PACIFIC JOURNAL OF MATHEMATICS
Vol. 113, No. 2, 1984

ORDINARY AND SUPERSINGULAR COVERS IN CHARACTERISTIC p

DAVID HARBATER

This paper studies Galois wildly ramified covers of the projective line in characteristic p. It is shown that for p-covers of tamely ramified covers, the monodromy is "generated by the branch cycles." But examples are given to show that this condition fails in general for towers taken in the opposite order and for other covers as well—even in the case of covers branched only over infinity. It is also shown that p-covers branched at a single point are supersingular and more generally that for any curve which arises as a p-cover, there is a bound on the p-rank which in general is less than the genus.

In 1957, S. Abhyankar observed [**Ab**] that while the monodromy group of a branched covering of the Riemann sphere is generated by loops around the branch points, the analogous condition fails to hold in characteristic p. He conjectured that the condition at least holds for tamely ramified covers. This is indeed the case, as A. Grothendieck showed by the technique of specialization (XIII, Cor. 2.12 of [**Gr**]). In §1 of this paper, we show that it also holds for Galois covers which are the "opposite" of tame—viz. those whose Galois group is a p-group. More generally, we show that Galois covers which arise as p-covers of tamely ramified covers are "ordinary" (i.e. satisfy the above condition). But as §1 shows, towers taken in the opposite order need not satisfy this condition, nor does every "extraordinary" cover arise in this manner. We also discuss the connection to the problem of groups occurring as Galois groups over the affine line. Section 2 relates these ideas to supersingularity, and more generally to the phenomenon of a curve having fewer étale p-covers than "expected" for its genus. It is shown that an ordinary cover of the projective line which is branched over a single point must be supersingular. More generally, a bound is given on the number of étale $\mathbf{Z}/p$-covers of a curve which arises as a branched p-cover of another curve, in terms of the degree and the ramification groups.

We fix our terminology: All curves are assumed to be smooth, and defined over an algebraically closed field k. If X is a connected curve, then a (branched) cover $Z \to X$ is a morphism of curves which is finite and generically separable. The branch locus is thus finite, and $Z \to X$ is étale if the branch locus is empty. A cover $Z \to X$ is called *Galois* with group G if

Z is connected and if the Galois group G (of automorphisms of Z over X) acts simply transitively on the generic fibre. A Galois cover whose group is a p-group is called a *p-cover*. A group G is said to "occur (as a Galois group) over X" if there is a Galois étale cover $Z \to X$ with group G. Given a finite group G, a *G-cover* consists of a cover $Z \to X$ (Z not necessarily connected) together with an inclusion of G into the Galois group, such that G acts simply transitively on generic fibres. If in addition $Z \to X$ is étale, it is called a *principal* G-cover.

I wish to thank M. Artin, M. Fried, and V. Srinivas for helpful conversations about material in this paper.

1. Ordinary covers. Let $\pi\colon Z \to X$ be a Galois covering of curves, having branch locus $\{x_1,\dots,x_n\}$. Following Abhyankar [**Ab**], we say that the monodromy of the cover is *generated by loops around the branch points* if there exist points $z_1,\dots,z_n \in Z$ with $x_i = \pi(z_i)$, such that the stabilizers of $z_1,\dots,z_n$ together generate the Galois group. If $X = \mathbf{P}^1$, we will also call such a cover *ordinary*. (Any other Galois cover of $\mathbf{P}^1$ is *extraordinary*.) If the characteristic of the ground field k is 0, then every Galois cover of $\mathbf{P}^1$ is ordinary (e.g. Theorem T in §7 of [**Ab**]); in general, tamely ramified Galois coverings of $\mathbf{P}^1$ are ordinary (XIII, Cor. 2.12 of [**Gr**]). Assume now (and for the rest of the paper) that k is of finite characteristic p. Below we show (Theorem 1.5) that a Galois cover of $\mathbf{P}^1$ must be ordinary if it arises as a p-cover of a tamely ramified cover of $\mathbf{P}^1$.

1.1. PROPOSITION. *Let G be a p-group and let $Z \to X$ be a G-cover of curves. Let $H \subset G$ and let $Y \to X$ be the subcover corresponding to H. Say $\{x_1,\dots,x_n\}$ is the branch locus of $Z \to X$, let $z_1,\dots,z_n \in Z$ be points lying over $x_1,\dots,x_n$ respectively, and let $P_i \subset G$ be the stabilizer of z_i in G. If $P_1,\dots,P_n$, H generate G, then Y is connected.*

Proof. Let Y' be a connected component of Y, and let z' be a connected component of Z lying over Y'. Let $z_1',\dots,z_n' \in Z'$ be points lying over $x_1,\dots,x_n$ respectively, and let $P_1',\dots,P_n'$ be their stabilizers in G. Let $K \subset G$ consist of the elements $\sigma \in G$ such that $\pi \circ \sigma(Z') = Y'$, where $\pi\colon Z \to Y$ is the canonical morphism. Then K is a subgroup containing $P_1',\dots,P_n'$, H. If $K \neq G$ then K is contained in a proper normal subgroup $N \lhd G$, since G is a p-group [**Hl**, 4.3.2]. Thus N contains the stabilizer of every ramification point of $Z \to X$. So N contains $P_1,\dots,P_n$, H, and hence equals G. This is a contradiction. So actually $K = G$. Thus $\pi(Z) = Y'$. So $Y = Y'$, i.e., Y is connected. $\square$

Taking H to be the trivial group, we obtain

1.2. COROLLARY. *Let G be a p-group and let $Z \to X$ be a G-cover of curves whose monodromy is generated by loops around the branch points. Then Z is connected.*

Call a curve X *supersingular* if X has no nontrivial principal $\mathbf{Z}/p$-covers, or equivalently if no Galois étale cover of X has group $\mathbf{Z}/p$. (In this terminology, the projective line is supersingular.) Since every maximal subgroup of a p-group is normal and of index p [**Hl**, 4.3.2], such a curve has no non-trivial étale p-covers.

