$, a contradiction. Hence, all non-trivial inertia subgroups $I_{\mathfrak{p}}$ are cyclic of order p. Note that the group H cannot be cyclic, since otherwise, it contains only one subgroup of order p, which must coincide with G. This is not possible, since then $G = I_{\mathfrak{p}}$, contradicting the assumption that G acts freely outside the closed point. Hence, H is elementary abelian of order p^2. □

Proposition 6.3 *If* (MR 1) *and* (MR 2) *hold, then the Galois group* H *is elementary abelian of order* p^n.

Proof We use here Proposition 6.1 and the fact that if H_1 and H_2 are two abelian subgroups of H such that $H_1 \cap H_2 = (0)$ and such that both H_1 and H_2 are normal in H, then the subgroup of H generated by H_1 and H_2 is also abelian and normal in H. To see this, simply note that a commutator $h_1 h_2 h_1^{-1} h_2^{-1}$ with $h_i \in H_i$ belongs to both H_1 and H_2. □

Assume that (MR 1) and (MR 2) hold. Since H is elementary abelian of order p^n, it contains exactly $(p^n - 1)/(p - 1)$ distinct subgroups of order p. Proposition 6.1 let us choose n distinct such cyclic subgroups $G_1, \ldots, G_n$ that are equal to the inertia subgroup of some ramified prime ideal of height one in A and such that the natural map

$$G_1 \times \cdots \times G_n \longrightarrow H$$

is an isomorphism. Each subgroup $G_i \subset H$ has a canonical complement, namely the subgroup $G_i^{\perp}$ of H generated by the subgroups G_j, $j \neq i$.

Consider the corresponding ring of invariants $A^{G_i^{\perp}} \subset A$. Then $\mathrm{Frac}(A^{G_i^{\perp}})/\mathrm{Frac}(R)$ is a cyclic extension of degree p, with Galois group $H/G_i^{\perp}$, which we identify with the group G_i. By hypothesis, G_i is the inertia group of a prime $\mathfrak{p}_i$ of A. It follows that the morphism $\mathrm{Spec}(A^{G_i^{\perp}}) \to \mathrm{Spec}(R)$ is ramified at $\mathfrak{p}_i \cap A^{G_i^{\perp}}$. By the Zariski–Nagata Purity Theorem, the branch locus of $\mathrm{Spec}\, A^{G_i^{\perp}} \to \mathrm{Spec}\, R$ is of the form $V(a_i)$ for some non-invertible element $a_i \in R = k[[x_1, \ldots, x_n]]$.

Consider the canonical homomorphism of R-algebras:

$$f : A^{G_1^{\perp}} \otimes_R \cdots \otimes_R A^{G_n^{\perp}} \longrightarrow A. \tag{6.4}$$

Lemma 6.5 *Keep the above notation, and assume that* (MR 1) *and* (MR 2) *hold. If the above map f is an isomorphism, then the extension $R \subset A^{G_i^{\perp}}$ is flat and the ring $A^{G_i^{\perp}}$ is regular for $i = 1, \ldots, n$. Moreover, the elements $a_1, \ldots, a_n$ form a system of parameters of R.*

Proof Let d_i denote the dimension of $A^{G_i^{\perp}} \otimes R/\mathfrak{m}_R$ as an $R/\mathfrak{m}_R$-vector space. By Nakayama's Lemma, there exists a surjective homomorphism $\varphi_i : R^{\oplus d_i} \to A^{G_i^{\perp}}$ of R-modules. Tensoring with $\mathrm{Frac}(A^{G_i^{\perp}})$, which has degree p over $\mathrm{Frac}(R)$, we find that $d_i \geq p$. Since A is free of rank p^n and f is an isomorphism, we have $\prod_{i=1}^{n} d_i = p^n$, which implies that $d_i = p$ for all $1 \leq i \leq n$. Since the R-module $R^{\oplus p}$ is torsion-free, we conclude that the morphism $\varphi_i : R^{\oplus p} \to A^{G_i^{\perp}}$ is an isomorphism for each $i = 1, \ldots, n$. Hence, the extension $R \subset A^{G_i^{\perp}}$ is flat for all $i = 1, \ldots, n$. It follows that the finite ring extensions $A^{G_i^{\perp}} \subset \bigotimes_{j=1}^{n} A^{G_j^{\perp}}$ are flat. Since A is regular, [20, IV.6.5.1] ensures that the rings $A^{G_i^{\perp}}$ are regular.

If $a_1, \ldots, a_n$ does not form a system of parameters in R, then the ideal $(a_1, \ldots, a_n)$ of R is contained in some non-maximal prime ideal $\mathfrak{q}$ of R. Let $s \in \mathrm{Spec}(R)$ be the corresponding non-closed point. Since s belongs to the branch locus of each morphism $\mathrm{Spec}(A^{G_i^{\perp}}) \to \mathrm{Spec}\, R$ by hypothesis, the preimage of s in each $\mathrm{Spec}(A^{G_i^{\perp}})$ is a singleton, with purely inseparable (possibly trivial) residue field extension. Since by hypothesis, $\mathrm{Spec}(A)$ is the fiber product of the $\mathrm{Spec}(A^{G_i^{\perp}})$, we find that the preimage t of s in $\mathrm{Spec}(A)$ is also a singleton with purely inseparable residue field extension. Hence, the inertia group at t for the action of G is not trivial, contradicting the hypotheses that the action of G on A is ramified precisely at the origin. □

Remark 6.6 Let $Y_i := \mathrm{Spec}(A^{G_i^{\perp}})$ and $S := \mathrm{Spec}(R)$. When $n = 2$, the morphism $Y_i \to S$ is flat since Y_i is normal and, hence, Cohen–Macaulay. When $n > 2$, Condition (MR 4) discussed below will imply that $Y_i \to S$ is flat. Note that the flatness would be automatic if the order of the group were prime to the residue characteristic. Indeed, it is proved in [51] that if R is a regular local ring and $L/\mathrm{Frac}(R)$ is a Galois extension with abelian Galois group H of order coprime to the residue characteristic p of R, then the integral closure B of R in L is

Cohen–Macaulay. It follows then that B/R is flat. An example is given in [51] that shows that the hypothesis $\gcd(|H|, p) = 1$ is needed in the proof of the statement. We note here that this hypothesis is also needed for the statement to hold in the equicharacteristic case. For this, let $G = \mathbb{Z}/p\mathbb{Z}$, and consider a moderately ramified G-action on $A = k[[u_1, \ldots, u_n]]$, with norm ring R, as in Theorem 6.19. Then the extension $\mathrm{Frac}(A^G)/\mathrm{Frac}(R)$ is elementary abelian with Galois group H of order p^{n-1}, and A^G is the integral closure of R in $\mathrm{Frac}(A^G)$. But A^G is not Cohen–Macaulay when $\dim(A) > 2$, in view of the facts reviewed in Proposition 3.2.

We do not know a counter-example to the Cohen–Macaulayness of the integral closure B when H is cyclic of order $p > 3$. When $p = 3$, such a counter-example is presented in [31, 2.4], in the mixed characteristic case. In Example 8.6, we exhibit such a counter-example when R is only assumed to be Cohen–Macaulay and H is generated by a generalized reflection (definition recalled in Remark 6.21). Under such weaker assumption on R, the case where $|H|$ is coprime to the residue characteristic of R is treated in [24, Propositions 13 and 15].

Our third condition below requires that the set of inertia subgroups for the morphism $\mathrm{Spec}(A) \to \mathrm{Spec}(R)$ be as small as possible. This condition is motivated by the statement of Proposition 6.7.

(MR 3) *There are only n subgroups $G_1, \ldots, G_n \subset H$ which are equal to the inertia subgroup of a ramified prime ideal of height one in A.*

When (MR 3) holds, up to the enumeration of the subgroups, the morphism (6.4) does not anymore depend on the choice of subgroups.

Proposition 6.7 *Keep the above notation, and assume that* (MR 1) – (MR 3) *hold. If the rings $A^{G_i^\perp}$ are Cohen–Macaulay for $1 \le i \le n$, then the morphism f is an isomorphism.*

Proof First, we verify that the ring $A' := A^{G_1^\perp} \otimes_R \cdots \otimes_R A^{G_n^\perp}$ is normal: Since R is regular and $A^{G_i^\perp}$ is Cohen–Macaulay, the extension $R \subset A^{G_i^\perp}$ is flat for all $i = 1, \ldots, n$ [39, (21.D) Theorem 51]. In turn, A' is free as an R-module, hence Cohen–Macaulay. It remains to check that A' is regular in codimension one. Let $\mathfrak{q} \subset R$ be a prime of height one. We claim that *all but possibly one of the extensions $R \subset A^{G_i^\perp}$ are unramified over* $\mathfrak{q}$. If this holds, we may assume without restriction that $R_\mathfrak{q} \subset (A^{G_i^\perp})_\mathfrak{q}$ is unramified for $i = 2, \ldots, n$. Then $A'_\mathfrak{q}$ is étale over $(A^{G_1^\perp})_\mathfrak{q}$ and the latter ring is normal, which ensures that $A'_\mathfrak{q}$ is normal too [39, (21.E) (iii)]. Summing up, A' is normal.

To verify the claim, let us assume *ab absurdo* that there exist two indices $i \neq j$ such that $R \subset A^{G_i^\perp}$ and $R \subset A^{G_j^\perp}$ are ramified over $\mathfrak{q}$. Upon renumbering if necessary, we may assume that $i = 1$ and $j = 2$. Since $\mathrm{Frac}(A^{G_i^\perp})/\mathrm{Frac}(R)$ is cyclic of degree p, there is only one prime ideal $\mathfrak{p}_1 \subset A^{G_1^\perp}$ and $\mathfrak{p}_2 \subset A^{G_2^\perp}$ lying over $\mathfrak{q}$. Choose some prime ideal $\mathfrak{p} \subset A$ lying over $\mathfrak{q}$. Clearly, $\mathfrak{p}$ lies over both $\mathfrak{p}_1$ and $\mathfrak{p}_2$. The extension $R \subset A$ is ramified at $\mathfrak{p}$ since $R \subset A^{G_1^\perp}$ is ramified at $\mathfrak{p}_1$. In particular, the inertia group $I_\mathfrak{p}$ is non-trivial. By Condition (MR 3), we have $I_\mathfrak{p} = G_j$ for some index $j \in [1, n]$. Thus we can always assume that either $I_\mathfrak{p} \neq G_1$ or $I_\mathfrak{p} \neq G_2$. Let us consider the case where $I_\mathfrak{p} \neq G_1$, the other one being similar. Since $I_\mathfrak{p} = G_j$ for some index $j \in [2, n]$, we find that by definition $I_\mathfrak{p} \subset G_1^\perp$. Hence, $A^{G_1^\perp} \subset A^{I_\mathfrak{p}}$. Since $R \subset A^{I_\mathfrak{p}}$ is unramified at $\mathfrak{p} \cap A^{I_\mathfrak{p}}$, we find that $R \subset A^{G_1^\perp}$ is unramified at $\mathfrak{p}_1$, which is a contradiction.

We proceed by proving that the localized morphism $f_\mathfrak{q}$ is bijective for the minimal prime $\mathfrak{q} = 0$ inside R. We need to show that the map

$$\mathrm{Frac}(A)^{G_1^\perp} \otimes_{\mathrm{Frac}(R)} \ldots \otimes_{\mathrm{Frac}(R)} \mathrm{Frac}(A)^{G_n^\perp} = A'_\mathfrak{q} \longrightarrow A_\mathfrak{q} = \mathrm{Frac}(A)$$

is an isomorphism. It follows from the Galois correspondence that the image of this map is the subfield of $\mathrm{Frac}(A)$ fixed by the subgroup $G_1^{\perp} \cap \ldots \cap G_n^{\perp}$. By construction, this latter subgroup is trivial so the map is surjective. Since both source and targets are vector spaces over $\mathrm{Frac}(R)$ of the same dimension, the map is an isomorphism, as desired.

Since A' is a free R-module, the canonical map $A' \to A'_{\mathfrak{q}}$ is injective, and we conclude that $f : A' \to A$ is injective. In particular, A' is integral, and we saw in the preceding paragraph that $\mathrm{Frac}(A') \to \mathrm{Frac}(A)$ is bijective. Since A' is normal, the finite extension $A' \subset A$ must be an equality. □

Proposition 6.7 motivates our next condition.

(MR 4) *The rings $A^{G_i^{\perp}}$ are Cohen–Macaulay, for all $1 \leq i \leq n$.*

When (MR 4) holds, we can use f to identify A with $A^{G_1^{\perp}} \otimes_R \cdots \otimes_R A^{G_n^{\perp}}$.

6.8 Let $Y_i := \mathrm{Spec}(A^{G_i^{\perp}})$ and $S := \mathrm{Spec}(R)$. Recall that we identify $H/G_i^{\perp}$ with G_i through the canonical bijection $G_i \to H/G_i^{\perp}$, so that we get a G_i-action on $A^{G_i^{\perp}}$ and Y_i/S. Let $\mathscr{G}_i/S$ be the effective model of the G_i-action on Y_i, as introduced in Theorem 4.3. This effective model is a finite flat group scheme over S, and comes with an S-action $\mathscr{G}_i \times_S Y_i \to Y_i$. We can now formulate the last of our cumulative conditions.

(MR 5) The scheme Y_i/S is a torsor for $\mathscr{G}_i/S$, for all $1 \leq i \leq n$.

When $\dim(S) = 1$, a similar condition is considered in Theorem 5.1. Our next lemma shows that Condition (MR 5) is automatic when $p = 2$.

Lemma 6.9 *If* (MR 1) – (MR 4) *hold and $p = 2$, then Condition* (MR 5) *also holds.*

Proof Set $B = A^{G_i^{\perp}}$ for convenience. Condition (MR 4) ensures that the extension $R \subset B$ is flat. Thus B is a free R-module of rank 2, and since R is local, we can find a basis for B as an R-module of the form $1, u$, where 1 is the unit element in R and $u \in B$. It follows that there exist $a, \xi \in R$ such that $u^2 = au + \xi$. Then $B = R[u]/(u^2 - au - \xi)$, and the action of $G/G_i^{\perp}$ is given by $u \mapsto u + a$. Proposition 4.16 describes the effective model $\mathscr{G}_i$ of the action of $\mathbb{Z}/2\mathbb{Z}$ on $Y_i = \mathrm{Spec}(B)$, and shows that the latter scheme is a torsor under $\mathscr{G}_i$. □

Definition 6.10 We say that a G-action on A is *moderately ramified* if it is ramified precisely at the origin, and there exists an admissible regular system of parameters $u_1, \ldots, u_n \in A$ with associated norm subring R such that the five conditions (MR 1) – (MR 5) hold.

Theorem 6.11 below is our main structure result for moderately ramified actions, and shows that such actions are easily described by explicit equations. Its converse in Theorem 6.19 shows in addition that moderately ramified actions are abundant.

Theorem 6.11 *Let A be a complete local ring that is regular of dimension $n \geq 2$, with field of representatives k and endowed with a moderately ramified action of the cyclic group G of order p. Then A, as a k-algebra with G-action, is isomorphic to*

$$k[[x_1, \ldots, x_n]][u_1, \ldots, u_n]/(u_1^p - a_1^{p-1}u_1 - x_1, \ldots, u_n^p - a_n^{p-1}u_n - x_n),$$

where $x_1, \ldots, x_n$ are indeterminates, the elements $a_1, \ldots, a_n \in k[[x_1, \ldots, x_n]]$ form a system of parameters of $k[[x_1, \ldots, x_n]]$, and the natural automorphism σ of order p, which sends u_i to $u_i + a_i$ for $i = 1, \ldots, n$ and fixes $k[[x_1, \ldots, x_n]]$, induces under this isomorphism a generator of G.

