JOURNAL OF ALGEBRA 125, 236–255 (1989)

Ramified Primes in the Field of Moduli of Branched Coverings of Curves

SYBILLA BECKMANN[1]

Department of Mathematics, Yale University, P.O. Box 2155, Yale Station, New Haven, Connecticut 06520

Communicated by Walter Feit

Received April 27, 1988

INTRODUCTION

The problem motivating this paper is to determine the fields of definition and the field of moduli of a branched covering of a curve over $\mathbb{C}$ from its topological description.

Roughly speaking, F is a field of definition of a curve $\mathscr{C}$ if the curve is the locus of polynomial equations whose coefficients all lie in F. The situation is similar for coverings. The field of moduli of a covering is, at least in certain circumstances, the intersection of all fields of definition, so it is a natural object of study.

From a topological viewpoint, to give a branched covering of a curve $\mathscr{D}$ is to give a subgroup of the fundamental group of $\mathscr{D}$ minus the branch points of the covering. The Riemann Existence Theorem (see [Fu, Proposition 1.2] and [GAGA]) says that if $\mathscr{D}$ is an algebraic curve, then any branched covering, $\mathscr{C} \to \mathscr{D}$, of $\mathscr{D}$ is (equivalent to one which is) algebraic. If $\mathscr{D}$ and the branch points of $\mathscr{D}$ are defined over a number field F then the branched covering is defined over some number field. The motivating problem above is to determine the relationship between the topological data for a branched covering and the resulting number fields.

One reason to study the above problem is that if a branched covering is galois, with galois group G, if $\mathscr{D} = \mathbb{P}^1$, and if the covering is defined over $\mathbb{Q}$, then by Hilbert's Irreducibility Theorem (see [L DG]) the group G occurs as a galois group over $\mathbb{Q}$.

The main result here is roughly as follows. Let $\mathscr{D}$ be an algebraic curve over $\mathbb{C}$ which is also defined over a number field F. Let $\mathscr{C} \xrightarrow{G} \mathscr{D}$ be a G-galois branched covering whose branch points are defined over a finite

[1] Research partially supported by NSF grant DMS 8512904.

0021-8693/89 $3.00

extension of F. Then the field of moduli of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ is ramified only over a subset of the union of

(1) the primes of bad reduction of $\mathscr{D}$,

(2) the primes dividing the degree of the covering, $|G|$, and

(3) the primes $\mathfrak{p}$ for which the branch locus becomes singular modulo $\mathfrak{p}$.

To illustrate the primes in (3), let $\mathscr{D} = \mathbb{P}^1$ and consider the affine patch $\mathrm{Spec}(\mathbb{C}[x])$. Suppose the branch locus of the covering is given by the ideals $(x-a_1)$, $(x-a_2)$, ..., $(x-a_r)$, where the a_i are all rational integers. Then the primes for which the branch locus becomes singular are the primes which divide some $a_i - a_j$ $(i \neq j)$.

The strategy of the proof is as follows: We first establish that the primes which ramify in the field of moduli are contained in the primes of bad reduction of the covering (Section 3). We then show that the primes of bad reduction of the covering are contained in the primes of (1), (2) and (3) (Sections 4 and 5).

Theorem 5.5 is a generalization of Theorem 3.5.3 of [B th]. The proof uses different techniques.

Notation and Conventions

If K is a number field then $\mathcal{O}_K$ denotes its ring of integers. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $\mathcal{O}_\mathfrak{p}$ denotes the localization of $\mathcal{O}_K$ at $\mathfrak{p}$.

Let $A \subset B$ be rings, with B of finite type over A. Let $\mathfrak{p}$ be a prime ideal of A and let $\mathfrak{q}$ be a prime ideal of B lying over $\mathfrak{p}$ (i.e. $\mathfrak{q} \cap A = \mathfrak{p}$). Then the extension $A \subset B$ is *unramified at* $\mathfrak{q}$ if $\mathfrak{p} \cdot B_\mathfrak{q} = \mathfrak{q} \cdot B_\mathfrak{q}$, and $B_\mathfrak{q}/\mathfrak{q} \cdot B_\mathfrak{q}$ is a separable extension of $A_\mathfrak{p}/\mathfrak{p} \cdot A_\mathfrak{p}$. If this fails to hold, then the extension is *ramified at* $\mathfrak{q}$. If B is unramified over every prime ideal which lies over $\mathfrak{p}$ then $\mathfrak{p}$ is *unramified in B*.

Section 1. Background Material and the Basic Setup

Throughout this paper, let $\mathscr{C} \to \mathscr{D}$ be a finite, dominant morphism of connected, complete, smooth curves over $\mathbb{C}$; this will be called a *branched covering* (of curves).

Let G be a finite group. Assume that $\mathbb{C}(\mathscr{C})$ is galois over $\mathbb{C}(\mathscr{D})$ with group G, where $\mathbb{C}(\mathscr{C})$ and $\mathbb{C}(\mathscr{D})$ denote the function fields of $\mathscr{C}$ and $\mathscr{D}$

respectively. The covering $\mathscr{C} \to \mathscr{D}$, together with a fixed G-action on $\mathscr{C}$ (or $\mathbb{C}(\mathscr{C})$), is called a *G-galois branched covering*, and is denoted $\mathscr{C} \xrightarrow{G} \mathscr{D}$.

The *branch points* of $\mathscr{C} \to \mathscr{D}$ are the points of $\mathscr{D}$ for which the number of points in the inverse image is less than the degree of the map (the degree is the same as $[\mathbb{C}(\mathscr{C}): \mathbb{C}(\mathscr{D})]$). (See [SGAI] for the definition of branch locus for morphisms in general.)

Assume that $\mathscr{D}$, and some point of $\mathscr{D}$, are defined over a number field F. In other words, there is a curve $\mathscr{D}_F$ which is connected, complete, and smooth over F, such that $\mathscr{D}_F \times_F \mathbb{C} \cong \mathscr{D}$. $\mathscr{D}_F$ will be called a *model for $\mathscr{D}$ over F*. If K is an extension of F then $\mathscr{D}_K$ will always mean $\mathscr{D}_F \times_F K$, the induced model for $\mathscr{D}$ over K.

Since $\mathscr{D}_F \times_F \mathbb{C} \cong \mathscr{D}$, there is a map $\mathscr{D} \to \mathscr{D}_F$. If P is a closed point of $\mathscr{D}$ then P *is defined over F* if the image of P in $\mathscr{D}_F$ is a closed point, and its residue field is F.

We will assume that each of the branch points of $\mathscr{C} \to \mathscr{D}$ is defined over some finite extension of F.

If $K \subset \mathbb{C}$ is an extension of F and if there are models $\mathscr{C}_K$, $\mathscr{D}_K$ for $\mathscr{C}$ and $\mathscr{D}$ over K and a finite morphism $\mathscr{C}_K \to \mathscr{D}_K$ which induces $\mathscr{C} \to \mathscr{D}$, then K is called a *field of definition* of $\mathscr{C} \to \mathscr{D}$. If, in addition, the function field extension, $K(\mathscr{C})/K(\mathscr{D})$, corresponding to $\mathscr{C}_K \to \mathscr{D}_K$ is galois with group G, then K is called a *field of definition of the G-galois branched covering* $\mathscr{C} \xrightarrow{G} \mathscr{D}$. Again, we write $\mathscr{C}_K \xrightarrow{G} \mathscr{D}_K$ to denote the covering together with a fixed G-action. Note that K is algebraically closed in both $K(\mathscr{C})$ and $K(\mathscr{D})$.

For example, $\mathbb{Q}(\zeta_3)$ (where ζ_3 denotes a primitive cube root of unity) is a field of definition of the $\mathbb{Z}/3$-galois covering corresponding to the field extension $\mathbb{C}(x) \subset \mathbb{C}(x)[y]/(y^3 - x)$ because $\mathbb{Q}(\zeta_3)(x) \subset \mathbb{Q}(\zeta_3)(x)[y]/(y^3 - x)$ is galois with group $\mathbb{Z}/3$, while $\mathbb{Q}$ is a field of definition of the covering without its group action.

If σ is an automorphism of $\mathbb{C}$ leaving F fixed then since $\mathscr{D}$ is defined over F (with model $\mathscr{D}_F$), σ induces a G-galois branched covering $\mathscr{C}^\sigma \xrightarrow{G} \mathscr{D}$ (where the G-action is the induced one). The *field of moduli* of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ (with respect to the model $\mathscr{D}_F$) is the fixed field in $\mathbb{C}$ of those automorphisms of $\mathbb{C}$ over F which take $\mathscr{C} \xrightarrow{G} \mathscr{D}$ to an equivalent G-galois covering. Two G-galois branched coverings $\mathscr{C} \xrightarrow{G} \mathscr{D}$ and $\mathscr{B} \xrightarrow{G} \mathscr{D}$ are called *equivalent* if there is an isomorphism from $\mathscr{B}$ onto $\mathscr{C}$ which factors through the identity on $\mathscr{D}$ and which takes the G-action on $\mathscr{B} \xrightarrow{G} \mathscr{D}$ to the G-action on $\mathscr{C} \xrightarrow{G} \mathscr{D}$.

Similarly, the *field of moduli* of $\mathscr{C} \to \mathscr{D}$ (*without* the G-action) is the fixed field in C of those automorphisms of $\mathbb{C}$ over F which take $\mathscr{C} \to \mathscr{D}$ to an equivalent covering, where $\mathscr{C} \to \mathscr{D}$ and $\mathscr{B} \to \mathscr{D}$ are *equivalent* if there is an isomorphism from $\mathscr{B}$ onto $\mathscr{C}$ which factors through the identity on $\mathscr{D}$.