1.3. PROPOSITION. *Let X be a supersingular curve, let G be a p-group, and let $Z \to X$ be a G-cover. The following are equivalent:*

(i) *Z is connected;*

(ii) *The monodromy of $Z \to X$ is generated by loops around the branch points;*

(iii) *If $\{z_1, \ldots, z_n\}$ is any lift of the branch locus of X, then the stabilizers of the points z_i together generate G.*

Proof. Since (iii) $\Rightarrow$ (ii) is trivial, and (ii) $\Rightarrow$ (i) by 1.2, it suffices to show (i) $\Rightarrow$ (iii). Let $H \subset G$ be the subgroup generated by the stabilizers of $z_1, \ldots, z_n$. If H is a proper subgroup of G, then H is contained in a proper normal subgroup N of G. Let $Y \to X$ be the subcover of $Z \to X$ corresponding to N. Then $Y \to X$ is an étale p-cover. This contradicts the supersingularity of X. □

1.4. COROLLARY. *Every p-cover of $\mathbf{P}^1$ is ordinary.*

More generally, we have

1.5. THEOREM. *A Galois cover of $\mathbf{P}^1$ is ordinary, provided that it is a p-cover of a tamely ramified cover of $\mathbf{P}^1$.*

Proof. Let $Z \to \mathbf{P}^1$ be a Galois cover which is a p-cover of a tame cover $Y \to \mathbf{P}^1$. We may assume that Y is maximal among tame subcovers of $Z \to \mathbf{P}^1$. Let G, P be the Galois groups of $Z \to \mathbf{P}^1$, $Z \to Y$. Then $P \lhd G$, since the Galois closure of $Y \to \mathbf{P}^1$ is a subcover of Z, and is also tame (e.g. by Prop. 7 of [**Ab**]). Since $Y \to \mathbf{P}^1$ is tame, it is ordinary. So over the branch points $x_1, \ldots, x_n$ of $Z \to X$ there exist $y_1, \ldots, y_n \in Y$ whose stabilizers in G/P generate G/P. Choose $z_i \in Z$ over y_i, for $1 \leq i \leq n$. Let H_i

be the stabilizer of z_i in G, and let $H \subset G$ be the group generated by the subgroups H_i. Then H and P generate G.

Observe that if $y \in Y$ lies over a branch point x_i, then some point of Z lying over y has its stabilizer lying in H. Namely, since H and P generate G, there exists $h \in H$ such that $h(z_i)$ lies over y. Since the stabilizer of $h(z_i)$ is equal to that of z_i conjugated by h, it follows that the stabilizer of $h(z_i)$ lies in H.

Since H and P generate G, it suffices to show $P \subset H$; for then $H = G$. Suppose otherwise. Then $H \cap P$ is a proper subgroup of P, and so is contained in a proper normal subgroup $N \lhd P$. Since N contains $H \cap P$, by the previous paragraph it follows that for each $y \in Y$ over x_i there is a $z \in Z$ over y whose stabilizer in P is contained in N. Since N is normal in P, the stabilizer of every ramification point of $Z \to Y$ is contained in N. Let $\overline{Y} \to Y$ be the subcover of $Z \to Y$ corresponding to N. Then $\overline{Y} \to Y$ is unramified and of degree greater than 1. So $\overline{Y} \to \mathbf{P}^1$ is tamely ramified. This contradicts the maximility of Y. $\square$

The proof of 1.5 actually shows more: Let $Y \to X$ be a tame Galois cover of curves branched at $x_1,\ldots,x_n$, and let $y_1,\ldots,y_n$ be points over $x_1,\ldots,x_n$ whose stabilizers generate the Galois group. If Z is a p-cover of Y which is Galois over X, and $z_1,\ldots,z_n \in Z$ lie respectively over $y_1,\ldots,y_n$, then the stabilizers of $z_1,\ldots,z_n$ generate the Galois group of $Z \to X$.

Since every p'-cover (i.e. Galois cover whose group has order prime to p) is tamely ramified, we have

1.6. Corollary. *If G is a group with a normal (equivalently, unique) Sylow p-subgroup, then every Galois cover of $\mathbf{P}^1$ with group G is ordinary.*

In the case of Galois covers of $\mathbf{P}^1$ branched at a single point, an ordinary cover is simply one which is totally ramified there. Since there are no tame covers of $\mathbf{P}^1$ branched at only one point, such a cover must be a p-cover.

