Algebra & Number Theory

Volume 7
2013
No. 1

Group actions of prime order on local normal rings

Franz Kiràly and Werner Lütkebohmert

msp

ALGEBRA AND NUMBER THEORY 7:1 (2013)
dx.doi.org/10.2140/ant.2013.7.63

Group actions of prime order on local normal rings

Franz Kiràly and Werner Lütkebohmert

Let B be a Noetherian normal local ring and $G \subset \mathrm{Aut}(B)$ be a cyclic group of local automorphisms of prime order. Let A be the subring of G-invariants of B and assume that A is Noetherian. We prove that B is a monogenous A-algebra if and only if the augmentation ideal of B is principal. If in particular B is regular, we prove that A is regular if the augmentation ideal of B is principal.

An important class of singularities is built by the famous Hirzebruch–Jung singularities. They arise by dividing out a finite cyclic group action on a smooth surface. Their resolution is well understood and has nice arithmetic properties related to continued fractions; see [Hirzebruch 1953; Jung 1908].

One can also look at such group actions from a purely algebraic point of view. So let B be a regular local ring and G a finite cyclic group of order n acting faithfully on B by local automorphisms. In the tame case, that is, the order of G is prime to the characteristic of the residue field k of B, there is a central result of J. P. Serre [1968] saying that the action is given by multiplying a suitable system of parameters $(y_1, \dots, y_d)$ by roots of unity $y_i \mapsto \zeta^{n_i} \cdot y_i$ for $i = 1, \dots, d$, where ζ is a primitive n-th root of unity. Moreover, the ring of invariants $A := B^G$ is regular if and only if $n_i \equiv 0 \bmod n$ for $d-1$ of the parameters. The latter is equivalent to the fact that $\mathrm{rk}((\sigma - \mathrm{id})|T) \leq 1$ for the action of $\sigma \in G$ on the tangent space $T := \mathfrak{m}_B/\mathfrak{m}_B^2$. For more details see [Bourbaki 1981, Chapter 5, ex. 7].

Only very little is known in the case of a wild group action, that is, when $\gcd(n, \operatorname{char} k) > 1$. In this paper we will restrict ourselves to the case of p-cyclic group actions, that is, where $n = p$ is a prime number. We will present a sufficient condition for the ring of invariants A to be regular. Our result is also valid in the tame case, that is, where n is a prime different from $\operatorname{char} k$. As the method of Serre depends on an intrinsic formula for writing down the action explicitly, we provide also an explicit formula for presenting B as a free A-module if our condition is fulfilled.

MSC2010: primary 14L30; secondary 13A50.
Keywords: algebraic geometry, commutative algebra, group actions.

The interest in our problem arises from investigating the relationship between the regular and the stable R-model of a smooth projective curve X_K over the field of fractions K of a discrete valuation ring R. In general, the curve X_K admits a stable model X' over a finite Galois extension $R \hookrightarrow R'$. Then the Galois group $G = G(R'/R)$ acts on X'. Our result provides a means to construct a regular model over R by starting from the stable model X'. As a special case, we discuss in Section 4 the situation where X_K has good reduction after a Galois p-extension $R \hookrightarrow R'$. In this case there is a criterion for when the quotient of the smooth model is regular. We intend to work out more general situations in a further article.

1. The main result

In this paper we will study only local actions of a cyclic group G of prime order p on a normal local ring B. We fix a generator σ of G and obtain the *augmentation map*

$$I := I_\sigma := \sigma - \mathrm{id} : B \to B, \quad b \mapsto \sigma(b) - b.$$

We introduce the B-ideal

$$I_G := (I(b);\ b \in B) \subset B$$

which is generated by the image $I(B)$. This ideal is called *augmentation ideal*. If this ideal is generated by an element $I(y)$, we call y an *augmentation generator*. Note that this ideal does not depend on the chosen generator σ of G. Moreover, if y is an augmentation generator with respect to a generator σ of G, then y is also an augmentation generator for any other generator of G. Since B is local, the ideal I_G is generated by an augmentation generator if I_G is principal. Namely, $I_G/\mathfrak{m}_B I_G$ is a vector space over the residue field $k_B = B/\mathfrak{m}_B$ of B of dimension 1. So it is generated by the residue class of $I(y)$ for some $y \in B$, and hence, by Nakayama's lemma, I_G is generated by $I(y)$.

Definition 1. An action of a group G on a regular local ring B by local automorphisms is called a *pseudoreflection* if there exists a system of parameters $(y_1, \ldots, y_d)$ of B such that $y_2, \ldots, y_d$ are invariant under G.

