Proc. Indian Acad. Sci. (Math. Sci.), Vol. 103, No. 2, August 1993, pp. 103–126.
© Printed in India.

Construction techniques foı Galois coverings of the affine line

SHREERAM S ABHYANKAR, HERBERT POPP* and WOLFGANG K SEILER*

Mathematics Department, Purdue University, West Lafayette, IN 47907, USA
*Fakultät für Mathematik und Informatik, Universität Mannheim, 68131 Mannheim, Germany

MS received 30 January 1993; revised 26 March 1993

Abstract. For constructing unramified coverings of the affine line in characteristic p, a general theorem about good reductions modulo p of coverings of characteristic zero curves is proved. This is applied to modular curves to realize $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$, with $\mathrm{GCD}(n, 6) = 1$, as Galois groups of unramified coverings of the affine line in characteristic p, for $p = 2$ or 3. It is applied to the Klein curve to realize $\mathrm{PSL}(2, 7)$ for $p = 2$ or 3, and to the Macbeath curve to realize $\mathrm{PSL}(2, 8)$ for $p = 3$. By looking at curves with big automorphism groups, the projective special unitary groups $\mathrm{PSU}(3, p^\nu)$ and the projective special linear groups $\mathrm{PSL}(2, p^\nu)$ are realized for all p, and the Suzuki groups $\mathrm{Sz}(2^{2\nu+1})$ are realized for $p = 2$. Jacobian varieties are used to realize certain extensions of realizable groups with abelian kernels.

Keywords. Good reduction; affine line; unramified covering; Galois group.

1. Introduction

In characteristic zero, the affine line is simply connected and therefore has no nontrivial unramified covering. In characteristic $p > 0$, however, only the prime-to-p part of its algebraic fundamental group is isomorphic to the prime-to-p part of the algebraic fundamental group of the corresponding characteristic zero curve and hence trivial. Its p-part, however, is nontrivial; in fact by a conjecture of Abhyankar [A03] it should be as nontrivial as can be: *Every group which is generated by its p-Sylow subgroups should occur as a Galois group of an unramified covering of the affine line.* Such groups are called *quasi p-groups.*

In the last few years, in support of this conjecture, several quasi p-groups have been realized as Galois groups of unramified coverings of the affine line in characteristic p; see [A10] to [A16], [AOS], [APS], [AYi], [Nor], and [Se2]; for a summary see [A14] to [A16]. It may be noted that the above *quasi p-group conjecture* is a special case of Abhyankar's *general conjecture* [A03] according to which the algebraic fundamental group $\pi_A(C_{g,w})$ coincides with the set of all finite groups G for which $G/p(G)$ is generated by $2g + w$ generators where $p(G)$ denotes the subgroup of G generated by all of its p-Sylow subgroups. Here $C_{g,w} = C_g \backslash \{w + 1 \text{ points}\}$ where w is a nonnegative integer and C_g is a nonsingular projective curve of genus g over an algebraically closed field of characteristic p. Recall that $\pi_A(C_{g,w})$ is defined to be the set of all finite groups which can be realized as Galois groups of unramified coverings of $C_{g,w}$. Thus, upon letting $\mathscr{A}_k^1$ = the affine line over an algebraically closed field k of characteristic p, and $Q(p)$ = the set of all quasi p-groups, the quasi p-group conjecture predicts that: $\pi_A(\mathscr{A}_k^1) = Q(p)$.

One aim of this paper is to construct unramified coverings of the affine line for some more quasi p-groups, mostly for simple groups or for groups which are closely related to simple groups. Note that a simple group is a quasi p-group iff its order is divisible by p, because then the p-Sylow subgroups generate a nonidentity normal subgroup.

A possible technique for doing this is the following: Having realized a group G of the type we are interested in as an automorphism group of an algebraic curve $\mathscr{X}$ in characteristic zero, we consider a reduction $\mathscr{X}'$ of $\mathscr{X}$ modulo p. Briefly speaking, the curve $\mathscr{X}$ can be given by various sets of polynomial equations with integer coefficients, and the curve $\mathscr{X}'$ over the finite field GF(p) is obtained by reducing the coefficients of a suitable set of equations of $\mathscr{X}$ modulo p. To compare the Galois theories of $\mathscr{X}$ and $\mathscr{X}'$ we regard them as the generic and special fibers E_T and $\mathfrak{Z}(T_E)$ of an arithmetic surface E fibered over a discrete valuation ring T. At any rate, if $\mathscr{X}'$ is irreducible and the quotient $\mathscr{X}'/G$ is the projective line then the quotient map $\mathscr{X}' \to \mathscr{X}'/G$ is a first candidate for the type of covering we are looking for, and we try to remove unwanted ramification points using Abhyankar's Lemma. In §2 we prove a general theorem (2.4) of this type, which (supplemented by (2.6)) is a principal result of this paper, and which briefly says that the prime-to-p parts of the ramification exponents of those point of the generic fiber which specialize to a given point of the special fiber are pairwise coprime and their product is the prime-to-p part of the ramification exponent of the given point of the special fiber, whereas the p-parts of the ramification exponents can (and often will) increase. In §1 we prepare the ground work for this; in particular, Proposition (1.4) is a local version of Theorem (2.4). In Remark (2.7) of §2 we give necessary conditions for a characteristic zero curve $\mathscr{X}$ to have a good reduction modulo p, i.e., briefly speaking, for the existence of equations for $\mathscr{X}$ which when reduced modulo p give a nonsingular irreducible curve.

In §3 we apply the general theorem to modular curves to get $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$ with $\mathrm{GCD}(n, 6) = 1$ for $p = 2$ or 3, where by "get" we mean "realize as Galois groups of unramified coverings of the affine line"; see (3.2). Likewise, in §4 we apply the general theorem to the Klein curve and the Macbeath curve to get PSL(2, 7) for $p = 2$ or 3 and PSL(2, 8) for $p = 3$; see (4.1.1) and (4.1.2); the Macbeath case was also done by Serre [Se5] and [Se6]. Note that the Klein curve and the Macbeath curve are curves of genus $g = 3$ and $g = 7$ in characteristic zero with automorphism groups of order $84(g-1)$ which is maximum possible by Hurwitz's Theorem. In §4 we also discuss the fact that, as discovered by Leopoldt [Leo], Stichtenoth [Sti] and Henn [Hen], automorphism groups of curves in positive characteristic can be much bigger than in characteristic zero, and by directly applying Abhyankar's Lemma to some of these curves with big automorphism groups we get the projective special unitary group $\mathrm{PSU}(3, p^\nu)$ and the projective special linear group $\mathrm{PSL}(2, p^\nu)$ for every p and the Suzuki group $\mathrm{Sz}(2^{2\nu+1})$ for $p = 2$, where ν is any positive integer; see (4.2.1) to (4.2.3); other methods of getting $\mathrm{PSL}(2, p^\nu)$ can be found in [A10] and [A16], and other methods of getting $\mathrm{PSU}(3, p^\nu)$ and $\mathrm{Sz}(2^{2\nu+1})$ were indicated by Serre in [Se3]. In (5.3) of §5, by using Jacobian varieties we show that given any $G \in \pi_A(L_k)$, for every positive integer $l \not\equiv 0(p)$ and for infinitely many positive integers γ, some extension of G with kernel $(\mathbb{Z}/l\mathbb{Z})^{2\gamma}$ belongs to $\pi_A(L_k)$; in some sense, this may be regarded as a special case of Serre's recent result [Se2] according to which every quasi-p extension of G with solvable kernel belongs to $\pi_A(\mathscr{A}^1_k)$; the special case is also indicated in Serre [Se4]. Finally, in § 6 we pose some problems.

1. Some lemmas from local algebra

Geometric outline: Let T be a discrete valuation ring with quotient field k^*, and let k' be the residue field of T, i.e., $k' = T/M(T)$ where $M(T)$ is the maximal ideal in T. Usually, the characteristic of k^* will be zero and the characteristic of k' will be $p > 0$; for instance T could be the localization of $\mathbb{Z}$ at prime p. Let $\mathscr{X} \to \mathscr{X}_0$ be a covering of curves over k^* and let $\mathscr{X}' \to \mathscr{X}'_0$ be the covering of curves over k' obtained by reducing it modulo p; we shall be mostly interested in the case when $\mathscr{X}_0$ and $\mathscr{X}'_0$ are the projective lines $\mathscr{P}^1_{k^*}$ and $\mathscr{P}^1_{k'}$ over k^* and k' respectively. To compare the Galois theories of these two coverings, we regard $\mathscr{X}$ and $\mathscr{X}'$ as the generic and special fibers E_T and $\mathfrak{Z}(T_E)$ of an arithmetic surface E over T, (where $\mathfrak{Z}(T_E)$ is the zero-set of the ideal T_E which will be defined in § 2). To visualize the surface E geometrically, as a first shot, we may think of it as consisting of two nonintersecting vertical curves, the generic fiber E_T on the left, and the special fiber $\mathfrak{Z}(T_E)$ on the right. Now it is not easy to compare the two curves E_T and $\mathfrak{Z}(T_E)$ when they are sitting isolatedly without any intermediaries between them. So we replace every point of the generic fiber E_T by a horizontal curve meeting the special fiber $\mathfrak{Z}(T_E)$ in the corresponding point. But remember that many points on the characteristic zero curve have the same reduction modulo p; for example the points $x = 1, p + 1, 2p + 1, \ldots$ are all reduced to the point $x = 1$. Thus, whereas a point of E_T uniquely determines its reduction on $\mathfrak{Z}(T_E)$, many horizontal curves are going to meet at a common point Q on the special fiber; indeed infinitely many! So the correspondence between E_T and $\mathfrak{Z}(T_E)$ is infinite to one, and that is why it is difficult to draw a good geometric picture.* At any rate, $\mathscr{X}_0$ and $\mathscr{X}'_0$ may also be regarded as the generic and special fibers of an arithmetic surface D over T, giving us a covering of surfaces $E \to D$. Postponing the global comparison of the Galois theories of $\mathscr{X}$ and $\mathscr{X}'$ to § 2, here we study the matter locally. To do this, choose a point P of $\mathfrak{Z}(T_D)$, let R be the local ring of P as a point of D, and let B be the semilocal ring of its inverse image on E. Also let Θ and U be the localizations of B and R at the prime ideals in them generated by $M(T)$. Note that then Θ and U are the local rings of $\mathfrak{Z}(T_E)$ and $\mathfrak{Z}(T_D)$ on E and D respectively. In any case Θ is a discrete valuation ring whose quotient field L coincides with the function field of $\mathscr{X}$, i.e., with the function field of E, and likewise U is a discrete valuation ring whose quotient field K coincides with the function field of $\mathscr{X}_0$, i.e., with the function field of D. Note that if Q lies above P then the local ring S of Q on E is the localization of B at a maximal ideal, and Θ together with the local rings (on E) of the infinitely many horizontal curves meeting in Q are exactly all the localizations of S at its nonzero minimal prime ideals and, by one of Krull's many theorems, S (being normal) coincides with their intersection; so the geometry of infinitely many curves meeting in a point is reproduced algebraically. Finally let K' and L' be the residue fields of U and Θ

*The other difficulty, namely the fact that only one curve passes through a point of the generic fiber, can be mollified by thinking of the generic fiber as a very fat curve whose points are so fat that, like the germs of analytic functions, each of them uniquely determines a curve passing through it.

respectively. Then by reducing R and B modulo p, i.e., by taking their images under the maps $U \to K'$ and $\Theta \to L'$, we get the local ring R' of P on $\mathscr{X}'_0$ and the semilocal ring B' of its inverse image on $\mathscr{X}'$. All this may be schematically depicted in the following diagrams, where we note that the second column in the right-hand diagram starting with Θ does not correspond to the second column in the left-hand diagram starting with E_T but it corresponds to the fourth column in the left-hand diagram starting with $\mathfrak{Z}(T_E)$.

$$\begin{tikzcd}
\mathscr{X} \arrow[r, equal] \arrow[d] & E_T \arrow[r] \arrow[d] & E & \mathfrak{Z}(T_E) \arrow[l] \arrow[r, phantom, "\approx"] \arrow[d] & \mathscr{X}' \arrow[d] \\
\mathscr{X}_0 \arrow[r, equal] \arrow[d, dash] & D_T \arrow[r] \arrow[d, dash] & D \arrow[d, dash] & \mathfrak{Z}(T_1) \arrow[l] \arrow[r, phantom, "\approx"] \arrow[d, dash] & \mathscr{X}'_0 \arrow[d, dash] \\
k^* \arrow[r, equal] & k^* & T \arrow[l] \arrow[r] & k' \arrow[r, equal] & k'
\end{tikzcd}
\qquad
\begin{tikzcd}
L & \Theta \arrow[l] & B \arrow[l] \arrow[r] & B' \arrow[r] & L' \\
K \arrow[u] & U \arrow[l] \arrow[u] & R \arrow[l] \arrow[r] \arrow[u] & R' \arrow[r] \arrow[u] & K' \arrow[u] \\
k^* \arrow[u] & T \arrow[l] \arrow[u] \arrow[r, equal] & T \arrow[u] \arrow[r] & k' \arrow[u] \arrow[r, equal] & k' \arrow[u]
\end{tikzcd}$$

Actually, in this section we are only concerned with the right-hand diagram. To recapitulate, B and B' are corresponding "semilocal pieces" of an arithmetic surface E and its special fiber $\mathfrak{Z}(T_E)$ whose local ring is Θ, and we want to relate the Galois theory of the points of B with the Galois theory of the points of B'; we do this by interposing the Galois theory of the above mentioned "horizontal curves" passing through the points of B; these horizontal curves correspond to those points of the generic fiber E_T of E whose specializations are the points of B', i.e., which when reduced modulo p give the points of B'. At any rate, we start with three preparatory Lemmas (1.1) to (1.3), and then we prove the main result of this section in Proposition (1.4), which, briefly, says that the prime-to-p parts of the ramification exponents of those point of the generic fiber which specialize to a given point of the special fiber are pairwise coprime and their product is the prime-to-p part of the ramification exponent of the given point of the special fiber, whereas the p-parts of the ramification exponents can (and often will) increase. In Lemmas (1.1) and (1.2) we deal with certain localized versions of Proposition (1.4); these localized versions remain valid in higher dimensions. In Lemma (1.3) we give a sufficient condition for two curves on a surface to meet transversally. All this is put together in Proposition (1.4). Then in Proposition (1.5) we recall some properties of prime divisors of second kind, and in Corollary (1.6) we deduce some of their consequences. In particular we shall see that $D_T \approx \mathscr{P}^1_{k^*}$ implies $\mathfrak{Z}(T_D) \approx \mathscr{P}^1_{k'}$ and that both the lines have a common "coordinate". First let us fix some algebraic terminology.