While Galois covers arising as p-covers of tame covers are ordinary, covers taken in the opposite order need not be. For example, let $Z \to \mathbf{P}^1$ be a Galois cover with group $\mathbf{Z}/p$, branched only at ∞. Such a cover may uniquely be written

$$z^p - z = \sum_{i=0}^{n} c_i x^i,$$

where $p \nmid n$ and $c_i = 0$ for $p \mid i$. The genus of Z is $(p-1)(n-1)/2$ [**Mi**], and in particular is positive whenever $n > 2$. Thus Z has unramified Galois covers of degree d, for all d prime to p. Given such a cover $Y \to Z$, let $V \to \mathbf{P}^1$ be the Galois closure of $Y \to \mathbf{P}^1$. Then V is branched only at ∞, but is not totally ramified there. Hence $V \to \mathbf{P}^1$, which arises as an étale cover of a p-cover, is extraordinary.

1.7. EXAMPLE. In characteristic 3, let $Z \to \mathbf{P}^1$ be the cyclic cover given (in affine coordinates) by

$$z^3 - z = x^2.$$

Then Z is of genus 1. Consider the étale cover $Y \to Z$, cyclic of degree 2, which is the normalization of

$$y^2 = z(z-1).$$

The Galois closure of $Y \to \mathbf{P}^1$ is a degree 2 cyclic cover of Y, and is the normalization of

$$y_1^2 = z(z+1), \quad y_2^2 = (z-1)(z+1), \quad yy_1y_2 = z(z-1)(z+1).$$

The group of this Galois closure is the alternating group A_4. The Galois closure is branched only at ∞, and the fibre there consists of four points, each with ramification index 3. □

As remarked above, only p-groups may occur as Galois groups of ordinary covers of $\mathbf{P}^1$ branched precisely at ∞. The existence of extraordinary covers, however, complicates the study of the fundamental group of the affine line, since other groups may thus occur over $\mathbf{A}^1$. Example 1.7 may lead one to suspect, though, that extraordinary covers must dominate p-covers, and thus that the corresponding groups must have a normal subgroup of index p. But this is not the case, as we show below (Prop. 1.11). First some lemmas are needed.

The following lemma was observed by V. Srinivas and A. Wassermann, and appears in [**KS**].

1.8. LEMMA. *Let $Y \to X$ be a connected degree p cover, and $Z \to X$ its Galois closure. If Z dominates a p-cyclic cover of X, then Y is Galois over X.*

This follows from the fact that the Galois group of Z is contained in the symmetric group S_p, which has no subgroup of index p^2. Namely, if Y were unequal to the given p-cyclic cover of X, the smallest subcover of Z dominating both would have degree p^2, a contradiction.

1.9. LEMMA. *Let $Y \to X$ be a cover whose branch locus contains a point $x \in X$. Suppose that for each $y \in Y$ over x, the extension $\hat{\mathcal{O}}_{X,x} \subset \hat{\mathcal{O}}_{Y,y}$ is of degree p but is not Galois. Then the Galois closure of $Y \to X$ does not dominate any p-cyclic Galois cover of X which is branched at x.*

Proof. Let $Z \to X$ be the Galois closure of $Y \to X$, and let $z \in Z$ lie over x. We may regard $\hat{\mathcal{O}}_{Z,z}$ as containing $\hat{\mathcal{O}}_{Y,y}$, and thus also containing the Galois closure $\hat{\mathcal{O}}^{\sim}_{Y,y}$ of $\hat{\mathcal{O}}_{Y,y}$ over $\hat{\mathcal{O}}_{X,x}$. In fact $\hat{\mathcal{O}}_{Z,z}$ is the compositum of its subrings $\hat{\mathcal{O}}^{\sim}_{Y,y}$, as $y \in Y$ ranges over the points lying over x (Lemma 1 of §5 of [**Ab**]). The Galois group of each $\hat{\mathcal{O}}_{X,x} \subset \hat{\mathcal{O}}^{\sim}_{Y,y}$ is a subgroup of S_p with no $\mathbf{Z}/p$-quotient (by 1.8), and it is a quotient of the Galois group G of $\hat{\mathcal{O}}_{X,x} \subset \hat{\mathcal{O}}_{Z,z}$. To prove the lemma, it is enough to show that G has no normal subgroup of index p. Since all stabilizers in characteristic p are cyclic-by-p (i.e. have normal Sylow p-subgroup with cyclic quotient), it suffices to show

Claim. Let G be a cyclic-by-p group and $N_1, \ldots, N_n \lhd G$ such that $\bigcap_i N_i = \{1\}$. Suppose that each G/N_i has no $\mathbf{Z}/p$-quotient and its Sylow p-subgroup has order p. Then G has no normal subgroup of index p.