The elements $u_1, \ldots, u_n$ form an admissible regular system of parameters for the action of $\langle\sigma\rangle$, and the subring $R := k[[x_1, \ldots, x_n]]$ is identified with the norm subring for the action of G. The Galois group H of the extension $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ *is generated by the automorphisms σ_i, $i = 1, \ldots, n$, where $\sigma_i(u_j) = u_j$ if $i \neq j$, and $\sigma_i(u_i) = u_i + a_i$. Let $G_i^{\perp}$ be the subgroup generated by the elements σ_j with $j \neq i$. Then the invariant subring $A^{G_i^{\perp}}$ introduced in Lemma 6.5 is isomorphic to $R[u_i]/(u_i^p - a_i^{p-1}u_i - x_i)$.*

Before we give the proof of Theorem 6.11 in 6.15, let us review the notion of *fixed scheme of the action* and mention two corollaries. Let a finite group G act on a ring A. The *fixed point scheme* of the G-action is the closed subscheme $\mathrm{Spec}\, A/I$ of $\mathrm{Spec}\, A$, where I is the ideal of A generated by the elements of the form $\sigma(a) - a$, for all $a \in A$ and all $\sigma \in G$. Assume now that $A = k[[u_1, \ldots, u_n]]$ and G acts by k-automorphisms. Then I is the ideal of A generated by the elements $\sigma(u_i) - u_i$, for $i = 1, \ldots, n$ and $\sigma \in G$. When the action of $G = \langle\sigma\rangle$ on $k[[u_1, \ldots, u_n]]$ is linear, with $\sigma(u_i) := \zeta_i u_i$ for $i = 1, \ldots, n$ and ζ_i is a non-trivial m-th root of unity for some m coprime to the characteristic of k, we find that the fixed point scheme is smooth, with ideal $I = (u_1, \ldots, u_n)$. Let us record now the following immediate consequences of Theorem 6.11.

Corollary 6.12 *Let A of dimension n be endowed with a moderately ramified G-action, as in Theorem 6.11. Let I be the ideal of A defining the fixed point scheme of the action. Then $I \subseteq \mathfrak{m}_A^p$ and the length of A/I is a multiple of p^n.*

Proof Consider the normal form for the ring A obtained in Theorem 6.11. It is clear from the explicit form of the action of G that $I = (a_1, \ldots, a_n)A$. Since $a_i \in \mathfrak{m}_R$ and $u_i^p - a_i^{p-1}u_i - x_i = 0$, we see that $x_i \in \mathfrak{m}_A^p$, so that $I \subseteq \mathfrak{m}_A^p$. We computed in Proposition 2.3 that the length of $A/(x_1, \ldots, x_n)A$ is equal to p^n. It follows from the facts that $a_1, \ldots, a_n \in R$ belong to $\mathfrak{m}_R = (x_1, \ldots, x_n)R$ and that A/R is flat, that the length of $A/(a_1, \ldots, a_n)A$ as an A-module is a multiple of the length of $A/(x_1, \ldots, x_n)A$ [45, 19.1]. □

The proof for the following consequence is left to the reader:

Corollary 6.13 *Let A_1 and A_2 be two regular complete local rings of positive dimension n_1 and n_2, respectively, of characteristic $p > 0$, and field of representatives k. Consider two moderately ramified actions of $G := \mathbb{Z}/p\mathbb{Z}$, on A_1 and A_2. Then the natural diagonal action of G on the completed tensor product $A_1 \hat{\otimes}_k A_2$ is also moderately ramified.*

Next we explain how the torsor condition on $Y_i \to S$ in (MR 5) leads to a simple equation for Y_i.

Lemma 6.14 *Consider a moderately ramified G-action on A and keep the notation introduced in this section. Suppose that $Y_i \to S$ is a $\mathscr{G}_i/S$-torsor. Then $A^{G_i^{\perp}}$ is isomorphic to $R[r_i]/(f_i)$ for some polynomial $f_i(r_i) = r_i^p - a_i^{p-1}r_i - \xi_i$ with coefficients $a_i, \xi_i \in \mathfrak{m}_R$.*

Proof It follows from the Tate–Oort classification recalled in Proposition 4.11 and 5.2 that $\mathscr{G}_i/S$ is isomorphic to the group scheme $\mathscr{G}_{\alpha_i,\beta_i}/S$, with $\mathscr{G}_{\alpha_i,\beta_i} = R[T]/(T^p - \alpha_i T)$ for some elements $\alpha_i, \beta_i \in R$ with $\alpha_i\beta_i = 0$ (since $w_p = 0$ when R has characteristic p). By construction, the generic fiber of $\mathscr{G}_i \to S$ is a constant group scheme. Since R is a normal domain, we conclude from Proposition 5.3 that $\beta_i = 0$, $\alpha_i \neq 0$, and α_i is a $(p-1)$-th power in R, say $\alpha_i = a_i^{p-1}$ with $a_i \in R$.

It follows from Lemma 4.14 and Proposition 4.16 that the torsor $Y \to S$ is isomorphic to the spectrum of $R[r_i]/(f_i)$ for some polynomial $f_i(r_i) = r_i^p - a_i^{p-1}r_i - \xi_i$. The coefficient a_i

is not a unit, because $R \subset A^{G_i^\perp}$ is ramified at the origin. The element ξ_i becomes a p-th power in the residue field $k = R/\mathfrak{m}_R$, because the extension $R \subset A^{G_i^\perp}$ has trivial residue field extension. Changing ξ_i by such p-th power from the field of representatives $k \subset R$, we obtain $\xi_i \in \mathfrak{m}_R$. □

6.15 *Proof of Theorem* 6.11. Suppose that the G-action on $A = k[[u_1, \ldots, u_n]]$ is moderately ramified, that is, Conditions (MR 1) – (MR 5) hold. We find from Proposition 6.7 that the map $f : A^{G_1^\perp} \otimes_R \cdots \otimes_R A^{G_n^\perp} \to A$ introduced in (6.4) is an isomorphism, and that each $A^{G_i^\perp}$ is in fact regular (Lemma 6.5). We may then apply Lemma 6.14 to write $A^{G_i^\perp} = R[r_i]/(f_i)$ for some polynomial $f_i(r_i) = r_i^p - a_i^{p-1} r_i - \xi_i$ with coefficients $a_i, \xi_i \in \mathfrak{m}_R$.

Lemma 6.16 *Keep all the preceding assumptions. Then the following hold:*

(a) *The elements $a_1, \ldots, a_n$ form a system of parameters of R.*
(b) *The elements $\xi_1, \ldots, \xi_n$ form a regular system of parameters of R.*
(b) *The elements $r_1, \ldots, r_n$ form a regular system of parameters of A.*

Proof Part (a) is immediate from Lemma 6.5. To proceed, note that the canonical map

$$R[r_1, \ldots, r_n]/(f_1, \ldots, f_n) \longrightarrow R[[r_1, \ldots, r_n]]/(f_1, \ldots, f_n)$$

from polynomial rings to power series rings is bijective. This is because the polynomials $f_i(r_i)$ are monic, so both sides are free R-modules of the same rank, with corresponding bases of monomials. Write $\mathfrak{a} \subset R[[r_1, \ldots, r_n]]$ for the ideal generated by the polynomials $f_1, \ldots, f_r$. Using Proposition 6.7 we get an identification $A = R[[r_1, \ldots, r_n]]/\mathfrak{a}$. The partial derivatives are

$$\begin{aligned} \frac{\partial}{\partial x_j}(r_i^p - a_i^{p-1} r_i - \xi_i) &= \frac{\partial a_i}{\partial x_j} a_i^{p-2} r_i - \frac{\partial \xi_i}{\partial x_j}, \quad \text{and} \\ \frac{\partial}{\partial r_j}(r_i^p - a_i^{p-1} r_i - \xi_i) &= a_i^{p-1}. \end{aligned} \tag{6.17}$$

Consider the Jacobian matrix $J \in \mathrm{Mat}_{n \times 2n}(k[[x_1, \ldots, x_n, r_1, \ldots, r_n]])$ of partial derivatives. Since A is regular, this matrix has maximal rank when its entries are reduced modulo the maximal ideal (use the Jacobian Criterion as in [44, Theorem on page 429, and Remark 1 on page 431]). So the same holds for the $n \times n$-matrix $(\partial \xi_i / \partial x_j)_{1 \le i,j \le n} \in \mathrm{Mat}_{n \times n}(R)$, because $a_i \in \mathfrak{m}_R$. By the Implicit Function Theorem [8, Chapter IV, §4, No. 7, Corollary to Proposition 10], the elements $x_1, \ldots, x_n$ can be expressed as formal power series in the $\xi_1 \ldots, \xi_n$, which proves (b). Using the relation $r_i^p - a_i^{p-1} r_i - \xi_i = 0$, the elements $x_1, \ldots, x_n$ can be expressed as formal power series in the $r_1, \ldots, r_n$. Thus $r_1, \ldots, r_n$ for a regular system of parameters of A, and (c) is proved. □

6.18 We can now conclude the proof of Theorem 6.11. We use the identification

$$k[[x_1, \ldots, x_n]][r_1, \ldots, r_n]/(f_1, \ldots, f_n) \longrightarrow A$$

to obtain an explicit isomorphism $(\mathbb{Z}/p\mathbb{Z})^n \to H$: Define an injective group homomorphism

$$\begin{aligned} (\mathbb{Z}/p\mathbb{Z})^n &\longrightarrow \mathrm{Aut}_R(A) \quad \subseteq \mathrm{Gal}(\mathrm{Frac}(A)/\mathrm{Frac}(R)) = H, \\ (h_1, \ldots, h_n) &\longmapsto (r_i \mapsto r_i + h_i a_i)_{1 \le i \le n}. \end{aligned}$$

In the definition above, we identify $\mathbb{Z}/p\mathbb{Z}$ with the prime subfield of k. Since $|H| = p^n$, we find then that this homomorphism is an isomorphism.

The subgroup G of H corresponds under this isomorphism to a subgroup of order p generated by some $(h_1, \ldots, h_n) \in (\mathbb{Z}/p\mathbb{Z})^n$. Lemma 3.3 shows that every coefficient h_i is non-zero. We thus have $h_i^{p-1} = 1$ for $i = 1, \ldots, n$. After replacing our choice of $a_i \in R$ by $h_i a_i$, we can assume that the subgroup G of H corresponds under the above bijection with the diagonal subgroup, generated by $(1, \ldots, 1)$. With such choice, the generator of G corresponding to $(1, \ldots, 1)$ acts via

$$r_i \longmapsto r_i + a_i.$$

It is easy to compute the norms of $r_i \in A$:

$$N_{A/A^G}(r_i) = \prod_{\ell=0}^{p-1} (r_i + \ell a_i) = r_i^p - a_i^{p-1} r_i = \xi_i.$$

We replace our original regular system of parameters $u_1, \ldots, u_n$ by the regular system of parameters $r_1, \ldots, r_n$. The norm elements $x_1, \ldots, x_n \in R$ for the initial regular system of parameters are then replaced by $\xi_1, \ldots, \xi_n$. Both regular systems of parameters produce the same norm subring $R \subset A$. After this change of parameters, we can write that $A = k[[u_1, \ldots, u_n]]$ and $R = k[[x_1, \ldots, x_n]]$, with

$$A = R[u_1, \ldots, u_n]/(u_1^p - a_1^{p-1} u_1 - x_1, \ldots, u_n^p - a_n^{p-1} u_n - x_n).$$

Moreover, the elements $(h_1, \ldots, h_n) \in (\mathbb{Z}/p\mathbb{Z})^n = H$ act on A via $u_i \mapsto u_i + h_i a_i$ and G is generated by the element corresponding to $(1, \ldots, 1)$. □

We now state the expected converse to Theorem 6.11.

Theorem 6.19 *Let $n \geq 2$. Let k be a field of characteristic $p > 0$. Let $R := k[[x_1, \ldots, x_n]]$ and let $a_1, \ldots, a_n \in \mathfrak{m}_R \backslash \{0\}$. Consider the ring*

$$A := R[u_1, \ldots, u_n]/(u_1^p - a_1^{p-1} u_1 - x_1, \ldots, u_n^p - a_n^{p-1} u_n - x_n).$$

(a) *Then A is a regular complete local ring with maximal ideal $(u_1, \ldots, u_n)$. The extension $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ is Galois with Galois group H isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$, generated by the automorphisms σ_i, $i = 1, \ldots, n$, with $\sigma_i(u_j) := u_j$ if $j \neq i$, and $\sigma_i(u_i) := u_i + a_i$. We have $R = A^H$.*

(b) *Assume now that the elements $a_1, \ldots, a_n$ form a system of parameters in R. Let σ be the automorphism of order p of A which sends u_i to $u_i + a_i$, for $i = 1, \ldots, n$ and fixes R (in other words, $\sigma = \sigma_1 \cdots \sigma_n$). Then the action of $\langle \sigma \rangle$ on A is moderately ramified.*

Proof (a) Clearly, $R \subset A$ is a finite flat extension of degree p^n, so $\dim(A) = \dim(R) = n$ by Going-Up and Going-Down. The fiber ring for this extension is $A/\mathfrak{m}_R A = k[u_1, \ldots, u_n]/(u_1^p, \ldots, u_n^p)$, which is local, so A is local by Hensel's Lemma. Furthermore, the residue classes of the x_i vanish in the cotangent space $\mathfrak{m}_A/\mathfrak{m}_A^2$, so the latter is generated by the residue classes of the u_i. Hence $\mathrm{edim}(A) \leq \dim(A)$, so A is regular.

It is clear that we can exhibit p^n automorphisms of A leaving R fixed: for each $(c_1, \ldots, c_n) \in (\mathbb{Z}/p\mathbb{Z})^n$, define $\sigma(c_1, \ldots, c_n)$ to be the R-automorphism of order p of A which sends u_i to $u_i + c_i a_i$, for $i = 1, \ldots, n$. Hence, $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ is Galois, and we obtained an explicit group homomorphism $H := (\mathbb{Z}/p\mathbb{Z})^n \to \mathrm{Gal}(\mathrm{Frac}(A)/\mathrm{Frac}(R))$.

Let us denote by G_i the subgroup generated by σ_i, with $\sigma_i(u_i) := u_i + a_i$ and $\sigma_i(u_j) := u_j$ if $j \neq i$. Let $G_i^{\perp}$ denote the subgroup of H generated by the groups G_j, $j \neq i$. Clearly, the ring of invariants $A^{G_i^{\perp}}$ contains u_i, and we obtain a natural ring homomorphism $R[u_i]/(f_i) \to$

$A^{G_i^\perp}$, which sends the class of u_i to the class of u_i. As in the preceding paragraph, one sees that the source ring is a regular complete local ring with field of fractions of degree p over $\mathrm{Frac}(R)$. It follows that this natural homomorphism is an isomorphism.

(b) Let $G := \langle\sigma\rangle$. The fixed scheme of the G-action on $X = \mathrm{Spec}(A)$ is defined by the ideal $(a_1, \ldots, a_n) \subset A$. Since we assume in (b) that $a_1, \ldots, a_n \in R = k[[x_1, \ldots, x_n]]$ is a system of parameters, it follows that the action of G is ramified precisely at the origin. The regular system of parameters $u_1, \ldots, u_n \in A$ is admissible since the group G induces the trivial representation on the cotangent space $\mathfrak{m}_A/\mathfrak{m}_A^2$ (Lemma 2.8). Clearly, $x_i = N_{A/A^G}(u_i)$, so that R is indeed the norm subring of A associated with the admissible system of parameters $u_1, \ldots, u_n$. It follows from (a) that $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ is Galois, showing that (MR 1) holds.

Let us show now that each G_i is the inertia group of a height one prime ideal of A. Indeed, let $\mathfrak{p}$ be minimal prime ideal in A which contains a_i. This ideal $\mathfrak{p}$ has height one, and it is clear that $G_i \subseteq I_\mathfrak{p}$. Since $a_1, \ldots, a_n$, is a system of parameters of A, we find that $\mathfrak{p}$ cannot contain a_j, for any $j \neq i$. It follows that no automorphism in H but those in G_i can induce the identity on $A/\mathfrak{p}$. Hence, $G_i = I_\mathfrak{p}$, as desired.