The field of moduli of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ is the intersection of all fields of definition of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ [C–H, Proposition 2.7] but the field of moduli need not be a field of definition (e.g., see [C–H, Example 2.6]). On the other hand, the field of moduli of $\mathscr{C} \to \mathscr{D}$ (without the group action) is the unique minimal field of definition of $\mathscr{C} \to \mathscr{D}$ [C–H, Proposition 2.5].

Since the branch points of $\mathscr{C} \to \mathscr{D}$ are defined over a finite extension of F, there is a *finite*, galois extension K of F, such that the branch points of $\mathscr{C} \to \mathscr{D}$ are all defined over F and such that K is a field of definition of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ (see, e.g., [C–H, Section 2]).

Assume there is a Noetherian, normal, connected scheme, $\mathscr{D}_F^\circ$ over $\mathcal{O}_F$ such that $\mathscr{D}_F^\circ \times_{\mathcal{O}_F} F \cong \mathscr{D}_F$ and such that the morphism from $\mathscr{D}_F^\circ$ to $\mathcal{O}_F$ is flat, proper, and of finite type. Such a scheme will be called a *normal model for* $\mathscr{D}_F$ *over* $\mathcal{O}_F$. Let $\mathscr{D}_K^\circ$ and $\mathscr{C}_K^\circ$ be the induced normal models for $\mathscr{D}_K$ and $\mathscr{C}_K$ over $\mathcal{O}_K$ (recall from the previous paragraph that K is a finite, galois extension of F over which $\mathscr{C} \xrightarrow{G} \mathscr{D}$ is defined). If $\mathscr{D}_F^\circ$ is given by affine patches Spec R_1, Spec R_2, ..., then $\mathscr{D}_K^\circ$ is just given by the affine patches Spec S_1, Spec S_2, ..., where S_i is the integral closure of R_i in $K(\mathscr{D})$. So there is a finite morphism $\mathscr{C}_K^\circ \to \mathscr{D}_K^\circ$. We will also refer to $\mathscr{C}_K^\circ \to \mathscr{D}_K^\circ$ as a covering. The group G acts on $\mathscr{C}_K^\circ$, so we will write $\mathscr{C}_K^\circ \xrightarrow{G} \mathscr{D}_K^\circ$ to denote the covering, together with the fixed group action on $\mathscr{C}_K^\circ$. Warning: $\mathscr{D}_K^\circ$ need not be $\mathscr{D}_F^\circ \times_{\mathcal{O}_F} \mathcal{O}_K$ (although this is true locally if $\mathscr{D}_F^\circ$ has good reduction). For example, consider the covering corresponding to the extension, $\mathbb{Z}[x] \subset \mathbb{Z}[x, y]/(y^2 - 3x)$, of integrally closed domains. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{3})$. Then $\mathbb{Z}[\sqrt{3}][x, y]/(y^2 - 3x)$ is not integrally closed.

Since $\mathscr{D} \cong \mathscr{D}_K^\circ \times_{\mathcal{O}_K} \mathbb{C}$, there is a map $\mathscr{D} \to \mathscr{D}_K^\circ$. Now the branch locus of $\mathscr{C} \to \mathscr{D}$ is a finite set of points of $\mathscr{D}$. Their image in $\mathscr{D}_K^\circ$ (think of "spreading out" the points over $\mathcal{O}_K$) is a subscheme whose irreducible components may meet at various points.

1.1. Definition. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$. The branch locus of $\mathscr{C} \to \mathscr{D}$ *does not become singular modulo* $\mathfrak{p}$ if no two irreducible components of the image of the branch locus in $\mathscr{D}_K^\circ$ meet in the fiber over $\mathfrak{p}$. (See the Introduction for an example.)

Summary of Notation and Assumptions

$\mathscr{C} \xrightarrow{G} \mathscr{D}$ is a G-galois branched covering over $\mathbb{C}$; $\mathbb{C}(\mathscr{C})/\mathbb{C}(\mathscr{D})$ is the corresponding G-galois function field extension.

$\mathscr{C}_K \xrightarrow{G} \mathscr{D}_K$ is a model for $\mathscr{C} \xrightarrow{G} \mathscr{D}$ over a number field K; $K(\mathscr{C})/K(\mathscr{D})$ is the corresponding G-galois function field extension.

$\mathscr{C}_K^\circ \xrightarrow{G} \mathscr{D}_K^\circ$ is a normal model for $\mathscr{C}_K \xrightarrow{G} \mathscr{D}_K$ over $\mathcal{O}_K$.

$\mathscr{D}_F^\circ$ is a normal model for $\mathscr{D}$ over $\mathcal{O}_F$.

K (as above) is a finite, galois extension of F, and $\mathscr{D}_F^\circ$ induces $\mathscr{D}_K^\circ$.

The branch points of $\mathscr{C} \to \mathscr{D}$ are defined over K. Some point of $\mathscr{D}$ is defined over F.

Section 2. Good Reduction and Integral Reduction

Recall that $\mathscr{C}_K \xrightarrow{G} \mathscr{D}_K$ is a G-galois branched covering over a number field K, with corresponding function field extension $\mathscr{K}(\mathscr{C})/K(\mathscr{D})$ which is galois with galois group G. $\mathscr{C}_K^\circ \xrightarrow{G} \mathscr{D}_K^\circ$ is the corresponding covering over $\mathcal{O}_K$.

If $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}_K$ with residue field $k = \mathcal{O}_K/\mathfrak{p}$ then we will denote $\mathscr{D}_K^\circ \times_{\mathcal{O}_K} k$ by $\mathscr{D}_k$, called the reduction modulo $\mathfrak{p}$ of $\mathscr{D}_K^\circ$. If $\mathscr{D}_k$ is reduced and irreducible we will denote its function field by $k(\mathscr{D})$.

2.1. Definitions. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_k$ and let $k = \mathcal{O}_K/\mathfrak{p}$. $\mathscr{D}_K^\circ$ has *good reduction at* $\mathfrak{p}$ if $\mathscr{D}_k$ is connected and smooth over k and if k is algebraically closed in $k(\mathscr{D})$. The covering $\mathscr{C}_K^\circ \xrightarrow{G} \mathscr{D}_K^\circ$ has good reduction at $\mathfrak{p}$ if both $\mathscr{C}_K^\circ$ and $\mathscr{D}_K^\circ$ have good reduction at $\mathfrak{p}$ and the field extension $k(\mathscr{C})/k(\mathscr{D})$ is galois with group $G = \mathrm{gal}(\mathscr{C}/\mathscr{D}) = \mathrm{gal}(K(\mathscr{C})/K(\mathscr{D}))$. $\mathscr{D}_K^\circ$ has *integral reduction at* $\mathfrak{p}$ if $\mathscr{D}_k$ is integral (i.e., reduced and irreducible) and k is algebraically closed in $k(\mathscr{D})$. The covering $\mathscr{C}_K^\circ \xrightarrow{G} \mathscr{D}_K^\circ$ has integral reduction at $\mathfrak{p}$ if $\mathscr{C}_k$ and $\mathscr{D}_k$ both have integral reduction at $\mathfrak{p}$ and the field extension $k(\mathscr{C})/k(\mathscr{D})$ is galois with group G.

Note that good reduction implies integral reduction.

Here are the above definitions translated into ring-theoretic terms.

2.2. Lemma. *$\mathscr{D}_K^\circ$ has integral reduction (respectively good reduction) at $\mathfrak{p}$ if and only if for every local ring A of a closed point on $\mathscr{D}_K^\circ$ in the fiber over $\mathfrak{p}$,*

(*) *the ring $A/\mathfrak{p} \cdot A$ is an integral domain (respectively a regular local ring of dimension one) and*

(**) *$k = \mathcal{O}_K/\mathfrak{p}$ is algebraically closed in $A/\mathfrak{p} \cdot A$.*

Proof. If $\mathscr{D}_K^\circ$ has integral (respectively good) reduction then it is clear (using the fact that smooth over k implies regular, see [M, Theorem 61]) that Conditions (*) and (**) hold for every local ring A of a closed point on $\mathscr{D}_K^\circ$ in the fiber over $\mathfrak{p}$.

Conversely, assume that (*) and (**) hold. We first show that $\mathscr{D}_k$ is connected. By the Stein factorization theorem, [H, Corollary 11.5 and Remark 11.1.1, or EGA III, Section 4], $f: \mathscr{D}_K^\circ \to \mathrm{Spec}(\mathcal{O}_K)$ can be factored as $g \circ f'$, where f' is a morphism with connected fibers and g is a finite morphism. But since K is algebraically closed in $K(\mathscr{C})$ and since $\mathcal{O}_K$ is integrally closed, f does not dominate any finite morphisms. Therefore f has connected fibers.

If $\mathscr{D}_K^\circ$ does not have integral reduction then there is some connected, affine open set of $\mathscr{D}_k$ such that the ring of functions on this open set is not an integral domain. Let B denote this ring of functions. Let $0 \neq b \in B$ be a zero divisor. Then since every prime ideal of B must contain either b or its annihilator, $\mathrm{Ann}(b)$, connectedness implies that some maximal ideal, $\mathfrak{b}$, of B contains both b and $\mathrm{Ann}(b)$. Thus b is a non-zero zero divisor in $B_\mathfrak{b}$. But now this is a contradiction, since $B_\mathfrak{b}$ is a local ring of the form $A/\mathfrak{p}\cdot A$ as in Condition $(*)$. The case of good reduction now follows from the fact that a local ring of dimension one containing $k = \mathcal{O}_K/\mathfrak{p}$ is smooth over k if and only if it is a regular local ring, see [M, Section 29]. ∎

2.3. *Remarks.* If $(*)$ holds then the above proof shows that $\mathscr{C}_k$ is integral. In this case $(**)$ is equivalent to: k is algebraically closed in $k(\mathscr{D})$. If Condition $(*)$ holds for all sufficiently large number fields K then Condition $(**)$ automatically holds. Also, if some point of $\mathscr{D}_K$ is defined over K, then its reduction modulo $\mathfrak{p}$ is defined over k, and again k is algebraically closed in $k(\mathscr{D})$.