Algebraic terminology: We shall use the terminology of quadratic transformations as given in [A01], the terminology of Galois theory as given in Chapter 1 of [A04], and the terminology of models as given in §2 and §3 of [A07] and §1 and §6 of [A08]. In particular, $\mathfrak{V}(A)$ stands for the set of all localizations of a domain A with respect to the various prime ideals in A. The maximal ideal in a local ring R is denoted by $M(R)$. A ring A (always commutative with 1) is said to be *pseudogeometric* if A is noetherian and, for every domain which is a homomorphic image of A, we have that its integral closure in any finite algebraic field extension of its quotient field is a finite module over it. A noetherian domain A is said to be *regular* if all members of $\mathfrak{V}(A)$ are regular. By a DVR we mean a discrete valuation ring. For $V \in \mathfrak{V}(R)$ where R is a local domain, *V has a simple point at R* means the local domain $R/(M(V) \cap R)$ is regular; if V is a DVR and R is regular then this is equivalent to saying that $M(V) \cap R \not\subset M(R)^2$. By a *prime divisor of second kind of a regular local domain R* we mean a DVR which birationally dominates R and for whose residual transcendence degree δ over R we have $\delta \geqslant (\dim R) - 1$ [and hence $\delta = (\dim R) - 1$]. Note that *birationally dominates* means dominates and has a common quotient field. Given a local domain U and a subring A of U, by a *residual transcendental generator of U over A* we mean an element x of U (if it exists) such that upon letting $\omega: U \to U/M(U)$ to be the canonical epimorphism and $\kappa =$ the quotient field of $\omega(A)$ we have that $\omega(x)$ is transcendental over κ and $U/M(U) = \kappa(\omega(x))$.

Given a normal local domain R and a finite algebraic field extension L of the quotient field K of R, by an *extension of R to L* we mean a localization of the integral closure of R in L at a maximal ideal; note that then R has at least one and at most a finite number of extensions to L; R is said to be *split* or *unsplit* in L according as it does or does not have more than one extension to L. An extension S of R to L is said to be *naively unramified over R* if $M(R)S = M(S)$; R is said to be *naively unramified in L* if every extension of R to L is naively unramified over R; S is said to be *unramified over R* if it is naively unramified and residually separable algebraic over R; R is said to be *unramified in L* if every extension of R to L is unramified over R; *ramified* means not unramified. If R is a DVR then, for any extension S of R to L, by the *ramification exponent* (resp: *reduced ramification exponent*) *of S over R* we mean the ramification exponent (resp: reduced ramification exponent) of ord_S over ord_R, where we note that the ramification exponent divided by the reduced ramification exponent equals the residual degree of inseparability of S over R, i.e., equals 1 or $[S/M(S):R/M(R)]_i$ according as the characteristic of R/M is zero or not; S is said to be *tamely ramified over R* if the ramification exponent of S over R equals its part which is prime to the residue characteristic of R, where by the *residue characteristic* of a local ring we mean the characteristic of its residue field, and for $w = 0$ or a prime number, by the *part of a positive integer which is prime to w* we mean the largest factor of that integer which is nondivisible by w; finally, R is said to be *tamely ramified in L* if every extension of R to L is tamely ramified over R. Note that if R is a DVR and L/K is normal then the ramification exponents (resp: reduced ramification exponents, their parts prime to the residue characteristic of R) of the various extensions of R to L coincide with each other. For a finite normal algebraic field extension L/K, as in the Galois ($=$ finite normal separable algebraic) case, by the *Galois group* of L over K we mean the group of all K-automorphisms of L and we denote it by $\text{Gal}(L, K)$.

Note that for any normal noetherian domain A, say because of Krull's Diskriminantensatz (see pages 32 to 34 of [A04]), at most a finite number of DVRs in $\mathfrak{V}(A)$ can be ramified in any given finite separable algebraic field extension of the quotient field of A. This observation, as well as other basic results from the Galois theory of local rings, as given in Chapter 1 of [A04] and Chapter V of [ZSa], may be used tacitly.

Lemma 1.1. *Let $K \subset L^* \subset L$ be fields such that L/L^* is a finite algebraic extension and L^*/K is a cyclic Galois extension whose degree is coprime to the degree of L/L^*. Let d be a positive integer and let R and S be d-dimensional pseudogeometric regular local domains with quotient fields K and L, respectively, such that S is integral and residually rational over R. Assume that $L^* \neq K$ and $[L^*:K]$ is a power of a prime number which is nondivisible by the characteristic of $R/M(R)$. Then $\mathfrak{V}(R)$ contains exactly one DVR V which is ramified in L^*. Moreover V is totally ramified in L^*, i.e., it has a unique extension to L^* and its reduced ramification exponent equals $[L^*:K]$. Finally, if V has a simple point at R, then for every field K^* with $K \subset K^* \subset L^*$ we have that $S \cap K^*$ is a d-dimensional regular local domain.*

Proof. Briefly speaking, this follows by extending residue fields, passing to completions, and using standard tricks about Kummer extensions of UFDs as employed in [A02]. In greater detail we may proceed thus.

Let $[L^*:K] = u$. By assumption $u = w^e$ where e is a positive integer, and w is a prime number which is nondivisible by the characteristic of $R/M(R)$. Let ζ_w and ζ_u respectively be primitive wth and uth roots of 1 in an overfield of L. Likewise let ζ'_w and ζ'_u respectively be primitive wth and uth roots of 1 in an overfield of $R/M(R)$. Since L^*/K is cyclic, there is a unique field $L^{\#}$ with $K \subset L^{\#} \subset L^*$ such that $L^{\#}/K$ is cyclic of degree w.

Let $[K(\zeta_w):K] = w^*$. Then $w^* < w$ and $K(\zeta_w)/K$ is an abelian Galois extension. Therefore the fields $L^{\#}$ and $K(\zeta_w)$ are linearly disjoint over K, and hence $L^{\#}(\zeta_w)/K(\zeta_w)$ and $L^{\#}(\zeta_w)/L^{\#}$ are abelian Galois extensions of degree w and w^* respectively. Let $R_1^{\#}, R_2^{\#}, \ldots, R_\gamma^{\#}$ be the distinct extensions of R to $K(\zeta_w)$, and let $[(R/M(R))(\zeta'_w):(R/M(R))] = w'$. Since w is a prime number which is nondivisible by the characteristic of $R/M(R)$, it follows that the Y-discriminant of the polynomial $Y^w - 1$ is a unit in R. Therefore $\gamma w' = w^*$ and for $1 \leqslant i \leqslant \gamma$ we have that $R_i^{\#}$ is unramified over R and $[R_i^{\#}/M(R_i^{\#}):R/M(R)] = w'$, and hence in particular $R_i^{\#}$ is a d-dimensional regular local domain. Let $S^{\#} = S \cap L^{\#}$. Then $S^{\#}$ is the unique extension of R to $L^{\#}$. Since $S^{\#}$ is residually rational over R, it follows that $S^{\#}$ has exactly γ distinct extensions $S_1^{\#}, S_2^{\#}, \ldots, S_\gamma^{\#}$ to $L^{\#}(\zeta_w)$, and for $1 \leqslant i \leqslant \gamma$ we have that $S_i^{\#}$ is unramified over $S^{\#}$ and $[S_i^{\#}/M(S_i^{\#}):S^{\#}/M(S^{\#})] = w'$. Since $S^{\#}$ is integral over R, the local rings $S_1^{\#}, S_2^{\#}, \ldots, S_\gamma^{\#}$ can be labelled so that $S_i^{\#}$ is integral and residually rational over $R_i^{\#}$ for $1 \leqslant i \leqslant \gamma$. Since $L^{\#}(\zeta_w)/K(\zeta_w)$ is cyclic of degree w, we can write $L^{\#}(\zeta_w) = K(\zeta_w)(z)$ with $0 \neq z^w \in K(\zeta_w)$. Since $R_1^{\#}$ is a UFD, upon dividing z by a suitable element in $R_1^{\#}$ we can arrange matters so that $z^w = \varepsilon z_1^{\beta_1}\ z_2^{\beta_2}, \cdots, z_\alpha^{\beta_\alpha}$ where β_i is a positive integer nondivisible by w for $1 \leqslant i \leqslant \alpha$, the ideals $z_1 R_1^{\#}, z_2 R_1^{\#} \ldots z_\alpha R_1^{\#}$ are pairwise distinct prime ideals in $R_1^{\#}$, and ε is a unit in $R_1^{\#}$. If α were equal to zero then the Y-discriminant of the polynomial $Y^w - z^w$ would be a unit in $R_1^{\#}$ and hence the sum of the separable parts of the residue degrees of the various extensions of $R_1^{\#}$ to $L^{\#}(\zeta_w)$ would equal w, and this would be a contradiction because $S_1^{\#}$ is the only extension of $R_1^{\#}$ to $L^{\#}(\zeta_w)$ and it is residually rational over $R_1^{\#}$. Therefore we must have $\alpha \neq 0$. Let V be the localization of R at the prime ideal $(z_1 R_1^{\#}) \cap R$.

Now clearly V is a DVR in $\mathfrak{B}(R)$ which is ramified in $L^{\#}$. Since L^*/K is cyclic of prime power degree nondivisible by the characteristic of $R/M(R)$, it follows that V *is totally ramified in* L^*, i.e., it has a unique extension to L^* and its reduced ramification exponent equals $[L^*:K]$.

Let $[K(\zeta_u):K] = u^*$. Then $u^* < u$ and $K(\zeta_u)/K$ is an abelian Galois extension. Since V is totally ramified in L^* and the Y-discriminant of the polynomial $Y^u - 1$ is a unit in R, we see that the fields L^* and $K(\zeta_u)$ are linearly disjoint over K. Therefore $L^*(\zeta_u)/K(\zeta_u)$ and $L^*(\zeta_u)/L^*$ are cyclic and abelian Galois extensions of degree u and u^* respectively. Let $R_1, R_2, \ldots, R_h$ be the distinct extensions of R to $K(\zeta_u)$, and let $[(R/M(R))(\zeta'_u):(R/M(R))] = u'$. Then $hu' = u^*$ and for $1 \leqslant i \leqslant h$ we have that R_i is unramified over R and $[R_i/M(R_i):R/M(R)] = u'$, and hence in particular R_i is a d-dimensional regular local domain. Let $S^* = S \cap L^*$. Then S^* is the unique extension of R to L^*. Since S^* is residually rational over R, it follows that S^* has exactly h distinct extensions $S_1^*, S_2^*, \ldots, S_h^*$ to $L^*(\zeta_u)$, and for $1 \leqslant i \leqslant h$ we have that S_i^* is unramified over S^* and $[S_i^*/M(S_i^*):S/M(S)] = u'$. Since S^* is integral over R, the local rings $S_1^*, S_2^*, \ldots, S_h^*$ can be labelled so that S_i^* is integral and residually rational over R_i for $1 \leqslant i \leqslant h$. Since $L^*(\zeta_u)/K(\zeta_u)$ is cyclic of degree u, we can write $L^*(\zeta_u) = K(\zeta_u)(y)$ with $0 \neq y^u \in K(\zeta_u)$. Since R_1 is a UFD, upon dividing y by a suitable element in R_1 we can arrange matters so that $y^u = \delta y_1^{b_1} y_2^{b_2} \cdots y_a^{b_a}$ where b_i is a positive integer nondivisible by u for $1 \leqslant i \leqslant a$, the ideals $y_1 R_1, y_2 R_1, \ldots, y_a R_1$ are pairwise distinct prime ideals in R_1, and δ is a unit in R_1. Since V is ramified in L^*, we must have $a \neq 0$ and upon labelling the elements $y_1, y_2, \ldots, y_a$ suitably we can arrange matters so that V be the localization of R at the prime ideal $(y_1 R_1) \cap R$. Since V is totally ramified in L^*, *we must have* $\mathrm{GCD}(b_1, u) = 1$.

Now the Y-discriminant of the polynomial $Y^u - 1$ is a unit in R as well as S, and hence the sum of the separable parts of the residue degrees of the various extensions of R to $K(\zeta_u)$ (resp: S to $L(\zeta_u)$) equals the field degree $[K(\zeta_u):K]$ (resp: $[L(\zeta_u):L]$); since S is the unique extension of R to L and it is residually rational over R, by equating the double sum from R to $L(\zeta_u)$ via L with the double sum from R to $L(\zeta_u)$ via $K(\zeta_u)$ we see that $[L(\zeta_u):L] \geqslant [K(\zeta_u):K]$; therefore $[L(\zeta_u):L] = [K(\zeta_u):K]$ and the fields L and $K(\zeta_u)$ must be linearly disjoint over K; (this also gives an alternative proof of linear disjointness in the above two situations). It follows that $L(\zeta_u)/L^*(\zeta_u)$ is a finite algebraic field extension and $L^*(\zeta_u)/K(\zeta_u)$ is a cyclic Galois extension of degree u which is coprime to the degree of $L(\zeta_u)/L^*(\zeta_u)$. Moreover, S has exactly h distinct extensions $S_1, S_2, \ldots, S_h$ to $L(\zeta_u)$, and for $1 \leqslant i \leqslant h$ we have that S_i is unramified over S and $[S_i/M(S_i):S/M(S)] = u'$, and hence in particular S_i is a d-dimensional regular local domain. Finally, the local rings $S_1, S_2, \ldots, S_h$ can be labelled so that S_i is integral and residually rational over S_i^* for $1 \leqslant i \leqslant h$.