Consider now a prime ideal $\mathfrak{p}$ of height one in A with $I_\mathfrak{p} \neq \{\mathrm{id}\}$. We are going to show that $I_\mathfrak{p} = G_j$ for some j, which in particular implies that Conditions (MR 2) and (MR 3) hold. Let $\tau \in I_\mathfrak{p}$ be a non-trivial element. Then the ideal $I(\tau)$ of the fixed scheme is contained in $\mathfrak{p}$. Since $\mathfrak{p}$ has height one, it follows that $I(\tau)$ can contain at most one of $a_1, \ldots, a_n$. We find using our explicit description in (a) of the automorphisms of $\mathrm{Frac}(A)$ over $\mathrm{Frac}(R)$ that the ideal $I(\tau)$ is not trivial and contains at least one of $a_1, \ldots, a_n$ since τ is not trivial. It follows that we can assume that $a_i \in I(\tau)$. Considering again the descriptions of the automorphisms, we see that this implies that $\tau \in \langle\sigma_i\rangle = G_i$. It follows that $I_\mathfrak{p} = G_i$.

Consider now the isomorphism $R[u_i]/(f_i) \to A^{G_i^\perp}$ found in (a). It is clear that $R \subset A^{G_i^\perp}$ is finite and flat, so (MR 4) holds. The scheme $\mathrm{Spec}\, A^{G_i^\perp} \to \mathrm{Spec}\, R$ is a torsor under the group scheme $\mathcal{G}_i := \mathrm{Spec}\, R[z]/(z^p - a_i^{p-1}z)$ and this group scheme is the effective model of the action on $\mathrm{Spec}\, A^{G_i^\perp}$, according to Proposition 4.16. Thus (MR 5) holds. □

There is one situation in which every action ramified precisely at the origin is moderately ramified, namely when $n = 2$ and $p = 2$, and k does not admit any separable quadratic extension. That $\mathbb{Z}/2\mathbb{Z}$-actions on $k[[x, y]]$ are very structured was already recognized by Artin in [4], leading to a description of the ring of invariants A^G that we recall in Theorem 7.7.

Proposition 6.20 *Let k be a field of characteristic $p = 2$ which does not admit any separable quadratic extension. Then, in dimension $n = 2$, any G-action on A that is ramified precisely at the origin is moderately ramified.*

Proof Proposition 2.9 shows that A contains an admissible regular system of parameters u_1, u_2, with norm ring $k[[x_1, x_2]]$. According to Theorem 3.4 (i), the field extension $\mathrm{Frac}(A^G)/k((x_1, x_2))$, which has degree $p^{n-1} = 2$, is not purely inseparable. Hence it must be Galois. We use our hypothesis on k with Theorem 3.4 (ii) to find that the extension $\mathrm{Frac}(A)/k((x_1, x_2))$ must be Galois as well. So Condition (MR 1) holds. Then Lemma 6.2 shows that (MR 2) holds. Hence, the Galois group H of order $p^n = 4$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and this group has precisely three nontrivial cyclic subgroups, one of which must be G. Since the action of G is ramified precisely at the origin, we find that G cannot be the inertia group in H of a prime of height 1. Proposition 6.1 shows that H is generated by cyclic groups which are inertia groups of primes of height 1. Thus H contains exactly two subgroups which are inertia groups of primes of height 1, and Condition (MR 3) holds. In dimension 2, Condition (MR 4) is always satisfied. Lemma 6.9 ensures that (MR 5) holds. □

Remark 6.21 Let B be any noetherian local ring. A ring automorphism $\sigma : B \to B$ of finite order is called a *generalized reflection* if $(\sigma - \mathrm{id})(B) \subseteq (xB)$ for some regular non-unit $x \in B$. In other words, the scheme of fixed points of σ in $\mathrm{Spec}(B)$ contains an effective Cartier divisor. The automorphism σ is called a *pseudo-reflection* if $(\sigma - \mathrm{id})(B) = (xB)$ for some regular non-unit $x \in B$. In this case, the scheme of fixed points of σ in $\mathrm{Spec}(B)$ is an effective Cartier divisor. When the order of σ is invertible in B, this latter definition is equivalent to the more classical definition where one requires that σ acts on the cotangent space $\mathfrak{m}_B/\mathfrak{m}_B^2$ through pseudo-reflections in the sense of linear algebra (see [6, (12) on page 168]).

Note that if $\sigma : B \to B$ is a generalized reflection (resp., a pseudo-reflection), then the conjugates $g\sigma g^{-1}$ and powers $\sigma^m \neq \mathrm{id}$, are also generalized reflections (resp., pseudo-reflections), where $g : B \to B$ is any automorphism. Indeed, $I(g\sigma g^{-1}) = g(I(\sigma))$, and when $n \geq 2$ is the order of σ, we have $I(\sigma^{n-1}) \subseteq \cdots \subseteq I(\sigma^2) \subseteq I(\sigma)$. Considering the same chain of inclusions with σ replaced by σ^{-1}, we find that all these inclusions are in fact equalities.

Let now A be a complete regular local ring of dimension $n \geq 2$ endowed with a moderately ramified action of $\mathbb{Z}/p\mathbb{Z}$, as in Theorem 6.11. Let $u_1, \ldots, u_n \in A$ be as in the statement of Theorem 6.11, and let $R := k[[x_1, \ldots, x_n]]$. As in Theorem 6.11, $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ is Galois of order p^n, with Galois group H generated by elements σ_i, $i = 1, \ldots, n$, such that $\sigma_i(u_i) = u_i + a_i$, and $\sigma_i(u_j) = u_j$ if $i \neq j$. It is clear from this expression for σ_i that the ideal $I(\sigma_i)$ is equal to $(a_i A)$, and is thus principal. Since we assume that $(a_1, \ldots, a_n)$ is a system of parameters in R, each of these ideals is proper. It follows that the group H is generated by pseudo-reflections. The next proposition shows that when only Condition (MR 1) holds (i.e., when $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ is Galois), then it is still possible to show that H is generated by generalized reflections. This proposition is nothing but a reformulation of a result of Serre [58, Théorème 2'].

Proposition 6.22 *Let B be a regular noetherian local ring with maximal ideal $\mathfrak{m}_B$. Let H be a finite group of ring automorphisms of B, and let $R := B^H$. Assume that B is a finitely generated R-module. The ring R is then a noetherian local ring with maximal ideal $\mathfrak{m}_R$, and we assume also that the natural map $R/\mathfrak{m}_R \to B/\mathfrak{m}_B$ is an isomorphism. Then H is generated by generalized reflections if R is regular.*

Remark 6.23 Conjecture 9 in [29] strengthens Proposition 6.22 in certain cases. Indeed, let B be a regular local ring with $\mathrm{char}(B/\mathfrak{m}_B) = p > 0$, and let $G = \langle\sigma\rangle$ be a cyclic group of order p acting on B by local automorphisms. With the definition of pseudo-reflection given in this article, [29, Conjecture 9], states that: *If B^G is regular, then σ is a pseudo-reflection*. The authors of [29] prove this conjecture when $p = 2$ and $p = 3$.

Theorem 2, (a) implies (d), in [29] proves the converse of the statement of Conjecture 9 above: *If σ is a pseudo-reflection, then B^G is regular*. We note below an example where σ is a generalized reflection, but B^G is not regular (see also Example 8.6). We do not have an example of a generalized reflection acting on a regular ring B such that B^G is not Cohen–Macaulay, and it would be interesting to determine whether such example exists. In the case where the order of σ is coprime to the residue characteristic of B, the invariant ring B^G is always Cohen–Macaulay [24, Proposition 13].

Theorem 7.14 lets us consider an action of G on $A := k[[u, v]]$ which is not ramified precisely at the origin, but such that the ring A^G can still be completely described. Indeed,

let $R := k[[x, y]]$. Let $a, b \in \mathfrak{m}_R$ with (a, b) a $\mathfrak{m}_R$-primary ideal. Let $\mu \in \mathfrak{m}_R$ such that (a, μ) and (b, μ) are $\mathfrak{m}_R$-primary ideals. Consider the ring

$$A := R[u, v]/(u^p - (\mu a)^{p-1}u - x, v^p - (\mu b)^{p-1}v - y).$$

Then A is a regular complete local ring with maximal ideal (u, v) (Theorem 6.19 (a)). The extension $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ is Galois with Galois group H isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$, generated by the automorphisms σ_1 and σ_2, with $\sigma_1(u) := u + \mu a$ and $\sigma_1(v) = v$, and $\sigma_2(v) := v + \mu b$ and $\sigma_2(u) = u$. We have $R = A^H$. The morphisms σ_1 and σ_2 are both pseudo-reflections, but the composite $\sigma := \sigma_1\sigma_2$ is only a generalized reflection: $I(\sigma) = (\mu a, \mu b)$. Let $G := \langle\sigma\rangle$. It follows that every prime ideal $\mathfrak{p}$ of A containing μ is ramified over $\mathfrak{p} \cap A^G$. We claim that the ring A^G is not regular. Indeed, consider $z := bu - av$, with the relation $f(z) := z^p - (\mu ab)^{p-1}z - a^p y + b^p x = 0$. Then $A^G = k[[x, y]][z]/(f)$, and this latter ring is singular at (x, y, z) (Theorem 7.14). Preliminary computations seem to indicate that the graph of the minimal desingularization $X \to \mathrm{Spec}\, A^G$ does not depend on μ.

7 Complete intersection subrings

Let as usual A be a complete regular local noetherian ring of dimension $n \geq 2$, characteristic $p > 0$, with field of representatives k, and endowed with the action of a cyclic group G of order p. The main result in this section is Theorem 7.7, which shows that for the class of moderately ramified actions introduced in Definition 6.10, the ring A^G can be described when $n = 2$ in terms of generators and relations.

7.1 Let $R := k[[x_1, \ldots, x_n]]$. Let $a_1, \ldots, a_n \in \mathfrak{m}_R$ be such that a_i and a_j are coprime if $i \neq j$. Let $\mu \in R\backslash\{0\}$ be such that μ and a_i are coprime, for $i = 1, \ldots, n$. Consider the ring

$$A := R[u_1, \ldots, u_n]/(u_1^p - (\mu a_1)^{p-1}u_1 - x_1, \ldots, u_n^p - (\mu a_n)^{p-1}u_n - x_n).$$

Theorem 6.19 (a) shows A is a regular complete local ring with maximal ideal $(u_1, \ldots, u_n)$. The extension $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ is Galois with Galois group H isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$, generated by the automorphisms σ_i, $i = 1, \ldots, n$, with $\sigma_i(u_j) := u_j$ if $j \neq i$, and $\sigma_i(u_i) := u_i + \mu a_i$. We have $R = A^H$.

Let σ be the automorphism of order p of A which sends u_i to $u_i + \mu a_i$, for $i = 1, \ldots, n$ and fixes R (in other words, $\sigma = \sigma_1 \cdots \sigma_n$). When $(\mu a_1, \ldots, \mu a_n)$ is a system of parameters of R, then the action of $G := \langle\sigma\rangle$ on A is moderately ramified (Theorem 6.19 (b)). Theorem 6.11 shows that any moderately ramified action of G corresponds to a ring A as above with $\mu = 1$ and $(\mu a_1, \ldots, \mu a_n)$ a system of parameters of R. When $\mu \notin R^*$, the action is not ramified precisely at the origin. Our goal is to describe the ring of invariants A^G explicitly in all cases when $n = 2$.

Identify the Galois group H of $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ with the elementary abelian p-group $(\mathbb{Z}/p\mathbb{Z})^n$, where an element $(\nu_1, \nu_2, \ldots, \nu_n)$ corresponds to the R-algebra automorphism given by $u_j \longmapsto u_j + \nu_j \mu a_j$. Under our identification, $(1, \ldots, 1)$ corresponds to the generator σ of G.

Let $s = (s_1, \ldots, s_n) \in (\mathbb{Z}/p\mathbb{Z})^n$ be a non-zero element, and consider the subgroup H_s of H of all elements of H perpendicular to s. In other words,

$$H_s := \left\{ (\nu_1, \nu_2, \ldots, \nu_n) \mid \sum_{i=1}^{n} \nu_i s_i = 0 \right\}.$$

Let

$$z_s := \left(\prod_{\{i\,|\,s_i\neq 0\}} a_i\right)\left(s_1\frac{u_1}{a_1}+\cdots+s_n\frac{u_n}{a_n}\right)\in A.$$

It is easy to verify that z_s satisfies the following relation:

$$z_s^p-\left(\mu\prod_{\{i\,|\,s_i\neq 0\}} a_i\right)^{p-1} z_s-\left(\prod_{\{i\,|\,s_i\neq 0\}} a_i\right)^{p}\left(s_1\frac{x_1}{a_1^p}+\cdots+s_n\frac{x_n}{a_n^p}\right)=0.$$

The reader will check that $h\in H$ is such that $h(z_s)=z_s$ if and only if $h\in H_s$. In particular, $\mathrm{Frac}(A^{H_s})=\mathrm{Frac}(R)(z_s)$ has degree p over $\mathrm{Frac}(R)$.

For convenience, let $\alpha := \prod_{\{i\,|\,s_i\neq 0\}} a_i$, and when $s_i\neq 0$, let $\alpha_i := \alpha/a_i$. By definition, $\alpha\in R$, and $\alpha_i\in R$ when $s_i\neq 0$. With this notation, define $f(z)\in R[z]$ by

$$f(z) := z^p-(\mu\alpha)^{p-1}z-\sum_{\{i\,|\,s_i\neq 0\}} s_i\alpha_i^p x_i.$$

Since $f(z_s)=0$ and the degree of z_s over R is p, we find that $f(z)$ is irreducible in $\mathrm{Frac}(R)[z]$, and also in $R[z]$ by Gauss' Lemma. Since $R[z]$ is factorial because R is, we find that $R[z]/(f(z))$ is a domain. We have a natural ring homomorphism $j: R[z]/(f(z))\to A^{H_s}$, which sends the class of z to z_s. After tensoring with $\mathrm{Frac}(R)$, the resulting homomorphism is surjective. It is thus also bijective, since the source and target have the same dimension over $\mathrm{Frac}(R)$. Since both rings $R[z]/(f(z))$ and A^{H_s} are integral domains, the map j is injective.

Theorem 7.2 *Let A be as in 7.1. Let H denote the Galois group of the associated extension $\mathrm{Frac}(A)/\mathrm{Frac}(R)$. Let H_s denote a subgroup of order p^{n-1} in H. Then the extension A^{H_s} is isomorphic to the ring $R[z]/(f(z))$, where $f(z)\in R[z]$ is given above. In particular, it is flat over R. The group H/H_s acts on the ring A^{H_s} through pseudo-reflections.*

Proof Since $R[z]/(f(z))$ is finitely generated and free over R, it is Cohen–Macaulay and, hence, satisfies the property S_2. We show below that $R[z]/(f(z))$ is regular in codimension 1. Then from Serre's criterion, $R[z]/(f(z))$ is normal, and injects into A^{H_s}, which is also normal, with same field of fractions. It follows that $R[z]/(f(z))\to A^{H_s}$ is an isomorphism.

Since R is complete, we can identify $R[z]/(f)$ with $k[[x_1,\ldots,x_n,z]]/(f)$. Consider the partial derivatives of f:

$$f_z=-(\mu\alpha)^{p-1}\quad\text{and}\quad f_{x_i}=(\mu\alpha)^{p-2}z(\mu\alpha)_{x_i}-s_i\alpha_i^p,\quad i=1,\ldots,n.$$

Suppose that $\mathfrak{p}$ is a prime ideal in $R[z]$ containing (f). Assume that the localization of $R[z]/(f)$ at the prime ideal $\mathfrak{p}/(f)$ is not regular. Then, according to the Jacobian Criterion, all the derivatives of f belong to $\mathfrak{p}$. In particular, $f_z\in\mathfrak{p}$, and so $\mu\alpha\in\mathfrak{p}$. We want to show that the prime $\mathfrak{p}/(f)$ has height at least 2 in $R[z]/(f)$.