Good reduction and integral reduction for coverings and for curves are almost the same.

2.4. LEMMA. *Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$. Assume that the characteristic of $\mathcal{O}_K/\mathfrak{p}$ does not divide the order of $G = \mathrm{gal}(\mathscr{C}/\mathscr{D})$. If both $\mathscr{D}_K^\circ$ and $\mathscr{C}_K^\circ$ have good (respectively integral) reduction at $\mathfrak{p}$ then the covering $\mathscr{C}_K^\circ \xrightarrow{G} \mathscr{D}_K^\circ$ has good (respectively integral) reduction at $\mathfrak{p}$.*

Proof. We must show that the reduced covering $\mathscr{C}_k \to \mathscr{D}_k$ is galois with galois group G.

Let A be the local ring of a point on $\mathscr{D}_K^\circ$ in the fiber over $\mathfrak{p}$ and let B be the integral closure of A in $K(\mathscr{C})$. Then by either integral reduction or good reduction, $\mathfrak{p}\cdot A$ and $\mathfrak{p}\cdot B$ are prime ideals of A and B respectively. Let $A_\mathfrak{p}$, $B_\mathfrak{p}$ be the localizations of A and B at $\mathfrak{p}\cdot A$ and $\mathfrak{p}\cdot B$ respectively. Then $k(\mathscr{D}) = A_\mathfrak{p}/\mathfrak{p}\cdot A_\mathfrak{p}$ and $k(\mathscr{C}) = B_\mathfrak{p}/\mathfrak{p}\cdot B_\mathfrak{p}$.

Since $\mathscr{D}_K^\circ$ is normal, A is integrally closed. Thus $A_\mathfrak{p}$ is a discrete valuation ring (dvr), because $\mathfrak{p}\cdot A$ is a prime ideal of A of height one. Similarly, $B_\mathfrak{p}$ is also a dvr. By applying the formula $\sum e_i f_i = n$ [S LF, Section 4, Proposition 10] to $A_\mathfrak{p} \subset B_\mathfrak{p}$, we have $[k(\mathscr{C})\colon k(\mathscr{D})] = [K(\mathscr{C})\colon K(\mathscr{D})]$. Since $[K(\mathscr{C})\colon K(\mathscr{D})] = |G|$ is prime to the characteristic of $k(\mathscr{D})$, it follows from [S LF, I, Section 7, Proposition 20] that $k(\mathscr{C})$ is a galois extension of $k(\mathscr{D})$ with galois group isomorphic to G. ∎

Good reduction and integral reduction behave well under base change, as the next proposition shows.

2.5. PROPOSITION. *Let L be a finite extension of K. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$, let $\mathfrak{q}$ be a maximal ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$, and let $k = \mathcal{O}_K/\mathfrak{p}$ and $l = \mathcal{O}_L/\mathfrak{q}$ be the corresponding residue fields.*

(a) *If $\mathscr{D}_K^\circ$ has good (respectively integral) reduction at $\mathfrak{p}$, then $\mathscr{D}_L^\circ$ has good (respectively integral) reduction at $\mathfrak{q}$.*

(b) *If either condition in* (a) *holds then $l(\mathscr{D}) \cong l \otimes_k k(\mathscr{D})$.*

We first need a lemma.

2.6. LEMMA. *Let R be a Noetherian domain and let T be the integral closure of R (in its fraction field). Assume that $\alpha \in R$ generates a prime ideal of R of height one. Then α generates a prime ideal in T.*

Proof. First observe that $R_{(\alpha)}$ is a regular local ring of dimension one since its maximal ideal is generated by α. Therefore $R_{(\alpha)}$ is integrally closed. Let $S = R - (\alpha)$. Then $S^{-1}T$ is integral over $S^{-1}R = R_{(\alpha)}$, and so $S^{-1}T = R_{(\alpha)}$. Now S does not meet any prime ideal of T lying over (α). Therefore the prime ideal $\mathfrak{p}$ of T, defined by $\mathfrak{p} = \alpha \cdot R_{(\alpha)} \cap T$, is the only prime ideal of T lying over (α) and hence the only height one prime ideal of T containing α. Note that $T_\mathfrak{p} = R_{(\alpha)}$ and $\mathfrak{p} \cdot T_\mathfrak{p} = \alpha \cdot R_{(\alpha)}$.

Since T is an integrally closed domain, [M, Theorem 38] says that every principal ideal of T is unmixed. In other words, the primes associated to a principal ideal all have height one. Thus, $\alpha \cdot T$ is a $\mathfrak{p}$-primary ideal. Since $T_\mathfrak{p}$ is a regular local ring of dimension one [M, Theorem 37], it follows that $\alpha \cdot T = \mathfrak{p}^{(n)}$ for some positive integer n, where $\mathfrak{p}^{(n)} = \mathfrak{p}^n \cdot T_\mathfrak{p} \cap T$, the nth symbolic power of $\mathfrak{p}$. But now $\mathfrak{p}^n \cdot T_\mathfrak{p} = \mathfrak{p}^{(n)} \cdot T_\mathfrak{p} = \alpha \cdot T_\mathfrak{p} = \mathfrak{p} \cdot T_\mathfrak{p}$, so $n = 1$ and α generates a prime ideal of T. ∎

Proof of Proposition 2.5. Let A be the local ring of a point P of $\mathscr{D}_K^\circ$ in the fiber over $\mathfrak{p}$. Let B be the integral closure of $\mathcal{O}_\mathfrak{q} \cdot A$ in $L(\mathscr{D})$, the function field of $\mathscr{D}_L^\circ$. Thus B is the semilocal ring of the points of $\mathscr{D}_L^\circ$ in the fiber over $\mathfrak{q}$ which lie over the point P.

Now $\mathfrak{p} \cdot \mathcal{O}_\mathfrak{p}$ and $\mathfrak{q} \cdot \mathcal{O}_\mathfrak{q}$ are both principal ideals, say $\mathfrak{p} \cdot \mathcal{O}_\mathfrak{p} = (p)$ and $\mathfrak{q} \cdot \mathcal{O}_\mathfrak{q} = (q)$. Since $\mathcal{O}_\mathfrak{p} \subset A$ and $\mathcal{O}_\mathfrak{q} \subset B$, we have $\mathfrak{q} \cdot A = p \cdot A$ and $\mathfrak{q} \cdot B = q \cdot B$. Consider the domain $\mathcal{O}_\mathfrak{q} \cdot A$. Since $\mathcal{O}_\mathfrak{q} \cap A = \mathcal{O}_\mathfrak{p}$ we have $\mathcal{O}_\mathfrak{q} \cdot A \cong \mathcal{O}_\mathfrak{q} \otimes A$, where the tensor product is over $\mathcal{O}_\mathfrak{p}$. Therefore $\mathcal{O}_\mathfrak{q} \cdot A/\mathfrak{q} \cdot (\mathcal{O}_\mathfrak{q} \cdot A) \cong l \otimes_k A/\mathfrak{p} \cdot A$ is a domain, since k is algebraically closed in $A/\mathfrak{p} \cdot A$ and since $A/\mathfrak{p} \cdot A$ is a domain in either case.

By applying (the previous) Lemma 2.6 to $\mathcal{O}_\mathfrak{q} \cdot A \subset B$ we see that q generates a prime ideal in B. Part (b) now follows from the previous paragraph. Also, since k is algebraically closed in $A/\mathfrak{p} \cdot A$ we have that l is algebraically closed in $l(\mathscr{D})$. By Lemma 2.2, $\mathscr{D}_L^\circ$ has integral reduction at $\mathfrak{q}$.

If $\mathscr{D}_K^\circ$ has good reduction at $\mathfrak{p}$ then $A/\mathfrak{p} \cdot A$ is smooth over k. Therefore

$\mathcal{O}_{\mathfrak{q}} \cdot A/\mathfrak{q} \cdot (\mathcal{O}_{\mathfrak{q}} \cdot A) \cong l \otimes_k A/\mathfrak{p} \cdot A$ is also smooth over l and hence integrally closed (see [M, Theorems 61 and 36]). Since $B/\mathfrak{q} \cdot B$ is integral over $\mathcal{O}_{\mathfrak{q}} \cdot A/\mathfrak{q} \cdot (\mathcal{O}_{\mathfrak{q}} \cdot A)$, it follows that $B/\mathfrak{q} \cdot B = \mathcal{O}_{\mathfrak{q}} \cdot A/\mathfrak{q} \cdot (\mathcal{O}_{\mathfrak{q}} \cdot A)$, and hence is smooth over l. This implies that $\mathscr{D}_L^{\circ}$ has good reduction at $\mathfrak{q}$. ▮

2.7. COROLLARY. *Let L be a finite extension of K. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_K$, and let $\mathfrak{q}$ be a maximal ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$. If $\mathscr{C}_K^{\circ} \xrightarrow{G} \mathscr{D}_K^{\circ}$ has good reduction (respectively integral reduction) at $\mathfrak{p}$, then $\mathscr{C}_L^{\circ} \xrightarrow{G} \mathscr{D}_L^{\circ}$ has good reduction (respectively integral reduction) at $\mathfrak{q}$.*

SECTION 3. INTEGRAL REDUCTION AND THE FIELD OF MODULI

In this section we prove variations on the following proposition: if the covering $\mathscr{C}_K^{\circ} \xrightarrow{G} \mathscr{D}_K^{\circ}$ has good reduction at all primes lying over $\mathfrak{p}$, then the field of moduli of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ is unramified over $\mathfrak{p}$.

The idea of the proof is roughly as follows. If the covering has good reduction at a prime $\mathfrak{q}$ over $\mathfrak{p}$ then the inertia group of $\mathfrak{q}$ acts on the covering (i.e., on G) in the same way as it acts on the reduction modulo $\mathfrak{q}$ of the covering, namely trivially. This allows the covering to descend to a field which is unramified over $\mathfrak{p}$. For technical reasons, the above can only be carried out by working over the field of moduli of $\mathscr{C} \to \mathscr{D}$, *without* the group action. But one then uses the fact that every covering is dominated by a nice one whose field of moduli, without its group action, is F (the base field throughout this paper).