Theorem 2. *Let B be a normal local ring with residue field $k_B := B/\mathfrak{m}_B$. Let p be a prime number and G a p-cyclic group of local automorphisms of B. Let I_G be the augmentation ideal. Let A be the ring of G-invariants of B. Consider the following conditions*:

(a) *$I_G := B \cdot I(B)$ is principal.*

(b) *B is a monogenous A-algebra.*

(c) *B is a free A-module.*

Then the following implications are true:

$$(a) \Longleftrightarrow (b) \Longrightarrow (c).$$

Assume, in addition, that B is regular. Consider the following conditions:

(d) *A is regular.*

(e) *G acts as a pseudoreflection.*

Then the condition (c) *is equivalent to* (d). *Moreover if, in addition, the canonical map $k_A \xrightarrow{\sim} k_B$ is an isomorphism, then condition* (a) *is equivalent to condition* (e).

We start the proof of the theorem with several preparations.

Remark 3. For $b_1, b_2, b \in B$, the following relations are true:

(i) $\qquad I(b_1 \cdot b_2) = I(b_1) \cdot \sigma(b_2) + b_1 \cdot I(b_2).$

(ii) $$I(b^n) = \left(\sum_{i=1}^{n} \sigma(b)^{i-1} b^{n-i}\right) \cdot I(b).$$

(iii) $$I\Big(\frac{b_1}{b_2}\Big) = \frac{I(b_1)b_2 - b_1 I(b_2)}{b_2\sigma(b_2)} \quad \text{if } b_2 \neq 0.$$

Proof. (i) follows by a direct calculation and (ii) by induction from (i).

As for (iii), the formula (i) holds for elements in the field of fractions as well. Therefore,

$$I(b_1) = I\Big(\frac{b_1}{b_2} b_2\Big) = I\Big(\frac{b_1}{b_2}\Big)\sigma(b_2) + \frac{b_1}{b_2} I(b_2),$$

and the formula follows. □

To prove that (a) implies (b) we need a technical lemma.

Lemma 4. *Let $y \in B$ be an augmentation generator. Then set, inductively,*

$$\begin{aligned} y_i^{(0)} &:= y^i && \text{for } i = 0, \ldots, p-1, \\ y_i^{(1)} &:= I(y_i^{(0)})/I(y_1^{(0)}) && \text{for } i = 1, \ldots, p-1, \\ y_i^{(n+1)} &:= I(y_i^{(n)})/I(y_{n+1}^{(n)}) && \text{for } i = n+1, \ldots, p-1. \end{aligned}$$

Then

$$y_i^{(n)} = \sum_{0 \le k_1 \le \cdots \le k_{i-n} \le n} \prod_{j=1}^{i-n} \sigma^{k_j}(y) \quad \text{for } i = n, \ldots, p-1,$$

and in particular,

$$y_n^{(n)} = 1, \qquad y_{n+1}^{(n)} = \sum_{j=1}^{n+1} \sigma^{j-1}(y), \qquad I(y_{n+1}^{(n)}) = \sigma^{n+1}(y) - y.$$

Furthermore, $y_{n+1}^{(n)}$ is again an augmentation generator for $n = 0, \ldots, p-2$.

Proof. We proceed by induction on n. For $n = 0$ the formulas are obviously correct. For the convenience of the reader we also display the formulas for $n = 1$. Due to Remark 3 one has

$$y_i^{(1)} = \frac{I(y_i^{(0)})}{I(y_1^{(0)})} = \frac{I(y^i)}{I(y)} = \sum_{j=1}^{i} \sigma(y)^{j-1} y^{i-j} = \sum_{0 \le k_1 \le \cdots \le k_{i-1} \le 1} \prod_{\nu=1}^{i-1} \sigma^{k_\nu}(y),$$

since the last sum can be viewed as a sum over an index j where $i - j$ is the number of k_ν equal to 0. In particular, the formulas are correct for $y_1^{(1)}$ and $y_2^{(1)}$. Moreover

$$I(y_2^{(1)}) = I(\sigma(y) + y) = \sigma^2(y) - y.$$

Since σ^2 is generator of G for $2 < p$, the element $y_2^{(1)}$ is an augmentation generator as well.

Now assume that the formulas are correct for n. Since $y_{n+1}^{(n)}$ is an augmentation generator, $I(y_{n+1}^{(n)})$ divides $I(y_i^{(n)})$ for $i = n+1, \ldots, p-1$. Then it remains to show, upon substituting the expressions from the lemma for $y_i^{(n)}$ and $y_i^{(n+1)}$, that

$$I(y_i^{(n)}) = (\sigma^{n+1}(y) - y) \cdot y_i^{(n+1)} \quad \text{for } i = n+1, \ldots, p-1.$$