Here G is a semi-direct product of its unique Sylow p-subgroup $P \lhd G$ with a cyclic group $C \subset G$ of order m, where $p \nmid m$. Each G/N_i is a semi-direct product of a (normal) cyclic subgroup of order p with a cyclic group of order m_i, where $m_i | m$, and it has no quotient of order p. Replacing N_i by $N_i \cap P$, we may assume that $N_i \subset P$ and $m_i = m$. Each N_i is then normal and of index p in P, and $\bigcap N_i = \{1\}$, so P has trivial Frattini subgroup. Thus P is an elementary p-group [**Hl**, 12.2.1]. Since $\bigcap_1^n N_i = \{1\}$, the rank of P is at most n. By eliminating some of the groups N_i, we may assume that no proper subset of $\{N_1, \ldots, N_n\}$ has trivial intersection, and thus that n equals the rank of P. Let $Q_i = \bigcap_{j \neq i} N_j \lhd G$. Then $\# Q_i = p$, and $Q_i \cap N_i = \{1\}$. Also, $\bigcap Q_i = \{1\}$ since $Q_1 \cap Q_2 \subset \bigcap N_i = \{1\}$. Since $\# Q_i = p$, and $Q_1, \ldots, Q_n$ lie in an elementary p-group P of rank n, it follows that $Q_1, \ldots, Q_n$ generate P. Let q_i be a generator of Q_i. Then $q_k \in N_j$ for $j \neq k$. Since $\bigcap_i N_i = \{1\}$, it follows that for all k, $q_k \notin N_k$. Thus the image of q_k in G/N_k has order p, and thus is a generator of the Sylow p-subgroup of G/N_k. Since $Q_i \lhd G$, the subgroup $P_i \subset G$ generated by Q_i and C is of order pm. So $P_i \xrightarrow{\sim} G/N_i$ under $G \to G/N_i$. Thus P_i has no normal subgroup of index p. Also, $P_1, \ldots, P_n$ generate G, since $Q_1, \ldots, Q_n$ generate P. Now suppose G had a normal subgroup H of index p. Then for each i, $(P_i : H \cap P_i) = 1$ or p. The latter case is impossible since P_i has no normal subgroup of index p. So $P_i \subset H$ for all i. Since $P_1, \ldots, P_n$ generate G, it follows that $H = G$. This is a contradiction, proving the claim, and the lemma. $\square$

1.10. LEMMA. *Let $Y = \operatorname{Spec} k[[t]]$ and $Z \to Y$ a Galois cover of degree p^n. Then the length of the $k[[t]]$-module $\Omega_{Z/Y}$ of relative differential forms is an even integer, and is at least $2p^n - 2$.*

Proof. Regarding $k[[t]]$ as the completion of the local ring of $\mathbf{P}^1$ at ∞, we obtain a morphism ϕ: $Y \to \mathbf{P}^1$. Let G be the Galois group of $Z \to Y$. By Corollary 2.4 of **[Ha]**, there is a Galois covering $V \xrightarrow{\pi} \mathbf{P}^1$ with group G, branched only at ∞ (where it is totally ramified), such that $Z \to Y$ is the pullback of π by ϕ. Applying the Hurwitz formula to $V \to \mathbf{P}^1$ yields

$$2g(V) - 2 = p^n(-2) + \operatorname{length} \Omega_{Z/Y},$$

where $g(V)$ is the genus of V. Since $g(V)$ is a nonnegative integer, the conclusion follows. $\square$

We can now show

1.11. PROPOSITION. *If the characteristic of k is an odd prime p, then there exist Galois covers of $\mathbf{P}^1$, branched only at ∞, which do not dominate any p-cyclic cover of $\mathbf{P}^1$. Such covers are extraordinary.*

Proof. Since (as observed after Corollary 1.6) every ordinary Galois cover of $\mathbf{P}^1$, branched only at ∞, is a p-cover, and since every p-group has $\mathbf{Z}/p$ as a quotient, the second sentence is immediate.

We now give examples of such covers in each odd characteristic. Let $a \in k$ be non-zero, and let $\alpha \in k$ be the unique pth root of a. Let π: $Z \to \mathbf{P}^1$ be the cover of the projective x-line given in affine coordinates by

$$z^{2p} - z - x(z^p - a) = 0.$$

Thus Z is the projective z-line, and π is of degree $2p$. The only branching is at $x = \infty$. The fibre there consists of the two points $z = \alpha, \infty$, with ramification index p at each of these points. Let n_1, n_2 be the lengths of the $\mathcal{O}_{\mathbf{P}^1,\infty}$-modules of relative differentials at these two points. Then by the Hurwitz formula,

$$-2 = 2p(-2) + n_1 + n_2,$$

i.e. $n_1 + n_2 = 4p - 2$.

Passing to the complete local ring at $x = \infty$, $z = \infty$, and using local coordinates $\bar{x} = x^{-1}$, $\bar{z} = z^{-1}$, we have

$$\bar{x} = \bar{z}^p(1 - a\bar{z}^p)(1 - \bar{z}^{-2p-1})^{-1} = \bar{z}^p - a\bar{z}^{2p} + \bar{z}^{3p-1} + \cdots;$$
$$d\bar{x} = \left(-\bar{z}^{3p-2} + \cdots\right) d\bar{z}.$$

So $n_2 = 3p - 2$, hence $n_1 = p$. Thus n_1 and n_2 are odd. So by Lemma 1.10, the complete localization of Z at either point is not Galois over $\hat{\mathcal{O}}_{\mathbf{P}^1,\infty}$ (but is of degree p). By Lemma 1.9, the Galois closure of $Z \to \mathbf{P}^1$ dominates no p-cyclic cover branched at $x = \infty$. Since Z is étale elsewhere, and $\mathbf{P}^1$ is simply connected, the Galois closure is as desired. □

By Lemma 1.8, a connected degree p étale cover of $\mathbf{A}^1$ must be Galois, provided that its Galois closure dominates a p-cyclic cover of $\mathbf{A}^1$. But by Proposition 1.11, not every Galois étale cover of $\mathbf{A}^1$ need dominate such a p-cyclic cover. Still, T. Kambayashi asks **[Ka]** whether *every* connected degree p étale of $\mathbf{A}^1$ is Galois. Equivalently, for G to occur as a Galois group over $\mathbf{A}^1$, is it necessary that every subgroup of index p be normal? This is trivial for $p = 2$. Kambayashi and V. Srinivas here observed **[KS]** that this is also true for $p = 3$, since otherwise the Galois closure would be an étale cover of $\mathbf{A}^1$ with group S_3—an impossibility in characteristic 3.