Throughout this section, let $M \supset F$ be the field of moduli (with respect to the model $\mathscr{D}_F$) of the covering $\mathscr{C} \to \mathscr{D}$, as a covering without its group action. Let $L \supset M$ be the field of moduli of $\mathscr{C} \xrightarrow{G} \mathscr{D}$, now as a covering *with* its group action (and again with respect to $\mathscr{D}_F$).

Recall that $\mathscr{C}_K \xrightarrow{G} \mathscr{D}_K$ and $\mathscr{C}_K^{\circ} \xrightarrow{G} \mathscr{D}_K^{\circ}$ are models for $\mathscr{C} \xrightarrow{G} \mathscr{D}$ over the number field K and its ring of integers, $\mathcal{O}_K$, respectively. Also $K \supset L \supset M \supset F$, and K is galois over F.

3.1. PROPOSITION. *Let $\mathfrak{q}$ be a maximal ideal of $\mathcal{O}_K$ lying over a maximal ideal* $\mathfrak{p}$ of $\mathcal{O}_M$. *Assume that $\mathscr{C}_K^{\circ} \xrightarrow{G} \mathscr{D}_K^{\circ}$ has integral reduction (respectively good reduction) at $\mathfrak{q}$ and that $\mathscr{D}_M^{\circ}$ has integral reduction (respectively good reduction) at $\mathfrak{p}$. Then there is a field N with $M \subset N \subset K$ and $\mathfrak{q}_N$ unramified over $\mathfrak{p}$, where $\mathfrak{q}_N$ is the prime of $\mathcal{O}_N$ lying under $\mathfrak{q}$, such that the following hold:*

(a) *The covering $\mathscr{C}_K^{\circ} \xrightarrow{G} \mathscr{D}_K^{\circ}$ descends to $\mathcal{O}_N$. That is, there is a normal model $\mathscr{C}_N^{\circ}$ for $\mathscr{C}$ over $\mathcal{O}_N$ and a G-galois covering $\mathscr{C}_N^{\circ} \xrightarrow{G} \mathscr{D}_N^{\circ}$ which induces $\mathscr{C}_K^{\circ} \xrightarrow{G} \mathscr{D}_K^{\circ}$. (Recall that $\mathscr{D}_N^{\circ}$ denotes the normal model induced from $\mathscr{D}_F^{\circ}$.)*

(b) *The covering* $\mathscr{C}_N^\circ \xrightarrow{G} \mathscr{D}_N^\circ$ *of part* (a) *has integral reduction* (*respectively good reduction*) *at* q_N.

Proof. By [B, Lemma 2.4] or [Mat, before Satz 1.1], $K(\mathscr{C})$ is galois over $M(\mathscr{D})$.

Let $\mathfrak{q}$ be a prime of $\mathcal{O}_K$ lying over $\mathfrak{p}$. Let $I_\mathfrak{q}$ be the inertia group at $\mathfrak{q}$, let N be its fixed field in K, and let $\mathfrak{q}_N = \mathfrak{q} \cap \mathcal{O}_N$. Let $\hat{}: \operatorname{gal}(K(\mathscr{D})/N(\mathscr{D})) \to \operatorname{gal}(K(\mathscr{C})/N(\mathscr{D}))$ be a section for the exact sequence of groups

$$1 \to \operatorname{gal}(K(\mathscr{C})/K(\mathscr{D})) \to \operatorname{gal}(K(\mathscr{C})/N(\mathscr{D})) \to \operatorname{gal}(K(\mathscr{D})/N(\mathscr{D})) \to 1. \qquad (*)$$

A section exists by [B, Lemma 2.5] or [Mat, Satz 1.1]. We will show that whenever $\sigma \in \operatorname{gal}(K(\mathscr{D})/N(\mathscr{D}))$, there exists

$$g_\sigma \in G = \operatorname{gal}(K(\mathscr{C})/K(\mathscr{D})), \qquad \text{such that } \hat{\sigma} g \hat{\sigma}^{-1} = g_\sigma^{-1} \cdot g \cdot g_\sigma, \text{ for all } g \in G.$$

Let R_N be the local ring of some point on $\mathscr{D}_N^\circ$ in the fiber over $\mathfrak{q}_N$. Let R, S be the integral closures of R_N in $K(\mathscr{D})$, $K(\mathscr{C})$ respectively. By the hypotheses and Lemma 2.2, the ideals $\mathfrak{q}_N \cdot R_N$, $\mathfrak{q} \cdot R$, and $\mathfrak{q} \cdot S$ are prime ideals of R_N, R, and S respectively. Let A_N, A, and B be the localizations of R_N, R, and S at $\mathfrak{q}_N \cdot R_N$, $\mathfrak{q} \cdot R$, and $\mathfrak{q} \cdot S$ respectively.

By Proposition 2.5 (b) and the fact that $\mathcal{O}_K/\mathfrak{q} = \mathcal{O}_N/\mathfrak{q}_N$, we have isomorphisms $A/\mathfrak{q} \cdot A \cong \mathcal{O}_K/\mathfrak{q} \otimes_{\mathcal{O}_N/\mathfrak{q}_N} (A_N/\mathfrak{q}_N \cdot A_N) \cong A_N/\mathfrak{q}_N \cdot A_N$. Note that the isomorphism between $A/\mathfrak{q} \cdot A$ and $A_N/\mathfrak{q}_N \cdot A_N$ is induced by the inclusion of R_N in R. By hypothesis and Lemma 2.2, $B/\mathfrak{q} \cdot B$ is galois over $A/\mathfrak{q} \cdot A$, with galois group isomorphic to G. Let $k(\mathscr{C}) = B/\mathfrak{q} \cdot B$ and $k(\mathscr{D}) = A/\mathfrak{q} \cdot A = A_N/\mathfrak{q}_N \cdot A_N$.

We now define a map

$$\Psi: \operatorname{gal}(K(\mathscr{C})/N(\mathscr{D})) \to \operatorname{gal}(k(\mathscr{C})/k(\mathscr{D})).$$

First, note that the elements of $\operatorname{gal}(K(\mathscr{C})/N(\mathscr{D}))$ take the rings R and S to themselves and the ideals $\mathfrak{q} \cdot R$ and $\mathfrak{q} \cdot S$ to themselves (because $\mathfrak{q}$ is the only prime ideal above $\mathfrak{q}_N$). Thus each element of $\operatorname{gal}(K(\mathscr{C})/N(\mathscr{D}))$ gives rise to a homomorphism of $B/\mathfrak{q} \cdot B$ onto itself which leaves $A_N/\mathfrak{q}_N \cdot A_N = A/\mathfrak{q} \cdot A$ fixed. But these homomorphisms have inverses and hence are automorphisms. Thus we have the map Ψ, which is obviously a homomorphism of groups.

Let $\Phi = \Psi|_G$ (recall that $G = \operatorname{gal}(K(\mathscr{C})/K(\mathscr{D}))$). Since R and S are integrally closed and since $\mathfrak{q} \cdot R$ and $\mathfrak{q} \cdot S$ are prime ideals of height one, it follows that A and B are discrete valuation rings. By [S LF, Section 7, Proposition 20], Φ maps G *onto* $\operatorname{gal}(k(\mathscr{C})/k(\mathscr{D}))$. Since $\operatorname{gal}(k(\mathscr{C})/k(\mathscr{D}))$ is isomorphic to G by hyothesis, Φ is an isomorphism.

Now let $\sigma \in \operatorname{gal}(K(\mathscr{D})/N(\mathscr{D}))$. Let $g_\sigma \in G = \operatorname{gal}(K(\mathscr{C})/K(\mathscr{D}))$ be the unique element of G such that $\Psi(\hat{\sigma}) = \Psi(g_\sigma^{-1})$. Then $\Psi(\hat{\sigma} \cdot g \cdot \hat{\sigma}^{-1}) =$

$\Psi(g_\sigma^{-1} \cdot g \cdot g_\sigma)$ for all $g \in G$. But since $\hat{\sigma} \cdot g \cdot \sigma^{-1} \in G$, and since $\Psi|_G$ is an isomorphism, we have $\hat{\sigma} \cdot g \cdot \sigma^{-1} = g_\sigma^{-1} \cdot g \cdot g_\sigma$ for all $g \in G$.

Define a new section $\tilde{\ }$: $\mathrm{gal}(K(\mathscr{D})/N(\mathscr{D})) \to \mathrm{gal}(K(\mathscr{C})/N(\mathscr{D}))$ for the exact sequence $(*)$ by $\tilde{\sigma} = g_\sigma \cdot \hat{\sigma}$ for $\sigma \in \mathrm{gal}(K(\mathscr{D})/N(\mathscr{D}))$. To see that $\tilde{\ }$ is a homomophism, note first that if $\rho \in \mathrm{gal}(K(\mathscr{D})/N(\mathscr{D}))$, then $\tilde{\rho}$ is characterized as the unique element in the kernel of Ψ which maps onto ρ in the natural map to $\mathrm{gal}(K(\mathscr{D})/N(\mathscr{D}))$. Now if $\sigma, \tau \in \mathrm{gal}(K(\mathscr{D})/N(\mathscr{D}))$, then $\tilde{\sigma} \cdot \tilde{\tau} \in \ker(\Psi)$, and maps to $\sigma \cdot \tau$, therefore $(\sigma \cdot \tau)^{\sim} = \tilde{\sigma} \cdot \tilde{\tau}$. Thus $\tilde{\ }$ is a section.