For the left hand side one computes

$$\begin{aligned}
\text{LHS} &= I\Bigg(\sum_{0 \le k_1 \le \cdots \le k_{i-n} \le n} \prod_{j=1}^{i-n} \sigma^{k_j}(y) \Bigg) = \sum_{0 \le k_1 \le \cdots \le k_{i-n} \le n} I\Bigg(\prod_{j=1}^{i-n} \sigma^{k_j}(y) \Bigg) \\
&= \sum_{0 \le k_1 \le \cdots \le k_{i-n} \le n} \Bigg(\prod_{j=1}^{i-n} \sigma^{k_j+1}(y) - \prod_{j=1}^{i-n} \sigma^{k_j}(y) \Bigg) \\
&= \sum_{1 \le k_1 \le \cdots \le k_{i-n} \le n+1} \prod_{j=1}^{i-n} \sigma^{k_j}(y) - \sum_{0 \le k_1 \le \cdots \le k_{i-n} \le n} \prod_{j=1}^{i-n} \sigma^{k_j}(y).
\end{aligned}$$

Now all terms occurring in both sums cancel. These are the terms with $k_{i-n} \le n$ in the first sum and $1 \le k_1$ in the second sum.
For the right hand side one computes

$$\begin{aligned}
\text{RHS} &= (\sigma^{n+1}(y) - y) \cdot \sum_{0 \le k_1 \le \cdots \le k_{i-n-1} \le n+1} \prod_{j=1}^{i-n-1} \sigma^{k_j}(y) \\
&= \sum_{0 \le k_1 \le \cdots \le k_{i-n} = n+1} \prod_{j=1}^{i-n} \sigma^{k_j}(y) - \sum_{0 = k_1 \le \cdots \le k_{i-n} \le n+1} \prod_{j=1}^{i-n} \sigma^{k_j}(y).
\end{aligned}$$

Both sides are seen to be equal. In particular we have

$$\begin{aligned} y_{n+1}^{(n+1)} &= 1, \\ y_{n+2}^{(n+1)} &= \sum_{0\le k_1\le n+1} \prod_{j=1}^{1} \sigma^{k_1}(y) = \sum_{j=1}^{n+2} \sigma^{j-1}(y), \\ I(y_{n+2}^{(n+1)}) &= \sigma^{n+2}(y) - y. \end{aligned}$$

So $y_{n+2}^{(n+1)}$ is an augmentation generator for $n+2 < p$, since σ^{n+2} generates G. This concludes the technical part. □

Proposition 5. *Assume that the augmentation ideal I_G is principal and let $y \in B$ be an augmentation generator. Then B decomposes into the direct sum*

$$B = A \cdot y^0 \oplus A \cdot y^1 \oplus \cdots \oplus A \cdot y^{p-1}.$$

Proof. Since $I(y) \neq 0$, the element y generates the field of fractions $Q(B)$ over $Q(A)$. Therefore

$$Q(B) = Q(A) \cdot y^0 \oplus Q(A) \cdot y^1 \oplus \cdots \oplus Q(A) \cdot y^{p-1}.$$

Then it suffices to show the following claim:

Let $a, a_0, \ldots, a_{p-1} \in A$. Assume that a divides

$$b = a_0 \cdot y^0 + a_1 \cdot y^1 + \cdots + a_{p-1} \cdot y^{p-1}.$$

Then a divides $a_0, a_1, \ldots, a_{p-1}$.

If $b = a \cdot \beta$, then $I(b) = a \cdot I(\beta)$. Since $I(\beta) = \beta_1 \cdot I(y)$, we get $I(b) = a\beta_1 \cdot I(y)$. So we see that a divides $I(b)/I(y) \in B$. Using the notation of Lemma 4, set

$$\begin{aligned} b^{(0)} &:= b = a_0 \cdot y^0 + a_1 \cdot y^1 + \cdots + a_{p-1} \cdot y^{p-1} \\ b^{(1)} &:= \frac{I(b^{(0)})}{I(y)} = a_1 + a_2 \frac{I(y^2)}{I(y)} + \cdots + a_{p-1} \frac{I(y^{p-1})}{I(y)} \\ &\qquad = a_1 \cdot y_1^{(1)} + a_2 \cdot y_2^{(1)} + \cdots + a_{p-1} \cdot y_{p-1}^{(1)} \\ b^{(n)} &:= \frac{I(b^{(n-1)})}{I(y_n^{(n-1)})} = a_n \cdot y_n^{(n)} + a_{n+1} \cdot y_{n+1}^{(n)} + \cdots + a_{p-1} \cdot y_{p-1}^{(n)}. \end{aligned}$$

Due to the observation above, by induction a divides $b^{(0)}, b^{(1)}, \ldots, b^{(p-1)}$, since $y_{n+1}^{(n)}$ is an augmentation generator for $n = 1, \ldots, p-2$. So we obtain

$$a \mid b^{(p-1)} = a_{p-1} \cdot y_{p-1}^{(p-1)} = a_{p-1}.$$

Now proceeding downwards, one obtains

$$a \,\big|\, b^{(p-2)} = a_{p-2} + a_{p-1} \cdot y_{p-1}^{(p-2)}, \quad \text{hence } a \,\big|\, a_{p-2},$$
$$a \,\big|\, b^{(n)} = a_n + a_{n+1} \cdot y_{n+1}^{(n)} + \cdots + a_{p-1} \cdot y_{p-1}^{(n)}, \quad \text{hence } a \,\big|\, a_n$$

for $n = p-1, p-2, \ldots, 0$. □

Proof of the first part of Theorem 2. (a) $\Longrightarrow$ (b): This follows from Proposition 5.