Assume first that $p\geq 3$, and that $s_i\neq 0$. Then the condition $f_{x_i}\in\mathfrak{p}$ immediately implies that $\alpha_i\in\mathfrak{p}$. In particular, α_i is not a unit. Since $\alpha=a_i\alpha_i=\prod_{\{j\,|\,s_j\neq 0\}} a_j$, and so there exists $\ell\neq i$ such that $s_\ell\neq 0$ and $a_\ell\in\mathfrak{p}$. But then from $s_\ell\neq 0$ and $f_{x_\ell}\in\mathfrak{p}$, it follows that $\alpha_\ell\in\mathfrak{p}$. Hence, among the factors of α_ℓ, we can find $a_m\in\mathfrak{p}$ for some $m\neq\ell$. By hypothesis, the ideal (a_ℓ,a_m) has height at least 2 since a_ℓ and a_m are coprime and, thus, $\mathrm{ht}(\mathfrak{p})\geq 2$.

Assume now that $p=2$. In view of the fact that $\mu\alpha\in\mathfrak{p}$, we will consider two cases: when $\alpha\in\mathfrak{p}$, and when $\mu\in\mathfrak{p}$. *Let us start with the case where $\alpha\in\mathfrak{p}$.* If two or more of the a_j's that divide α belong to $\mathfrak{p}$, then as before $\mathrm{ht}(\mathfrak{p})\geq 2$ and we are done. Thus we are reduced

to consider only the case where $a_i \in \mathfrak{p}$ for some i with $s_i \neq 0$ and $a_j \notin \mathfrak{p}$ for all $j \neq i$ such that $s_j \neq 0$. We show now that this case cannot happen. Recalling that $\alpha = \alpha_i a_i$, we find using the product rule that $f_{x_i} = z(\mu\alpha)_{x_i} - s_i\alpha_i^2 = z(\mu\alpha_i)_{x_i}a_i + z(\mu\alpha_i)(a_i)_{x_i} - s_i\alpha_i^2$. From $f_{x_i}, a_i \in \mathfrak{p}$ and $\alpha_i \notin \mathfrak{p}$, we obtain that

$$z\mu(a_i)_{x_i} + s_i\alpha_i \in \mathfrak{p}. \tag{7.3}$$

We conclude in particular from this last expression that $z \notin \mathfrak{p}$.

Since a_i divides α_j when $j \neq i$ and $s_j \neq 0$, we find that $s_j\alpha_j^2 x_j \in \mathfrak{p}$. By hypothesis, $f(z) := z^2 - (\mu\alpha)z - \sum_{\{j|s_j\neq 0\}} s_j\alpha_j^2 x_j$ belongs to $\mathfrak{p}$, and so

$$z^2 + s_i\alpha_i^2 x_i \in \mathfrak{p}. \tag{7.4}$$

We are now ready to conclude as follows. First, (7.3) shows that $(z\mu(a_i)_{x_i} + s_i\alpha_i)^2 \in \mathfrak{p}$. Using that $s_i = 1 = s_i^2$ and (7.4), we obtain that $z^2(1 + (\mu(a_i)_{x_i})^2 x_i) \in \mathfrak{p}$. This is a contradiction, since $(1 + (\mu(a_i)_{x_i})^2 x_i)$ is a unit, and we noted above that $z \notin \mathfrak{p}$.

Consider now the case where $\mu \in \mathfrak{p}$. If a_i belongs to $\mathfrak{p}$ for some i, then $\mathrm{ht}(\mathfrak{p}) \geq 2$ by our hypothesis that μ is coprime to a_i. So let us assume that $a_i \notin \mathfrak{p}$ for all i with $s_i \neq 0$. From $f_{x_i} \in \mathfrak{p}$ and $\alpha_i \notin \mathfrak{p}$, we conclude that $z\mu_{x_i}a_i + s_i\alpha_i \in \mathfrak{p}$ whenever $s_i \neq 0$. In particular, $z \notin \mathfrak{p}$. From the relation $f = 0$ we find that $z^2 + \sum_{\{i|s_i\neq 0\}} s_i\alpha_i^2 x_i \in \mathfrak{p}$. It follows that $z^2(1 + \sum_{\{i|s_i\neq 0\}}(\mu_{x_i}a_i)^2 x_i) \in \mathfrak{p}$. This is a contradiction as before, since $(1 + \sum_{\{i|s_i\neq 0\}}(\mu_{x_i}a_i)^2 x_i)$ is a unit, and $z \notin \mathfrak{p}$. This concludes the proof that $R[z]/(f(z)) \to A^{H_s}$ is an isomorphism.

Pick any standard basis vector e_i of $(\mathbb{Z}/p\mathbb{Z})^n$ which does not belong to H_s (i.e., such that $s_i \neq 0$). Then the group H/H_s is cyclic of order p, generated by the image $\overline{e}_i$ of e_i, and acts on A^{H_s}. It is easy to check that $\overline{e}_i(z_s) - z_s = s_i\mu\prod_{s_j\neq 0} a_j$, so that the ideal of the fixed scheme of $\overline{e}_i$ is $I(\overline{e}_i) = \mu(\prod_{s_j\neq 0} a_j)A^{H_s}$, showing that $\overline{e}_i$ is a pseudo-reflection as defined in Remark 6.21. □

In the definition of a moderately ramified action on a complete local regular noetherian ring A of dimension $n \geq 2$, Condition (MR 5) imposes some structure requirement on n subrings of A^G, denoted $A^{G_i^\perp}$ in 6.8, of rank p over R. Our next corollary implies that all subrings of the form A^{H_s} of rank p over R satisfy the same structure requirement.

Corollary 7.5 *Let A be a complete local regular noetherian ring of dimension $n \geq 2$ and characteristic $p > 0$, with field of representatives k. Assume that A is endowed with a moderately ramified action of a cyclic group G of order p. Let H denote the Galois group of the associated extension* $\mathrm{Frac}(A)/\mathrm{Frac}(R)$. *Let H_s denote a subgroup of order p^{n-1} in H. Then the extension A^{H_s} is isomorphic to a ring of the form $R[z]/(f(z))$, where $f(z) = z^p - \alpha^{p-1}z - \beta$, with $\alpha, \beta \in R$. In particular, it is flat over R. The group H/H_s acts on the ring A^{H_s} through pseudo-reflections.*

Proof Theorem 6.11 lets us identify A with a ring of the form

$$R[u_1, \ldots, u_n]/(u_1^p - a_1^{p-1}u_1 - x_1, \ldots, u_n^p - a_n^{p-1}u_n - x_n),$$

where $R := k[[x_1, \ldots, x_n]]$ and $a_1, \ldots, a_n \in R$ is a system of parameters of R. Theorem 7.2 can then be applied. □

Keep the notation introduced in 7.1. Recall that $x_i := N_{A/A^G}(u_i) = u_i^p - (\mu a_i)^{p-1}u_i$ is a *norm element*. In light of the G-action $u_i \mapsto u_i + \mu a_i$, the elements

$$z_{ij} := a_i u_j - a_j u_i, \quad i \neq j$$

are also clearly G-invariant. We call these elements *minor elements*. Denoting by $e_1, \ldots, e_n$ the standard vectors of $(\mathbb{Z}/p\mathbb{Z})^n$ and setting $s = e_j - e_i$, we find that $z_{ij} = z_s$ (notation as in 7.1). The minor elements satisfy the obvious relations:

$$\begin{aligned} z_{ij}^p - (\mu^{p-1} a_i^{p-1} a_j^{p-1} z_{ij} + a_i^p x_j - a_j^p x_i) = 0, \quad & 1 \le i < j \le n, \text{ and} \\ a_i z_{jk} - a_j z_{ik} + a_k z_{ij} = 0, \quad & 1 \le i < j < k \le n. \end{aligned} \tag{7.6}$$

When $n = 2$, there is only one interesting element z_{ij}, namely z_{12}, and Theorem 7.2 shows that it generates A^G. Our next theorem shows that A^G in this case can be explicitly described.

Theorem 7.7 *Let A be a complete local regular noetherian ring of dimension two and characteristic $p > 0$, with field of representatives k. Assume that A is endowed with a moderately ramified action of a cyclic group G of order p. Then there exists a system of parameters a, b in $k[[x, y]]$ such that A^G is isomorphic to the domain*

$$k[[x, y, z]]/(z^p - a^{p-1} b^{p-1} z - a^p y + b^p x).$$

Conversely, for any system of parameters $a, b \in k[[x, y]]$, the above ring is the ring of invariants of a moderately ramified G-action on some complete regular local noetherian ring A of dimension two.

Proof The first part of the statement follows immediately from Corollary 7.5. For the converse, we use the ring $A := k[[x, y]][u, v]/(u^p - a^{p-1} u - x, v^p - b^{p-1} v - y)$ and apply Theorem 6.19 to find that A is regular. □

Remark 7.8 When $p = 2$ and $n = 2$, we noted in Proposition 6.20 that every action ramified precisely at the origin is in fact already moderately ramified when k has no separable quadratic extensions. Putting this result together with Theorem 7.7, we recover Artin's description in [4] of the ring A^G when $n = 2$, $p = 2$, and k has no separable quadratic extensions. Note that this hypothesis on k does not appear in Artin's description in [4], and we have not been able to provide a proof of this description without such hypothesis on k.

Remark 7.9 Let A be a complete local regular noetherian ring of dimension two and characteristic $p > 0$, with field of representatives k. Assume that A is endowed with a moderately ramified action of a cyclic group G of order p, and consider the ring A^G as described in Theorem 7.7. Let I denote the ideal of A^G generated by x and y. Then $I \neq IA \cap A^G$. Indeed, the element $z \in A^G$ does not belong to I since A^G/I is isomorphic to $k[z]/(z^p)$. On the other hand, since $(a, b) \subseteq I$ and $z = av - bu$, we find that $z \in IA \cap A^G$. This example generalizes Example 2 in [17]. Note that it follows that A^G is not a direct summand of the A^G-module A (see [23, Proposition 1], or [24, Proposition 10]).

Remark 7.10 Axioms (MR 1) and (MR 2) in the definition of moderately ramified action specify the existence of a regular system of parameters $u_1, \ldots, u_n$ in the complete regular local ring A such that the associated norm subring $R := k[[x_1, \ldots, x_n]]$ is such that $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ is a Galois extension of degree p^n with elementary abelian Galois group (see Proposition 6.3). In particular, any moderately ramified action $\sigma : A \to A$ comes equipped with a subgroup of $\mathrm{Aut}_k(A)$ isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$. We note below that when $p = 2 = n$, much more is true.

Assume that $n = p = 2$ and that k is algebraically closed. Let $\sigma : A \to A$ be a moderately ramified action. Consider a regular system of parameters u, v such that $A = k[[u, v]]$, $R := k[[x, y]]$ is the norm subring, and $a, b \in k[[x, y]]$ are such that $\sigma(u) = u + a$ and

$\sigma(v) = v + b$. Clearly, there are then two non-trivial involutions in $\mathrm{Aut}_k(A)$ which commute with σ, namely the involution which fixes v and sends u to $u + a$, and the involution which fixes u and sends v to $v + b$. We show below that in fact, *the centralizer of* $\langle\sigma\rangle$ *in the group* $\mathrm{Aut}_k(A)$ *contains infinitely many non-trivial involutions.*

For each $c \in k^*$, consider the regular system of parameters $u + cv$, v, with norms X and $Y = y$ with respect to σ, where

$$X := (u + cv)(\sigma(u) + c\sigma(v)) = x + c^2 y + c(u\sigma(v) + v\sigma(u)).$$

For the regular system of parameters $u + cv$, v, the norm subring is $k[[X, Y]]$. Since u, v is an admissible regular system of parameters (Definition 2.2) and $a, b \in (u, v)^2$, one checks that $u + cv$, v, is also an admissible regular system of parameters, so the homomorphism $k[[X, Y]] \to A$ has degree 4. Theorem 3.4 (i) shows that the field extension $\mathrm{Frac}(A^G)/k((X, Y))$, which has degree $p^{n-1} = 2$, is not purely inseparable. Hence it must be Galois. Since k is algebraically closed, Theorem 3.4 (ii) implies that the extension $\mathrm{Frac}(A)/k((X, Y))$ must be Galois as well. We find that $k[[x, y]] = k[[X, Y]]$ if and only if $(u\sigma(v) + v\sigma(u)) \in k[[x, y]]$. In our case, we can compute explicitly that $u\sigma(v) + v\sigma(u) = av + bu$, which is nothing but the minor element $z = z_{12}$ generating A^G over $k[[x, y]]$. Hence, the extension $\mathrm{Frac}(A)/\mathrm{Frac}(R)$ and $\mathrm{Frac}(A)/k((X, Y))$ are distinct, and thus correspond to two distinct elementary abelian subgroups H_0 and H_c in $\mathrm{Aut}_k(A)$ of order 4, intersecting in $\langle\sigma\rangle$. It is not hard to check that the groups H_c, $c \in k$, are pairwise distinct.

7.11 Let A_{ci} denote the R-subalgebra of A^G generated by the $n - 1$ minor elements $z_{12}, \ldots, z_{1n}$. We show in Theorem 7.14 that this subring is a complete intersection which gives us a useful approximation of A^G. Call the R-subalgebra generated by all minor elements z_{ij}, $1 \le i < j \le n$, the *minor subring* A_{mnr} of A^G. This subring captures the regular locus of $\mathrm{Spec}(A^G)$ (Corollary 7.15).

For the definition of the ring homomorphism below, regard z_{ij} as an indeterminate, and set $r_{ij} := z_{ij}^p - (\mu a_i a_j)^{p-1} z_{ij} - a_i^p x_j + a_j^p x_i$, viewed as an element of the polynomial ring $R[z_{ij}]$. Set $B := R[z_{12}, \ldots, z_{1n}]/(r_{12}, \ldots, r_{1n})$. Then we have a natural homomorphism of R-algebras:

$$B = R[z_{12}, \ldots, z_{1n}]/(r_{12}, \ldots, r_{1n}) \longrightarrow A, \tag{7.12}$$

whose image is A_{ci}. We show in Theorem 7.14 that the homomorphism $B \to A_{\mathrm{ci}}$ is an isomorphism.

Lemma 7.13 *The ring B is a complete intersection, free of rank p^{n-1} over R. The ring $B[1/(\mu a_1)]$ is normal.*

Proof Consider the natural isomorphism

$$\bigotimes_{j=2}^{n} R[z_{1j}]/(r_{1j}) \longrightarrow B := R[z_{12}, \ldots, z_{1n}]/(r_{12}, \ldots, r_{1n})$$

Since the polynomial rings $R[z_{1j}]$ are domains and each r_{1j} is non-zero, each tensor factor on the left and, hence, also B, is a complete intersection [37, Theorem 2]. Each tensor factor is free of rank p over R, so B is free of rank p^{n-1} over R.

Consider now the fibers of the map $\mathrm{Spec}(R[z_{1j}]/(r_{1j})) \to \mathrm{Spec}(R)$. The Jacobian Criterion tells us that the fibers over points outside of the closed subset $V(\mu a_1 a_j)$ are etale. Theorem 7.2 shows that $\mathrm{Spec}(R[z_{1j}]/(r_{1j}))$ is regular in codimension 1. Let $\mathfrak{q}$ be a prime

ideal of height 1 in B that does not contain μa_1. Then $\mathfrak{q}$ can contain at most one a_j with $j \neq 1$. When $\mathfrak{q}$ does not contain any a_j, $j \neq 1$, the map $\operatorname{Spec} B \to \operatorname{Spec} R$ is etale at $\mathfrak{q}$, and thus $B_{\mathfrak{q}}$ is regular. When $\mathfrak{q}$ contains a_j for some $j \neq 1$, let B_j denote the natural subring of B isomorphic to $R[z_{1j}]/(r_{1j})$. The map $\operatorname{Spec} B \to \operatorname{Spec} B_j$ is etale at $\mathfrak{q}$, and thus $B_{\mathfrak{q}}$ is regular since B_j is regular in codimension 1. We conclude that $B[1/(\mu a_1)]$ is regular in codimension 1. Since B is a complete intersection, it is Cohen–Macaulay and, hence, satisfies Condition S_2. It follows that $B[1/(\mu a_1)]$ is normal. □

Theorem 7.14 *The homomorphism $B \to A_{\mathrm{ci}}$ induced by (7.12) is an isomorphism. The ring A_{ci} is a complete intersection domain, with $A_{\mathrm{ci}}[1/(\mu a_1)] = A^G[1/(\mu a_1)]$. When $n = 2$, $A_{\mathrm{ci}} = A^G$. When $n \geq 3$, the ring A_{ci} is not regular in codimension one, and $A_{\mathrm{ci}} \neq A^G$.*

Proof Let us show first that the morphism $B \to A$ is injective. For this, let $B_{ij} := R[z_{ij}]/(r_{ij})$. We will show that both natural maps

$$B_{12} \otimes_R \cdots \otimes_R B_{1n} \longrightarrow \operatorname{Frac}(B_{12}) \otimes_{\operatorname{Frac}(R)} \cdots \otimes_{\operatorname{Frac}(R)} \operatorname{Frac}(B_{1n})$$

and

$$\operatorname{Frac}(B_{12}) \otimes_{\operatorname{Frac}(R)} \cdots \otimes_{\operatorname{Frac}(R)} \operatorname{Frac}(B_{1n}) \longrightarrow \operatorname{Frac}(A)$$

are injective. The first map is injective because each B_{1j} is free (and thus flat) over R. To show that the second map is injective, we consider its source and target as finitely generated vector spaces over $\operatorname{Frac}(R)$. We find that the dimension of the source is p^{n-1}, and that the image is the smallest subfield of $\operatorname{Frac}(A)$ generated by $\operatorname{Frac}(R)$ and $z_{12}, \ldots, z_{1n}$. It is easy to check that this subfield has dimension p^{n-1}, since $H_{12} \cap \cdots \cap H_{1n} = \langle \sigma \rangle$.