Let $N(\mathscr{C})$ be the fixed field of $\mathrm{gal}(K(\mathscr{D})/N(\mathscr{D}))^{\sim}$ in $K(\mathscr{C})$. Then $N(\mathscr{C})$ is galois over $N(\mathscr{D})$, with galois group isomorphic to G, and $K(\mathscr{C}) = K \cdot N(\mathscr{C})$. Corresponding to the G-galois field extension, $N(\mathscr{C})/N(\mathscr{D})$, is the covering $\mathscr{C}_N^\circ \xrightarrow{G} \mathscr{D}_N^\circ$, where $\mathscr{C}_N^\circ$ is a normal model for $\mathscr{C}$ over N (recall that $\mathscr{D}_N^\circ$ denotes the normal model induced from $\mathscr{D}_L^\circ$). To finish, we must show that $\mathscr{C}_N^\circ \xrightarrow{G} \mathscr{D}_N^\circ$ has good reduction (respectively integral reduction) at $\mathfrak{q}_N$.

Let S_N be the integral closure of R_N in $N(\mathscr{C})$. Let $\mathfrak{r} = \mathfrak{q} \cdot S \cap S_N$. Then $\mathfrak{r}$ is the only prime ideal of S_N lying over $\mathfrak{q}_N \cdot R_N$. Let B_N be the localization of S_N at $\mathfrak{r}$. Thus we have an extension of fields; $k(\mathscr{D}) \subset B_N/\mathfrak{r} \cdot B_N \subset k(\mathscr{C})$ (recall that $k(\mathscr{D}) = A_N/\mathfrak{q}_N \cdot A_N$ and $k(\mathscr{C}) = B/\mathfrak{q} \cdot B$). As before, $\mathrm{gal}(K(\mathscr{C})/N(\mathscr{C}))$ maps onto $\mathrm{gal}(k(\mathscr{C})/(B_N/\mathfrak{r} \cdot B_N))$. But $\mathrm{gal}(K(\mathscr{C})/N(\mathscr{C}))$ is precisely the kernel of the map from $\mathrm{gal}(K(\mathscr{C})/N(\mathscr{D}))$ to $\mathrm{gal}(k(\mathscr{C})/k(\mathscr{D}))$. Therefore $k(\mathscr{C}) \cong B_N/\mathfrak{r} \cdot B_N$. The formula $\sum e_i \cdot f_i = n$ implies that the ramification degree of $\mathfrak{r} \cdot B_N$ in B is equal to $[K(\mathscr{C}) : N(\mathscr{C})] = [K : N]$. Since the ramification degree of $\mathfrak{q}_N \cdot A_N$ in B is also equal to $[K : N]$, we conclude that $\mathfrak{q}_N \cdot A_N$ does not ramify in B_N. Thus $\mathfrak{q}_N \cdot B_N = \mathfrak{r} \cdot B_N$. To finish, we need only show that $\mathfrak{q}_N \cdot S_N = \mathfrak{r}$.

Since the localization of $\mathcal{O}_N$ at $\mathfrak{q}_N$ is contained in S_N it follows that $\mathfrak{q}_N \cdot S_N$ is generated by a single element, say q. Now S_N is integrally closed, so by [M, Theorem 38], every principal ideal of S_N is unmixed. In other words, the prime ideals of S_N associated to $q \cdot S_N$ all have height one. But from the last paragraph we know that $\mathfrak{r}$ is the only height one prime ideal of S_N containing $q \cdot S_N$. Therefore $\mathfrak{q}_N \cdot S_N$ is $\mathfrak{r}$-primary. Since $\mathfrak{q}_N$ generates the maximal ideal of the localization of S_N at $\mathfrak{r}$, it follows from [A-M, Proposition 4.8] that $\mathfrak{q}_N \cdot S_N = \mathfrak{r} \cdot B_N \cap S_N = \mathfrak{r}$. ∎

The question of whether $\mathscr{C}_K \xrightarrow{G} \mathscr{D}_K$ descends to a covering over a field $N' \supset M$ such that N'/M is unramified over *all* primes of good reduction of the covering should be closely related to the question of whether there is an unramified cover of the corresponding Hurwitz space (see, e.g., [C-H] or [Fr]) over which there is a family.

Recall from the beginning of this section that M and L are the fields of moduli of $\mathscr{C} \to \mathscr{D}$ and $\mathscr{C} \xrightarrow{G} \mathscr{D}$ respectively.

3.2. PROPOSITION. *Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_M$. If $\mathscr{C}_K^\circ \xrightarrow{G} \mathscr{D}_K^\circ$ has* *integral reduction at all maximal ideals of $\mathcal{O}_K$ lying over $\mathfrak{p}$, then the extension L/M is unramified over $\mathfrak{p}$.*

Proof. This follows immediately from the previous proposition and the fact that L is the intersection of all fields of definition of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ (see [C H, Proposition 2.7]). ∎

3.3. LEMMA (see also [Mat, Folg. 1.4]). *Let M be the field of moduli of $\mathscr{C} \to \mathscr{D}$ (without the group action, and with respect to $\mathscr{D}_F$). There are a finite group G' and a G'-galois branched covering $\mathscr{B} \xrightarrow{G'} \mathscr{D}$ which dominates $\mathscr{C} \xrightarrow{G} \mathscr{D}$ (i.e., $\mathscr{B} \to \mathscr{C} \to \mathscr{D}$) such that*

(1) *G' is a subgroup of $G \oplus \cdots \oplus G$, t times, where $t = [M : F]$,*

(2) *the field of moduli of $\mathscr{B} \to \mathscr{D}$ (without the group action) is F, and*

(3) *the branch locus of $\mathscr{B} \to \mathscr{D}$ is the same as the branch locus of $\mathscr{C} \to \mathscr{D}$.*

Proof. Let $\mathfrak{U}$ be an algebraic closure of $F(\mathscr{D})$ containing $K(\mathscr{C})$. Let $K(\mathscr{B})$ be the galois closure of $K(\mathscr{C})/F(\mathscr{D})$ inside $\mathfrak{U}$. Then $K(\mathscr{B})$ is the compositum in $\mathfrak{U}$ of all $\sigma(K(\mathscr{C}))$, where σ runs over all extensions of elements of $\mathrm{gal}(K/F)$ to automorphisms of $\mathfrak{U}$ leaving $F(\mathscr{D})$ fixed. Thus $K(\mathscr{B})$ is galois over $K(\mathscr{D})$ with galois group G', which is a subgroup of $G \oplus \cdots \oplus G$, t times, where $t = [M : F]$.

Let $\mathscr{B} \xrightarrow{G'} \mathscr{D}$ be the covering (of nonsingular, complete curves over $\mathbb{C}$) corresponding to the field extension $K(\mathscr{B})/K(\mathscr{D})$ tensored with $\mathbb{C}$. Since $K(\mathscr{B})$ is galois over $F(\mathscr{D})$, the field of moduli of $\mathscr{B} \to \mathscr{D}$ (without the group action) is F [B, Lemma 2.4].

(3) holds since the branch points of $\mathscr{C} \to \mathscr{D}$ are defined over K. ∎

The following lemma uses a result of Section 5. This lemma and the proposition following it are not used in the proof of Theorem 5.5.

3.4. LEMMA. *Let $\mathscr{B} \xrightarrow{G'} \mathscr{D}$ be the covering of (the previous) Lemma 3.3. Let $\mathscr{B}_K^\circ \xrightarrow{G'} \mathscr{D}_K^\circ$ be the induced covering of normal curves over $\mathcal{O}_K$. Fix $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$, a prime of good reduction of $\mathscr{C}_K^\circ \xrightarrow{G} \mathscr{D}_K^\circ$, and assume that $\mathfrak{p}$ does not divide $|G|$. Then, possibly after enlarging K, $\mathscr{B}_K^\circ \xrightarrow{G'} \mathscr{D}_K^\circ$ has good reduction at $\mathfrak{p}$.*

Proof. By Lemma 2.4 and the fact that the only primes dividing $|G'|$ also divide $|G|$, it suffices to show that $\mathscr{B}_K^\circ$ has good reduction at $\mathfrak{p}$.

Let $\sigma_1, ..., \sigma_t \in \mathrm{gal}(K/F)$ represent the t cosets of $\mathrm{gal}(K/M)$ in $\mathrm{gal}(K/F)$ (notation as in the previous Lemma 3.3). Assume $\sigma_1 = 1$. Let $\mathscr{C}_i \xrightarrow{G} \mathscr{D}$ be the covering corresponding to the field extension $\sigma_i(K(\mathscr{C}))$ of $K(\mathscr{D})$ (tensored with $\mathbb{C}$) and let $\mathscr{C}_{K,i}^\circ \xrightarrow{G} \mathscr{D}_{K,i}^\circ$ be the induced covering of normal curves over $\mathcal{O}_K$. Let A be the local ring of a point of $\mathscr{D}_K^\circ$ in the fiber over

$\mathfrak{p}$, let C_i be the integral closure of A in $\sigma_i(K(\mathscr{C}))$, and let B be the integral closure of A in $K(\mathscr{B})$. Let $\mathfrak{m}$ be the maximal ideal of A and let $\mathfrak{b}_1, ..., \mathfrak{b}_r$ be the prime ideals of A which come from the branch points of $\mathscr{C} \to \mathscr{D}$. By Lemmas 5.1 and 5.2 and by possibly enlarging K, we may assume that these, together with $\mathfrak{m}$ if $r > 0$, are the only prime ideals of A that ramify in C_1.

Since the branch points of $\mathscr{C} \to \mathscr{D}$ are all defined over K it follows that $\mathfrak{b}_1, ..., \mathfrak{b}_r$, $\mathfrak{m}$ (if $r > 0$) are precisely the prime ideals of A that ramify in C_i for all i. Now the $\mathfrak{b}_i$ are all tamely ramified in the C_j, so by Abhyankar's lemma, [SGAI, X, Lemma 3.6], no height one prime ideal of C_1 ramifies in B.