(b) $\Longrightarrow$ (a): If $B = A[y]$ is monogenous, then $I_G = B \cdot I(y)$ is principal.

(b) $\Longrightarrow$ (c) is clear. Namely, if $B = A[y]$, the minimal polynomial of y over the field of fraction is of degree p and the coefficients of this polynomial belong to A. Then B has $y^0, y^1, \ldots, y^{p-1}$ as an A-basis. □

Next we do some preparations for proving the second part of the theorem where B is assumed to be regular.

Proposition 6. *Keep the assumption of the second part of Theorem* 2, *namely that B is regular and that the canonical morphism $k_A \xrightarrow{\sim} k_B$ is an isomorphism. Let $(y_1, \ldots, y_d)$ be a generating system of the maximal ideal $\mathfrak{m}_B$. Then the following assertions are true*:

(i) $I_G = B \cdot I(y_1) + \cdots + B \cdot I(y_d)$.

(ii) *If the ideal $I_G = B \cdot I(B)$ is principal, then there exists an index $i \in \{1, \ldots, d\}$ with $I_G = B \cdot I(y_i)$.*

Proof. (i) Recall that $A = B^G$ denotes the ring of invariants. Due to the assumption, we have $B = A + \mathfrak{m}_B$, and hence, $I(B) = I(\mathfrak{m}_B)$. Furthermore, we have

$$\mathfrak{m}_B = \mathfrak{m}_B^2 + \sum_{i=1}^{d} A \cdot y_i.$$

Since I is A-linear, we get

$$I(\mathfrak{m}_B) = I(\mathfrak{m}_B^2) + \sum_{i=1}^{d} A \cdot I(y_i).$$

Due to Remark 3, one knows $I(\mathfrak{m}_B^2) \subset \mathfrak{m}_B \cdot I(\mathfrak{m}_B)$. So, one obtains

$$I(\mathfrak{m}_B) \subset \mathfrak{m}_B \cdot I(\mathfrak{m}_B) + \sum_{i=1}^{d} B \cdot I(y_i).$$

Since B is local, Nakayama's lemma yields

$$I_G = B \cdot I(B) = B \cdot I(\mathfrak{m}_B) = \sum_{i=1}^{d} B \cdot I(y_i).$$

(ii) Since I_G is principal, $I_G/\mathfrak{m}_B I_G$ is generated by one of the $I(y_i)$, and hence, again by Nakayama's lemma, $I_G = B \cdot I(y_i)$ for a suitable $i \in \{1, \dots, d\}$. $\square$

Proof of the second part of Theorem 2. (c) $\Longrightarrow$ (d) follows from [Matsumura 1980, Theorem 51]. Namely, B is noetherian due to the definition of a regular ring. Since $A \to B$ is faithfully flat, A is noetherian. Then one can apply [loc. cit.].

(d) $\Longrightarrow$ (c) follows from [Serre 1965, IV, Prop. 22].

(a) $\Longrightarrow$ (e): We assume that the canonical map $k_A \to k_B$ of the residue fields is an isomorphism. If I_G is principal, one can choose an augmentation generator $y \in \mathfrak{m}_B$ that is part of a system of parameters $(y, y_2, \dots, y_d)$ due to Proposition 6. Due to Proposition 5, we know that B decomposes into the direct sum

$$B = A \cdot y^0 \oplus A \cdot y^1 \oplus \cdots \oplus A \cdot y^{p-1}.$$

Now we can represent

$$y_j = \sum_{i=0}^{p-1} a_{i,j} \cdot y^i \quad \text{for } j = 2, \dots, d.$$

Then, set

$$\tilde{y}_j := y_j - \sum_{i=1}^{p-1} a_{i,j} y^i = a_{0,j} \in A \cap \mathfrak{m}_B = \mathfrak{m}_A \quad \text{for } j = 2, \dots, d.$$

So $(y, \tilde{y}_2, \dots, \tilde{y}_d)$ is a system of parameters of B as well. Thus G acts by a pseudoreflection.