Since A is a domain and $B \to A$ is injective, we find that B is a domain. The injection $B \subset A^G$ induces a bijection on field of fractions. As A^G and $B[1/\mu a_1]$ are both normal (Lemma 7.13), we find that the inclusion $B[1/\mu a_1] \to A^G[1/\mu a_1]$ is an isomorphism.

The case $n = 2$ is treated in Theorem 7.2. To prove the last statement in Theorem 7.14, suppose that $n \geq 3$. Then Proposition 3.2 shows that A^G is not Cohen–Macaulay. Being a complete intersection, the ring B is Cohen–Macaulay. If B were regular in codimension one, then it would be normal since it is S_2, and the inclusion $B \subset A^G$ would be an equality, a contradiction. □

Corollary 7.15 *The morphism of schemes $\operatorname{Spec}(A^G) \to \operatorname{Spec}(A_{\mathrm{mnr}})$ is an isomorphism outside the closed points.*

Proof By definition, we have $A_{\mathrm{ci}} \subset A_{\mathrm{mnr}} \subset A$. Using Theorem 7.14, we infer that A_{mnr} becomes normal after inverting a_1. But it also contains the other complete intersection subrings, defined with $z_{i1}, \ldots, \widehat{z_{ii}}, \ldots, z_{in}$ for $1 \leq i \leq n$. Whence A_{mnr} becomes normal after inverting any of the a_i. Since $a_1, \ldots, a_n \in R$ is a system of parameters, we conclude that the localizations $(A_{\mathrm{mnr}})_{\mathfrak{p}}$ are normal for any non-maximal prime ideal $\mathfrak{p}$. It follows that $\operatorname{Spec}(A^G) \to \operatorname{Spec}(A_{\mathrm{mnr}})$ is an isomorphism outside the closed points. □

8 The invariant ring in higher dimension

Let k be a ground field of characteristic $p > 0$, and consider the polynomial ring in $2n$ variables

$$B := k[u_1, \ldots, u_n, a_1, \ldots, a_n],$$

endowed with the action of the cyclic group G of order p given by identifying a generator of G with the k-linear automorphism σ of order p defined by

$$u_i \longmapsto u_i + a_i \quad \text{and} \quad a_i \longmapsto a_i, \quad 1 \le i \le n.$$

The subring B^G of B is an object extensively studied in modular representation theory. In this section, we review some known results on the structure of B^G in Proposition 8.1, and use them to obtain information on the invariant subring A^G for certain moderately ramified group actions on complete local rings A obtained as quotients of the completion $\widehat{B}$ of B at $(u_1, \ldots, u_n, a_1, \ldots, a_n)$. We also provide in Example 8.6 an example where the integral closure of a Cohen–Macaulay local ring R in a Galois extension $L/\operatorname{Frac}(R)$ generated by a generalized reflection of prime order p is not Cohen–Macaulay (see Remark 6.6 for a related example).

Generators for the invariant ring B^G have been determined. As in the previous section, the norm elements and the minor elements

$$\begin{aligned} x_i &:= N_{B/B^G}(u_i) = u_i^p - a_i^{p-1}u_i, \quad 1 \le i \le n, \\ z_{ij} &:= a_i u_j - a_j u_i, \quad 1 \le i < j \le n \end{aligned}$$

are clearly G-invariant. Additional natural G-invariant elements are the traces

$$t_\epsilon := \operatorname{Tr}_{B/B^G}(u_1^{\epsilon_1} \cdot \cdots \cdot u_n^{\epsilon_n}) = \sum_{\nu=0}^{p-1} \left(\prod_{i=1}^{n} (u_i + \nu a_i)^{\epsilon_i} \right),$$

where $\epsilon = (\epsilon_1, \ldots, \epsilon_n) \in \mathbb{N}^n$. For the purpose of generating B^G, we recall below that it suffices to consider only the n-tuples $(\epsilon_1, \ldots, \epsilon_n)$ subject to the conditions

$$0 \le \epsilon_i \le p-1 \quad \text{and} \quad \sum_{i=1}^{n} \epsilon_i > 2p-2.$$

Let us call such a tuple *relevant*. Note that there are no relevant tuples when $n = 2$. When $n = 3$ and $p = 2$, there is only one relevant tuple, namely $\epsilon = (1, 1, 1)$. The element $t_\epsilon \in B^G$ attached to a relevant tuple ϵ is called *trace element*.

Write $\widehat{B}$ for the formal completion of the polynomial ring B with respect to the maximal ideal $\mathfrak{m} = (u_1, \ldots, u_n, a_1, \ldots, a_n)$. Then $\widehat{B}^G$ coincides with the formal completion of B^G with respect to $\mathfrak{m} \cap B^G$. Recall that the *embedding dimension* of a local noetherian ring C is the vector space dimension of the *cotangent space* $\mathfrak{m}_C/\mathfrak{m}_C^2$ over the residue field $\kappa = C/\mathfrak{m}_C$.

Proposition 8.1 *The ring B^G is generated as a k-algebra by the indeterminates a_i, the norm elements x_i, the minor elements z_{ij}, and the trace elements t_ϵ. These elements yield a basis for the cotangent space $\mathfrak{m}_{\widehat{B}^G}/\mathfrak{m}_{\widehat{B}^G}^2$, which has dimension*

$$\operatorname{edim}(\widehat{B}^G) = 2n + \binom{n}{2} + p^n - \binom{2p+n-2}{n} + n\binom{p+n-2}{n}. \tag{8.2}$$

Furthermore, the ring $\widehat{B}^G$ has depth $n+2$.

Proof First note that the grading on the polynomial ring B induces a grading on the ring of invariants $B^G \subset B$. According to [27, Proposition 2.1, together with Lemma 2.2], these gradings ensure that the minimal number of generators for the k-algebra B^G coincides with $\operatorname{edim}(\widehat{B}^G)$.

Richman conjectured that the indeterminates together with the norms, minors and traces generate the ring of invariants [50, page 32]. This was established in full generality by Campbell and Hughes [13]. Later, Shank and Wehlau showed that the elements form a minimal set of generators, if one discards the non-relevant traces [60, Corollary 4.4]. In turn, these yield a basis for the cotangent space $\mathfrak{m}_{\widehat{B}^G}/\mathfrak{m}^2_{\widehat{B}^G}$.

The indeterminates a_i, together with the norm elements x_i and minor elements z_{ij} contribute $2n+\binom{n}{2}$ members of the basis. It remains to count the number of monomials $u_1^{\epsilon_1}\dots u_n^{\epsilon_n}$ corresponding to relevant tuples $\epsilon \in \mathbb{N}^n$. There are p^n monomials that have degree $\leq p-1$ in each variable, and there are $\sum_{d=0}^{2p-2}\binom{d+n-1}{n-1} = \binom{2p+n-2}{n}$ monomials with total degree $\leq 2p-2$. Among the latter one sees that there are $\sum_{d=0}^{p-2}\binom{d+n-1}{n-1} = \binom{p+n-2}{n}$ excess monomials that have degree $\geq p$ in a fixed variable u_i. Our formula for $\operatorname{edim}(\widehat{B}^G)$ follows.

The statement about the depth of the local ring of B^G at the origin is proved by Ellingsrud and Skjelbred [15, Theorem 3.1], under the assumption that the ground field k is algebraically closed. In the notation of their result, we interpret F_{-1} to be the empty set, and note that F_0 is the closed set $V(a_1,\dots,a_n)$ in $\operatorname{Spec} B$, which as dimension n. Since depths are invariant under ground field extensions and formal completions, the formula holds in general. □

Recall that x_i denote the norm from B to B^G of the element u_i. We now write $\widehat{B} = k[[u_1,\dots,u_n,a_1,\dots,a_n]]$ and identify the norm of u_i from $\widehat{B}$ to $\widehat{B}^G$ with x_i. Thus, $\widehat{B}$ contains $R := k[[x_1,\dots,x_n]]$ as subring. Choose $\alpha_1,\dots,\alpha_n \in \mathfrak{m}_R$, and consider the elements

$$b_i := a_i - \alpha_i \in \widehat{B}.$$

Since $(u_1,\dots,u_n,a_1,\dots,a_n) = (u_1,\dots,u_n,b_1,\dots,b_n)$ we conclude that the $b_1,\dots,b_n$ are part of a regular system of parameters of $\widehat{B}$ (use [40, 17.4]). Let $\mathfrak{b}$ denote the ideal of $\widehat{B}$ generated by $b_1,\dots,b_n$. It follows from the equality of ideals just mentioned that the ring $A := \widehat{B}/\mathfrak{b}$ is regular of dimension n, with maximal ideal generated by the classes of $u_1,\dots,u_n$. Clearly, $b_i \in \widehat{B}^G$. The ring $A = \widehat{B}/\mathfrak{b}$ has thus an induced action of G.

Lemma 8.3 *The ring A is isomorphic to the ring $k[[x_1,\dots,x_n]][u_1,\dots,u_n]/I$, where the ideal I is generated by $u_i^p - \alpha_i^{p-1}u_i - x_i$ for $1 \leq i \leq n$. When $\alpha_1,\dots,\alpha_n$ is a system of parameters in R, then the G-action on A is moderately ramified.*

Proof Follows from the Implicit Function Theorem, the definition of a moderately ramified action and Theorem 6.19. □

The elements $b_1,\dots,b_n$ are G-invariant, so they define ideals in both $\widehat{B}^G$ and $\widehat{B}$. We have a natural homomorphism

$$\varphi : \widehat{B}^G/(b_1,\dots,b_n)\widehat{B}^G \longrightarrow (\widehat{B}/(b_1,\dots,b_n)\widehat{B})^G = A^G.$$

Under suitable assumptions, this map is bijective, as we now show.

Proposition 8.4 *Keep the above notation and assumptions. Assume that $b_1,\dots,b_n$ is a regular sequence in $\widehat{B}^G$, and that at least one $\alpha_i \in \mathfrak{m}_R$ is non-zero. Then the following holds.*

(i) *The map $\varphi : \widehat{B}^G/(b_1,\dots,b_n)\widehat{B}^G \to A^G$ is an isomorphism.*
(ii) *We have* $\operatorname{edim}(A^G) = n + \binom{n}{2} + p^n - \binom{n+2p-2}{n} + n\binom{n+p-2}{n}$.

Proof (i) The ring $\widehat{B}^G$ has dimension $2n$ and, according to Proposition 8.1, it has depth $n+2$. Hence, the quotient ring $\widehat{B}^G/(b_1,\dots,b_n)$ acquires dimension n and depth 2. Since the ring

extension $B^G \subset B$ is finite, the induced map on affine schemes $\mathrm{Spec}(B) \to \mathrm{Spec}(B^G)$ is surjective. This continues to hold for

$$\mathrm{Spec}(\widehat{B}/(b_1, \ldots, b_n)) \longrightarrow \mathrm{Spec}(\widehat{B}^G/(b_1, \ldots, b_n)).$$

The scheme on the left is irreducible, whence the same holds for the scheme on the right. Now consider the exact sequence

$$0 \longrightarrow N \longrightarrow \widehat{B}^G/(b_1, \ldots, b_n) \xrightarrow{\varphi} A^G \longrightarrow F \longrightarrow 0$$

defining the kernel N and cokernel F for our map in question. Clearly, the image of φ contains the norm and minor elements, thus the cokernel F has finite length, by Corollary 7.15. Moreover, its kernel N contains only nilpotent elements, because $\widehat{B}^G/(b_1, \ldots, b_n)$ is n-dimensional with only one minimal prime ideal. We conclude that N equals this minimal prime ideal. If we could show that $N = 0$, then the morphism of schemes

$$\mathrm{Spec}(A^G) \longrightarrow \mathrm{Spec}(\widehat{B}/(b_1, \ldots, b_n))$$

is an isomorphism outside the closed points. Since $\widehat{B}/(b_1, \ldots, b_n)$ has depth 2, this ring must be normal, and the map φ is bijective by Zariski's Main Theorem.

To see that $N = 0$, we regard the ring of invariants B^G as a finite algebra over the polynomial ring $k[x_1, \ldots, x_n, a_1, \ldots, a_n]$ generated by the norms x_i and the variables a_i. The scheme $\mathrm{Spec}(B^G)$ is regular outside the image of the fixed scheme in $\mathrm{Spec}(B)$, the latter being defined by the ideal generated by $a_1, \ldots, a_n$. It follows that

$$\mathrm{Spec}(B^G) \to \mathbb{A}^{2n} = \mathrm{Spec}(k[x_1, \ldots, x_n, a_1, \ldots, a_n])$$

is finite and flat, of degree p^{n-1}, at least over the complement of the subscheme defined by a_i, $1 \leq i \leq n$. The subscheme defined by $b_i = a_i - \alpha_i$, $1 \leq i \leq n$ is not contained in this, because some α_i is non-zero, and it follows that $\widehat{B}^G/(b_1, \ldots, b_n)$ has degree p^{n-1} as module over

$$R = k[[x_1, \ldots, x_n]] = k[[x_1, \ldots, x_n, a_1, \ldots, a_n]]/(b_1, \ldots, b_n).$$

The same holds for A^G. Tensoring with the fraction field of R, we deduce that $N \otimes_R \mathrm{Frac}(R) = 0$ by counting vector space dimensions. Since $\widehat{B}^G/(b_1, \ldots, b_n)$ has no embedded components, this already ensures $N = 0$.

(ii) In light of (i), we merely have to check that the $b_i = a_i - \alpha_i$, $1 \leq i \leq n$ are linearly independent in the cotangent space of B^G. This indeed holds, because the $x_i = u_i^p - a_i u_i$ vanish and the a_i are linearly independent in the cotangent space of the ring B. □

In dimension $n = 3$, we obtain the following unconditional result when the formal power series $\alpha_1, \alpha_2, \alpha_3$, are polynomials.

Theorem 8.5 *Let $n = 3$. Choose polynomials $\alpha_i = \alpha_i(x_1, x_2, x_3) \in k[x_1, x_2, x_3]$, $i = 1, 2, 3$, such that $\alpha_1, \alpha_2, \alpha_3$ form a system of parameters in $R = k[[x_1, x_2, x_3]]$. Then the induced G-action on $A := \widehat{B}/\mathfrak{b}$ is moderately ramified and the natural homomorphism $\widehat{B}^G/(b_1, b_2, b_3) \to A^G$ is bijective. In particular, A^G is generated as a complete local k-algebra by the norm elements x_1, x_2, x_3, the minor elements z_{12}, z_{13}, z_{23} and the $(p^3 - p)/6$ trace elements $t_\epsilon \in A^G$. Moreover, we have* $\mathrm{edim}(A^G) = 6 + (p^3 - p)/6$.