But for $p \geq 5$, a negative answer to Kambayashi's question would be implied by a conjecture of Abhyankar. Namely, Abhyankar conjectured **[Ab**, §4] that for an affine curve X, a group G occurs over X if and only if the p'-group G/N does, where N is the (normal) subgroup generated by the Sylow p-subgroups of G. In the case of the affine line, this may be rephrased as follows. Call a finite group G a *quasi-p-group* if G is generated by its Sylow p-subgroups, or equivalently if G has no quotients of order prime to p other than the trivial group. Then Abhyankar's conjecture says that the groups which occur over $\mathbf{A}^1$ are precisely the quasi-p-groups. For $p \geq 5$, this would imply that the alternating group A_p occurs as the Galois group of a Galois cover $Z \to \mathbf{P}^1$ in characteristic p. Regard $A_{p-1} \subset A_p$, and let $Y \to \mathbf{P}^1$ be the subcover corresponding to A_{p-1}. Then $Y \to \mathbf{P}^1$ is of degree p and is étale over $\mathbf{A}^1$, yet is not Galois. Thus for $p \geq 5$, an affirmative answer to Kambayashi's question is incompatible with Abhyankar's conjecture.

2. Supersingular covers. This section relates the previous ideas to supersingularity. Proposition 2.3 shows that the smooth completion of every étale p-cover of the affine line is supersingular. More generally, 2.5 and 2.6 give a bound on the number of principal $\mathbf{Z}/p$-covers which a

p-cover $X \to Y$ may have. This bound is generically less than the expected number p^g, where g is the genus of X. First we need

2.1. LEMMA. *Let G be a finite group, and $H \lhd K \lhd G$ such that the index $(K: H)$ is a power of p. Then H contains a subgroup N which is normal in G, such that $(K: N)$ is a power of p.*

Proof. Let $H = H_1, H_2, \ldots, H_n$ be the conjugates of H in G. Thus all $H_i \lhd K$. Let $J_i = H_1 \cap \cdots \cap H_i$ for $i = 1, \ldots, n$. It suffices to prove that the index of each J_i in K is a power of p; for then we may take $N = J_n$. We proceed by induction on i. By assumption, $J_1 = H$ has p-power index in K. Suppose the same holds for J_i. Since H_{i+1} is normal in K of p-power index, it follows that $J_{i+1} = H_{i+1} \cap J_i$ is normal in J_i of p-power index. So the index of J_{i+1} in K is a power of p. □

2.2. COROLLARY. *If $X \to Y$ and $Y \to Z$ are p-covers, then so is the Galois closure of $X \to Z$.*

2.3. PROPOSITION. *Every p-cover of the projective line which is branched at a single point is supersingular.*

Proof. Let $Z \to \mathbf{P}^1$ be such a cover branched only at ∞. Suppose $Y \to Z$ is a Galois étale cover with group $\mathbf{Z}/p$. Then the fibre of $Y \to \mathbf{P}^1$ consists of p points. Now by Corollary 2.2, the Galois closure $\tilde{Y} \to \mathbf{P}^1$ of $Y \to \mathbf{P}^1$ is a p-cover. By the remark after Corollary 1.6, $\tilde{Y} \to \mathbf{P}^1$ is totally ramified over ∞. Hence so is $Y \to \mathbf{P}^1$, which is a contradiction. □

2.4. EXAMPLE. By [Mi], the genus 1 $\mathbf{Z}/3$-covers of $\mathbf{P}^1$ in characteristic 3, branched only at ∞, are precisely those given by

$$(*) \qquad z^3 - z = cx^2 + dx \qquad (c \neq 0),$$

where c, d lie in the ground field. By Proposition 2.3, all such covers are supersingular. But up to isomorphism, there is a unique supersingular elliptic curve in characteristic 3, viz. the curve $v^3 - v = u^2$. And indeed, the change of variables

$$u = \sqrt{c}\,x - d/\sqrt{c},$$
$$v = z + \xi \qquad (\text{where } \xi^3 - \xi = d^2/c)$$

transforms the curve $(*)$ into this form. (Question: In general, to what extent are supersingular curves "accounted for" in this manner?) □

Proposition 2.3 does not hold if more than one branch point is allowed. For example, let $Y_1 \to \mathbf{P}^1$ and $Y_2 \to \mathbf{P}^1$ be p-cyclic Galois covers branched respectively at 0 and ∞. Let $Y = Y_1 \times_{\mathbf{P}^1} Y_2$. Thus $Y \to \mathbf{P}^1$ is Galois with group $\mathbf{Z}/p \times \mathbf{Z}/p$. Let $Z \to \mathbf{P}^1$ be the quotient of Y by the diagonal subgroup. Then $Y \to Z$ is étale and cyclic of degree p, so Z is not supersingular.