(e) $\Longrightarrow$ (a): If G is a pseudoreflection, I_G is generated by $I(y)$ due to Proposition 6, where $y, x_2, \dots, x_p$ is a system of parameters with $x_i \in \mathfrak{m}_A$ for $i = 2, \dots, p$ if $k_A = k_B$. $\square$

2. An example

If $k_A \to k_B$ is not an isomorphism, the implication (e) $\Longrightarrow$ (a) is false:

Example 7. Let k be a field of positive characteristic p and look at the polynomial ring $R := k[Z, Y, X_1, X_2]$ over k. We define a p-cyclic action of $G = \langle\sigma\rangle$ on R by

$$\sigma|k := \mathrm{id}_k, \quad \sigma(Z) = Z + X_1, \quad \sigma(Y) = Y + X_2, \quad \sigma(X_i) = X_i \quad \text{for } i = 1, 2.$$

This is a well-defined action of order p, since $p \cdot X_i = 0$ for $i = 1, 2$, and it leaves the ideal $\mathfrak{I} := (Y, X_1, X_2)$ invariant. Furthermore, for any $g \in k[Z] - \{0\}$ the image is given by $\sigma(g) = g + I(g)$ with $I(g) \in X_1 \cdot k[Z, X_1]$.

Then consider the polynomial ring $S := k(Z)[Y, X_1, X_2]$ over the field of fractions $k(Z)$ of the polynomial ring $k[Z]$. Then S has the maximal ideal $\mathfrak{m} = (Y, X_1, X_2)$.

Then set $B := S_{\mathfrak{m}} = k(Z)[Y, X_1, X_2]_{(Y, X_1, X_2)}$. We can regard all these rings as subrings of the field of fractions of R:

$$R \subset S \subset B \subset k(Z, Y, X_1, X_2).$$

Clearly, σ acts on R, and hence it induces an action on its field of fractions; denote this action by σ as well. Then we claim that the restriction of σ to B induces an action on B by local automorphisms. For this, it suffices to show that for any $g \in R - \mathfrak{I}$ the image $\sigma(g)$ does not belong to $\mathfrak{I}$. The latter is true, since $\sigma(g) = g + I(g)$ with $I(g) \in \mathfrak{I}$. The augmentation ideal $I_G = B \cdot X_1 + B \cdot X_2$ is not principal although G acts through a pseudoreflection.

3. A conjecture

Remark 8. In the tame case $p \neq \operatorname{char}(k_B)$, the converse (d) $\Longrightarrow$ (a) is also true due to the theorem of Serre, as explained in the introduction.

In the case of a wild group action, that is, $p = \operatorname{char}(k_B)$, it is not known whether the converse is true, but we conjecture it.

Conjecture 9. Let B be a regular local ring and let G be a p-cyclic group acting on B by local automorphisms. Then the following conditions are *conjectured* to be equivalent:

(1) I_G is principal.

(2) $A := B^G$ is regular.

The implication (1) $\Longrightarrow$ (2) was shown in Theorem 2. Of course the converse is true if $\dim A \leq 1$. In higher dimension, the converse (2) $\Longrightarrow$ (1) is uncertain, but it holds for small primes $p \leq 3$ as we explain now. Since A is regular, the ring B is a free A-module of rank p; see [Serre 1965, IV, Proposition 22]. So,

$$B/B\mathfrak{m}_A^n \text{ is a free } A/\mathfrak{m}_A^n\text{-module of rank } p \text{ for any } n \in \mathbb{N}. \tag{$*$}$$

In the case $p = 2$, the rank of $\mathfrak{m}_B/B\mathfrak{m}_A$ is 0 or 1. In the first case, k_B is an extension of degree $[k_B : k_A] = 2$ over k_A and $\mathfrak{m}_B = B\mathfrak{m}_A$. So there exists an element $\beta \in B$ such that $B/B\mathfrak{m}_A$ is generated by the residue classes of 1 and β. Due to Nakayama's lemma, $B = A[\beta]$ is monogenous, and hence, I_G is principal. In the second case, where $k_A \to k_B$ is an isomorphism, there exists an element $\beta \in \mathfrak{m}_B$ such that $\mathfrak{m}_B = B\beta + B\mathfrak{m}_A$. Then G acts as a pseudoreflection, and hence, I_G is principal.

In the case $p = 3$ we claim that $B\mathfrak{m}_A \not\subset \mathfrak{m}_B^2$.