Let $\hat{R}_1$, $\hat{S}_1^*$ and $\hat{S}_1$ be the respective completions of R_1, S_1^* and S_1. Then $\hat{R}_1$ and $\hat{S}_1$ are d-dimensional regular local domains, and hence they are integrally closed in their respective quotient fields $\hat{K}_1$ and $\hat{L}_1$. In view of (37.8) on page 140 of [Nag] we see that $\hat{S}_1^*$ is also a d-dimensional local domain which is integrally closed in its quotient field $\hat{L}_1^*$. In view of (10.13) on page 243 of [A08] we may assume that $\hat{R}_1 \subset \hat{S}_1^* \subset \hat{S}_1$ and $\hat{K}_1 \subset \hat{L}_1^* \subset \hat{L}_1$, and then in view of standard properties of completions as given in §2 to §6 of Chapter VIII of [ZSa] we see that: $\hat{L}_1/\hat{L}_1^*$ is a finite algebraic field extension with $[\hat{L}_1:\hat{L}_1^*] = [L:L^*]$; $\hat{L}_1^*/\hat{K}_1$ is a cyclic Galois extension of degree $u = w^e$ which is coprime to $[\hat{L}_1:\hat{L}_1^*]$; e is a positive integer and w is a prime number which is nondivisible by the characteristic of $\hat{R}_1/M(\hat{R}_1)$; $\hat{S}_1^*$ and $\hat{S}_1$ are the unique extensions of $\hat{R}_1$ to $\hat{L}_1^*$ and $\hat{L}_1$ respectively; $\hat{S}_1$ is residually rational over $\hat{R}_1$; and $\hat{L}_1^* = \hat{K}_1(y)$. By (36.4) and (36.5) on page 132 of [Nag], for $1 \leqslant i \leqslant a$ we have $y_i = \delta_i y_{i1} y_{i2} \cdots y_{iv_i}$ where v_i is a positive integer, the ideals $y_{i1}\hat{R}_1, y_{i2}\hat{R}_1, \ldots, y_{iv_i}\hat{R}_1$ are pairwise distinct prime ideals in $\hat{R}_1$, and δ_i is a unit in $\hat{R}_1$. Taking a factorization of y in the UFD $\hat{S}_1$, raising it to the uth power, and then comparing the two factorizations of y^u in $\hat{R}_1$, we get $\xi_i^u = \rho_i y_{i1}^{b_i}$ with $\xi_i \in \hat{S}_1$ and $\rho_i \in \hat{S}_1 \backslash M(\hat{S}_1)$ for $1 \leqslant i \leqslant a$. Since $\hat{S}_1$ is residually rational over $\hat{R}_1$, we can find a unit σ_i in $\hat{R}_1$ with $\rho_i - \sigma_i \in M(\hat{S}_1)$ for $1 \leqslant i \leqslant a$. For $1 \leqslant i \leqslant a$ we can take an element τ_i in an overfield of $\hat{L}_1$ such that $\tau_i^u = \sigma_i$.

Let $\check{K}_1 = \hat{K}_1(\tau_1, \ldots, \tau_a)$, $\check{L}_1^* = \hat{L}_1^*(\tau_1, \ldots, \tau_a)$ and $\check{L}_1 = \hat{L}_1(\tau_1, \ldots, \tau_a)$. Let $\check{R}_1$ and $\check{S}_1$ be the integral closures of $\hat{R}_1$ and $\hat{S}_1$ in $\check{K}_1$ and $\check{L}_1$ respectively. Now the Y-discriminants of the polynomials $Y^u - \sigma_1, \ldots, Y^u - \sigma_a$ are units in $\hat{R}_1$, the local rings $\hat{R}_1$ and $\hat{S}_1$ are d-dimensional complete regular local domains, and $\hat{S}_1$ is residually rational over $\hat{R}_1$; therefore: the fields $\hat{L}_1$ and $\check{K}_1$ are linearly disjoint over the field $\hat{K}_1$; $\check{L}_1/\check{L}_1^*$ is a finite algebraic field extension with $[\check{L}_1:\check{L}_1^*] = [\hat{L}_1:\hat{L}_1^*]$; $\check{L}_1^*/\check{K}_1$ is a cyclic Galois extension of degree $u = w^e$ which is coprime to $[\check{L}_1:\check{L}_1^*]$; e is a positive integer and w is a prime number which is nondivisible by the characteristic of $\check{R}_1/M(\check{R}_1)$; $\check{R}_1$

and $\check{S}_1$ are d-dimensional regular local domains with respective quotient fields $\check{K}_1$ and $\check{L}_1$ such that $\check{S}_1$ dominates and is integral and residually rational over $\check{R}_1$; the ring $\check{R}_1$ contains ζ_u which is a primitive uth root of 1; and $y_{11}\check{R}_1, y_{21}\check{R}_1, \ldots, y_{a1}\check{R}_1$ are pairwise distinct prime ideals in $\check{R}_1$. Upon letting $\omega_1: \check{S}_1 \rightarrow \check{S}_1/M(\check{S}_1)$ to be the canonical epimorphism, for $1 \leqslant i \leqslant a$, the polynomial $Y^u - \omega_1(\rho_i)$ completely factors in $\omega_1(\check{S}_1)[Y]$ into pairwise distinct monic linear factors and hence by Hensel's Lemma we get $\mu_i^u = \rho_i$ for some $\mu_i \in \check{S}_1$; therefore upon letting $\eta_i = \xi_i/\mu_i$ we obtain $\eta_i^u = y_{i1}^{b_i}$ with $\eta_i \in \check{S}_1$; since $u/[\mathrm{GCD}(u, b_i)] \neq 1 = \mathrm{GCD}(u, [\check{L}_1:\check{L}_1^*])$, we must have $\eta_i \in \check{L}_1^*$. Upon letting $\lambda = \Pi_{1 \leqslant i \leqslant a} u/[\mathrm{GCD}(u, b_i)]$ we clearly have: $a \neq 1 \Leftrightarrow \lambda > u$. By considering ramification of the DVRs obtained by localizing $\check{R}_1$ at the prime ideals $y_{11}\check{R}_1, y_{21}\check{R}_1, \ldots, y_{a1}\check{R}_1$, we see that $[\check{K}_1(\eta_1, \ldots, \eta_a):\check{K}_1] = \lambda$. Since $[\check{L}_1^*:\check{K}_1] = u$, *we must have* $a = 1$. *Therefore V is the only DVR in $\mathfrak{B}(R)$ which is ramified in L^*.*

Now it only remains to show that, assuming V to have a simple point at R and given any field K^* with $K \subset K^* \subset L^*$, the local ring $S \cap K^*$ is regular. Since $\mathrm{GCD}(u, b_1) = 1$, we can find positive integers b_0 and u_0 such that $b_0 b_1 - u_0 u = 1$, and upon letting $y^* = y^{b_0}/y_1^{u_0}$ we get $L^* = K(y^*)$ and $y^{*u} = \delta^* y_1$ with $\delta^* \in R_1 \backslash M(R_1)$. Let $[K^*:K] = \bar{u}$ and $\bar{y} = y^{*u/\bar{u}}$. Then $\bar{u} = w^{\bar{e}}$ with nonnegative integer $\bar{e} \leqslant e$ and we have $K^*(\zeta_u) = K(\zeta_u)(\bar{y})$ with $\bar{y}^{\bar{u}} = \delta^* y_1$. Let $R^* = S \cap K^*$ and $R_1^* = S_1^* \cap K^*(\zeta_u)$. Then R^* and R_1^* are the unique extensions of R and R_1 to K^* and $K^*(\zeta_u)$ respectively, R^* is unramified in $K^*(\zeta_u)$, and R_1^* is an extension of R_1^* to $K^*(\zeta_u)$. Since V has a simple point at R, we must have $y_1 \in M(R_1) \backslash M(R_1)^2$, and hence R_1^* is a d-dimensional regular local domain. Therefore the completion $\hat{R}_1^*$ of R_1^* is a d-dimensional regular local domain, and hence in particular $\hat{R}_1^*$ is integrally closed in its quotient field $\hat{K}_1^*$. In view of (37.8) on page 140 of [Nag] we see that $\hat{R}^*$ is also a d-dimensional local domain which is integrally closed in its quotient field $\hat{K}^*$. In view of (10.13) on page 243 of [A08] we may assume that $\hat{R}^* \subset \hat{R}_1^*$ and $\hat{K}^* \subset \hat{K}_1^*$, and then in view of standard properties of completions as given in §2 to §6 of Chapter VIII of [ZSa] we see that: $\hat{K}_1^*/\hat{K}^*$ is a finite algebraic separable field extension, $\hat{R}_1^*$ is the unique extension of $\hat{R}^*$ to $\hat{K}_1^*$, $\hat{R}^*$ is unramified in $\hat{K}_1^*$, and $\hat{R}_1^*$ is regular. Now by Proposition 26 on page 12 of [A06] we conclude that $\hat{R}^*$ is regular. Therefore R^* is regular, i.e., $S \cap K^*$ *is regular.*

Lemma 1.2. *Let $K \subset L^* \subset L$ be fields such that L/L^* is a finite algebraic extension and L^*/K is a cyclic Galois extension whose degree is coprime to the degree of L/L^*. Let d be a positive integer and let R and S be d-dimensional pseudogeometric regular local domains with quotient fields K and L, respectively, such that S is integral and residually rational over R. Assume that $L^* \neq K$ and $[L^*:K]$ is nondivisible by the characteristic of $R/M(R)$. Then there is at least one and at most a finite number of (pairwise distinct) DVRs $V_1, V_2, \ldots, V_m$ in $\mathfrak{B}(R)$ which are ramified in L^*. Moreover, upon letting r_i to be the reduced ramification exponent of an extension of V_i to L^*, we have that the integers $r_1, r_2, \ldots, r_m$ are pairwise coprime and their product $r_1 r_2 \cdots r_m$ equals $[L^*:K]$. Finally, if for every field K^* with $K \subset K^* \subset L^*$ for which $S \cap K^*$ is a regular local domain, and for every DVR V in $\mathfrak{B}(S \cap K^*)$ which is ramified in L^*, we have that V has a simple point at $S \cap K^*$, then for every field K^* with $K \subset K^* \subset L^*$ we have that $S \cap K^*$ is a d-dimensional regular local domain, and if also $L \neq L^*$ then some DVR in $\mathfrak{B}(S \cap L^*)$ must be ramified in L.*

Proof. We can take a factorization $[L^*:K] = w_1^{e_1} w_2^{e_2} \cdots w_{\mu}^{e_{\mu}}$ with positive integers $e_1, e_2, \ldots, e_\mu$ and pairwise distinct prime numbers $w_1, w_2, \ldots, w_\mu$. Since L^*/K is cyclic, for $1 \leqslant \nu \leqslant \mu$, there is a unique field L_ν^* with $K \subset L_\nu^* \subset L^*$ such that $[L_\nu^*:K] = w_\nu^{e_\nu}$. By Lemma (1.1) we have a surjective map ψ of the integral segment $[1, \mu]$ onto the integral segment $[1, m]$ such that, for $1 \leqslant \nu \leqslant \mu$, the DVR $V_{\psi(\nu)}$ is totally ramified in L_ν^* and the DVR V_i is unramified in L_ν^* for every $i \in [1, m] \backslash \{\psi(\nu)\}$. Obviously $r_i = \Pi_{\nu \in \psi^{-1}(i)} w_\nu^{e_\nu}$ for $1 \leqslant i \leqslant m$, and hence the integers $r_1, r_2, \ldots, r_m$ are pairwise coprime and their product $r_1 r_2, \ldots, r_m$ equals $[L^*:K]$. By induction on the sum $e_1 + e_2 + \cdots + e_\mu$, we shall now prove the *claim* that if: (*) for every field K^* with $K \subset K^* \subset L^*$ for which $S \cap K^*$ is a regular local domain, and for every DVR V in $\mathfrak{B}(S \cap K^*)$ which is ramified in L^*, we have that V has a simple point at $S \cap K^*$, then: (′) for every field K^* with $K \subset K^* \subset L^*$ we have that $S \cap K^*$ is a d-dimensional regular local domain. If the sum is 1 then the claim follows from Lemma 1.1. So let the sum be at least 2 and assume that the claim is true for all values of the sum smaller than the given value. Also assume (*) and let there be given any field $K \subset K^* \subset L^*$. Now if $K^* \neq L^*$ then by the induction hypothesis it follows that $S \cap K^*$ is a d-dimensional regular local domain. On the other hand, if $K^* = L^*$ then we can take a field K_0 with $K \subset K_0 \subset K^*$ such that $[K^*:K_0]$ is a prime number, and now by the induction hypothesis we see that $S \cap K_0$ is a d-dimensional regular local domain and hence by Lemma 1.1 we conclude that $S \cap K^*$ is a d-dimensional regular local domain. This completes the induction and hence proves the claim. Finally, continue to assume (*) and also assume that $L \neq L^*$; now by the claim we know that $S \cap L^*$ is regular and hence by the *purity of branch locus* (see Theorem 41.1 on page 158 of [Nag]) we conclude that some DVR in $\mathfrak{B}(S \cap L^*)$ must be ramified in L.