The ideal $\mathfrak{p} \cdot \mathcal{O}_{\mathfrak{p}}$ is generated by a single element, call it p. Let $\mathfrak{n}$ be a maximal ideal of C_1. Then since $\mathcal{O}_{\mathfrak{p}} \subset A$ and since $\mathscr{C}_K^\circ$ has good reduction at $\mathfrak{p}$, it follows that there is some $\gamma \in C_1$ such that (γ, p) is the maximal ideal of $(C_1)_{\mathfrak{n}}$. Thus $(C_1)_{\mathfrak{n}}$ is a regular local ring. This, together with the conclusion of the previous paragraph, allows us to apply "purity of branch locus", [N, Theorem 41.1], which says that B is unramified over C_1.

Now if $\mathfrak{r}$ is a maximal ideal of B lying over $\mathfrak{n}$, then the maximal ideal of $B_{\mathfrak{r}}$ is (γ, p). This implies that every local ring of $B/(p)$ is regular (of dimension one). By enlarging K again if necessary, we may assume that some point of $\mathscr{B}_k = \mathscr{B}_K^\circ \times_{\mathcal{O}_K} (\mathcal{O}_K/\mathfrak{p})$ is defined over $k = \mathcal{O}_K/\mathfrak{p}$. Then k is algebraically closed in the function field of $\mathscr{B}_k$. By Lemma 2.2, $\mathscr{B}_K^\circ$ has good reduction at $\mathfrak{p}$, as was to be shown. ∎

The above proof does not work for integral reduction because an unramified cover of a curve with integral reduction does not necessarily have integral reduction. For example, consider an unramified cover of the elliptic curve $y^2 = x(x-1)(x-p)$, where p is a prime number. The elliptic curve has integral reduction at p, but the unramified cover of it need not.

3.5. Proposition. *Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_F$ such that $\mathscr{C}_K^\circ \xrightarrow{G} \mathscr{D}_K^\circ$ has good reduction at all primes $\mathfrak{q}$ of $\mathcal{O}_K$ lying over $\mathfrak{p}$. Then the field of moduli of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ is unramified over $\mathfrak{p}$.*

Proof. Let $\mathscr{B} \xrightarrow{G'} \mathscr{D}_K$ and $\mathscr{B}_K^\circ \xrightarrow{G'} \mathscr{D}_K^\circ$ be the coverings of Lemmas 3.3 and 3.4. By Lemma 3.2, the field of moduli of $\mathscr{B} \xrightarrow{G'} \mathscr{D}$ is unramified over $\mathfrak{p}$. The result now follows from the fact that the field of moduli of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ is contained in the field of moduli of $\mathscr{B} \xrightarrow{G'} \mathscr{D}$. ∎

Section 4. Some Ring Theory

Throughout this section, let A be a Noetherian, integrally closed, local domain of dimension two and let $\mathfrak{A}$ be its fraction field. Let G be a finite group, let $\mathfrak{B}$ be a Galois extension of $\mathfrak{A}$ with galois group G, and let B be the integral closure of A in $\mathfrak{B}$.

One should think of A as the local ring of some point of $\mathscr{D}_K^\circ$ in the fiber over a prime $\mathfrak{p}$ of $\mathcal{O}_K$ and B as the semi-local ring of the points of $\mathscr{C}_K^\circ$ lying over it. Roughly speaking, the goal is to prove that if the branch locus of $\mathscr{C} \to \mathscr{D}$ does not meet in the fiber over $\mathfrak{p}$, if $\mathfrak{p}$ does not divide $|G|$, and if $\mathfrak{p} \cdot A$ is a prime ideal of A, then $\mathfrak{p} \cdot B$ is a prime ideal of B.

The idea of the proof is to "pull back" by an appropriate cyclic cover of $\mathscr{D}_K^\circ$ which is branched only along the component of the branch locus that meets $\mathfrak{p}$ (if there is one). One then has a bigger covering which is unramified over both $\mathscr{C}_K^\circ$ and the cyclic cover of $\mathscr{D}_K^\circ$. It is easy to check that this big covering has good reduction at $\mathfrak{p}$, since it is an unramified cover of a cyclic cover. Finally, one shows (roughly) that if $\mathfrak{p}$ generates a prime ideal in an unramified extension of B then it generates a prime ideal in B.

4.1. LEMMA. *Let e be a positive integer. Assume, in addition to the above assumptions, that A is a regular local ring and that $\alpha, \beta \in A$ are chosen so that (α, β) is the maximal ideal of A. Then the ring $C = A[x]/(x^e - \alpha)$ is a regular local ring with maximal ideal $(\bar{x}, \beta)$, where x is an indeterminate and $\bar{x}$ is the image of x in C.*

Proof. Let $C = A[x]/(x^e - \alpha)$ and let $\bar{x}$ denote the image of x in C. Since C is integral over A, every maximal ideal of C must contain the maximal ideal of A. Therefore every maximal ideal of C contains $(\bar{x}, \beta)$. But $C/(\bar{x}, \beta) \cong A/(\alpha, \beta)$ is a field. Therefore $(\bar{x}, \beta)$ is a maximal ideal and C is a regular local ring. ∎

4.2. COROLLARY. *Let A, α, β, and C be as in (the previous) Lemma* 4.1. *Then C is an integrally closed domain and $C/(\beta)$ is a regular local ring of dimension one whose maximal ideal is generated by $\bar{x}$.*

Proof. See [M, Theorem 36]. ∎

4.3. LEMMA. *Keep the assumptions of Lemma* 4.1 *and assume in addition that the integer e is invertible in A. Then (α) is the only prime ideal of height one of A that ramifies in C, and the ramification degree of (α) in C is e.*

Proof. Let $\mathfrak{p}$ be a prime ideal of A of height one which does not contain α. Let k be the field $A_\mathfrak{p}/\mathfrak{p} \cdot A_\mathfrak{p}$ and let $\bar{\alpha}$ be the image of α in k. Now let $f_1(x) \cdot f_2(x) \cdot \cdots \cdot f_r(x) = x^e - \bar{\alpha}$ be the factorization of $x^e - \bar{\alpha}$ into irreducible polynomials in $k[x]$. Since e is invertible in A, it is also invertible in k and therefore, since α is not in $\mathfrak{p}$, the polynomial $x^e - \bar{\alpha}$ has no multiple factors. Thus if $i \neq j$, then $(f_i(x), f_j(x))$ is the unit ideal in $k[x]$.

Let $g_1(x), \ldots, g_r(x)$ be polynomials in $A_\mathfrak{p}[x]$ which map to $f_1(x), \ldots, f_r(x)$. Thus any prime ideal of $A_\mathfrak{p}[x]/(x^e - \alpha)$ containing the image of $\mathfrak{p}$ must contain the image of exactly one of the $g_i(x)$. This proves that there are precisely r primes of C lying over $\mathfrak{p}$ and that each contains the image of precisely one of the $g_i(x)$.

Let $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ be the prime ideals of C lying over $\mathfrak{p}$, where we assume that $g_i(x)$ is contained in $\mathfrak{q}_i$. Let $f_i = [C_{\mathfrak{q}_i}/\mathfrak{q}_i \cdot C_{\mathfrak{q}_i} : A_\mathfrak{p}/\mathfrak{p} \cdot A_\mathfrak{p}]$. Then $f_1 + f_2 + \cdots + f_r = e$, so by the formula $\sum e_i f_i = n$ [S LF, I, Section 4, Proposition 10], $\mathfrak{p}$ is unramified in C.

Since $\bar{x}$, the image of x in C, generates a prime ideal (by Corollary 4.2), and since $\bar{x}^e = \alpha$ in C, it is clear that (α) ramifies in C and that its ramification degree in C is e. ∎

4.4. Lemma. *Let $E \subset F$ be Noetherian, integrally closed local domains and assume that F is the localization of an integral extension of E at a maximal ideal. If $\gamma \in E$ generates a prime ideal in F, then γ generates a prime ideal in E.*

Proof. Let $\gamma \cdot E = \mathfrak{r}_1 \cap \mathfrak{r}_2 \cap \cdots \cap \mathfrak{r}_s$ be a minimal primary decomposition of $\gamma \cdot E$ and let $\mathfrak{q}_i$ be the radical of $\mathfrak{r}_i$. Since E is an integrally closed domain, every principal ideal of E is unmixed [M, Theorem 38]. In other words, the prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ all have height one.

Since $\gamma \cdot F$ is a prime ideal of height one which is contained in $\mathfrak{q}_i \cdot F$, it follows that $\gamma \cdot F = \mathfrak{q}_i \cdot F$. Thus $\gamma \cdot F$ is the only prime ideal lying above $\mathfrak{q}_i$ and so $\mathfrak{q}_1 = \mathfrak{q}_2 = \cdots = \mathfrak{q}_s$. Let $\mathfrak{q} = \mathfrak{q}_1$ and $\mathfrak{r} = \mathfrak{r}_1$. Therefore $\gamma \cdot E = \mathfrak{r}$ is $\mathfrak{q}$-primary.

Since $\mathfrak{q}$ has height one and since E is integrally closed, $E_\mathfrak{q}$ is a discrete valuation ring. Also, by [A–M, Proposition 4.8], $\mathfrak{r} \cdot E_\mathfrak{q}$ is primary and $\mathfrak{r} \cdot E_\mathfrak{q} \cap E = \mathfrak{r}$. Therefore $\mathfrak{r} = \mathfrak{q}^{(n)}$ for some positive integer n, where $\mathfrak{q}^{(n)} = (\mathfrak{q}^n \cdot E_\mathfrak{q}) \cap E$, the nth symbolic power of $\mathfrak{q}$.