Proof In view of Proposition 8.4, we start by proving that $b_1, b_2, b_3 \in B^G$ form a regular sequence. Using the case $r = 1$ of Theorem 1.4 in [26], we have to check that the map

$$B \longrightarrow B^{\oplus 3}, \quad x \longmapsto (b_1 x, b_2 x, b_3 x)$$

induces an injective map $H^1(G, B) \to H^1(G, B^{\oplus 3})$ on group cohomology. Using the decomposition $H^1(G, B^{\oplus 3}) = H^1(G, B)^{\oplus 3}$ and symmetry, is suffices to verify that the map $b_3 : H^1(G, B) \to H^1(G, B)$ is injective.

Let $B^\flat \subset B$ be the $k[a_1, a_2, a_3]$-submodule generated by all monomials $u_1^{n_1} u_2^{n_2} u_3^{n_3}$ with exponents $n_1, n_2, n_3 \leq p-1$. Clearly, $B^\flat \subset B$ is G-invariant. According to [60, Proposition 6.2], the canonical map

$$k[x_1, x_2, x_3] \otimes_k H^1(G, B^\flat) \longrightarrow H^1(G, B)$$

is bijective (in loc. cit. the symbols $k[W]^\flat$ are defined at the end of Section 2 on page 310, and the symbol B is defined on page 318 before Lemma 6.1). Multiplication by the element $b_3 = a_3 - \alpha_3(x_1, x_2, x_3)$ on the right corresponds to the k-linear mapping $f = \mathrm{id} \otimes a_3 - \alpha_3(x_1, x_2, x_3) \otimes \mathrm{id}$ on the left. Let $\mathrm{Fil}_i \subset k[x_1, x_2, x_3]$ by the vector subspace of all polynomials of total degree $\leq i$. This is an ascending filtration that is exhaustive and discrete, in the sense that $\bigcup_i \mathrm{Fil}^i = k[x_1, x_2, x_3]$ and $\mathrm{Fil}_i = 0$ for $i = -1$. By abuse of notation we denote the induced filtration $\mathrm{Fil}^i \subset k[x_1, x_2, x_3] \otimes_k H^1(G, B^\flat)$ by the same symbol. Clearly, $f(\mathrm{Fil}^i) \subset \mathrm{Fil}^{i+d}$, where $d \geq 1$ is the total degree of $\alpha_3(x_1, x_2, x_3)$. Moreover, the induced map $f : \mathrm{Gr}^i \to \mathrm{Gr}^{i+d}$ on the associated graded coincides with the multiplication by $\alpha_3(x_1, x_2, x_3) \otimes \mathrm{id}$, and the latter is injective because $\alpha_3 \in k[x_1, x_2, x_3]$ is a regular element. It follows that our original multiplication map $b_3 : H^1(G, B) \to H^1(G, B)$ is injective (compare for example [61, Lemma 1 (e)]). This shows that $b_1, b_2, b_3 \in B^G$ form a regular sequence. In turn, they form a regular sequence in the flat extension $\widehat{B}^G$.

Now it follows from Proposition 8.4 that the map $\widehat{B}^G/(b_1, b_2, b_3)\widehat{B}^G \to A^G$ is bijective, with indicated embedding dimension. The generators of $\widehat{B}^G$ are given in Proposition 8.1. According to Lemma 8.3, the ring $A := \widehat{B}/\mathfrak{b}$ equals

$$k[[x_1, x_2, x_3, u_1, u_2, u_3]]/(u_1^p - \alpha_1^{p-1} u_1 - x_1, u_2^p - \alpha_2^{p-1} u_2 - x_2, u_3^p - \alpha_3^{p-1} u_3 - x_3),$$

and the G-action given by $u_i \mapsto u_i + \alpha_i$ is moderately ramified. □

Example 8.6 Let A denote a complete noetherian regular local ring of dimension n and characteristic $p > 0$, endowed with a moderately ramified action of a cyclic group G of order p. *Then the ring A^G is endowed with a group of automorphisms of order p^{n-1} generated by generalized reflections of order p.* Indeed, A is endowed with an elementary abelian group of automorphisms H, and by construction, H/G acts on A^G. In the presentation of A given in Theorem 6.11, we find that the ideal $I(\sigma_i)$ of the fixed scheme of the pseudo-reflection $\sigma_i : A \to A$ is $a_i A$. Thus the image $\overline{\sigma}_i : A^G \to A^G$ of σ_i in H/G has an ideal $I(\overline{\sigma}_i)$ contained in $a_i A^G$ (since $a_i \in A^G$). In particular, $\overline{\sigma}_i$ is a generalized reflection of order p. We note in the example below that the ideal $I(\overline{\sigma}_i)$ is not principal in general.

Consider the case where $n = 3$. In this case, A^G is not Cohen–Macaulay (use Proposition 3.2 (i)), and Theorem 8.5 gives us a set of generators that we can use to obtain information about the ideal $I(\overline{\sigma}_1)$. We find that $\overline{\sigma}_1(z_{12}) - z_{12} = -a_1 a_2$ and $\overline{\sigma}_1(z_{13}) - z_{13} = -a_1 a_3$, so that $(a_1 a_2, a_1 a_3) \subseteq I(\overline{\sigma}_1)$. From the relation $z_{23}^p - (a_2 a_3)^{p-1} z_{23} - a_2^p x_3 + a_3^p x_2$, we find that $a_1 z_{23}^p \in (a_1 a_2, a_1 a_3)$. Note now that $I(\sigma_2 \sigma_3) = (a_2, a_3)A$. Since $\overline{\sigma}_1 = (\overline{\sigma}_2 \overline{\sigma}_3)^{-1}$, we find that $I(\overline{\sigma}_1) \subseteq (a_1)A \cap (a_2, a_3)A \cap A^G$ (with $(a_2, a_3)A \cap A^G \supseteq (a_2, a_3, z_{23})A^G$).

Assume now that in addition $p = 2$. By considering the last generator of A^G found in Theorem 8.5, namely $t := u_1 u_2 u_3 + \sigma(u_1 u_2 u_3)$, we find that $\overline{\sigma}_1(t) - t = a_1 z_{23} + a_1 a_2 a_3$. Thus in this case $I(\overline{\sigma}_1) = (a_1)(a_2, a_3, z_{23})$, which shows that $I(\overline{\sigma}_1)$ is not principal.

We note that Theorem 7.2 shows that the invariant ring $(A^G)^{\langle \overline{\sigma}_1 \rangle}$ is a complete intersection and, thus, is Cohen–Macaulay. Consider a Cohen–Macaulay local ring R and a Galois extension $L/\mathrm{Frac}(R)$ of prime order. Let B denote the integral closure of R in L. When the Galois

group of $L/\mathrm{Frac}(R)$ is generated by a generalized reflection $\sigma : B \to B$, one may wonder whether B is always Cohen–Macaulay. This question is given a partial positive answer when the order of σ is coprime to the residue characteristic of R in [24, Proposition 15]. The above example with $(A^G)^{\langle\overline{\sigma}_1\rangle} \subset A^G$ shows that the answer to this question is negative in general. We note however that $(A^G)^{\langle\overline{\sigma}_1\rangle}$ is Gorenstein, and that A^G is shown in Theorem 9.6 to be quasi-Gorenstein.

9 Class group and canonical class

Let A be a complete local noetherian ring that is regular of dimension $n \geq 2$ and characteristic $p > 0$, with a field of representatives k, and endowed with an action of a cyclic group G of order p that is ramified precisely at the origin. Let A^G be the ring of invariants, and denote by $\mathrm{Cl}(A^G)$ its *class group* of Weil divisors modulo linear equivalence. Since A^G is normal, the group $\mathrm{Cl}(A^G)$ is trivial if and only if A^G is factorial.

The canonical module K_{A^G} of A^G is reflexive of rank one. Since $\mathrm{Cl}(A^G)$ is naturally isomorphic to the rank one reflexive class group, we obtain using this isomorphism a canonical class $[K_{A^G}] \in \mathrm{Cl}(A^G)$. The main result of this section, Theorem 9.6, states that the canonical class $[K_{A^G}]$ is trivial when the G-action is moderately ramified.

Let us start with a description of the group $\mathrm{Cl}(A^G)$, which follows from a result of Waterhouse [66], generalizing work of Samuel [55, Théorème (1)].

Proposition 9.1 *Let A be as above, endowed with a G-action ramified precisely at the origin. Let U_1 denote the kernel of the map $A^* \to k^*$. Then $\mathrm{Cl}(A^G)$ is isomorphic to $H^1(G, A^*)$, and there is a short exact sequence*

$$0 \longrightarrow U_1^G/(U_1^G)^p \longrightarrow (U_1/U_1^p)^G \longrightarrow \mathrm{Cl}(A^G) \longrightarrow 0.$$

Proof That $\mathrm{Cl}(A^G)$ is isomorphic to $H^1(G, A^*)$ follows from [66, Corollary 1, page 545], applied to the Galois extension $\mathrm{Frac}(A)/\mathrm{Frac}(A^G)$ of degree p with Galois group G. Indeed, it is clear that A is the integral closure of A^G in $\mathrm{Frac}(A)$, and that every minimal prime of A^G (and by this, [66] means the primes in A^G of height 1, see proof of Theorem 1) are unramified in A, since we assume that the G-action is ramified precisely at the origin. The definition of $\mathcal{P}(A^G, A)$ as the kernel of the natural map $\mathrm{Cl}(A^G) \to \mathrm{Cl}(A)$ is given in the abstract of the paper, and we find that since A is regular and, hence, factorial, $\mathcal{P}(A^G, A) = \mathrm{Cl}(A^G)$.

Recall that the G-action is k-linear. Hence $1 \to U_1 \to A^* \to k^* \to 1$ is an exact sequence of G-modules, and induces an exact sequence

$$1 \longrightarrow H^1(G, U_1) \longrightarrow H^1(G, A^*) \longrightarrow H^1(G, k^*).$$

Since the action on k^* is trivial, $H^1(G, k^*) = \mathrm{Hom}(G, k^*) = (0)$. It follows that $H^1(G, U_1) \to H^1(G, A^*)$ is bijective. The short exact sequence $(1) \to U_1 \xrightarrow{p} U_1 \to U_1/U_1^p \to (1)$ of G-modules gives an exact sequence

$$H^0(G, U_1) \xrightarrow{p} H^0(G, U_1) \longrightarrow H^0(G, (U_1/U_1^p)) \longrightarrow H^1(G, U_1) \xrightarrow{p} H^1(G, U_1).$$

The map on the right is the trivial map, because the cohomology group $H^1(G, U_1)$ is annihilated by $\mathrm{ord}(G) = p$. The assertion follows. □

The group $\mathrm{Cl}(A^G)$ is expected to be frequently non-trivial. When $n = 2$, this expectation is implied by Theorem 25.1 in [32]. A direct proof that $\mathrm{Cl}(A^G)$ is not trivial for certain

moderately ramified actions is presented in our next lemma. When $n > 2$, examples of non-Cohen–Macaulay unique factorization domains are known (see [33, section 4], for a survey on this matter, and [43]). In the context of ring of invariants for an action of $G := \mathbb{Z}/p\mathbb{Z}$ on $A := k[[x_1, \ldots, x_n]]$, Theorem 1.3 in [7] exhibits examples of complete local rings A^G with $n \leq p$ which are not unique factorization domains.

Let $n = 3$. Choose polynomials $\alpha_1, \alpha_2 \in k[x_1, x_2]$, and $\alpha_3 \in k[x_1, x_2, x_3]$ such that $\alpha_1, \alpha_2, \alpha_3$ form a system of parameters in $R = k[[x_1, x_2, x_3]]$. Consider the associated action of G on $A := k[[u_1, u_2, u_3]]$ as in Theorem 8.5. We obtain from Theorem 8.5 a description of a minimal set of generators $x_1, x_2, x_3, w_1, \ldots, w_s$ for A^G, which includes the minor element $z_{12} := \alpha_1 u_2 - \alpha_2 u_1$. Write $A^G = k[[x_1, x_2, x_3, w_1, \ldots, w_s]]/I$, where I is the ideal of relations between the generators of A^G. Since we are considering a minimal set of generators, we find that $I \subset J^2$, where $J = (x_1, x_2, x_3, w_1, \ldots, w_s)$. Recall (7.6) that z_{12} satisfies the relation

$$z_{12}^p - (\alpha_1\alpha_2)^{p-1} z_{12} - \alpha_1^p x_2 + \alpha_2^p x_1 = 0.$$

Lemma 9.2 *Keep the above notation. Suppose that $\alpha_1^p x_2 - \alpha_2^p x_1$ can be factored in $k[[x_1, x_2]]$ into a product of at least $p + 1$ non-units. Then the ring A^G is not factorial.*

Proof In the ring A^G, we have a factorization

$$\alpha_1^p x_2 - \alpha_2^p x_1 = \prod_{i \in \mathbb{F}_p} (z_{12} - i\alpha_1\alpha_2). \tag{9.3}$$

We claim that each factor $z_{12} - i\alpha_1\alpha_2$ is irreducible in A^G. Indeed, if $z_{12} - i\alpha_1\alpha_2$ is reducible, there exists power series $f, g, h \in k[[x_1, x_2, x_3, w_1, \ldots, w_s]]$ such that

$$z_{12} - i\alpha_1\alpha_2 = fg + h,$$

with $f, g \in J$ and $h \in I \subseteq J^2$, since the images of $x_1, x_2, x_3, w_1, \ldots, w_s$ form a minimal system of generators. It follows from this expression for z_{12} that $z_{12} \in J^2$, which is a contradiction.

Now assume that A^G is factorial. Then the elements $z_{12} - i\alpha_1\alpha_2 \in A^G$, $i \in \mathbb{F}_p$, are prime elements, and the existence and uniqueness of prime factorization shows that $\alpha_1^p x_2 - \alpha_2^p x_1$ does not factor into more than p non-units. □

It is easy to produce examples of elements $a, b \in k[[x, y]]$ such that $a^p y - b^p x$ factors into a product of $p + 1$ elements. For instance, set $a = x$ and $b = y$, to obtain $a^p y - b^p x = yx^p - xy^p = xy \prod_{i \in \mathbb{F}_p^*} (x - iy)$. When k contains a primitive $p + 1$-root of unity ζ, we can take $a = y$ and $b = x$, to obtain $a^p y - b^p x = y^{p+1} - x^{p+1} = \prod_i (y - \zeta^i x)$.

We now briefly review some facts regarding canonical modules. Let S be any complete local noetherian ring of dimension n with maximal ideal $\mathfrak{m}$ and residue field $k := S/\mathfrak{m}$. Let $E_S(k)$ be the injective hull of the residue field k. If M is any S-module, let $H^i_{\mathfrak{m}}(M)$ denote the i-th local cohomology group. Then the functor

$$M \longmapsto \mathrm{Hom}_S(H^n_{\mathfrak{m}}(M), E_S(k))$$

is representable by a module K_S. This module is called the *canonical module* of S [22], or the *dualizing module* [9]. By Yoneda's Lemma, it is unique up to isomorphism. The S-module K_S is finitely generated, of dimension $\dim(K_S) = n$, and satisfies Serre's Condition (S_2).

These statements are proved for instance in [22, 5.2, and 5.16]. Note that these hold without the requirement that the ring be Cohen–Macaulay.

When S is Cohen–Macaulay, the canonical module is isomorphic to S if and only if S is Gorenstein [22, 5.9]. In particular, if $S = k[[x_1, \ldots, x_n]]$, then K_S is isomorphic to S.

9.4 Suppose that T is a complete local ring and $\phi : S \to T$ is an injective local homomorphism of local rings, such that T is finite over S. Then $K_T := \mathrm{Hom}_S(T, K_S)$ is the canonical module of T [22, 5.14].

Assume now that $P \in \mathrm{Spec}\, S$ is such that $\dim S = \dim S/P + \mathrm{height}(P)$. Then K_{S_P} is isomorphic to $(K_S)_P$ [22, 5.22]. The prime ideal P belongs to the support of K_S if and only if $\dim S = \dim S/P + \mathrm{height}(P)$ [3, 1.9]. In particular, if S is normal and P has height one, we find that S_P is regular and, thus, K_{S_P} is trivial. Hence, $(K_S)_P$ is free of rank 1 for every prime P of height one. The module K_S satisfies Serre's condition S_2 [3, 1.10].