Still, under quite general hypotheses, a weaker version of 2.3 holds. We consider an invariant which measures how far a curve is from being supersingular. For a curve X in characteristic p, define $\sigma = \sigma(X)$ to be the rank of the elementary p-group consisting of the p-torsion points on the Jacobian of X. Then

$$0 \leq \sigma(X) \leq g(X),$$

and $\sigma = g$ for a generic curve of genus g. There are exactly p^σ principal $\mathbf{Z}/p$-covers of X, and so a curve X is supersingular if and only if $\sigma(X) = 0$. (Since $\mathbf{Z}/p$ is abelian, p^σ is also the number of *pointed* principal $\mathbf{Z}/p$-covers of X, if a base point of X is chosen.) Moreover the p^n-torsion points on the Jacobian form the group $(\mathbf{Z}/p^n)^\sigma$, so there are exactly $p^{n\sigma}$ principal $\mathbf{Z}/p^n$-covers of X. The integer σ can also be described as the rank of the Nth iterate (for $N \gg 0$) of the p-linear Frobenius map F: $H^1(X, \mathcal{O}) \to H^1(X, \mathcal{O})$. In the case of elliptic curves, σ is the Hasse invariant. See **[Se]** for details.

For any p-group G, let r_G be the minimum possible length of the $k[[t]]$-module of relative differentials $\Omega_{Z/Y}$, where Z ranges over all Galois covers of $Y = \mathrm{Spec}[[t]]$ having group G. By Lemma 1.10, $r_G \geq 2 \cdot \#G - 2$. Applying the Hurwitz formula to the genus 0 cover $z^p - z = x$ of the line, we see that $r_G = 2p - 2$ if G is cyclic of order p. (Is $r_G = 2 \cdot \#G - 2$ in general?)

The following result gives an upper bound on $\sigma(Z)$ and a lower bound on $g(Z)$, where $Z \to X$ is a p-cover. It relies on results of **[Ha]**.

2.5. THEOREM. *Let $Z \to X$ be a p-cover with group G. Let $x_1, \ldots, x_n$ be the branch points, let $z_i \in Z$ be a point over x_i, and let $P_i \subset G$ be the stabilizer of z_i. Then*

$$2\sigma(Z) - 2 \leq \#G\left(2g(X) - 2 + \sum_{i=1}^{n} r_{P_i}/\#P_i\right) \leq 2g(Z) - 2.$$

Proof. The second inequality follows immediately from the Hurwitz formula and the definition of r_G.

For the first inequality, we begin by reducing to the case that the monodromy of $Z \to X$ is generated by loops around the branch points. To do this, let $Y \to X$ be a maximal unramified subcover of $Z \to X$. Then Y is unique, and the Galois group of $Z \to Y$ is a normal subgroup $H \lhd G$, since any two unramified subcovers are dominated by a third. So $Y \to X$ is Galois, with group G/H, say of order m. Let $y_{i1}, \ldots, y_{im} \in Y$ be the points over x_i, and choose a point $z_{ij} \in Z$ over y_{ij}. The stabilizer P_{ij} of z_{ij} in H is the same as the stabilizer of z_{ij} in G, since $Y \to X$ is unramified; so $P_{ij} \approx P_i$.

We claim that $\{P_{ij}\}_{ij}$ generates H, and thus that the monodromy of $Z \to Y$ is generated by loops around the branch points. If not, the subgroups P_{ij} generate a proper subgroup of H which, since H is a p-group, lies in a proper normal subgroup $N \lhd H$ [**Hl**, 4.3.2]. The stabilizer in H of every point in Z must lie in N, since $N \lhd H$ and N already contains the stabilizer of some point in each fibre of $Z \to Y$. The subcover of $Z \to Y$ corresponding to N is thus unramified over Y, and hence over X. The maximality of Y implies $N = H$, which is a contradiction. This proves the claim.

It suffices to verify the theorem with X replaced by Y. For then,

$$2\sigma(Z) - 2 \leq \#H\left(2g(Y) - 2 + \sum_{i=1}^{n} \sum_{j=1}^{m} r_{P_{ij}}/\#P_{ij}\right).$$

But

$$2g(Y) - 2 = \#(G/H)(2g(X) - 2).$$

So

$$\begin{aligned} 2\sigma(Z) - 2 &\leq \#H\left(\#(G/H)(2g(X) - 2) + \sum_{i=1}^{n} mr_{P_i}/\#P_i\right) \\ &= \#G\left(2g(X) - 2 + \sum_{i=1}^{n} r_{P_i}/\#P_i\right) \end{aligned}$$

as desired. So we are reduced to the case that the monodromy of $Z \to X$ is generated by loops around the branch points.

For any p-group A, let M_A^{loc} be the moduli space of pointed A-covers of $\operatorname{Spec} k[[x]]$, and let $M_A^{0\,\mathrm{loc}}$ be the subspace corresponding to connected A-covers (cf. §2 of [**Ha**]). Pick a base point of X other than $x_1, \ldots, x_n$, and pick a base point for Z over that. Let M_A be the moduli space of pointed principal A-covers of $X - \{x_1, \ldots, x_n\}$. For $1 \leq i \leq n$, let $\zeta_i \in M_{P_i}^{0\,\mathrm{loc}}$ correspond to the extension $\hat{\mathcal{O}}_{X,x_i} \subset \hat{\mathcal{O}}_{Z,z_i}$, and let ξ_i be a point of $M_{P_i}^{0\,\mathrm{loc}}$