Lemma 1.3. *Let R be a 2-dimensional local domain dominating a DVR T such that $R/M(T)R$ is regular. Then R is regular and upon letting U to be the DVR in $\mathfrak{B}(R)$ obtained by localizing R at $M(T)R$ we have that U has a simple point at R, and for every DVR V in $\mathfrak{B}(R) \backslash \{U\}$ which is residually rational over T we have that $\{U, V\}$ has a normal crossing at R and hence in particular V has a simple point at R. Morever, if there does exist a DVR in $\mathfrak{B}(R) \backslash \{U\}$ which is residually rational over T, then R must be residually rational over T.*

Proof. Since T is a DVR, we have $M(T) = tT$ for some $0 \neq t \in T$. By assumption R is a 2-dimensional local domain dominating T such that $R/M(T)R$ is regular; therefore $R/M(T)R$ must be a 1-dimensional regular local domain and hence its maximal ideal is generated by the image of some $0 \neq y \in M(R)$. Clearly $M(R) = (y, t)R$ and hence R is regular; also $M(U) \cap R = M(T)$ and hence U has a simple point at R. Given any DVR V in $\mathfrak{B}(R) \backslash \{U\}$, we have $M(V) \cap R = zR$ for some $z \in M(R) \backslash (tR)$. Now assume that V is residually rational over T. Then, for any $\eta \in R$ we can find η' in the quotient field of T such that $\eta - \eta' \in M(V)$. If $\eta' \notin T$ then there is a positive integer b such that $t^b \eta' \in T \backslash M(T)$, and this gives $t^b \eta - t^b \eta' \in M(V) \cap R \subset M(R)$ which is a contradiction because $t^b \eta \in M(R)$ and $t^b \eta' \notin M(R)$. Therefore $\eta' \in T$ and hence $\eta - \eta' \in M(V) \cap R = (zR) \subset M(R)$; It follows that if $\eta \in M(R)$ then $\eta' \in M(R) \cap T = (tR)$; consequently $(z, t)R = M(R)$ and hence $\{U, V\}$ have a normal crossing at R and V has a simple point at R. Since for every $\eta \in R$ we have $\eta - \eta' \in M(R)$ with $\eta' \in \mathrm{T}$, we also see that R is residually rational over T.

PROPOSITION 1.4.

Let R be a 2-dimensional regular local domain dominating a DVR T such that $R/M(T)R$ is regular, and let U be the DVR in $\mathfrak{B}(R)$ obtained by localizing R at $M(T)R$. Let B

be the integral closure of R in a Galois extension L of the quotient field K of R. Assume that $B/M(T)B$ is a regular domain, and let Θ be the localization of B at the prime ideal $M(T)B$. [Clearly then: Θ is a DVR which is the integral closure of U in L, and U is unsplit and naively unramified in L.] Let $\tilde{G}$ and $\tilde{L}$ respectively be the inertia group and the inertia field of Θ over U, let $\phi:\Theta \to L' = \Theta/M(\Theta)$ be the canonical epimorphism, let $K' = \phi(U)$ and *$\tilde{L}' = \phi(\tilde{\Theta})$ with $\tilde{\Theta} = \Theta \cap \tilde{L}$, and let $k' = \phi(T)$ and $R' = \phi(R)$ and $B' = \phi(B)$.*

[Clearly then (see Chapter 1 of [A04] and Chapter V of [ZSa]): $M(\Theta) \cap U = M(U)$ and $K' \approx U/M(U)$; $M(\Theta) \cap T = M(T)$ and $k' \approx T/M(T)$; $M(\Theta) \cap R = M(T)R$ and $R' \approx R/M(T)R$; $M(\Theta) \cap B = M(T)B$ and $B' \approx B/M(T)B$; $\tilde{G}$ is a normal subgroup of $\mathrm{Gal}(L, K)$ and L is the fixed field of G; the order of $\tilde{G}$ equals 1 or a nonnegative power of the characteristic of k' according as the said characteristic is zero or not; U is unramified in $\tilde{L}$; L'/K' is a finite normal algebraic field extension and ϕ induces an epimorphism of $\mathrm{Gal}(L, K)$ onto $\mathrm{Gal}(L', K')$ with kernel $\tilde{G}$; $L'/\tilde{L}'$ is purely inseparable with $[L':\tilde{L}'] = [L:\tilde{L}] = |\tilde{G}|$; $\tilde{L}'/K'$ is a Galois extension with $\mathrm{Gal}(\tilde{L}', K') \approx \mathrm{Gal}(L', K')$; R' is a DVR with quotient field K' and subfield k'; and B' is the integral closure of R' in L'.]

Assume that every extension to L of any DVR in $\mathfrak{B}(R)\backslash\{U\}$, which is ramified in L, is residually rational over T. Let $V_1, V_2, \ldots, V_m$ be all the distinct DVRs in $\mathfrak{B}(R)\backslash\{U\}$ which are ramified in L. For $1 \leqslant i \leqslant m$, let r_i be the ramification exponent of an extension of V_i to L, and let s_i be the part of r_i prime to the residue characteristic of T. Let r be the reduced ramification exponent of an extension of R' to L', and let s be the part of r prime to the residue characteristic of T. Then we have the following.

If $m = 0$ then: R' is unramified in $\tilde{L}'$. If $m > 0$ then: $s_1, s_2, \ldots, s_m$ are pairwise coprime, and their product $s_1, s_2, \ldots, s_m$ equals s. If $m > 0$ then: R is residually rational over T, and V_i has a simple point at R for $1 \leqslant i \leqslant m$. If $m > 0$ then: R' is residually rational over k', and $r/s \geqslant r_i/s_i$ for $1 \leqslant i \leqslant m$. Finally, if $m > 0$ then: $r = s \Leftrightarrow L = \tilde{L}$ and $r_i = s_i$ for $1 \leqslant i \leqslant m$.

Proof. Let $S_1, S_2, \ldots, S_h$ be all the distinct extensions of R to L, i.e., the localizations of B at its various maximal ideals. Note that $M(T)B \subset M(S_j) \cap B$ for $1 \leqslant j \leqslant h$ and let S'_j be the localization of B' at its maximal ideal $\phi(M(S_j \cap B))$. Then clearly $S'_1, S'_2, \ldots, S'_h$ are exactly all the distinct extensions of R' to L'. Let $\tilde{S}'_j = S'_j \cap \tilde{L}'$ for $1 \leqslant j \leqslant h$. Then $\tilde{S}'_1, \tilde{S}'_2, \ldots, \tilde{S}'_h$ are exactly all the distinct extensions of R' to $\tilde{L}'$, and for $1 \leqslant j \leqslant h$ we have that S'_j is the unique extension of $\tilde{S}'_j$ to L'.

For $1 \leqslant j \leqslant h$, let G^{σ}_j and G^{τ}_j be the splitting and inertia groups of S_j over R and note that then G^{σ}_j is a subgroup of $\mathrm{Gal}(L, K)$ and G^{τ}_j is a normal subgroup of G^{σ}_j, and let K^{σ}_j and K^{τ}_j be the splitting and inertia fields of S_j over R and note these are the fixed fields of G^{σ}_j and G^{τ}_j respectively. Let $\phi_{\mathrm{gal}}:\mathrm{Gal}(L, K) \to \mathrm{Gal}(L', K')$ and $\tilde{\phi}_{\mathrm{gal}}:\mathrm{Gal}(L, K) \to \mathrm{Gal}(\tilde{L}', K')$ be the epimorphisms induced by ϕ, and note that for every $g \in \mathrm{Gal}(L, K)$ we have $\tilde{\phi}_{\mathrm{gal}}(g) = \phi_{\mathrm{gal}}(g)|\tilde{L}'$, and for $1 \leqslant j \leqslant h$ we have $\ker(\phi_{\mathrm{gal}}) = \ker(\tilde{\phi}_{\mathrm{gal}}) = \tilde{G} \subset G^{\tau}_j$. Again for $1 \leqslant j \leqslant h$, let $\tilde{G}'^{\sigma}_j$ and $\tilde{G}'^{\tau}_j$ be the splitting and inertia groups of $\tilde{S}'_j$ over R' and note that then $\tilde{G}'^{\sigma}_j$ is a subgroup of $\mathrm{Gal}(\tilde{L}', K')$ and $\tilde{G}'^{\tau}_j$ is a normal subgroup of $\tilde{G}'^{\sigma}_j$, and let $\tilde{K}'^{\sigma}_j$ and $\tilde{K}'^{\tau}_j$ be the splitting and inertia fields of $\tilde{S}'_j$ over R' and note these are the fixed fields of $\tilde{G}'^{\sigma}_j$ and $\tilde{G}'^{\tau}_j$ respectively. Now clearly $\tilde{\phi}_{\mathrm{gal}}(G^{\sigma}_j) = \tilde{G}'^{\sigma}_j$ and $\tilde{\phi}_{\mathrm{gal}}(G^{\tau}_j) = \tilde{G}'^{\tau}_j$ for $1 \leqslant j \leqslant h$.

Since U is unramified in $\tilde{L}$, in view of (10.13) of [A08] and (37.8) and (41.4) of [Nag] and §2 to §6 of Chapter VIII [ZSa], we see that if $m = 0$ then $K^{\tau}_j = \tilde{L}$ for $1 \leqslant j \leqslant h$ and hence $\tilde{G}'^{\tau}_j =$ for $1 \leqslant j \leqslant h$, and therefore R' is unramified in $\tilde{L}'$.

So henceforth assume that $m > 0$. Then in view of Lemma (1.3) we see that $S_1, S_2, \ldots, S_h$ are residually rational over T, and hence R and R' are residually rational over T and k' respectively, and $S_1, S_2, \ldots, S_h$ are residually rational over R, and therefore $G_j^\sigma = G_j^\tau$ for $1 \leqslant j \leqslant h$, and hence $\tilde{G}_j'^\sigma = \tilde{G}_j'^\tau$ for $1 \leqslant j \leqslant h$. By Lemma (1.3) we also see that V_i has a simple point at R for $1 \leqslant i \leqslant m$.

Since R' is a DVR, for $1 \leqslant j \leqslant h$, the group $\tilde{G}_j'^\tau$ has a unique (normal) p-Sylow subgroup $\tilde{G}_j'^*$ where p is the residue characteristic of T (take $\tilde{G}_j'^* = 1$ in case the residue characteristic of T is zero) and the factor group $\tilde{G}_j'^\tau / \tilde{G}_j'^*$ is cyclic; now upon letting $\tilde{K}_j'^*$ to be the fixed field of $\tilde{G}_j'^*$ we clearly have $[L' : \tilde{K}_j'^\tau] = r$ and $[\tilde{L}_j'^* : \tilde{K}_j'^\tau] = s$, and hence upon letting L_j^* to be the fixed field of $\tilde{\phi}_{\mathrm{gal}}^{-1}(\tilde{G}_j'^*)$ we see that: $K \subset K_j^\sigma = K_j^\tau \subset L_j^* \subset \tilde{L} \subset L$, the extension L_j^* / K_j^τ is a cyclic Galois extension of degree s which is nondivisible by the residue characteristic of T, and the extension L/L_j^* is a Galois extension of degree r/s where r/s equals 1 or a nonnegative power of the residue characteristic of T according as the said characteristic is zero or not.

Upon letting $R_1^\tau = S_1 \cap K_1^\tau$ we have that R and R_1^τ are d-dimensional regular local domains such that R_1^τ is unramified and residually rational over R; for $1 \leqslant i \leqslant m$, we know that V_i has a simple point at R and every extension of V_i to L is residually rational over T, and hence V_i has a unique extension V_i^τ to K_1^τ which belongs to $\mathfrak{V}(R_j^\tau)$ and this unique extension V_i^τ is unramified and residually rational over V_i, and therefore r_i is the ramification exponent of every extension of V_i^τ to L, and s_i is the part of r_i prime to the residue characteristic of T. Upon letting $U_1^\tau = \Theta \cap K_1^\tau$ we see that U_1^τ is a DVR in $\mathfrak{V}(R_1^\tau)$, and $V_1^\tau, V_2^\tau, \ldots, V_m^\tau$ are exactly all the DVRs in $\mathfrak{V}(R_1^\tau) \backslash \{U_1^\tau\}$ which are ramified in L; since U is unramified in L, we see that U_1^τ is unramified in L_j^*.

Upon relabelling $V_1, V_2, \ldots, V_m$ suitably, we can arrange matters so that $V_1^\tau, V_2^\tau, \ldots, V_n^\tau$ are ramified in L_1^* and $V_{n+1}^\tau, V_{n+2}^\tau, \ldots, V_m^\tau$ are unramified in L_1^*. Now clearly $s_{n+1} = s_{n+2} = \cdots = s_m = 1$, and for $1 \leqslant i \leqslant n$ we have that s_i is the ramification exponent of every extension of V_i^τ to L_1^*, and for $1 \leqslant i \leqslant m$ we have that r_i/s_i is the ramification exponent of every extension of V_i^τ to L and hence $r/s \equiv 0(r_i/s_i)$.

If $L_1^* = K_1^\tau$ then $s = 1$ and $n = 0$, and hence obviously: the local ring $S_1 \cap R_1^*$ is regular, the integers $s_1, s_2, \ldots, s_m$ are pairwise coprime, and their product $s_1 s_2 \cdots s_m$ equals s. If $L_1^* \neq K_1^\tau$ then by taking $(K_1^\tau, L_1^*, L, R_1^\tau, S_1, n, V_1^\tau, V_2^\tau, \ldots, V_n^\tau, s_1, s_2, \ldots, s_n)$ for $(K, L^*, L, R, S, m, V_1, V_2, \ldots, V_m, r_1, r_2, \ldots, r_m)$ in Lemma (1.2) we see that: $n > 0$, the local ring $S_1 \cap L_1^*$ is regular, the integers $s_1, s_2, \ldots, s_m$ are pairwise coprime, and their product $s_1 s_2 \cdots s_m$ equals s.