If we assume the contrary $B\mathfrak{m}_A \subset \mathfrak{m}_B^2$, then these ideals coincide; $B\mathfrak{m}_A = \mathfrak{m}_B^2$. Namely, the rank of $B/B\mathfrak{m}_A$ as $A/\mathfrak{m}_A$-module is 3 and the rank of $B/\mathfrak{m}_B^2$ is at least 3 due to $d := \dim B \geq 2$, so $B\mathfrak{m}_A = \mathfrak{m}_B^2$. Therefore the length of $B/B\mathfrak{m}_A^2 = B/\mathfrak{m}_B^4$

is 3 times the length of $A/\mathfrak{m}_A^2$, which is $3\cdot(\dim A+1)$. On the other hand the rank of $B/\mathfrak{m}_B^4$ is equal to

$$(1+\dim \mathfrak{m}_B/\mathfrak{m}_B^2)+\dim \mathfrak{m}_B^2/\mathfrak{m}_B^3+\dim \mathfrak{m}_B^3/\mathfrak{m}_B^4=\sum_{n=0}^{3}\binom{d+n-1}{d-1},$$

which is larger than $(1+\dim \mathfrak{m}_A/\mathfrak{m}_A^2)+(1+\dim \mathfrak{m}_A/\mathfrak{m}_A^2)+(1+\dim \mathfrak{m}_A/\mathfrak{m}_A^2)$, since for $d\geq 2$ both

$$\binom{d+1}{d-1}=\frac{(d+1)d}{2}\geq 1+d=1+\dim \mathfrak{m}_A/\mathfrak{m}_A^2$$

and

$$\binom{d+3-1}{d-1}=\frac{(d+2)(d+1)d}{2\cdot 3}>1+d$$

hold. Here we used the formula for the number $\lambda_{n,d}$ of monomials $T_1^{m_1}\cdots T_d^{m_d}$ in d variables of degree $n=m_1+\cdots+m_d$:

$$\lambda_{n,d}=\binom{d+n-1}{d-1}.$$

So, using only the condition $(*)$ and proceeding by induction on $\dim(A)$, we see that there exists a system of parameters $\alpha_1,\ldots,\alpha_d$ of A such that $\alpha_2,\ldots,\alpha_d$ is part of a system of parameters of B. In the case where $k_A\to k_B$ is an isomorphism, G acts as a pseudoreflection, and hence I_G is principal. If $k_A\to k_B$ is not an isomorphism, then we must have $\mathfrak{m}_B=B\mathfrak{m}_A$; otherwise the rank of $B/\mathfrak{m}_B$ is at least 4. Since $[k_B:k_A]\leq 3$, the field extension $k_A\to k_B$ is monogenous, and hence $A\to B$ is monogenous due to the lemma of Nakayama.

4. Relationship between the regular and the stable model of a smooth curve

As explained in the introduction, our incentive to study the invariant rings under a p-cyclic group action stems from the study of the relationship between the regular and the stable model of a smooth projective curve over the field of fractions K of a discrete valuation ring R. So let $R\hookrightarrow R'$ be a Galois extension of discrete valuation rings of prime order p and let π and π' be uniformizers of R and of R', respectively. Denote by K' the field of fractions of R' and let k and k' be the residue fields of R and R', respectively. Assume that $k=k'$ is algebraically closed and that $\mathrm{char}(k)=p$. Let G be the Galois group of R' over R.

In the tame case, the action can always be diagonalized and the invariant rings have the well-known Hirzebruch–Jung singularities. The tame case of higher dimension is also settled in [Edixhoven 1992, Proposition 3.5]. If the action of G is wild, this is in general not the case and the situation becomes quite capricious.

For example, consider an elliptic curve E over K having good reduction over K', and let X' be the corresponding proper smooth R'-model of $E \otimes_K K'$. Then G acts naturally on X', and hence one can consider the quotient $Y = X'/G$, which is a normal proper flat R-model of E. Assume that E has reduction of Kodaira type I_0^* over K; see [Silverman 1986, Theorem 15.2]. Curves of this type exist, since elliptic curves with Kodaira type I_0^* have integer j-invariant and thus potentially good reduction. Moreover, that a wild extension might be needed can be checked via Tate's algorithm [1975]. Let X be the minimal regular R-model of E. Then X happens to be a minimal blowing-up of Y and, in general, Y has singularities that are not of Hirzebruch–Jung type, since the special fiber of X contains components having three neighbors.

Our result now provides a tool to study the correspondence between X and the singularities of Y by looking at the group action G on X' and on R'-models Z', which are obtained by blowing-up G-invariant centers of X'. On these models, one can study the augmentation ideal and thereby obtain statements about which components have to occur in a desingularization of Y and in the regular model X, respectively. Since this analysis is beyond the scope of this article, we intend to explain this in greater detail in a further paper.

In the following we will look at Conjecture 9 in the case of relative curves.