such that the module of relative differentials of the corresponding finite extension of $k[[x]]$ is of minimal length (viz. r_{P_i}). As in the proof of Corollary 2.10 of **[Ha]**, the inclusion $P_i \hookrightarrow G$ induces a morphism ϕ_i: $M_{P_i}^{\mathrm{loc}} \hookrightarrow M_G^{\mathrm{loc}}$. Let ζ, $\xi \in (M_G^{\mathrm{loc}})^n$ be the respective images of $(\zeta_1, \ldots, \zeta_n)$ and $(\xi_1, \ldots, \xi_n)$under $\phi = (\phi_1, \ldots, \phi_n)$. Let π_G: $M_G \to (M_G^{\mathrm{loc}})^n$ be the Hurwitz morphism (2.6) of **[Ha]**, assigning to each G-cover the ramification moduli over the branch points. By Proposition 2.7 of **[Ha]**, this is an étale cover, and its degree is the number of pointed principal G-covers of X. Choose a point of M_G lying over ξ, and let $W \to X$ be the corresponding pointed G-cover of X. By construction there is a point $w_i \in W$ over x_i whose stabilizer is $P_i \subset G$. Since $P_1, \ldots, P_n$ generate G, W is connected by Corollary 1.2. By the Hurwitz formula,

$$2g(W) - 2 = \#G(2g(X) - 2) + \sum_{i=1}^{n} r_{P_i}(G: P_i).$$

Since $\sigma(W) \leq g(W)$, this proves the theorem for W. It remains to show that $\sigma(Z) = \sigma(W)$.

For any principal $\mathbf{Z}/p$-cover $S \to X$, let $S_Z \to Z$ be the pullback. Thus is also a principal $\mathbf{Z}/p$-cover. The association $S \mapsto S_Z$ corresponds to the group homomorphism

$$\mathrm{Hom}(\pi_1(X), \mathbf{Z}/p) \to \mathrm{Hom}(\pi_1(Z), \mathbf{Z}/p)$$

induced by $Z \to X$. We claim that this homomorphism is injective. For suppose $S \to X$ is a principal $\mathbf{Z}/p$-cover corresponding to a point in the kernel. Thus $S_Z \to Z$ is trivial. Since the monodromy of $Z \to X$ is generated by loops around the branch points, the same is true for the pullback $S_Z \to S$. Thus by Corollary 1.2, S_Z is connected, provided S is. Since $S_Z \to Z$ is trivial, S must be disconnected, and hence is trivial. So indeed the kernel is trivial.

Thus there are exactly $p^{\sigma(X)}$ principal $\mathbf{Z}/p$-covers of Z which are induced by such a cover of X. The same is true with Z replaced by W. So it remains to show that Z and W have the same number of principal $\mathbf{Z}/p$-covers which are not induced by a principal $\mathbf{Z}/p$-cover of X. Since $\mathbf{Z}/p$ is abelian, we may equivalently consider pointed principal $\mathbf{Z}/p$-covers.

Given such a pointed $\mathbf{Z}/p$-cover $V \to Z$, let $\tilde{V} \to X$ be the Galois closure of $V \to X$. By Corollary 2.2, the Galois group P of $\tilde{V} \to X$ is a p-group. Let A, $B \subset P$ be the subgroup corresponding to V, Z. For any point $v \in \tilde{V}$ over z_i, the stabilizer of v is a subgroup of P which maps isomorphically to P_i under the quotient map $P \to G$. So there exist $P_1', \ldots, P_n' \subset P$ which map isomorphically to P_i under $P \to G$, such that the point of M_P corresponding to $\tilde{V}$ is sent, under the Hurwitz morphism π_P: $M_P \to (M_P^{\mathrm{loc}})^n$, to a point lying in the image of $\prod_{i=1}^n M_i^{0\,\mathrm{loc}}$. The cover $V \to X$ thus determines data $P, A, B, P_1', \ldots, P_n'$ satisfying:

(i) P is a p-group, and $A \lhd B \lhd P$;

(ii) $(B:A) = p$, and A contains no non-trivial normal subgroup of P;

(iii) $P/B \approx G$, and the quotient map $P \to G$ maps P_i' isomorphically onto P_i;

(iv) $P_1', \ldots, P_n'$, A generate P.

Here (i)–(iii) are clear. To verify (iv), note first that $P_1', \ldots, P_n'$, B generate P, since $P_1, \ldots, P_n$ generate G. So by (ii), the group $Q \subset P$ generated by $P_1', \ldots, P_n'$, A is of index 1 or p. If (iv) is false, then Q is a normal subgroup of index p, since P is a p-group [**HI**, 4.3.2]. Let $S \to X$ be the subcover of $\tilde{V} \to X$ corresponding to Q. Thus $S \to X$ is cyclic of degree p. Since $P_1', \ldots, P_n' \subset Q$ and $Q \lhd P$, all the stabilizers of ramification points of $\tilde{V} \to X$ lie in Q. So $S \to X$ is étale. Since $P_1', \ldots, P_n'$, B generate P, it follows that $B \not\subset Q$. But Q is of index p in P, so Q and B generate P. since $Q \lhd P$, $(P\colon Q \cap B) = p(P\colon B) = p \cdot \#G$. Thus the smallest subcover $V_1 \to X$ of $\tilde{V} \to X$ dominating Z and S is of degree $p \cdot \#G$. This is also the degree of $Z \times_X S \to X$, and of $V \to X$ (which dominates Z and S). The morphisms $V \to V_1 \to Z \times_X S$ are thus isomorphisms, and so V arises as a pullback of a principal $\mathbf{Z}/p$-cover of X. This is a contradiction, proving (iv).