Now it only remains to note that if $L = \tilde{L}$ and $r_i = s_i$ for $1 \leqslant i \leqslant m$ then $S_1 \cap L_1^*$ is a regular local domain with quotient field L_1^*, S_1 is the unique extension if $S_1 \cap L_1^*$ to L, S_1 is residually rational over $S_1 \cap L_1^*$, and every DVR in $\mathfrak{V}(S_1 \cap L_1^*)$ is unramified in L, and hence, in view of (10.13) of [A08]. and (41.4) of [Nag] and §2 to §6 of Chapter VIII [ZSa], we must have $L = L_1^*$ and therefore $r = s$.

The following proposition about divisors of second kind is proved in [A01].

PROPOSITION 1.5.

Let U be a prime divisor of second kind of a 2-dimensional regular local domain R and let $R = R_0 \subset R_1 \subset R_2 \subset \cdots$ be the quadratic sequence along U. Then the residue field of U is a simple transcendental extension of a finite algebraic extension of the residue field of R and there is a unique positive integer s such that $R_0 \neq R_1 \neq R_2 \cdots \neq R_s = U = R_{s+1} = R_{s+2} = \ldots$. Moreover, $\dim R_i = 2$ for $1 \leqslant i \leqslant s$, and $\mathrm{ord}_U(z) = \mathrm{ord}_{R_{s-1}}(z)$

for every element z in the quotient field of R. Finally, if $M(R)=(x_0,t)R$ with $\mathrm{ord}_U(t)=1$, the residue field of R is relatively algebraically closed in the residue field of U, and $\mathfrak{k}$ is a coefficient set for R, then there exist unique elements $c_1,c_2,\dots,c_s$ in $\mathfrak{k}$ with $c_s=0$ such that upon letting $x_i=x_{i-1}t^{-1}-c_i$ for $1\leqslant i\leqslant s$ we have $M(R_i)=(x_i,t)R_i$ for $1\leqslant i\leqslant s$, and x_s is a residual transcendental generator of U over R.

As a consequence of the above Proposition (1.5) we have the following.

COROLLARY 1.6

Let U be a DVR dominating another DVR T such that: the quotient field K of U is a simple transcendental extension of the quotient field k^* of T, the residue field of U is transcendental over the residue field of T, the residue field of T is relatively algebraically closed in the residue field of U, and $M(U)=M(T)U$. Then $K=k^*(x)$ for some x which is a residual transcendental generator of U over T. Moreover, for every such x we have that U is the localization of $T[x]$ at the prime ideal $M(T)\ T[x]$.

Namely, by assumption $M(T)=tT$ for some t, and $K=k^*(x^*)$ for some x^*. Now $\mathrm{ord}_U(t)=1$, and we can find an integer e such that $e+\mathrm{ord}_U(x^*)>0$. Let $x_0=t^ex^*$, let R be the localization of $T[x_0]$ at the prime ideal $(x_0,t)\ T[x_0]$, and let $\mathfrak{k}$ be a coefficient set for T. Then U is a prime divisor of second kind of the 2-dimensional regular local domain R, and $\mathfrak{k}$ is a coefficient set for R, and hence it suffices to take $x=x_s$ with x_s as in the above Proposition (1.5).

2. Specializations of coverings of the line

Referring to the preamble to § 1 for geometric outline, we want to compare the Galois theories of the generic and special fibers of an arithmetic surface over a discrete valuation ring. As remarked before, the correspondence between these two fibers is infinite to one, which causes some difficulty in showing that different automorphisms of the generic fiber induce different automorphisms of the special fiber. Assuming the genus to be at least two, this is overcome by passing to points of finite order of the Jacobian varieties of the two fibers. In precise algebraic terms we proceed thus.

Let L/k^* be a 1-dimensional function field, i.e., L is a field which is finitely generated and of transcendence degree 1 over the subfield k^*. Recall that for any subring $\bar{k}$ of any field $\bar{L}$, the *Riemann–Zariski space* $\mathfrak{R}(\bar{L}/\bar{k})$ is the set of all valuation rings of $\bar{L}$ which contain $\bar{k}$. In our case, $L\in\mathfrak{R}(L/k^*)$ and the members of $\mathfrak{R}(L/k^*)\backslash\{L\}$ are DVRs which are in 1–1 correspondence with the points of a nonsingular projective algebraic curve over k^*. More precisely, $\mathfrak{R}(L/k^*)$ is the unique nonsingular projective model of L/k^*; L is its generic point and all others are its closed points. So we may visualize $\mathfrak{R}(L/k^*)$ as a (nonsingular projective algebraic) *curve*. Eventually we shall assume that L/k^* is *regular* (as a function field), i.e., k^* is relatively algebraically closed in L and L is separably generated over k^*.

Let T be a pseudogeometric DVR *with quotient field k^**; note that a DVR of characteristic zero is automatically pseudogeometric. Eventually we shall assume that the residue field of T is perfect; note that a finitely generated field extension of a perfect field is automatically separably generated, and also note that a field of characteristic zero is always perfect.

Let E be a projective model of L/T; for definition see page 27 of [A08]. Now

$\dim E = 2$ and hence we may think of E as an *arithmetic surface.* Let E_T be the set of all those members of E which do not dominate T; obviously E_T is a projective model of L/k^* and we call it *the generic fiber of E over T.* We shall only be interested in the case when E_T is nonsingular; note that this is so iff $E_T = \mathfrak{R}(L/k^*)$. Clearly there is a unique ideal T_E on E such that for every $S \in E$ we have $T_E S = M(T)S$ and for every affine ring A over T with $\mathfrak{V}(A) \subset E$ we have $A \cap T_E = M(T)A$; we call T_E *the ideal induced by T on E*; for the definition of an ideal on a model see page 169 of [A08]. Note that E is the disjoint union of E_T and the zero-set $\mathfrak{Z}(T_E)$. The zero-set $\mathfrak{Z}(T_E)$ together with the ideal T_E may be called the *special fiber of E at T*; since we are only interested in the case when the special fiber is *reduced*, i.e., when its ideal $\mathfrak{I}(\mathfrak{Z}(T_E), E)$ on E is equal to T_E, we may simply *refer to $\mathfrak{Z}(T_E)$ as the special fiber.* Note that if $\mathfrak{Z}(T_E)$ is irreducible then its generic point is 1-dimensional and its remaining points are exactly all the 2-dimensional members of E.

Henceforth assume that E is good (as a model of L/T), by which we mean that $\mathfrak{Z}(T_E)$ is irreducible and nonsingular and for its ideal on E we have $\mathfrak{I}(\mathfrak{Z}(T_E), E) = T_E$. In view of (1.3) we see that E is nonsingular, and hence in particular $E_T = \mathfrak{R}(L/k^*)$ and the generic point Θ of $\mathfrak{Z}(T_E)$ is a DVR dominating T. Also note that every $S \in \mathfrak{Z}(T_E) \backslash \{\Theta\}$ is the intersection of all the DVRs in $\mathfrak{V}(S)$. Let $\phi: \Theta \to L' = \Theta/M(\Theta)$ be the canonical epimorphism, and let $k' = \phi(T)$. Now clearly L'/k' is a 1-dimensional function field and $S \mapsto \phi(S)$ gives a bijection of $\mathfrak{Z}(T_E)$ onto $\mathfrak{R}(L'/k')$. Some of the things said so far may be depicted in the following diagram.

$$\begin{tikzcd}
L \arrow[d, dash] & \Theta \arrow[l] \arrow[r, "\phi"] \arrow[d, dash] & L' \arrow[d, dash] \\
k^* & T \arrow[l] \arrow[r, "\phi"] & k'
\end{tikzcd}$$

Now let $\mathrm{Div}(L/k^*)$ be the group of all divisors of L/k^* which we regard as functions $\mathfrak{R}(L/k^*) \backslash \{L\} \to \mathbb{Z}$ with finite support, let $\mathrm{Prin}(L/k^*) \subset \mathrm{Div}_0(L/k^*) \subset \mathrm{Div}(L/k^*)$ be the subgroups of principal divisors and divisors of degree zero respectively, and let $\mathrm{Jac}(L/k^*)$ be the factor group $\mathrm{Div}_0(L/k^*)/\mathrm{Prin}(L/k^*)$; likewise for L'/k'. By referring to [Lam] for details, for $W \in \mathfrak{R}(L/k^*) \backslash \{L\}$ we get $\phi_{\mathrm{val}}(W) \in \mathrm{Div}(L'/k')$ by putting $\phi_{\mathrm{val}}(W)(\phi(S)) = 0$ if $S \in \mathfrak{Z}(T_E) \backslash \{\Theta\}$ is such that $W \notin \mathfrak{V}(S)$, and $\phi_{\mathrm{val}}(W)(\phi(S)) = \mathrm{ord}_{\phi(S)} \phi(M(W) \cap S)$ if $S \in \mathfrak{Z}(T_E) \backslash \{\Theta\}$ is such that $W \in \mathfrak{V}(S)$, and we note that the degree of $\phi_{\mathrm{val}}(W)$ equals $[W/M(W): k^*]$. In particular, for every $W \in \mathfrak{R}(L/k^*) \backslash \{L\}$ we have $W \in \mathfrak{V}(S)$ for some $S \in \mathfrak{Z}(T_E) \backslash \{\Theta\}$, and hence the members of $\mathfrak{Z}(T_E) \backslash \{\Theta\}$ are exactly all the closed points of E. By additivity this gives a degree preserving (group) homomorphism $\phi_{\mathrm{div}}: \mathrm{Div}(L/k^*) \to \mathrm{Div}(L'/k')$. It is easily seen that ϕ_{div} preserves principalness and hence it gives rise to a homomorphism $\phi_{\mathrm{jac}}: \mathrm{Jac}(L/k^*) \to \mathrm{Jac}(L'/k')$. For any positive integer v, this induces a homomorphism $\phi_{\mathrm{jac}}^{(v)}: \mathrm{Jac}^{(v)}(L/k^*) \to \mathrm{Jac}^{(v)}(L'/k')$ where $\mathrm{Jac}^{(v)}(L/k^*)$ and $\mathrm{Jac}^{(v)}(L'/k')$ are the respective subgroups of $\mathrm{Jac}(L/k^*)$ and $\mathrm{Jac}(L'/k')$ consisting all those points whose order divides v.

Henceforth assume that $T/M(T)$ is perfect, some member of $\mathfrak{R}(L/k^*)$ is residually rational over k^*, and L is separably generated over k^*; note that then L/k^* and L'/k' are regular function fields. Under these conditions, by a result of Hironaka [Hir] and Popp [Pop] we have the following.

PROPOSITION 2.1.

The genus of L'/k' equals the genus of L/k^*.

Henceforth assume that the genus of L/k^* is at least 2, and let K be a subfield of L such that L/K is Galois and K is a simple transcendental extension of k^*. Let $U = \Theta \cap K$, and note that then U is a DVR with quotient field K such that U dominates T and $M(T)U = M(U)$; also Θ is the unique extension of U to L, and Θ is naively unramified over U. *Let $K' = \phi(U)$ and note that then L'/K' is a finite normal field extension and L'/k' is a simple transcendental extension*; also we get an epimorphism $\phi_{\text{gal}}:\text{Gal}(L,K) \to \text{Gal}(L',K')$ whose kernel is the inertia group $\tilde{G}$ of Θ over U and we have that: ϕ_{gal} is injective $\Leftrightarrow$ L'/K' is Galois. With all these assumptions, in Proposition (2.2) we shall now prove that we can find a good "common" coordinate function x for K and K' as indicated in the following diagram.

$$\begin{tikzcd}
L & \Theta \arrow[l] \arrow[r, "\phi"] & L' \\
K = k^*(x) \arrow[u, dash] & U = T[x] \arrow[l] \arrow[r, "\phi"] \arrow[u, dash] & K' = k'(\phi(x)) \arrow[u, dash] \\
k^* \arrow[u, dash] & T \arrow[l] \arrow[r, "\phi"] \arrow[u, dash] & k' \arrow[u, dash]
\end{tikzcd}$$

PROPOSITION 2.2.

There exists a residual transcendental generator x of U over T and, for any such x, the localization of $T[x]$ at the prime ideal $M(T)\,T[x]$ coincides with U. Moreover, upon letting D to be the projective line over T defined by x, i.e., upon letting D to be the model of K/T given by $D = \mathfrak{B}(T[x]) \cup \mathfrak{B}(T[1/x])$, we have that E is the normalization of D in L, i.e., E consists of all the extensions of the various members of D to L. (Therefore $D = E \cap K$ in the sense that: for any field extension $L^\flat/K^\flat$ and any set $E^\flat$ of subrings of $L^\flat$, by $E^\flat \cap K^\flat$ we may denote the set of subrings of $K^\flat$ given by $\{S^\flat \cap K^\flat : S^\flat \in E^\flat\}$).

Proof. By (1.6) there exists a residual transcendental generator x of U over T and, for any such x, the localization of $T[x]$ at the prime ideal $M(T)\,T[x]$ coincides with U, and hence upon letting D to be the projective line over T defined by any such x, i.e., upon letting D to be the model of K/T given by $D = \mathfrak{B}(T[x]) \cup \mathfrak{B}(T[1/x])$, we have $U \in D$. Let E^* be the normalization of D in L. Then clearly $(\mathfrak{R}(L/k^*) \cup \{\Theta\}) \subset E^*$ and $E^* \backslash (\mathfrak{R}(L/k^*) \cup \{\Theta\})$ is a set of 2-dimensional normal local domains. Also L' is the residue field of Θ and by (2.1) we know that the genus of L'/k' is at least two. Consequently by (1.5) we see that in the birational correspondence between E and E^* there can be no fundamental points on E, and hence E dominates E^*, and therefore by ZMT (= Zariski's Main Theorem) we must have $E = E^*$, (for the arithmetic versions of ZMT and the concept of fundamental points etc., see [A07] and [A08]).