Proposition 10. *Keep the situation of above. Let Y be an affine smooth relative curve over R' such that its closed fiber $Y \otimes_{R'} k'$ is irreducible. Assume that G acts on $Y \to \operatorname{Spec}(R')$ equivariantly. Let $B := \mathcal{O}_Y(Y)$ be the coordinate ring of Y. Then the following assertions are equivalent*:

(1) *The augmentation ideal I_G is locally principal.*

(2) *The ring $A := B^G$ of invariants is regular and $A/\mathfrak{p}$ is regular where $\mathfrak{p} = A \cap B\pi'$.*

Proof. (1) $\Longrightarrow$ (2). It follows from Theorem 2 that A is regular. It remains to show that the special fiber is regular. For showing this, it is enough to prove it after the π-adic completion, since the group action extends to the completion, taking invariants commutes with completion, and regularity of $A/\mathfrak{p}$ can be checked after π-adic completion. So we may assume that B is the coordinate ring of the associated formal completion of Y with respect to its special fiber. So set

$$\mathfrak{P} := B\pi' \quad \text{and} \quad \mathfrak{p} := A \cap \mathfrak{P}.$$

Then we obtain a finite extension of discrete valuation rings $A_\mathfrak{p} \hookrightarrow B_\mathfrak{P}$. Namely, the localization with respect to $A - \mathfrak{p}$ yields a finite flat extension $A_\mathfrak{p} \hookrightarrow B_\mathfrak{p}$. Since $\mathfrak{P}$ is the unique prime ideal of B lying above $\mathfrak{p}$, so $B_\mathfrak{p}$ is a local Dedekind ring, and hence we get $B_\mathfrak{p} = B_\mathfrak{P}$. Since A is regular, and hence locally factorial, the ideal $\mathfrak{p}$ is locally principal. The extended ideal $B\mathfrak{p}$ is locally principal and a power of $\mathfrak{P}$ and, hence, globally a power of $\mathfrak{P}$, that is, $\mathfrak{P}^e = B\mathfrak{p}$. The degree of the residue extension is denoted by $f := [Q(B/\mathfrak{P}) : Q(A/\mathfrak{p})]$. Moreover we have $p = e \cdot f$. In the case $f = p$ and $e = 1$ we have $\mathfrak{P} = B\mathfrak{p}$. Since $A \hookrightarrow B$ is faithfully flat, so $A/\mathfrak{p} \to B/\mathfrak{P}$ is faithfully flat as well. Then, due to [Matsumura 1980, Theorem 51], the ring $A/\mathfrak{p}$ is regular.

In the case $f = 1$, $e = p$, the ideal $\mathfrak{p}$ contains the uniformizer π of R. Since $\mathfrak{p}B = \mathfrak{P}^p$ due to $e = p$ and $\mathfrak{P} = B\pi'$ as Y is smooth over S, we obtain by faithfully flat descent $\mathfrak{p} = A\pi$. Therefore $A \otimes_R k$ is reduced and hence geometrically reduced. Then A is the set of all G-invariant functions f on Y that are bounded by 1 and also B consists of all functions on Y that are bounded by 1; see [Bosch et al. 1984, 6.4.3/4]. Moreover, it follows from [loc. cit.] that $A \otimes_R R'$ coincides with B. Thus we see that $A \otimes_R k = A \otimes_R R' \otimes_{R'} k' = B \otimes_{R'} k'$ is regular.

(2) $\Longrightarrow$ (1). For the converse implication, A is regular. Since B is regular as well, the extension $A \to B$ is faithfully flat; see [Serre 1965, IV, Proposition 22]. As above, we have the finite extension of discrete valuation rings $A_{\mathfrak{p}} \hookrightarrow B_{\mathfrak{P}}$ and its associated numbers e and f. In the case, $f = 1$ and $e = p$ the finite ring extension $A/\mathfrak{p} \to B/\mathfrak{P}$ is birational, and hence an isomorphism as $A/\mathfrak{p}$ is regular. So any local parameter of $A/\mathfrak{p}$ gives rise to a local parameter of $B/\mathfrak{P}$. Therefore, any maximal ideal of B is generated by a G-invariant element and π'. Therefore, $I_G = B \cdot I(\pi')$ is principal.

Now consider the case $f = p$ and $e = 1$. Since A is regular, the ideal $\mathfrak{p}$ is locally principal. So we may assume that $\mathfrak{p} = A\alpha$ is principal. Due to $e = 1$, we obtain $\mathfrak{P} = B\alpha$. Since $B/\mathfrak{P}$ is regular, any maximal ideal of B is generated by α and a lifting of a local parameter of $B/\mathfrak{P}$. Therefore, I_G is locally principal as it is generated by the $I(\beta)$, where β is a lifting of the local parameter $\overline{\beta}$ of $B/\mathfrak{P}$. □

Conjecture 11. In the case of an affine arithmetic surface, that is, Y is regular with irreducible special fiber, one conjectures that the following conditions are equivalent, where $\mathfrak{P} \subset B$ is the prime ideal whose locus is the special fiber and $\mathfrak{p} := A \cap \mathfrak{P}$:

(1) I_G is locally principal and $B/\mathfrak{P}$ is regular.

(2) A is regular and $A/\mathfrak{p}$ is regular.