Let M be a finitely generated S-module, and recall the functor $M \mapsto M^* := \mathrm{Hom}_S(M, S)$. The module M is called *reflexive* if the natural map $M \to (M^*)^*$ is an isomorphism. It follows from the facts in the previous paragraph and [21, Theorem 1.9], that when S is normal, then K_S is reflexive.

Recall that a prime ideal $\mathfrak{p}$ of height 1 in a normal ring S is reflexive, and that there is a natural isomorphism of groups between the class group $\mathrm{Cl}(S)$ and the rank one reflexive class group, which sends the class of $\mathfrak{p}$ to the class of $\mathfrak{p}$ [67, Theorem 1].

We return now to the ring A with a G-action as at the beginning of this section, and denote by K_{A^G} the canonical module for the complete local ring A^G. Since it follows from above that K_{A^G} is reflexive, we can consider the element

$$[K_{A^G}] \in \mathrm{Cl}(A^G),$$

called the *canonical class* of A^G.

Remark 9.5 In general, the canonical class $[K_{A^G}]$ need not be trivial. Indeed, it is possible to exhibit in dimension $n = 2$ diagonal actions on products of ordinary algebraic curves over an algebraically closed field k such that the associated quotient singularities are rational singularities [34, 4.1]. In general, these singularities are not Gorenstein since the only Gorenstein rational singularities are the double points [63, 2.5].

Our next theorem shows that when A^G is obtained from a moderately ramified action, then its canonical class is trivial.

Theorem 9.6 *Let A be a complete local regular noetherian ring of dimension $n \geq 2$, characteristic $p > 0$, and endowed with a moderately ramified action of a cyclic group G of order p. Then the canonical class $[K_{A^G}]$ is trivial in $\mathrm{Cl}(A^G)$.*

The proof of Theorem 9.6 uses some methods from non-commutative algebra and is presented after the proof of Proposition 9.11. Recall that the free A-module on the elements of G can be endowed with an associative multiplication, turning it into a ring called the *skew group ring* $A * G$. On elements of the form $a\sigma$ and $b\eta$ with $a, b \in A$ and $\sigma, \eta \in G$, the multiplication is

$$a\sigma \cdot b\eta := (a\sigma(b))(\sigma\eta),$$

and this multiplication is extended to all elements by bilinearity. Since G is abelian, the center of this associative algebra is $A^G * G$. Using the inclusion $A^G e \subset A^G * G$, where $e \in G$ is

the neutral element, we may regard the associative ring $A * G$ as an algebra over the central subring A^G, or over any subring R of A^G.

The ring A is endowed with the structure of a left $A * G$-module as follows: for $c, a \in A$ and $\sigma \in G$, let $(c\sigma)a := c\sigma(a)$. The following injective homomorphism of A^G-algebras

$$A^G \longrightarrow \mathrm{End}_{A*G}(A), \quad a \longmapsto (x \mapsto ax), \tag{9.7}$$

is easily seen to be an isomorphism. Indeed, given $\varphi : A \to A$ in $\mathrm{End}_{A*G}(A)$, we have $\varphi(\sigma \cdot 1) = \sigma(\varphi(1)) = \varphi(\sigma(1))$, so that $\varphi(1) \in A^G$. We also have $\varphi(a) = a\varphi(1)$ for all $a \in A$. We show below in Proposition 9.9 that in the case of moderately ramified actions the natural homomorphism of A^G-algebras

$$A * G \longrightarrow \mathrm{End}_{A^G}(A), \quad a\sigma \longmapsto (x \mapsto a\sigma(x)), \tag{9.8}$$

is also an isomorphism.

Let $R \subset A^G$ be a normal noetherian subring such that A^G is a finite R-algebra. Let $\mathfrak{p} \in \mathrm{Spec}\, R$. Let M be a finitely generated left $A * G$-module. Then $M_{\mathfrak{p}}$ and $(A * G)_{\mathfrak{p}}$ are well-defined $R_{\mathfrak{p}}$-modules. It turns out that $(A * G)_{\mathfrak{p}}$ is in fact an $R_{\mathfrak{p}}$-algebra when endowed with the natural multiplication $(\lambda/s) \cdot (\lambda'/s') := (\lambda\lambda')/(ss')$, where $\lambda, \lambda' \in A * G$ and $s, s' \in R\backslash\mathfrak{p}$. In addition, $M_{\mathfrak{p}}$ is a left $(A * G)_{\mathfrak{p}}$-module. Recall that the $A * G$-module M is projective if the functor $N \mapsto \mathrm{Hom}_{A*G}(M, N)$ is exact, and that homological algebra in module categories is the same over any ring, commutative or not (see for instance [54]).

Proposition 9.9 *Keep the above notation. Assume that the G-action on A is unramified in codimension one. Let $R \subset A^G$ be a normal noetherian subring such that A^G is a finite R-algebra.*

(i) *The R-modules A^G, A, $A * G$, and $\mathrm{End}_{A^G}(A)$ are reflexive.*
(ii) *The homomorphism $A * G \to \mathrm{End}_{A^G}(A)$ in (9.8) is an isomorphism.*
(iii) *For each $\mathfrak{p} \subset R$ of height one, the left $(A * G)_{\mathfrak{p}}$-module $A_{\mathfrak{p}}$ is projective.*

Proof (i) According to [21, Theorem 1.9], a finitely generated R-module $M \neq 0$ is reflexive if and only if it satisfies Serre's Condition (S_2). Since R is local, this means $\mathrm{depth}(M) \geq 2$. It follows that the reflexivity of M does not depend on the chosen subring R, as remarked in [25, page 1094]. Applying this principle to $R \subset A$, we see that the R-module A is reflexive, and it follows that $A * G$ is reflexive as well. To proceed, let $g_1, \ldots, g_r \in A^G$ be a system of module generators over R. Then we have a short exact sequence

$$0 \longrightarrow \mathrm{End}_{A^G}(A) \longrightarrow \mathrm{End}_R(A) \longrightarrow \bigoplus_{i=1}^{r} \mathrm{End}_R(A),$$

where the map on the right sends an R-linear map $f : A \to A$ to the tuple of commutators $fg_i - g_i f$. The two terms on the right are reflexive R-modules, that is, satisfy Serre's Condition (S_2). Using local cohomology, we infer that the term on the left satisfies (S_2), whence is reflexive. Analogous arguments apply to $\mathrm{End}_{A*G}(A)$.

(ii) For this, we regard $A * G$, $\mathrm{End}_{A^G}(A)$ and A^G as modules over A^G. These modules are reflexive by (i). Hence Theorem 1.12 in [21] shows that it suffices to check that the maps are bijective after localizing at each prime ideal $\mathfrak{p} \subset A^G$ of height one. So we may replace A^G by the localization $(A^G)_{\mathfrak{p}}$. By faithfully flat descent we even may replace it by the strict henselization $(A^G)_{\mathfrak{p}} \subset C$. Since the G-action is free in codimension one, we get an isomorphism $A \otimes_{A^G} C \simeq C \times G = C^p$ of C-algebras, with the permutation action of $G = \mathbb{Z}/p\mathbb{Z}$.

The first map in question takes the form $(C \times G) * G \to \mathrm{End}_C(C \times G)$. Since domain and range are free C-modules of rank p^2, it suffices to check that the map is surjective, by Nakayama's Lemma. Let $\sigma, \eta \in G$. Since matrix rings are generated by elementary matrices, it suffices to check that the endomorphism that is zero on all standard basis vectors except that $(1, \sigma) \mapsto (1, \eta)$ lies in the image. Indeed, it is the image of $(1, \eta)\sigma^{-1} \in (C \times G) * G$.

(iii) We have to show that $\mathrm{Ext}^1(A_{\mathfrak{p}}, M)$ vanishes for each module M over the ring $(A * G)_{\mathfrak{p}}$. This Ext group can be computed with injective resolutions of M, or alternatively with free resolutions of $A_{\mathfrak{p}}$. Being a finitely generated $R_{\mathfrak{p}}$-module, the associative ring $(A * G)_{\mathfrak{p}}$ is noetherian, whence we may choose a free resolution with finitely generated terms. Consequently, the formation of $\mathrm{Ext}^1(A_{\mathfrak{p}}, M)$ commutes with flat base-change in $R_{\mathfrak{p}}$. Thus we can reduce to the strict henselization $R_{\mathfrak{p}} \subset D$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset A^G$ be the prime ideals lying over $\mathfrak{p} \subset R$. Then $C = (A^G) \otimes_R D$ decomposes as $C = C_1 \times \ldots \times C_r$, where $(A^G)_{\mathfrak{p}_i} \subset C_i$ are the strict henselizations. As above, we get $A \otimes_R D = C \times G = C^p$, and $(C \times G) * G = \mathrm{End}_C(C^p)$. As a left module, C^p is a direct summand of $\mathrm{End}_C(C^p)$, whence a projective module. □

Let S be a commutative ring, and let Λ be an associative S-algebra. Then the S-module Λ carries the structure of a Λ-bimodule via $a \cdot x \cdot b := axb$, for all $a, b, x \in \Lambda$. Similarly, the dual S-module $\mathrm{Hom}_S(\Lambda, S)$ becomes a Λ-bimodule, via

$$(a \cdot \phi \cdot b)(x) := \phi(bxa),$$

for all $\phi \in \mathrm{Hom}_S(\Lambda, S)$ and $a, b, x \in \Lambda$. Any homomorphism of left Λ-modules $\Lambda \to \mathrm{Hom}_S(\Lambda, S)$ is of the form $y \longmapsto y\phi$ for some $\phi \in \mathrm{Hom}_S(\Lambda, S)$. We leave the proof of our next lemma to the reader.

Lemma 9.10 *Any homomorphism $\Lambda \to \mathrm{Hom}_S(\Lambda, S)$ of Λ-bimodules is of the form $y \mapsto y\phi$ for some element $\phi \in \mathrm{Hom}_S(\Lambda, S)$ with $\phi(xy) = \phi(yx)$ for all $x, y \in \Lambda$.*

As in [25, page 1095], the S-algebra Λ is called *symmetric* if the Λ-bimodules $\mathrm{Hom}_S(\Lambda, S)$ and Λ are isomorphic. In other words, the S-algebra Λ is symmetric if there exists some $\phi \in \mathrm{Hom}_S(\Lambda, S)$ such that $\phi(xy) = \phi(yx)$ for all $x, y \in \Lambda$, and such that $\Lambda \to \mathrm{Hom}_S(\Lambda, S)$, $y \mapsto y\phi$, is bijective.

Proposition 9.11 *Let k be a field of characteristic $p > 0$, and let $R := k[[x_1, \ldots, x_n]]$. Let $a_1, \ldots, a_n \in \mathfrak{m}_R$ be arbitrary elements, not all zero. Let A be the regular (see Theorem 6.19) complete local noetherian ring given by*

$$A := R[u_1, \ldots, u_n]/(u_1^p - a_1^{p-1}u_1 - x_1, \ldots, u_n^p - a_n^{p-1}u_n - x_n).$$

Let G denote the subgroup of automorphisms of A fixing R generated by the natural automorphism of order p which sends u_i to $u_i + a_i$ for $i = 1, \ldots, n$. Then the R-algebra $A * G$ is symmetric.

Proof We abused notation in the above statement and did not distinguish between $u_i \in R[u_1, \ldots, u_n]$ and its class in A. We will continue to do so in the proof below to lighten our notation. First observe that the skew group ring $A * G$ is a free R-algebra of rank p^{n+1} because the group G has order p and the R-algebra A is free of rank p^n. In fact, the elements

$$u_1^{i_1} \cdots u_n^{i_n}\sigma^i \in A * G, \quad 0 \le i_1, \ldots, i_n, i \le p - 1,$$

form an R-basis. Following Braun [11], who studied the linear case, we consider the element $\phi \in \mathrm{Hom}_R(A * G, R)$ given on the basis elements by

$$u_1^{i_1} \cdots u_n^{i_n} \sigma^i \longmapsto \begin{cases} 1 & \text{if } i_1 = \ldots = i_n = p-1 \text{ and } i = 0; \\ 0 & \text{else.} \end{cases}$$

Consider the map

$$A * G \longrightarrow \mathrm{Hom}_R(A * G, R), \quad y \longmapsto y\phi. \tag{9.12}$$

We claim this map is an isomorphism of $A * G$-bimodules. Let us start by showing that it is a homomorphism of bimodules. For this, it suffices to verify that $\phi(xy) = \phi(yx)$ for all $x, y \in A * G$ (Lemma 9.10).

Obviously it suffices to show that for any $x \in A * G$ and any basis element $y = u_1^{j_1} \cdots u_n^{j_n} \sigma^j$, we have $\phi(xy) = \phi(yx)$. We proceed using induction on $j_1 + \cdots + j_n + j$. Assume that the conclusion holds for $j_1 + \cdots + j_n + j < t$ and let us prove it for $j_1 + \cdots + j_n + j = t$. When $t > 1$, it is always possible to write $y = y_1 y_2$, where y_1 and y_2 are two basis vectors to which we can apply the induction hypothesis. Then $\phi(xy) = \phi(x(y_1 y_2)) = \phi(y_2(xy_1)) = \phi(y_1(y_2 x)) = \phi(yx)$. It remains to prove the case where $j_1 + \cdots + j_n + j = 1$. This means $y = \sigma$ or $y = u_s$ for some $1 \leq s \leq n$. To show that $\phi(xy) = \phi(yx)$, it is easy to see that it suffices to treat the case where $x := u_1^{i_1} \cdots u_n^{i_n} \sigma^i$ is itself a basis vector.

Consider first the case $y = \sigma$. We have $\sigma(u_r) = u_r + a_r$, which implies that

$$xy = u_1^{i_1} \cdots u_n^{i_n} \sigma^{i+1} \quad \text{and} \quad yx = (u_1 + a_1)^{i_1} \cdots (u_n + a_n)^{i_n} \sigma^{i+1}.$$

Expanding the factors of yx shows that $yx = xy + h$ with h a linear combination of basis vectors $u_1^{i_1'} \cdots u_n^{i_n'} \sigma^{i+1}$ with $0 \leq i_r' < i_r$ for $r = 1, \ldots, n$. In particular $0 \leq i_1', \ldots, i_n' < p - 1$. Consequently $\phi(h) = 0$, and we find that $\phi(yx) = \phi(xy)$.

Now let $y = u_s$ for some $1 \leq s \leq n$. Using $\sigma^i(u_s) = u_s + i a_s$, we get

$$xy = u_1^{i_1} \cdots u_n^{i_n} (u_s + i a_s) \sigma^i \quad \text{and} \quad yx = u_1^{i_1} \cdots u_s^{i_s + 1} \cdots u_n^{i_n} \sigma^i.$$

By definition, both $\phi(xy)$ and $\phi(yx)$ vanish if $i \neq 0$. In the remaining case where $i = 0$, one gets $xy = yx$, and we again find that $\phi(xy) = \phi(yx)$.

It remains to check that the homomorphism (9.12) is bijective. Since the domain and range are both finitely generated free R-modules of the same rank, it suffices to verify that this map of R-modules is surjective. By Nakayama's Lemma, it is enough to show that the induced map

$$(A * G) \otimes_R R/\mathfrak{m}_R \longrightarrow \mathrm{Hom}_R(A * G, R) \otimes_R R/\mathfrak{m}_R \tag{9.13}$$

is surjective. Let $\overline{A} := A \otimes_R R/\mathfrak{m}_R = k[[u_1, \ldots, u_n]]/(u_1^p, \ldots, u_n^p)$. Since the action of G is given by $\sigma(u_s) = u_s + a_s$ with $a_s \in \mathfrak{m}_R$, we find that G acts trivially on $\overline{A}$, and $(A * G) \otimes_R R/\mathfrak{m}_R$ is isomorphic to the commutative algebra

$$\overline{A} * G = k[u_1, \ldots, u_n, \sigma]/(u_1^p, \ldots, u_n^p, \sigma^p - 1).$$

The right-hand side of (9.13) is isomorphic to the k-vector space $\mathrm{Hom}_k(\overline{A} * G, k)$, because the R-module $A * G$ is finitely generated. Let $\bar{\phi} \in \mathrm{Hom}_k(\overline{A} * G, k)$ denote the class of ϕ.