With all the above assumptions in force, we shall now prove the following.

PROPOSITION 2.3

ϕ_{gal} is injective.

Proof. Let g be the genus of L/k^*, and hence by (2.1) also the genus of L'/K'. Let $\check{k}$ be an algebraic closure of k^*, let $\check{k}'$ be an algebraic closure of k', and let $\check{K} = K(\check{k})$, $\check{L} = L(\check{k})$, $\check{K}' = K'(\check{k}')$, and $\check{L}' = L'(\check{k}')$. Then the genus of $\check{L}/\check{k}$ as well as that of $\check{L}'/\check{k}'$

is g, and $\mathrm{Gal}(\check{L}, \check{K})$ and $\mathrm{Gal}(\check{L}', \check{K}')$ can be identified with $\mathrm{Gal}(L, K)$ and $\mathrm{Gal}(L', K')$ respectively. Let l be a prime number nondivisible by the characteristic of k', and let $v = l^m$ where m is a positive integer. Then by Weil's Theorem on points of finite order of abelian varieties (see Corollary 1 on page 127 of [Wei]) we have $|\mathrm{Jac}^{(v)}(\check{L}/\check{k})| = v^{2g} = |\mathrm{Jac}^{(v)}(\check{L}'/\check{k}')|$. Therefore the homomorphism $\phi^{(v)}_{\mathrm{jac}}$ induces an isomorphism $\check{\phi}^{(v)}\colon \mathrm{Jac}^{(v)}(\check{L}/\check{k})\ \mathrm{Jac}^{(v)}(\check{L}'/\check{k}')$. Since g is positive, the Galois groups act faithfully on the corresponding Jacobians, and by Weil's Theorem on Tate modules (see Theorem 3 on page 176 of [Mum] and Lemma 12.2 on page 122 of [Mil]) we know that, for large enough m, the Galois groups $\mathrm{Gal}(\check{L}, \check{K}) = \mathrm{Gal}(L/K)$ and $\mathrm{Gal}(\check{L}', \check{K}') = \mathrm{Gal}(L'/K')$ act faithfully on $\mathrm{Jac}^{(v)}(\check{L}/\check{k})$ and $\mathrm{Jac}^{(v)}(\check{L}'/\check{k}')$ respectively. Therefore ϕ_{gal} is injective.

Note that, in the Riemann–Hurwitz genus formula, the contribution of a nontamely ramified point is greater than the contribution in characteristic zero for the same ramification exponent. Therefore, in view of (2.1) to (2.3), by (1.4) we get the following General Theorem.

General theorem 2.4. *Recall that L/k^* is a 1-dimensional regular function field such that some member of $\mathfrak{R}(L/k^*)$ is residually rational over k^*, the genus of L/k^* is at least 2, T is a pseudogeometric DVR with quotient field k^* such that the residue field of T is perfect, E is a good projective model of L/T, $E_T = \mathfrak{R}(L/k^*) =$ the generic fiber of E over T, the DVR Θ with quotient field L is the generic point of the special fiber $\mathfrak{Z}(T_E)$ of E over T, $\phi\colon \Theta \to L' = \Theta/M(\Theta)$ is the canonical epimorphism, $k' = \phi(T)$, K is a subfield of L such that L/K is Galois and K/k^* is a simple transcendental extension, the DVR U with quotient field K is defined by putting $U = \Theta \cap K$, $K' = \phi(U)$, and by (2.3) ϕ induces an isomorphism $\phi_{\mathrm{gal}}\colon Gal(L, K) \to Gal(L', K')$.*

Now assume that all the members of $\mathfrak{R}(L/k^*)$, which are ramified over their contractions to K, are residually rational over k^*, and let $x' = \phi(x)$ with x as in (2.2). Then $K' = k'(x')$ and L'/K' is a Galois extension whose Galois group is isomorphic to the Galois group of L/K. Let $P_1, P_2, \ldots, P_a$ be the branch points of L'/K', i.e., those members of $\mathfrak{R}(K'/k')$ which are ramified in L'. Then there is a disjoint partition $\Pi_{1 \leqslant i \leqslant a}\{V_{i1}, V_{i2}, \ldots, V_{im_i}\}$ of the set of all branch points of L/K, with $m_i > 0$ and $V_{ij} \neq V_{ij'}$ for $1 \leqslant i \leqslant a$ and $1 \leqslant j < j' \leqslant m_i$, such that, for $1 \leqslant i \leqslant a$, upon letting R_i to be the unique member of D with $\phi(R_i) = P_i$ where D is as in (2.2), we have that $V_{i1}, V_{i2}, \ldots, V_{im_i}$ are exactly those branch points of L/K which belong to $\mathfrak{B}(R_i)$. Let r_i be the ramification exponent of an extension of P_i to L' and let s_i be the part of r_i prime to the residue characteristic of T. Also let r_{ij} be the ramification exponent of an extension of V_{ij} to L and let s_{ij} be the part of r_{ij} prime to the residue characteristic of T. Then for $1 \leqslant i \leqslant a$ we have that the integers $s_{i1}, s_{i2}, \ldots, s_{im_i}$ are pairwise coprime and their product equals s_i, and $r_i/s_i \geqslant r_{ij}/s_{ij}$ for $1 \leqslant j \leqslant m_i$, and moreover: $r_i = s_i \Leftrightarrow r_{ij} = s_{ij}$ for $1 \leqslant j \leqslant m_i$. Finally, if the ramification exponent of an extension to L of some member of $\mathfrak{R}(K/k^*)$ is divisible by the residue characteristic of T, then we must have $m_i > 1$ for some i.

DEFINITION 2.5.

If a good model E of L/T exists, we may express this by saying that L/k^* (or the corresponding nonsingular projective algebraic curve $\mathscr{X}$) *has a good reduction via T or modulo $M(T)$*, and we may refer to L'/k' (or the corresponding nonsingular projective algebraic curve $\mathscr{X}'$) as *a good reduction of L/k^* via T or modulo $M(T)$*; we may also call K' *the corresponding reduction of K*. In case the characteristic of T is zero and the characteristic of $T/M(T)$ is $p > 0$, briefly speaking, we may talk of *reduction modulo* p instead of reduction modulo $M(T)$.*

Abhyankar's Lemma 2.6. This has many versions. For one version see pages 181–186 of [A05]. At any rate, using it we see that if k' is a field of characteristic $p>0$ and L' is a Galois extension of $k'(x')$ which is unramified except at $x'=\infty$ and $x'=0$ and for which the ramification exponent at $x'=0$ is nondivisible by p, then upon letting $\Lambda = L'(k(X))$, where $X^\rho = x'$ with any positive integer ρ divisible by the ramification exponent at $x'=0$ and k is any algebraically closed overfield of k' such that X is transcendental over k', we have that the Galois extension $\Lambda/k(X)$ is unramified except at $X=\infty$. Moreover, if the extensions of $x'=\infty$ to L' are residually rational over k' then $\mathrm{Gal}(L'/K')$ remains unchanged when we replace k' by its algebraic closure and hence, in view of (3.1) of [A10], $\mathrm{Gal}(\Lambda, k(X))$ is (isomorphic to) a normal subgroup of $\mathrm{Gal}(L', k'(x'))$ and the corresponding factor group is a cyclic group whose order divides ρ but is nondivisible by p; consequently, in view of Result 4 on page 841 of [A03], $\mathrm{Gal}(L', k'(x'))/p(\mathrm{Gal}(L', k'(x')))$ must be cyclic and we must have $\mathrm{Gal}(\Lambda, k(X)) = p(\mathrm{Gal}(L', k'(x')))$; (recall that for any finite group G, by $p(G)$ we denote the normal subgroup of G generated by all of its p-Sylow subgroups). Therefore in the situation of (2.4), if the characteristic of k' is $p>0$ and L/K has at most three branch points, exactly one of which has ramification exponent divisible by p, then, by making a suitable fractional linear transformation on x', we get a Galois extension $L'/k'(x')$, having $x'=\infty$ as the only nontame branch point and having $x'=0$ as the only other possible branch point, such that $\mathrm{Gal}(L'/k'(x')) = \mathrm{Gal}(L, K)$, and hence upon letting $\Lambda = L'(k(X))$, where $X^\rho = x'$ with any positive integer ρ divisible by the ramification exponent at $x'=0$ and k is any algebraically closed overfield of k' such that X is transcendental over k', we get a Galois extension $\Lambda/k(X)$, having $X=\infty$ as the only branch point, such that $\mathrm{Gal}(\Lambda, k(X)) = p(\mathrm{Gal}(L, K))$.

Remark 2.7. Let $\mathscr{X}$ be a nonsingular Galois covering of the projective line $\mathscr{P}^1$ in characteristic zero. Let $r_1, r_2, \ldots, r_h$ be the ramification exponents of the branch points on $\mathscr{P}^1$. Let p be a prime number and let $s_1, s_2, \ldots, s_h$ be the prime to p parts of $r_1, r_2, \ldots, r_h$ respectively. Assume that $\mathrm{GCD}(s_i, s_j) > 1$ for all $i \neq j$. Also assume that $r_i \equiv 0(p)$ for some i. Finally assume that the genus of $\mathscr{X}$ is at least 2. Then by (2.4) we see that $\mathscr{X}$ *cannot have a good reduction modulo p.*

3. Modular curves

Recall that for any ring A and positive integer m, the group of all m by m matrices with entries in A and with determinant a unit in A, is denoted by $\mathrm{GL}(m, A)$, and the subgroup of those matrices whose determinant is 1 is denoted by $\mathrm{SL}(m, A)$. Moreover $\mathrm{GL}(m, A)/\{\pm 1\}$ and $\mathrm{SL}(m, A)/\{\pm 1)$ are the factor groups by the subgroups consisting of the diagonal matrices with all the entries 1 or all the entries -1; in case of $\mathrm{SL}(m, A)$ we take the latter only if $(-1)^n = 1$. Likewise $\mathrm{PGL}(m, A)$ and $\mathrm{PSL}(m, A)$ are the factor groups of $\mathrm{GL}(m, A)$ and $\mathrm{SL}(m, A)$ by their subgroups of scalar matrices, i.e., diagonal matrices with all entries in the diagonal equal to each other.

*See Remark (3.3) of § 3.

For the finite field $\mathrm{GF}(q)$ of q elements, we may write $\mathrm{GL}(m,q)$, $\mathrm{SL}(m,q),\ldots$ and so on in place of $\mathrm{GL}(m,\mathrm{GF}(q))$, $\mathrm{SL}(m,\mathrm{GF}(q)),\ldots$ and so on. Note that the *projective special linear group* $\mathrm{PSL}(m,q)$ is a finite simple group provided $m \geqslant 2$ with the exclusion of $(m,q)=(2,2)$, $(2,3)$. Likewise, the *projective special unitary group* $\mathrm{PSU}(m,q)$ is a finite simple group provide $m \geqslant 2$ with the exclusion of $(m,q)=(2,2)$, $(2,3)$, $(3,2)$. For a discussion of unitary groups, reference may be made to [Car] or [Suz]. In particular note that the *general unitary group* $\mathrm{GU}(m,q)$ is the subgroup of those members of $\mathrm{GL}(m,q^2)$ which leave a Hermitian form invariant, the *special unitary group* $\mathrm{SU}(m,q)$ is the group consisting of those members of $\mathrm{GU}(m,q)$ whose determinant is 1, and the *projective general unitary group* $\mathrm{PGU}(m,q)$ and the *projective special unitary group* $\mathrm{PSU}(m,q)$ are the factor groups of $\mathrm{GU}(m,A)$ and $\mathrm{SU}(m,A)$ by their subgroups of scalar matrices. Also recall that $|\mathrm{PGL}(2,q)|=(q+1)q(q-1)$, $|\mathrm{PGL}(2,q)/\mathrm{PSL}(2,q)|=\mathrm{GCD}(2,q+1)$, $|\mathrm{PGU}(3,q)|=(q^3+1)q^3(q^2-1)$ and $|\mathrm{PGU}(3,q)/\mathrm{PSU}(3,q)|=\mathrm{GCD}(3,q+1)$; it follows that if q is a power of the prime p then $\mathrm{PSL}(2,q)$ (resp: $\mathrm{PSU}(3,q)$) is the only quasi-p normal subgroup of $\mathrm{PGL}(2,q)$ (resp: $\mathrm{PGU}(3,q)$) such that the corresponding factor group is cyclic. Now $\mathrm{PSL}(m,q)$ and $\mathrm{PSU}(m,q)$ are two of the 16 infinite families of finite simple groups (for a survey of finite simple groups see [A10]). The third infinite family of finite simple groups relevant to us is the family of *Suzuki groups* $\mathrm{Sz}(q)$ with $q=2^{2\nu+1}$ where ν is any positive integer. Note that $\mathrm{Sz}(q)$ is a certain subgroup of $\mathrm{GL}(4,q)$ and for its order we have $|\mathrm{Sz}(q)|=(q^2+1)q^2(q-1)$; this also holds for $q=2$, but $\mathrm{Sz}(2)$ is not simple. The relevance of the unitary groups and the Suzuki groups for us will become clear in (4.2.1) and (4.2.3) respectively.