So given any pointed principal $\mathbf{Z}/p$-cover of Z (or similarly, of W) which is not induced by such a cover of X, we obtain data $(P, A, B, P_1', \ldots, P_n')$ satisfying (i)–(iv) above. In order to complete the proof that $\sigma(Z) = \sigma(W)$, it suffices to show that the number of such covers of Z inducing given data is equal to the number of such covers of W. Specifically, we claim that this number is $\#\mathrm{Hom}(\pi_1(X), P)/\#\mathrm{Hom}(\pi_1(X), G)$.

To see this, consider the diagram

$$\begin{tikzcd}
M_P \arrow[rr, "\alpha"] \arrow[d, "\pi_P"'] & & M_G \arrow[d, "\pi_G"] \\
(M_P^{\mathrm{loc}})^n \arrow[rr] & & (M_G^{\mathrm{loc}})^n \\
& \prod_i M_{P_i}^{\mathrm{loc}} \arrow[ul, hook, "i_P"] \arrow[ur, hook', "i_G"'] &
\end{tikzcd}$$

Here π_P and π_G are the Hurwitz morphisms, and are étale coverings of degrees $\#\mathrm{Hom}(\pi_1(X), P)$ and $\#\mathrm{Hom}(\pi_1(X), G)$ respectively. The morphisms i_P and i_G are the inclusions induced by $P_i \xrightarrow{\sim} P_i' \hookrightarrow P$ and by $P_i \hookrightarrow G$.

Pulling back to $\prod_i M_{P_i}^{\mathrm{loc}}$, we obtain

$$\begin{array}{ccc} M'_P & \overset{\alpha'}{\to} & M'_G \\ \pi'_P \searrow & & \swarrow \pi'_G \\ & \prod\limits_i M_{P_i}^{\mathrm{loc}} & \end{array}$$

Here π'_P and π'_G are covering maps of degrees equal to those of π_P and π_G, respectively. So α' is a covering map whose degree is the quotient of these integers. Let $\bar{\zeta} \in M'_G \subset M_G$ be the point corresponding to $Z \to X$. Each point in the fibre $\alpha'^{-1}(\bar{\zeta})$ corresponds to a pointed P-cover $U \to X$. The subgroup $A \subset P$ determines a subcover $V \to X$ of $U \to X$. By 1.1, V is connected. By (ii), $U \to X$ is the Galois closure of $V \to X$, and so $V \to X$ yields the data (P, A, B, P'). Thus the points in the fibre $\alpha'^{-1}(\bar{\zeta})$ correspond to the pointed principal $\mathbf{Z}/p$-covers of Z with the given data. So there are $\#\mathrm{Hom}(\pi_1(X), P)/\#\mathrm{Hom}(\pi_1(X), G)$ such covers. Similarly, this is the number of such covers of W. This verifies the claim, thus showing that $\sigma(Z) = \sigma(W)$, and hence proving the theorem. $\square$

Observe that Proposition 2.3 is a special case of Theorem 2.5. Since $r_G \geq 2 \cdot \#G - 2$, Theorem 2.5 also shows that

$$g(Z) \geq 1 + \#G\Big(g(X) - 1 + \sum_i (1 - 1/\#P_i)\Big),$$

where $Z \to X$ is a p-cover with group G, and groups P_i occurring as stabilizers. In addition, a p-cover $Z \to X$ satisfies $\sigma(Z) < g(Z)$ unless the length of the relative local differentials is minimal at each branch point (in which case $g(Z)$ is minimal among all covers with the given Galois group and stabilizers).

Postscript. R. Crew has informed me that he has proven a result which implies Theorem 2.5. Namely, using crystalline cohomology, he has shown [**Cr**, Cor. 1.8]

$$\sigma(Z) - 1 = \#G(\sigma(X) - 1) + \sum_{i=1}^{n} (G : P_i)(\#P_i - 1),$$

in the notation of Theorem 2.5.

References

[Ab] S. Abhyankar, *Coverings of algebraic curves*, Amer. J. Math., **79** (1957), 825–856.

[Cr] R. Crew, *Etale p-covers in characteristic p*, to appear in Compositio Mathematica.

[Gr] A. Grothendieck, *Revêtements Etales et Groupe Fondamental* (SGA 1), Lecture Notes in Mathematics 224, Springer, New York, 1970.

[Hl] M. Hall, *The Theory of Groups*, MacMillan, New York, 1959.
[Ha] D. Harbater, *Moduli p-covers of curves*, Comm. Algebra, **8** (12) (1980), 1095–1122.
[Ka] T. Kambayashi, *Review of* [**Mi**], Math Reviews 82c: 14015.
[KS] T. Kambayashi and V. Srinivas, *On étale coverings of the affine space*, Proc. 3rd Midwest Algebra Geometry Conf., (Ann Arbor, Nov. 1981).
[Mi] M. Miyanishi, *p-cyclic coverings of the affine space*, J. Algebra, **63** (1980), 279–284.
[Se] J.-P. Serre, *Sur la topologie des variétés algébriques en caractéristic p*, Symp. Intl. de Topol. Alg. (Mexico, 1956), 24–53.

Received December 13, 1982 and in revised form April 19, 1983. This research was supported in part by grants from the NSF.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CAMBRIDGE, MA 02139

Current address: Department of Mathematics
University of Pennsylvania
Philadelphia, PA 19104