Finally, $\gamma \cdot F = \mathfrak{q}^{(n)} \cdot F \subset (\mathfrak{q}^n \cdot E_\mathfrak{q} \cdot F \cap F) \subset (\gamma^n \cdot F_{(\gamma)} \cap F) \subset \gamma \cdot F$, so that we have equality everywhere. But $\gamma^n \cdot F_{(\gamma)} \cap F = \gamma \cdot F$ implies that $n = 1$. Therefore $\gamma \cdot E = \mathfrak{r} = \mathfrak{q}^{(1)} = \mathfrak{q}$ is a prime ideal, as was to be shown. ∎

Remark (on the proof of Lemma 4.4). If F is flat (equivalently, free) E-module then F is faithfully flat over E and, in this case, lemma 4.4 follows trivially from the fact that for any ideal I of E, $I \cdot F \cap E = I$.

4.5. Proposition. *Assume that A is a regular local ring in which $|G|$, the order of the group G, is invertible and such that all the $|G|$th roots of unity are contained in $\mathfrak{A}$. Let (α, β) be the maximal ideal of A. Assume that (α) is the only prime ideal of height one that ramifies in B, and that B is tamely ramified over (α). Let $\mathfrak{n}$ be any maximal ideal of B. Then β generates a prime ideal in the local ring $B_\mathfrak{n}$.*

Proof. Since (α) is tamely ramified, the inertia groups of the primes lying over it are all cyclic (see, e.g., [Z–S, Chap. V, Section 10]). Suppose they all have order e. Let $C = A[x]/(x^e - \alpha)$. Let $\mathfrak{C}$ be the fraction field of C and let $\mathfrak{D}$ be the compositum of $\mathfrak{B}$ and $\mathfrak{C}$ inside some fixed algebraic closure of $\mathfrak{A}$. Let D be the integral closure of A in $\mathfrak{D}$.

Since $\mathfrak{A}$ contains all the eth roots of unity, $\mathfrak{C}$ is galois over $\mathfrak{A}$ and the galois group is cyclic of order e. Thus by Lemma 4.3 and the fact that C/A is also tamely ramified over (α), Abhyankar's lemma [SGA, X, Lemma 3.6] applies to say that no prime ideal of height one of either C or B ramifies in D.

By Lemma 4.1, C is a regular local ring with maximal ideal $(\bar{x}, \beta)$ (with the same notation as in the lemma). Therefore, by "purity of branch locus" [N, Theorem 41.1], D is unramified over C. So if $\mathfrak{m}$ is a maximal ideal of D, then the maximal ideal of the local ring $D_{\mathfrak{m}}$ is generated by $\bar{x}$ and β. Thus $D_{\mathfrak{m}}$ is a regular local ring and by [M, Theorem 36], β generates a prime ideal of $D_{\mathfrak{m}}$ of height one and $D_{\mathfrak{m}}/(\beta)$ is a regular local ring of dimension one.

Now apply Lemma 4.4, with $E = B_{\mathfrak{n}}$, $F = D_{\mathfrak{m}}$ and $\gamma = \beta$. ∎

4.6. *Remark* (on Proposition 4.5). If D is flat over B then D is étale over B and in this case one can conclude that $B_{\mathfrak{n}}$ is a regular local ring and that β is part of a system of parameters.

SECTION 5. GEOMETRIC INTERPRETATION OF SECTION 4

In this section we prove (Proposition 5.3) that if $\mathscr{D}_K^\circ$ has good reduction at $\mathfrak{p}$, where $\mathfrak{p} \nmid |G|$, and if the branch locus of $\mathscr{C} \to \mathscr{D}$ does not become singular modulo $\mathfrak{p}$, then the covering $\mathscr{C}_K^\circ \xrightarrow{G} \mathscr{D}_K^\circ$ has integral reduction at all primes lying over $\mathfrak{p}$. This is then used, together with the results of Section 3, to prove that the field of moduli of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ is unramified away from the primes of bad reduction of $\mathscr{D}_F^\circ$, the primes dividing $|G|$, and the primes $\mathfrak{p}$ for which the branch locus of $\mathscr{C} \to \mathscr{D}$ becomes singular modulo $\mathfrak{p}$ (Theorem 5.5).

Theorem 3.3 of [Fu] is similar to (and more general than) Proposition 5.3 here, but the hypotheses and methods of proof are different.

5.1. LEMMA. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ which does not divide $|G|$ and assume that $\mathscr{D}_K^\circ$ has good reduction at $\mathfrak{p}$. Let $P \subset \mathscr{D}_K^\circ$ be the fiber over $\mathfrak{p}$ in the map $\mathscr{D}_K^\circ \to \mathrm{Spec}(\mathcal{O}_K)$. After possibly enlarging K, P is not contained in the branch locus of $\mathscr{C}_K^\circ \to \mathscr{D}_K^\circ$.*

Equivalently, if K is sufficiently large then if D is the local ring of any point on $\mathscr{D}_K^\circ$ in the fiber over $\mathfrak{p}$ and if C is the integral closure of D in $K(\mathscr{C})$, the function field of $\mathscr{C}_K^\circ$, then $\mathfrak{p} \cdot D$ does not ramify in C.

Proof. Let A be a ring such that $\operatorname{Spec}(A)$ is an affine patch of $\mathscr{D}_K^\circ$ which meets the fiber over $\mathfrak{p}$. Since $\mathscr{D}_K^\circ$ has good reduction at $\mathfrak{p}$, it follows that $\mathfrak{p}\cdot A$ is a prime ideal of A. Let B be the integral closure of A in $K(\mathscr{C})$. Thus $\operatorname{Spec}(B)$ is an affine patch for $\mathscr{C}_K^\circ$. Since $\mathscr{D}_K^\circ$ is covered by finitely many affine patches, it suffices to show that after possibly enlarging K, the prime ideal $\mathfrak{p}\cdot A$ does not ramify in B.

Since $\mathfrak{p}$ does not divide $|G|$, B is tamely ramified over $\mathfrak{p}$. Therefore the inertia groups of the primes lying over $\mathfrak{p}$ are all cyclic [Z S, Chap. V, Section 10], say of order e. Let $L = K[x]/(x^e - p)$, where $p \in \mathfrak{p}$ generates $\mathfrak{p}$ locally. L is galois over K since K contains the eth roots of unity, and $\mathfrak{p}$ is tamely ramified in L with ramification degree e. Let $\mathfrak{q}$ be the prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Let A' be the integral closure of A in $L(\mathscr{D})$—the function field of $\mathscr{D}_L^\circ$ (the normal model for $\mathscr{D}$ over L obtained from $\mathscr{D}_K^\circ$). Then by Proposition 2.5, $\mathfrak{q}\cdot A'$ is a prime ideal of A' and hence is the only prime ideal of A' lying over $\mathfrak{p}\cdot A$. Therefore the ramification degree of $\mathfrak{p}\cdot A$ in A' is also e.

Let B' be the integral closure of A' in $L(\mathscr{C})$—the function field of $\mathscr{C}_L^\circ$. By Abhyankar's lemma [SGAI, X, Lemma 3.6], $\mathfrak{q}\cdot A'$ does not ramify in B'. Since $\operatorname{Spec}(A')$ and $\operatorname{Spec}(B')$ are affine patches for $\mathscr{D}_L^\circ$ and $\mathscr{C}_L^\circ$ respectively, the lemma now follows. ▮

5.2. Lemma. *If $\mathscr{D}_K^\circ$ is regular (i.e. all local rings are regular) then the branch locus of $\mathscr{C}_K^\circ \to \mathscr{D}_K^\circ$ consists of the image of the branch locus of $\mathscr{C} \to \mathscr{D}$ and some vertical fibers from the map $\mathscr{D}_K^\circ \to \operatorname{Spec}(\mathcal{O}_K)$.*

More precisely, Let D be the local ring of some regular point on $\mathscr{D}_K^\circ$ in the fiber over $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$, and let C be the semi-local ring of points of $\mathscr{C}_K^\circ$ lying over the given point of $\mathscr{D}_K^\circ$. Let $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ be the prime ideals of D which come from points of $\mathscr{D}$ which ramify in $\mathscr{C}$. Let $\mathfrak{m}$ be the maximal ideal of D and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the height one prime ideals of D which contain $\mathfrak{p}$. Then the set of prime ideals of D that ramify in C is either empty or is $\{\mathfrak{b}_1, \ldots, \mathfrak{b}_n, \mathfrak{m}\} \cup S$, where S is a subset of $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$.

Proof. Since D is a regular local ring and C is integrally closed we may apply "purity of branch locus," [N, Theorem 41.1]. This theorem says that if $\mathfrak{m}$ ramifies in C then some prime ideal of height one of D must ramify in C. Let $\mathfrak{r}$ be a prime ideal of height one of D that ramifies in C.

If $\mathfrak{p}$ is contained in $\mathfrak{r}$ then $\mathfrak{r}$ is one of the $\mathfrak{p}_i$. So assume that $\mathfrak{p}$ is not contained in $\mathfrak{r}$. Then since $\mathcal{O}_\mathfrak{p}$ is contained in D, we have $\mathfrak{p}\cdot\mathcal{O}_\mathfrak{p} \cap \mathfrak{r} = (0)$, because $\mathfrak{p}\cdot\mathcal{O}_\mathfrak{p}$ is generated by a single element. Therefore $D_\mathfrak{r}$ contains K, which implies that $D_\mathfrak{r}$ is the local ring of a point of $\mathscr{D}_K$, and hence the point of $\mathscr{D}_K^\circ$ corresponding to $\mathfrak{r}$ is in the image of the map $\mathscr{D} \to \mathscr{D}_K^\circ$.