For any positive integer n, let $\bar{\Gamma}(n)$ be the *inhomogeneous principal congruence subgroup of level* n, i.e., the kernel of the natural epimorphism

$$\mathrm{SL}(2,Z)/\{\pm 1\}\rightarrow \mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})/\{\pm 1\}.$$

Referring to [Sch] for details, $\mathrm{SL}(2,Z)/\{\pm 1\}$ acts in a natural way on the upper half plane $\mathfrak{H}$ (consisting of all complex numbers with positive imaginary part) and has the complex projective line $\mathscr{P}^1_{\mathbb{C}}$ as compactified quotient. This induces an action of $\bar{\Gamma}(n)$ on $\mathfrak{H}$ and now the compactified quotient is called the *modular curve* $\mathscr{X}(n)$ *of level* n. Clearly $\bar{\Gamma}(1)=\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$ and hence $\mathscr{X}(1)=\mathscr{P}^1_{\mathbb{C}}$. Let $\mathfrak{F}_{n,\mathbb{C}}$ be the function field of $\mathscr{X}(n)$. Then $\mathfrak{F}_{1,\mathbb{C}}$ is generated over $\mathbb{C}$ by the famous transcendental function j, and $\mathfrak{F}_{n,\mathbb{C}}/\mathfrak{F}_{1,\mathbb{C}}$ is a Galois extension with Galois group $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$.

Let $\mathbb{Q}_n$ be the field extension of $\mathbb{Q}$ obtained by adjoining to it all the nth roots of 1 in $\mathbb{C}$.* Then, referring to [Shi] for details, the modular curve $\mathscr{X}(n)$ is defined over $\mathbb{Q}_n$ in the sense that there are a finite number of generators $\{f_a : a\in n^{-1}\mathbb{Z}^2\backslash\mathbb{Z}^2\}$ of $\mathfrak{F}_{n,\mathbb{C}}$ over $\mathbb{C}(j)$, called Fricke functions in [Lan], which are algebraic over $\mathbb{Q}(j)$, and upon letting $\mathfrak{F}_n$ to be the field generated by them over $\mathbb{Q}(j)$ we have that the algebraic closure of $\mathbb{Q}$ in $\mathfrak{F}_n$ is $\mathbb{Q}_n$. Moreover, $\mathfrak{F}_n/\mathbb{Q}(j)$ and $\mathfrak{F}_n/\mathbb{Q}_n(j)$ are Galois extensions with Galois groups $\mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$ and $\mathrm{SL}(2,\mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$ respectively.

Henceforth assume that $n>6$. Then by the classical theory [Sch] it follows that $\mathfrak{F}_n/\mathbb{Q}_n(j)$ has exactly three branch points, which are all residually rational over $\mathbb{Q}_n$, and the ramification exponents of their extensions to $\mathfrak{F}_n$ are $2,3,n$. We can take a finite algebraic field extension $\mathbb{Q}^*_n$ of $\mathbb{Q}_{6n}$ in $\mathbb{C}$ such that, for any algebraic field extension k^*_n of $\mathbb{Q}^*_n$ in $\mathbb{C}$, upon letting K_n and L_n to be the compositums of $\mathbb{Q}_n(j)$

*Our notation $\mathbb{Q}_n$ should not be confused with the notation $\mathbb{Q}_l$ frequently used for l-adic numbers.

and $\mathfrak{F}_n$ with k_n^* we have that the extensions to L_n of any branch point of L_n/K_n are all residually rational over k_n^*. Now clearly K_n/k_n^* and L_n/k_n^* are 1-dimensional regular function fields, K_n/k_n^* is a simple transcendental extension, the genus of L_n/k_n^* is at least 2, L_n/K_n is a Galois extension with Galois group $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$ and with exactly three branch points, and the ramification exponents of their extensions to L_n are $2, 3, n$. By the (Riemann–Hurwitz) genus formula, it follows that *the genus of L_n/k_n^* is at least 2*.

Given a prime number p, in view of Lemma 12 on page 138 of [A07] we can take k_n^* to be the quotient field of a pseudogeometric DVR T_n such that $T_n/M(T_n)$ is an algebraic closure of $\mathrm{GF}(p)$. The following beautiful result was proved by Igusa [Igu] (for a more modern treatment see 4a on page 152 of [DRa] or Chapter 2 of [MWi] or Chapter 12 of [KMa]).

PROPOSITION 3.1.

If $n \not\equiv 0(p)$ then L_n/k_n^* has a good reduction L'_n/k'_n modulo $M(T_n)$.

Let K'_n be the corresponding reduction of K_n. Now, according to Feit [Fe1], if $\mathrm{GCD}(n, 6) = 1$ then $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$ is a quasi 2-group as well as a quasi 3-group. Therefore, in view of (3.1) and Abhyankar's Lemma (2.6), by (2.4) we get the following.

Theorem 3.2. *Assume that $n \not\equiv 0(p)$ and $p = 2$ or 3. Then K'_n is a simple transcendental extension of the algebraically closed field k'_n of characteristic p, L'_n/k'_n is a 1-dimensional regular function field of genus at least 2, L'_n/K'_n is a Galois extension with Galois group $SL(2, \mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$, and, for a suitable choice of x' with $K'_n = k'_n(x')$, we have that $x' = \infty$ is a nontame branch point of L'_n/K'_n, $x' = 0$ is the only other possible branch point of L'_n/K'_n, and the reduced ramification exponent of any extension to L of $x' = 0$ is a factor of $6n/p$. Moreover, if $GCD(n, 6) = 1$, then upon letting $\Lambda_n = L'_n(k_n(X))$, where X is an element in an overfield of L'_n with $X^{6n/p} = x'$ and k_n is any algebraically closed overfield of k'_n such that X is transcendental over k_n, we have that $\Lambda_n/k_n(X)$ is a Galois extension with $X = \infty$ as the only branch point and with Galois group $SL(2, \mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$.*

Note 3.2*. Let us call a group **anti-*p*** if it is finite and does not have any nonidentity normal subgroup whose order is a power of *p*; note that then a nonabelian finite simple group is always anti-*p*. Now in the situation of (2.3), assuming the characteristic of k' to be $p > 0$, the order of the kernel of ϕ_{gal} is a power of *p*, and hence if $\mathrm{Gal}(L/k^*)$ is an anti-*p* group then obviously (and hence without invoking the present proof of (2.3)) ϕ_{gal} is injective. According to Feit [Fe2], assuming $\mathrm{GCD}(n, 6) = 1$, the group $\mathrm{SL}(2, \mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$ is always anti-3, and moreover: it is anti-2$\Leftrightarrow n$ is a power of a single prime. Therefore in these cases of the above theorem we can disregard the present proof of (2.3).

Remark 3.3. Instead of considering good reductions when they exist, Mumford [MFo] introduces the more general concept of stable reduction, where the reduction is allowed to be a reducible curve but is required to be free from multiple components and have no singularities worse than nodes; it is also required that every rational component of the reduction intersect the other components in at least 3 different points so that the automorphism group of the reduction is always finite. He goes on to prove that it always exists provided we allow for a finite extension $\tilde{T}$ of T. In brief, start with any reduction, i.e., any arithmetic surface, over a pseudogeometric DVR T, with given generic fiber. Resolve its singularities by Abhyankar [A07] and Abhyankar [A09]. Then shrink unwanted (= exceptional) curves to get a minimal model à la [Lic] or [Saf] on which the special fiber is stable. To achieve this, we may have to make a "base change" by replacing T by an extension $\tilde{T}$ of T to a finite algebraic field extension $\tilde{k}$ of the quotient field k^* of T. So instead of saying "assume good reduction", we may say "assume the stable reduction to be good". Here the article "the" before "stable" is justified because Mumford proved that the stable reduction is essentially unique. If we follow this route, then we could shorten some of the proofs in § 1 and § 2 by citing Theorem 1.11 and Lemma 1.12 of [DMu]. We did not have to refer to [Lic] or [Saf] because we could fall back on [A01] where much of the ground work for minimal models in the arithmetical case was done.

In point of fact, Mumford was not doing all this only for reduction modulo p. His objective was to get a compact moduli variety M_g of curves of genus g. Namely, if we follow the classical approach and restrict to nonsingular curves of genus g, then the moduli variety is not compact. Permitting stable curves, makes it compact.

With the notion of stable curves at hand, we could have formulated Proposition (2.3) slightly more generally thus. For every geometrically irreducible curve of genus at least 2 over a perfect field k^*, by Corollary 2.7 of [DMu], we can find a finite algebraic field extension $\tilde{k}/k^*$ and an extension $\tilde{T}$ of T to $\tilde{k}$ such that reduction of the curve modulo $M(\tilde{T})$ is a stable curve. Given any subfield K of the function field L of the curve such that $k^* \subset K$ and L/K is Galois, by Theorem 1.11 and Lemma 1.12 of [DMu], every automorphism of L/K can be extended to a $\tilde{T}$-automorphism of the corresponding arithmetic surfaces such that no two automorphisms coincide after specialization. Therefore, we do not really need good models; it would be sufficient to demand that the stable reduction is irreducible, because then every automorphism of the special fiber defines a unique automorphism of the nonsingular model of this fiber. It seems to be a problem, however, to find a criterion, which shows irreducibility of the special fiber without proving nonsingularity.

Remark 3.4. The modular curve $\mathfrak{X}(n)$ can be interpreted as parametrizing the space of all elliptic curves (and their stable reductions) with a level-n-structure, i.e., with assigned basis for the group of points whose order divides n. In Deuring [De2] and [De3], it is shown that a similar interpretation can be given to $\mathfrak{X}(n)$ in characteristic $p > 0$ provided $n \not\equiv 0(p)$.* An alternative treatment of (3.2) could be based on this work of Deuring. Briefly, the inertia group of a point in the covering $\mathfrak{X}(n) \to \mathfrak{R}(k'_n(j)/k'_n)$ is equal to the reduced automorphism group of the elliptic curve which corresponds to that point, and hence by Deuring [De2] we obtain an explicit description of the said inertia group. According to Deuring, in characteristic 3 or 2, only the elliptic curves with $j = 0 = 12^3$ have nontrivial automorphisms. The reduced automorphism group of such a curve has order 6 or 12 according as the characteristic is 3 or 2. And so on.

*It may be noted that, in [MWi] and [KMa], an analogous interpretation of $\mathfrak{X}(n)$ for $n \equiv 0(p)$ is given, by using the so called Drinfeld bases.

4. Curves with big automorphism groups

Hurwitz Groups (4.1). By Hurwitz [Hur], a curve of genus $g \geqslant 2$ in characteristic zero has at most $84(g-1)$ automorphisms. This bound is sharp for infinitely many g. The structure of maximal automorphism groups is known: they are called Hurwitz groups and are defined as finite groups which can be generated by two elements of orders 2 and 3 respectively, whose product has order 7; they occur as Galois groups of characteristic zero coverings $\mathscr{X} \to \mathscr{P}^1$ with three ramification points of exponents 2, 3, and 7; for a survey of Hurwitz groups see [Con]. Therefore Hurwitz groups are candidates for Galois groups to be realized in characteristics 2, 3, and 7.

Klein Curve 4.1.1. In § 3 we assumed $n > 6$, and so $\mathscr{X}(7)$ was the smallest level modular curve which gave rise to an unramified covering of the affine line in positive characteristic, namely $p = 2$ and $p = 3$. The genus of $\mathscr{X}(7)$ is 3 and the resulting Galois group is $\mathrm{SL}(2, \mathbb{Z}/7\mathbb{Z})/\{\pm 1\} = \mathrm{PSL}(2, 7)$. In view of what was said in § 3, clearly $\mathscr{X}(7)$ is a Hurwitz curve. Klein [Kle] gave $x^3y + y^3z + z^3x = 0$ as a homogeneous equation for a plane model of $\mathscr{X}(7)$, and showed that its full automorphism group is indeed $\mathrm{PSL}(2, 7)$. Hence this is called the *Klein curve*. By direct calculation we see that, for $p = 2$ and $p = 3$, this equation gives a nonsingular irreducible curve. This confirms the fact that $\mathscr{X}(7)$ has good reductions modulo 2 and modulo 3 which, in view of Abhyankar's Lemma (2.6), by (2.4)[†] *give rise to unramified coverings of the affine line with Galois group* $\mathrm{PSL}(2, 7)$ *for* $p = 2$ *and* $p = 3$.

Macbeath Curve 4.1.2. Macbeath [Mac] showed that the next possible genus of a Hurwitz curve is 7, and constructed such a curve $\mathscr{X}$, which is now called the *Macbeath curve*, with full automorphism group $G = \mathrm{PSL}(2, 8)$. Regarding G as acting on the projective line over GF(8), its 1-point stabilizer G_1 is the group of all affine linear transformations $x \mapsto ax + b$ with a and b in GF(8) and $a \neq 0$. Upon letting $\mathscr{X}_1$ to be the quotient $\mathscr{X}/G_1$, Macbeath [Mac] has shown that $\mathscr{X}_1$ has genus zero and the Galois covering $\mathscr{X} \to \mathscr{X}_1$ has three ramification points with exponents 2, 7, and 7. We can find a specialization of $\mathscr{P}^1$ modulo 3 such that no two of these three points coincide, and then, in characteristic 3, construct a nonsingular covering with the same ramification exponents which is a specialization of the covering from characteristic zero. Since all three ramification points are tame, this covering again has genus 7. Thus $\mathscr{X}$ has good reduction modulo 3 and hence, in view of Abhyankar's Lemma (2.6), by (2.4)** *we get an unramified covering of the affine line in characteristic* 3 *with Galois group* $\mathrm{PSL}(2, 8)$. As indicated by Serre [Se6], an explicit equation for this covering can be deduced from the discussion of the Macbeath curve given in Serre [Se4].

Positive Characteristic 4.2. For an algebraically closed field k of positive characteristic p, it is no longer true that a curve of genus $g \geqslant 2$ has at most $84(g-1)$ automorphisms. In an effort to get some other bound, Leopoldt [Leo], Stichtenoth [Sti] and Henn [Hen] have studied curves with big automorphism groups G; in Satz 1 of his paper, Henn gives a complete list of all curves for which $|G| \geqslant 8g^3$. In all cases, the curves

[†] Since PSL(2, 7) is simple, the present proof of (2.3) can be avoided; see Note (3.2*).