Let $x := u_1^{i_1} \cdots u_n^{i_n} \sigma^i$ be any basis vector, and consider the linear form $\varphi_x : \overline{A} * G \to k$ such that $\varphi_x(x) = 1$ and $\varphi_x(z) = 0$ for any other basis vector z. We exhibit now an element

y such that $y\bar{\phi} = \varphi_x$. Consider the element $y := u_1^{j_1} \cdots u_n^{j_n} \sigma^j$ with the complementary exponents

$$j_1 := p - 1 - i_1, \ \ldots, \ j_n := p - 1 - i_n, \quad \text{and} \quad j = p - i.$$

Then $(y\bar{\phi})(x) = \bar{\phi}(xy) = 1$ by definition of ϕ. For every other basis vector $z = u_1^{j'_1} \cdots u_n^{j'_n} \sigma^{j'}$, we have $(y\bar{\phi})(z) = \bar{\phi}(zy) = 0$. It follows that $\overline{A} * G \to \mathrm{Hom}_k(\overline{A} * G, k)$ is surjective. □

Proof of Theorem 9.6 By hypothesis, A is a complete regular local domain of dimension $n \geq 2$ with field of representatives k and endowed with a moderately ramified action of the cyclic group G of order p. Then Theorem 6.11 shows that the ring A, as a k-algebra with G-action, is isomorphic to

$$k[[x_1, \ldots, x_n]][u_1, \ldots, u_n]/(u_1^p - a_1^{p-1}u_1 - x_1, \ldots, u_n^p - a_n^{p-1}u_n - x_n),$$

where $x_1, \ldots, x_n$ are indeterminates, the elements $a_1, \ldots, a_n \in k[[x_1, \ldots, x_n]]$ form a system of parameters of $k[[x_1, \ldots, x_n]]$, and the natural automorphism of order p which sends u_i to $u_i + a_i$ and fixes $k[[x_1, \ldots, x_n]]$ induces under this isomorphism a generator of G. As usual, we let $R := k[[x_1, \ldots, x_n]]$. Clearly $R \subset A^G \subset A$, and we may thus consider the skew group ring $A * G$ as an R-algebra.

Using 9.4 and the fact that $K_R = R$ because R is regular, we find that $K_{A^G} = \mathrm{Hom}_R(A^G, R)$. To prove Theorem 9.6, it thus suffices to show that there exists an isomorphism of A^G-modules $A^G \to \mathrm{Hom}_R(A^G, R)$. For this we need the following fact (Proposition 2.4 (3) in [25]):

9.14 *Suppose that S is a normal noetherian ring, and Λ is an associative S-algebra that is finitely generated as S-module. Let M be a finitely generated left Λ-module such that M is reflexive as an S-module, and such that given any prime ideal $\mathfrak{p} \subset S$ of height one, $M_\mathfrak{p}$ is a projective $\Lambda_\mathfrak{p}$-module. If the S-algebra Λ is symmetric, then the S-algebra $\mathrm{End}_\Lambda(M)$ is symmetric as well.*

Let us now check that we can apply 9.14 to the case where $S := R$, $\Lambda := A * G$ and $M := A$. Clearly R is normal since it is regular, and $A * G$ is a finitely generated R-module. According to Proposition 9.9, the R-module A is reflexive, and for each prime ideal $\mathfrak{p} \subset R$ of height one, the $(A * G)_\mathfrak{p}$-module $A_\mathfrak{p}$ is projective. Finally, Proposition 9.11 shows that $A * G$ is a symmetric R-algebra. Thus 9.14 can be applied and we find that the R-algebra $\mathrm{End}_{A*G}(A)$ is symmetric: In other words, we have an isomorphism of $\mathrm{End}_{A*G}(A)$-bimodules between $\mathrm{End}_{A*G}(A)$ and $\mathrm{Hom}_R(\mathrm{End}_{A*G}(A), R)$. Using (9.7), we find an isomorphism of A^G-algebras $A^G \to \mathrm{End}_{A*G}(A)$. Hence, the A^G-modules A^G and $K_{A^G} = \mathrm{Hom}_R(A^G, R)$ are isomorphic, as desired. □

Remark 9.15 Recall that when a complete local ring is Cohen–Macaulay, its canonical module is free of rank 1 if and only if the ring is Gorenstein [22, 5.9]. Local rings with trivial canonical class are called *quasi-Gorenstein* by Platte and Storch [47, page 5]. Theorem 9.6 provides a rich supply of quasi-Gorenstein rings which are not Cohen–Macaulay when they have dimension bigger than 2 (use Proposition 3.2 (i)).

Recall also that if a finite group G acts on a Cohen–Macaulay ring A and $|G|$ is invertible in A, then the ring A^G is Cohen–Macaulay [24, Proposition 13]. A necessary and sufficient condition for A^G to be Gorenstein when A is regular is given in [65, Theorem 2]. Theorem 4 in [64] shows that A^G is Gorenstein if the image of the associated map $\lambda : G \to \mathrm{GL}(\mathfrak{m}_A/\mathfrak{m}_A^2)$

is in $\mathrm{SL}(\mathfrak{m}_A/\mathfrak{m}_A^2)$. See also Conjecture 5 in [28] when $|G|$ is not invertible in $A = k[V]$, where V is a k-vector space with an action of G.

Acknowledgements The authors thank the referee for a careful reading of the manuscript and for useful comments. The authors gratefully acknowledges funding support from the research training group *Algebra, Algebraic Geometry, and Number Theory* at the University of Georgia, from the National Science Foundation RTG grant DMS-1344994, from the Simons Collaboration Grant 245522, and the research training group *GRK 2240: Algebro-geometric Methods in Algebra, Arithmetic and Topology* of the Deutsche Forschungsgemeinschaft.

References

1. Abramovich, D.: Raynaud's group-scheme and reduction of coverings. With an appendix by Jonathan Lubin. In: Number Theory, Analysis and Geometry, pp. 1–18. Springer, New York (2012)
2. Altman, A., Kleiman, S.: Introduction to Grothendieck duality theory. Lecture Notes in Mathematics, vol. 146. Springer, Berlin (1970)
3. Aoyama, Y.: Some basic results on canonical modules. J. Math. Kyoto Univ. **23**, 85–94 (1983)
4. Artin, M.: Wildly ramified $Z/2$ actions in dimension two. Proc. Am. Math. Soc. **52**, 60–64 (1975)
5. Auslander, M., Buchsbaum, D.: Codimension and multiplicity. Ann. Math. **68**, 625–657 (1958)
6. Avramov, L.: Pseudoreflection group actions on local rings. Nagoya Math. J. **88**, 161–180 (1982)
7. Benson, D., Webb, P.: Unique factorization in invariant power series rings. J. Algebra **319**(2), 702–715 (2008)
8. Bourbaki, N.: Algebra II, Chapters 4–7. Translated from the French by P. M. Cohn and J. Howie. Elements of Mathematics (Berlin). Springer, Berlin, (1990)
9. Bourbaki, N.: Algèbre commutative. Chapitre 10, Reprint of the 1998 original. Springer, Berlin (2007)
10. Boutot, J.-F.: Singularités rationnelles et quotients par les groupes réductifs. Invent. Math. **88**, 65–68 (1987)
11. Braun, A.: On the Gorenstein property for modular invariants. J. Algebra **345**, 81–99 (2011)
12. Brieskorn, E.: Rationale Singularitäten komplexer Flächen. Invent. Math. **4**, 336–358 (1967/1968)
13. Campbell, H., Hughes, I.: Vector invariants of $U_2(\mathbb{F}_p)$: a proof of a conjecture of Richman. Adv. Math. **126**(1), 1–20 (1997)
14. Cartan, H.: Quotient d'un espace analytique par un groupe d'automorphismes. In: Fox, R. (ed.) Algebraic geometry and topology, pp. 90–102. Princeton University Press, Princeton (1957)
15. Ellingsrud, G., Skjelbred, T.: Profondeur d'anneaux d'invariants en caractéristique p. Compos. Math. **41**, 233–244 (1980)
16. Fogarty, J.: On the depth of local rings of invariants of cyclic groups. Proc. Am. Math. Soc. **83**(3), 448–452 (1981)
17. Gilmer, R.: Contracted ideals with respect to integral extensions. Duke Math. J. **34**, 561–571 (1967)
18. Giraud, J.: Cohomologie non abélienne, Die Grundlehren der mathematischen Wissenschaften, vol. 179. Springer, Berlin (1971)
19. Grothendieck, A.: Techniques de construction et théorèmes d'existence en géométrie algébrique. IV. Les schémas de Hilbert, Séminaire Bourbaki, vol. 6, Exp. No. 221, pp. 249–276. Soc. Math. France, Paris (1995)
20. Grothendieck, A., Dieudonné, J.: Éléments de géométrie algébrique, Publ. Math. IHÉS **4** (Chapter 0, 1–7, and I, 1–10), **8** (II, 1–8), **11** (Chapter 0, 8–13, and III, 1–5), **17** (III, 6–7), **20** (Chapter 0, 14–23, and IV, 1), **24** (IV, 2–7), **28** (IV, 8–15), and **32** (IV, 16–21), (1960–1967)
21. Hartshorne, R.: Generalised divisors on Gorenstein schemes. K-Theory **8**, 287–339 (1994)
22. Herzog, J., Kunz, E. (eds.) Der kanonische Modul eines Cohen–Macaulay-Rings, Lect. Notes Math., vol. 238. Springer, Berlin (1971)
23. Hochster, M.: Contracted ideals from integral extensions of regular rings. Nagoya Math. J. **51**, 25–43 (1973)
24. Hochster, M., Eagon, J.: Cohen–Macaulay rings, invariant theory, and the generic perfection of determinantal loci. Am. J. Math. **93**, 1020–1058 (1971)
25. Iyama, O., Reiten, I.: Fomin–Zelevinsky mutation and tilting modules over Calabi–Yau algebras. Am. J. Math. **130**, 1087–1149 (2008)
26. Kemper, G.: On the Cohen–Macaulay property of modular invariant rings. J. Algebra **215**, 330–351 (1999)
27. Kemper, G.: Loci in quotients by finite groups, pointwise stabilizers and the Buchsbaum property. J. Reine Angew. Math. **547**, 69–96 (2002)

28. Kemper, G., Körding, E., Malle, G., Matzat, B., Vogel, D., Wiese, G.: A database of invariant rings. Exp. Math. **10**(4), 537–542 (2001)
29. Kiràly, F., Lüktebohmert, W.: Group actions of prime order on local normal rings. Algebra Number Theory **7**(1), 63–74 (2013)
30. Klopsch, B.: Automorphisms of the Nottingham group. J. Algebra **223**, 37–56 (2000)
31. Koh, J.: Degree p extensions of an unramified regular local ring of mixed characteristic p. J. Algebra **99**(2), 310–323 (1986)
32. Lipman, J.: Rational singularities, with applications to algebraic surfaces and unique factorization. Inst. Hautes Études Sci. Publ. Math. **36**, 195–279 (1969)
33. Lipman, J.: Unique factorization in complete local rings. In: Algebraic Geometry (Proc. Sympos. Pure Math., vol. 29, Humboldt State Univ., Arcata, Calif., 1974), pp. 531–546. Amer. Math. Soc., Providence (1975)
34. Lorenzini, D.: Wild quotients of products of curves. Eur. J. Math. **4**, 525–554 (2018)
35. Lorenzini, D., Schröer, S.: Discriminant groups of wild cyclic quotient singularities **(in preparation)**
36. Lubin, J.: Torsion in the Nottingham group. Bull. Lond. Math. Soc. **43**(3), 547–560 (2011)
37. Majadas, J.: On tensor products of complete intersections. Bull. Lond. Math. Soc. **45**(6), 1281–1284 (2013)
38. Marrama, A.: A Purity Theorem for Torsors, ALGANT Master Thesis (2016). http://algant.eu/algant_theses.php
39. Matsumura, H.: Commutative Algebra, 2nd edn. Benjamin/Cummings, Reading (1980)
40. Matsumura, H.: Commutative Ring Theory. Cambridge University Press, Cambridge (1989)
41. Mollier, D.: Descente de la propriété noethérienne. Bull. Sci. Math. (2) **94**, 25–31 (1970)
42. Moret-Bailly, L.: Un théorème de pureté pour les familles de courbes lisses. C. R. Acad. Sci. Paris Sér. I Math. **300**(4), 489–492 (1985)
43. Mori, S.: On affine cones associated with polarized varieties. Jpn. J. Math. (N.S.) **1**(2), 301–309 (1975)
44. Nagata, M.: On the purity of branch loci in regular local rings. Ill. J. Math. **3**, 328–333 (1959)
45. Nagata, M.: Local rings. Interscience Tracts in Pure and Applied Mathematics, No. 13, Interscience Publishers a division of Wiley, New York (1962)
46. Peskin, B.: Quotient-singularities and wild p-cyclic actions. J. Algebra **81**, 72–99 (1983)
47. Platte, E., Storch, U.: Invariante reguläre Differentialformen auf Gorenstein-Algebren. Math. Z. **157**, 1–11 (1977)
48. Raynaud, M.: Spécialisation des revêtements en caractéristique $p>0$. Ann. Sci. École Norm. Sup. (4) **32**(1), 87–126 (1999)
49. *Revêtements étales et groupe fondamental* (French), Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1). Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de Michèle Raynaud. Lecture Notes in Mathematics, vol. 224. Springer, Berlin (1971)
50. Richman, D.: On vector invariants over finite fields. Adv. Math. **81**, 30–65 (1990)
51. Roberts, P.: Abelian extensions of regular local rings. Proc. Am. Math. Soc. **78**(3), 307–310 (1980)
52. Romagny, M.: Effective model of a finite group action. arXiv:math/0601639v1
53. Romagny, M.: Effective models of group schemes. J. Algebr. Geom. **21**, 643–682 (2012)
54. Rotman, J.: An Introduction to Homological Algebra, 2nd edn. Springer, New York (2009)
55. Samuel, P.: Classes de diviseurs et dérivées logarithmiques. Topology **3**, 81–96 (1964)
56. Samuel, P.: Groupes finis d'automorphismes des anneaux de séries formelles. Bull. Sci. Math. **90**, 97–101 (1966)
57. Serre, J.-P.: Algèbre locale. Multiplicités. Springer, Berlin (1965)
58. Serre, J.-P.: Groupes finis d'automorphismes d'anneaux locaux réguliers, 1968 Colloque d'Algèbre (Paris, 1967), Exp. 8, Secrétariat mathématique, Paris
59. Serre, J.-P.: Linear representations of finite groups, Translated from the second French edition by Leonard L. Scott. Graduate Texts in Mathematics, vol. 42. Springer, New York (1977)
60. Shank, R., Wehlau, D.: Computing modular invariants of p-groups. J. Symb. Comput. **34**, 307–327 (2002)
61. Sjödin, G.: On filtered modules and their associated graded modules. Math. Scand. **33**(1973), 229–249 (1974)
62. Tate, J., Oort, F.: Group schemes of prime order. Ann. Sci. École Norm. Sup. **3**, 1–21 (1970)
63. Wahl, J.: Equations defining rational singularities. Ann. Sci. École Norm. Sup. (4) **10**(2), 231–263 (1977)
64. Watanabe, K.: Certain invariant subrings are Gorenstein I. Osaka J. Math. **11**, 1–8 (1974)
65. Watanabe, K.: Certain invariant subrings are Gorenstein II. Osaka J. Math. **11**, 379–388 (1974)
66. Waterhouse, W.: Divisor classes in pseudo Galois extensions. Pac. J. Math. **36**, 541–548 (1971)
67. Yuan, S.: Reflexive modules and algebra class groups over noetherian integrally closed domains. J. Algebra **32**, 405–417 (1974)

68. Zariski, O., Samuel, P.: Commutative Algebra, vol. II, The University Series in Higher Mathematics, D. Van Nostrand Co., Inc., Princeton (1960)