The proof of the last proposition tells us that the implication (1) $\Longrightarrow$ (2) is true in the case $f = p$ and $e = 1$. In the case $f = 1$ and $e = p$, we used the fact that the formation of the ring of 1-bounded functions is compatible with base change; this is true when the multiplicity is 1. But it is not clear if one only knows that both models A and B have the same multiplicity in the special fiber over their base rings.

The implication (2) $\Longrightarrow$ (1) is true in the case $f = 1$ and $e = p$, as seen by the same arguments as given in Proposition 10. But the case $f = p$ and $e = 1$, is uncertain, although in this case the multiplicity behaves well.

Acknowledgements

S. Wewers [2010] has obtained partial versions of our results by different methods. It is our pleasure to thank the referee for a careful reading of the manuscript.

References

[Bosch et al. 1984] S. Bosch, U. Güntzer, and R. Remmert, *Non-Archimedean analysis: A systematic approach to rigid analytic geometry*, Grundlehren der Mathematischen Wissenschaften **261**, Springer, Berlin, 1984. MR 86b:32031 Zbl 0539.14017

[Bourbaki 1981] N. Bourbaki, *Éléments de mathématique: Groupes et algèbres de Lie, Chapitres 4, 5 et 6*, Masson, Paris, 1981. MR 83g:17001 Zbl 0483.22001

[Edixhoven 1992] B. Edixhoven, "Néron models and tame ramification", *Compositio Math.* **81**:3 (1992), 291–306. MR 93a:14041 Zbl 0759.14033

[Hirzebruch 1953] F. Hirzebruch, "Über vierdimensionale Riemannsche Flächen mehrdeutiger analytischer Funktionen von zwei komplexen Veränderlichen", *Math. Ann.* **126** (1953), 1–22. MR 16,26d Zbl 0093.27605

[Jung 1908] H. W. E. Jung, "Darstellung der Funktionen eines algebraischen Körpers zweier unabhängiger Veränderlicher x, y in der Umgebung einer Stelle $x = a$, $y = b$", *Journal für die Reine und Angewandte Mathematik* **133** (1908), 289–314. JFM 39.0493.01

[Matsumura 1980] H. Matsumura, *Commutative algebra*, 2nd ed., Mathematics Lecture Note Series **56**, Benjamin/Cummings, Reading, MA, 1980. MR 82i:13003 Zbl 0441.13001

[Serre 1965] J.-P. Serre, *Algèbre locale: Multiplicités* (Cours au Collège de France, 1957–1958), 2nd ed., Lecture Notes in Mathematics **11**, Springer, Berlin, 1965. MR 34 #1352 Zbl 0142.28603

[Serre 1968] J.-P. Serre, "Groupes finis d'automorphismes d'anneaux locaux réguliers", pp. 11 in *Colloque d'Algèbre, Exp. 8* (Paris, 1967), Secrétariat mathématique, Paris, 1968. MR 38 #3267 Zbl 0200.00002

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

[Tate 1975] J. Tate, "Algorithm for determining the type of a singular fiber in an elliptic pencil", pp. 33–52 in *Modular functions of one variable, IV* (Antwerp, 1972), edited by B. J. Birch and W. Kuyk, Lecture Notes in Math. **476**, Springer, Berlin, 1975. MR 52 #13850 Zbl 1214.14020

[Wewers 2010] S. Wewers, "Regularity of quotients by an automorphism of order p", preprint, 2010. arXiv 1001.0607

Communicated by David Eisenbud
Received 2011-04-14 Revised 2012-01-23 Accepted 2012-02-20

franz.j.kiraly@tu-berlin.de *Berlin Institute of Technology, Machine Learning Group, Marchstraße 23, 10587 Berlin, Germany*

Freie Universität Berlin, Discrete Geometry Group, Arnimallee 2, 14195 Berlin, Germany

Mathematisches Forschungsinstitut Oberwolfach, Schwarzwaldstraße 9-11, 77709 Oberwolfach, Germany

werner.luetkebohmert@uni-ulm.de
Dept. of Pure Mathematics, University of Ulm, Helmholtzstraße 18, 89069 Ulm, Germany

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2013 is US $200/year for the electronic version, and $350/year (+$40, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 7 No. 1 2013

Powers of ideals and the cohomology of stalks and fibers of morphisms 1
MARC CHARDIN

Graphs of Hecke operators 19
OLIVER LORSCHEID

Group actions of prime order on local normal rings 63
FRANZ KIRÀLY and WERNER LÜTKEBOHMERT

On the arithmetic and geometry of binary Hamiltonian forms 75
JOUNI PARKKONEN and FRÉDÉRIC PAULIN

L-functions and periods of adjoint motives 117
MICHAEL HARRIS

Galois module structure of local unit groups 157
ROMYAR SHARIFI

On the invariant theory for tame tilted algebras 193
CALIN CHINDRIS

Period functions and cotangent sums 215
SANDRO BETTIN and BRIAN CONREY

1937-0652(2013)7:1;1-C