**Since PSL(2, 8) is simple, the present proof of (2.3) can be avoided; see Note (3.2*).

are coverings of the projective line $\mathscr{P}^1_k$ with exactly one wild and at most one tame ramification point; (it may be noted that by pages 536–537 of [Sti], this is so whenever $g > 2$ and $|G| > 24g^2$). Using Abhyankar's Lemma (2.6), we can get rid of the tame ramification point, if it occurs, and therefore all these curves lead to examples of unramified coverings of $\mathscr{A}^1_k$. There are the following four series, all of which are given by equations for their affine plane models, where v is any positive integer and where "can be realized" means "belongs to $\pi_A(\mathscr{A}^1_k)$".

4.2.1. The unitary Fermat curve $x^n + y^n + 1 = 0$ with $n = p^v + 1$. Here $G = \mathrm{PGU}(3, p^v)$, and hence $\mathrm{PSU}(3, p^v)$ can be realized in characteristic p. (Henn [Hen] writes $\mathrm{PGU}(3, p^{2v})$ and $\mathrm{PSU}(3, p^{2v})$ for what we have called $\mathrm{PGU}(3, p^v)$ and $\mathrm{PSU}(3, p^v)$ respectively). (Another way of realizing $\mathrm{PSU}(3, p^v)$, by using Deligne–Lusztig curves, is indicated in Serre [Se3]).

4.2.2. The Fermat-like curve $x^n + y^m + 1 = 0$ with $n = p^v + 1$ and m a proper divisor of n. In this case, G has $C = \mathbb{Z}/m\mathbb{Z}$ as its centre, and $G/C \cong \mathrm{PGL}(2, p^v)$. Therefore $\mathrm{PSL}(2, p^v)$ can be realized in characteristic p. (For other ways of realizing $\mathrm{PSL}(2, p^v)$ see [A10] and [A16]).

4.2.3. The equation $x^q + x = y^{q+q'} + y^{q'+1}$ with $q = 2q'^2$ and $q' = 2^v$, in characteristic $p = 2$ has the Suzuki group $\mathrm{Sz}(2^{2v+1})$ as automorphism group. Therefore $\mathrm{Sz}(2^{2v+1})$ can be realized in characteristic $p = 2$. (Another way of realizing $\mathrm{Sz}(2^{2v+1})$, by using Deligne–Lusztig curves, is indicated in Serre [Se3]).

4.2.4. The equation $x^p - x = y^{1+p^n}$ for $n > 1$ also defines a curve with a big automorphism group G in characteristic p. The corresponding curve is a covering of $\mathscr{P}^1_k$ with only one ramification point, so G is explicitly realized; the structure of G has been determined by Serre [Se6].

5. Use of unramified abelian coverings

If $\mathscr{Y} \to \mathscr{A}^1_k$ is an unramified covering of the affine line over an algebraically closed field k of positive characteristic p, and if $\mathscr{Y}^* \to \mathscr{Y}$ is an unramified covering of $\mathscr{Y}$, then, of course, we get as new unramified covering $\mathscr{Y} \to \mathscr{A}^1_k$. This holds in particular, even if we have an unramified covering $\mathscr{X}^* \to \mathscr{X}$ where $\mathscr{X} \to \mathscr{P}^1_k$ is the corresponding covering of the projective line which is ramified only at ∞. Among the unramified coverings $\mathscr{X}^* \to \mathscr{X}$, the abelian ones are well-known: They correspond biuniquely to the finite subgroups of the Jacobian $\mathrm{Jac}(\mathscr{X})$ (see for example [De1] or [Se1]). Therefore we get the following.

Theorem 5.1. *Let $\mathscr{X} \to \mathscr{P}^1_k$ be a Galois covering with Galois group G, ramified only at ∞, and let N be a finite subgroup of Jac $(\mathscr{X})$, invariant under all automorphisms of $\mathscr{X}$. Then there exists a covering $X^* \to \mathscr{P}^1_k$, ramified only at ∞, whose Galois group G^* is an extension of G with kernel N.*

This implies, in particular, that G^* is a quasi p-group. Note that for group extensions which are *known* to be quasi-p, Serre [Se2] has proved a stronger result which says that: with G as above, for any extension

$$0 \to N \to G^* \to G \to 0$$

with solvable kernel N and a quasi-p group G, we have $G^* \in \pi_A(\mathscr{A}_k^1)$.

By corollary 1 on page 127 of [Wei] we know that, for any positive integer l nondivisible by p, the points of Jac($\mathscr{X}$) whose order divides l constitute a subgroup which is isomorphic to $(\mathbb{Z}/l\mathbb{Z})^{2g}$. Therefore as a consequence of (5.1) we get the following.

COROLLARY 5.2

Let $\mathscr{X} \to \mathscr{P}_k^1$ be a Galois covering with Galois group G, ramified only at ∞, and let g be the genus of $\mathscr{X}$. Then, for any l prime to p, there exists an extension

$$0 \to (\mathbb{Z}/l\mathbb{Z})^{2g} \to G^* \to G \to 0$$

for which we have $G^* \in \pi_A(\mathscr{A}_k^1)$.

As in §4 of [A12], while keeping G unchanged, we can make the genus of $\mathscr{X}$ arbitrarily large. Therefore by (5.2) we get the following.

COROLLARY 5.3

Given any $1 \neq G \in \pi_A(\mathscr{A}_k^1)$, for every positive integer $l \not\equiv 0(p)$ and for infinitely many positive integers γ, some extension of G with kernel $(\mathbb{Z}/l\mathbb{Z})^{2\gamma}$ belongs to $\pi_A(\mathscr{A}_k^1)$.

6. Problems

Problem 6.1. Given an algebraically closed field k of characteristic $p > 0$, for several quasi p-groups G we have constructed Galois extensions $\Lambda/k(X)$ which are ramified only at $X = \infty$ and whose Galois group is G. It would be interesting to find explicit expressions for small degree monic polynomials in Y with coefficients in $k[X]$ and with splitting field Λ.

Problem 6.2. In (2.7) we have given necessary conditions for the existence of good reduction. Can we refine these into sufficient conditions?

Acknowledgements

Abhyankar's work was partly supported by NSF grant DMS 91-01424 and NSA grant MDA 904-92-H-3035.

As in all Galois theory considerations, thanks are due to Feit and Serre for useful discussions.

References

[A01] Abhyankar S S, On the valuations centered in a local domain, *Am. J. Math.* **78** (1956) 321–348

[A02] Abhyankar S S, Simultaneous resolution for algebraic surfaces, *Am. J. Math.* **78** (1956) 761–790

[A03] Abhyankar S S, Coverings of algebraic curves, *Am. J. Math.* **79** (1957) 825–856

[A04] Abhyankar S S, Ramification Theoretic Methods in Algebraic Geometry, 1959 (Princeton: University Press)

[A05] Abhyankar S S, Tame coverings and fundamental groups of algebraic varieties, Part III: Some other sets of conditions for the fundamental group to be abelian, *Am. J. Math.* **82** (1960) 179–190

[A06] Abhyankar S S, Uniformization of Jungian local domains, *Math. Ann.* **159** (1965) 1–43

[A07] Abhyankar S S, Resolution of singularities of arithmetical surfaces, Arithmetical Algebraic Geometry, (Harper and Row) (1965) 111–152

[A08] Abhyankar S S, Resolution of Singularities of Embedded Algebraic Surfaces, 1966 (New York: Academic Press)

[A09] Abhyankar S S, Resolution of singularities of algebraic surfaces, *Proceedings of 1968 Bombay Int. Colloq. Algebraic Geometry held at the Tata Institute of Fundamental Research*, (1969) (Oxford University Press), 1–11

[A10] Abhyankar S S, Galois theory on the line in nonzero characteristic, *Bull. Am. Math. Soc.* **27** (1992) 68–133

[A11] Abhyankar S S, Square-root parametrization of plane curves, Algebraic Geometry and Applications, *Collection of papers from Shreeram Abhyankar's 60th Birthday Conference*, (Springer) (to appear)

[A12] Abhyankar S S, Group enlargements, *C.R. Acad. Sci. Paris* **312** (1991) 763–768

[A13] Abhyankar S S, Alternating group coverings of the affine line for characteristic greater than two, *Math. Ann.* (to appear)

[A14] Abhyankar S S, Wreath product and enlargements of groups, Discrete Mathematics, (to appear)

[A15] Abhyankar S S, Linear disjointness of polynomials, *Proc. Am. Math. Soc.* **116** (1992) 7–12

[A16] Abhyankar S S, Fundamental group of the affine line in positive characteristic, *Proc. of 1992 Bombay Int. Colloq. on Geometry and Analysis held at the Tata Institute of Fundamental Research*, (to appear)

[AOS] Abhyankar S S, Ou J and Sathaye A, Alternating group coverings of the affine line in characteristic two, *Discrete Math.* (to appear)

[APS] Abhyankar S S, Popp H and Seiler W K, Mathieu-group coverings of the affine line, *Duke Math. J.* **68** (1992) 301–311

[AYi] Abhyankar S S and Yie I, Small degree coverings of the affine line in characteristic two, *Discrete Math.* (to appear)

[Con] Conder M, Hurwitz groups: a brief survey, *Bull. Am. Math. Soc.* **23** (1990) 359–370

[De1] Deuring M, Zur arithmetischen Theorie der algebraischen Funktionenkörper, *Math. Ann.* **106** (1932) 77–106

[De2] Deuring M, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Univ. Hamburg* **14** (1941) 197–272

[De3] Deuring M, Zur Theorie der elliptischen Funktionenkörper, *Abh. Math. Sem. Univ. Hamburg* **15** (1945) 211–261

[DMu] Deligne P and Mumford D, The irreducibility of the space of moduli of a given genus, *Publ. Math. IHES* **36** (1969) 75–110

[DRa] Deligne P and Rapoport M, Les schémas de modules de courbes elliptiques, Modular functions of one variables II, *Springer Lecture Notes in Math.* **349** (1973) 143–316

[Fe1] Feit W, *e-mail to Abhyankar dated* 13 *August* 1992

[Fe2] Feit W, *e-mail to Abhyankar dated* 7 *October* 1992

[Hen] Henn H W, Funktionenkörper mit grosser Automorphismengruppe, *Crelle J.* **302** (1978) 96–115

[Hir] Hironaka H, A note on algebraic geometry over ground rings, *Ill. J. Math.* **2** (1958) 355–366

[Hur] Hurwitz A, Über algebraische Gebilde mit eindeutigen Transformationen in sich, *Math. Ann.* **41** (1893) 403–442

[Igu] Igusa J I, Kroneckerian model of fields of elliptic modular functions, *Am. J. Math.* **81** (1959) 561–577

[KMa] Katz N M and Mazur B, Arithmetic Moduli of Elliptic Curves, (Princeton: University Press) 1985

[Kle] Klein F, Über die Transformationen siebenter Ordnung der elliptischen Funktionen, *Math. Ann.* **14** (1879) 428–471

[Lam] Lamprecht, Restabbildungen von Divisoren, *Archiv. Math.* **8** (1957) 255–264

[Lan] Lang S, Elliptic Functions, (Reading: Addison Wesley) 1973

[Leo] Leopoldt H W, Über die Automorphismengruppe des Fermatkörpers, Unpublished (1970)

[Lic] Lichtenbaum S, Curves over discrete valuation rings, *Am. J. Math.* **90** (1968) 380–405

[Mac] Macbeath A M, On a curve of genus 7, *Proc. London Math. Soc.* **15** (1965) 527–542

[MWi] Mazur B and Wiles A, Class fields of abelian extensions of $\mathbb{Q}$, Invent. Math. **76** (1984) 179–330

[Mil] Milne J S, *Jacobian varieties*, Arithmetic Geometry, (ed) G Cornell and J S Silverman (1985) (Springer) 167–212

[Mum] Mumford D, *Abelian Varieties*, (Oxford University Press) 1974

[MFo] Mumford D and Fogarty J, *Geometric Invariant Theory*, (Springer) 1982

[Nag] Nagata M, *Local Rings*, (New York: Interscience) 1962

[Nor] Nori M V, Unramified coverings of the affine line in positive characteristic, Algebraic Geometry and Applications, *Collection of papers from Shreeram Abhyankar's 60th Birthday Conference*, (Springer), (to appear)

[Pop] Popp H, Über das Verhalten des Geschlechts eines Funktionenkörpers einer Variablen bei Konstantenreduktion, *Math. Zeit.* **106** (1968) 17–35

[Saf] Šafarevič I R, Lectures on Minimal Models and Birational Transformations, Tata Institute of Fundamental Research, 1966

[Sch] Schoeneberg B, *Elliptic Modular Functions*, (Berlin: Springer–Verlag) 1974

[Se1] Serre J P, *Groupes algébriques et corps de classes*, (Paris: Hermann) 1959

[Se2] Serre J P, Construction de revêtements étales de la droite affine en caractéristique p, *C. R. Acad. Sci. Paris* **311** (1990) 341–346

[Se3] Serre J P, Letter to Abhyankar dated 15 November 1988

[Se4] Serre J P, Letter to Abhyankar dated 24 July 1990

[Se5] Serre J P, A letter as an appendix to the square-root parametrization paper of Abhyankar, Algebraic Geometry and Applications, *Collection of papers from Shreeram Abhyankar's 60th Birthday Conference*, Springer (to appear)

[Se6] Serre J P, Letter to Abhyankar dated 14 September 1992

[Shi] Shimura G, *Arithmetic Theory of Automorphic Functions*, (Princeton: University Press) 1971

[Sti] Stichtenoth H, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, *Archiv Math.* **24** (1973) I: 527–544, II: 615–631

[Wei] Weil A, *Variétés Abéliennes et Courbes Algébriques*, (Paris: Herrman) 1948

[ZSa] Zariski O and Samuel P, *Commutative Algebra*, vols I and II, (Princeton: Van Nostrand) 1958 and 1960