Now the point of $\mathscr{D}_K$ corresponding to $D_\mathfrak{r}$ must be ramified in $\mathscr{C}_K$. But $D_\mathfrak{r} \otimes_K C$ is unramified over $D_\mathfrak{r}$, so a generator for the maximal ideal of $D_\mathfrak{r}$

locally generates the maximal ideals of $D_{\mathfrak{r}} \otimes_K \mathbb{C}$, and a similar statement is true for local rings of $\mathscr{C}_K$. Therefore the points of $\mathscr{D}$ which map to the point of $\mathscr{D}_K$ corresponding to $D_{\mathfrak{r}}$ all ramify in $\mathscr{C}$. Therefore $\mathfrak{r}$ is one of the $\mathfrak{b}_i$. This proves that the prime ideals of D of height one that ramify in C are contained in $\{\mathfrak{b}_1, ..., \mathfrak{b}_n, \mathfrak{m}\} \cup \{\mathfrak{p}_1, ..., \mathfrak{p}_s\}$.

Now assume that $n \neq 0$. Since $D_{\mathfrak{b}_i} \otimes_K \mathbb{C}$ is unramified over $D_{\mathfrak{b}_i}$, it follows as above that each $\mathfrak{b}_i$ ramifies in C. ∎

5.3. PROPOSITION. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ which does not divide $|G|$. Assume that $\mathscr{D}_F^\circ$ has good reduction at $\mathfrak{p}$ and assume that the branch locus of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ does not become singular modulo $\mathfrak{p}$. Then if K sufficiently large, the covering $\mathscr{C}_K^\circ \xrightarrow{G} \mathscr{D}_K^\circ$ has integral reduction at all primes of $\mathcal{O}_K$ lying over $\mathfrak{p}$.*

Proof. Pick K sufficiently large, containing F, so that

(1) all the $|G|$th roots of unity are contained in K,

(2) the fiber of the map $\mathscr{D}_K^\circ \to \operatorname{Spec}(\mathcal{O}_K)$ over any prime $\mathfrak{q}$ of $\mathcal{O}_K$ lying over $\mathfrak{p}$ does not ramify in $\mathscr{C}_K^\circ$ (see Lemma 5.1).

Fix a prime $\mathfrak{q}$ of $\mathcal{O}_K$ lying over $\mathfrak{p}$. Let D be the local ring of some point on $\mathscr{D}_K^\circ$ in the fiber over $\mathfrak{q}$ and let C be the integral closure of D in $K(\mathscr{C})$, so C is the semi-local ring of points of $\mathscr{C}_K^\circ$ lying over the point of $\mathscr{D}_K^\circ$ corresponding to D. Since $\mathcal{O}_{\mathfrak{q}} \subset D$ and since the maximal ideal $\mathfrak{q} \cdot \mathcal{O}_{\mathfrak{q}}$ is generated by a single element, say q, we have that $\mathfrak{q} \cdot D$ is generated by q. Now D has good reduction at $\mathfrak{q}$ (Proposition 2.5), therefore $D/\mathfrak{q} \cdot D$ is a regular local ring of dimension one, and so D is a regular local ring of dimension two and q is part of a system of parameters for D.

By (2) and Lemma 5.2, the only height one prime ideals of D that ramify in C are prime ideals that come from branch points of $\mathscr{C} \to \mathscr{D}$. Let $\mathfrak{b}_1, ..., \mathfrak{b}_r$ be these height one prime ideals of D. Since the branch locus does not become singular modulo $\mathfrak{p}$ it also does not become singular modulo $\mathfrak{q}$. Thus r is either 1 or 0.

Case 1. $r = 0$. Then C is unramified over D (by purity of branch locus, as in Lemma 5.2). Thus the localizations of C at its maximal ideals are regular local rings and q generates a prime ideal in each of them [M, Theorem 36].

Case 2. $r = 1$. Let $\mathfrak{b}_1 = \mathfrak{b}$. Then since the branch points of $\mathscr{C} \to \mathscr{D}$ are defined over K (by hypothesis, see Section 1), the image of $\mathfrak{b}$ in $D/\mathfrak{q} \cdot D$ generates the maximal ideal of $D/\mathfrak{q} \cdot D$. Then there is some $b \in \mathfrak{b}$ such that the image of b in $D/\mathfrak{q} \cdot D$ generates the maximal ideal of $D/\mathfrak{q} \cdot D$. So (b, q) is the maximal ideal of D, and b generates a prime ideal of D of height one.

Therefore $\mathfrak{b} = (b)$. Proposition 4.5 now says that q generates a prime ideal in the localization of C at any maximal ideal.

In either case we have concluded that q generates a prime ideal in the localization of C at any maximal ideal. Therefore every local ring of $\mathscr{C}_k = \mathscr{C}_K^{\circ} \times_{\mathcal{O}_K} (\mathcal{O}_K/\mathfrak{q})$ is an integral domain. If K is sufficiently large then some point of $\mathscr{C}_K$ is defined over K and so the corresponding point of $\mathscr{C}_k$ is defined over k. Then k is algebraically closed in the function field of $\mathscr{C}_k$. By Lemma 2.2, $\mathscr{C}_K^{\circ}$ has integral reduction at $\mathfrak{q}$. Thus the covering $\mathscr{C}_K^{\circ} \xrightarrow{G} \mathscr{D}_K^{\circ}$ has integral reduction at $\mathfrak{q}$ by Lemma 2.4. ∎

5.4. *Remark.* Using the proof of Lemma 4.5 (see Remark 4.6), one can show that the covering $\mathscr{C}_K^{\circ} \xrightarrow{G} \mathscr{D}_K^{\circ}$ is dominated by a galois covering (of $\mathscr{D}_K^{\circ}$) with a galois group whose order is divisible only by the primes dividing $|G|$ and which has *good* reduction at $\mathfrak{q}$. If one knew that this bigger curve were flat over $\mathscr{C}_K^{\circ}$ then one could conclude that in fact $\mathscr{C}_K^{\circ} \xrightarrow{G} \mathscr{D}_K^{\circ}$ has good reduction at $\mathfrak{q}$.

Recall that G is a finite group, that $\mathscr{C} \xrightarrow{G} \mathscr{D}$ is a G-galois branched covering of curves over $\mathbb{C}$, that $\mathscr{D}$ is defined over a number field F with a model $\mathscr{D}_F$ over F, and that the branch points of $\mathscr{C} \to \mathscr{D}$ are defined over F. For this theorem we allow the normal model $\mathscr{D}_F^{\circ}$ for $\mathscr{D}_F$ over $\mathcal{O}_F$ to vary, while $\mathscr{D}_F$ remain fixed.

5.5. THEOREM. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ which does not divide $|G|$, the order of G. If there is some normal model $\mathscr{D}_F^{\circ}$ for $\mathscr{D}_F$ over $\mathcal{O}_F$ such that the branch locus of $\mathscr{C} \to \mathscr{D}$ does not become singular modulo $\mathfrak{p}$ and such that $\mathscr{D}_F^{\circ}$ has good reduction at $\mathfrak{p}$, then the field of moduli of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ (with respect to $\mathscr{D}_F$) is unramified over $\mathfrak{p}$.*

Proof. Let $\mathscr{B} \xrightarrow{G'} \mathscr{D}$ be the covering of Lemma 3.3. So $\mathscr{B} \xrightarrow{G'} \mathscr{D}$ dominates $\mathscr{C} \xrightarrow{G} \mathscr{D}$, has the same branch locus as $\mathscr{C} \to \mathscr{D}$, and the field of moduli of $\mathscr{B} \to \mathscr{D}$ (without the group action) is F. Furthermore, the primes dividing $|G'|$ are the same as the primes dividing $|G|$. Now apply Proposition 5.3 and 3.2 to $\mathscr{B} \xrightarrow{G'} \mathscr{D}$ and use the fact that the field of moduli of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ is contained in the field of moduli of $\mathscr{B} \xrightarrow{G'} \mathscr{D}$. ∎

5.6. COROLLARY. *The group G, the branch points of $\mathscr{C} \to \mathscr{D}$ and the model $\mathscr{D}_F$ determine the field of moduli (with respect to $\mathscr{D}_F$) of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ up to finitely many fields.*

Proof. Let M be the field of moduli of $\mathscr{C} \xrightarrow{G} \mathscr{D}$, and let r be the number of branch points of the covering. By [Fr, Section 4B] or [Mat, Satz 3.1], $[M : F] \leqslant |G|^r$ (Satz 3.1 gives a much better bound than the one stated here). Now Theorem 5.5 gives a finite set of primes, S, of F such that every prime dividing the discriminant of M over F belongs to S. This set S depends only on $|G|$, the branch points of the covering, and $\mathscr{D}_F$. By a theorem of Hermite [Has, p. 595], there are only finitely many number fields K, containing F, such that $[K:F] \leqslant |G|^r$ and the primes dividing the discriminant of K over F are all in S. ▌

5.7. COROLLARY. *If $\mathscr{D} = \mathbb{P}^1_{\mathbb{C}}$ and the covering $\mathscr{C} \to \mathscr{D}$ has only three rational branch points then the field of moduli of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ is unramified over primes that do not divide $|G|$.*

Proof. $\mathbb{P}^1$ has a model over $\mathbb{Z}$ with good reduction everywhere, namely $\mathbb{P}^1_{\mathbb{Z}}$. By using a fractional linear transformation, one can take the three branch points to $\{0, 1, \infty\}$. This does not change the field of moduli. Now apply Theorem 5.5. ▌

ACKNOWLEDGMENTS

I thank David Harbater, Dick Freije, Mike Fried, Will Kazez, and Serge Lang for helpful conversations. I also thank the Caltech mathematics department for allowing me to use their facilities while I wrote this paper.

REFERENCES

[A-M] M. ATIYAH AND I. G. MACDONALD, "Introduction to Commutative Algebra," Addison-Wesley, Reading, MA, 1969.

[B th] S. BECKMANN, "Fields of definition of solvable branched coverings, Ph.D. thesis, University of Pennsylvania, 1986.

[B] S. BECKMANN, Galois groups of fields of definition of solvable branched coverings, *Compositio Math.* **66** (1988), 121-144.

[C-H] K. COOMBES AND D. HARBATER, Hurwitz families and arithmetic Galois groups, *Duke Math. J.* **52** (1985), 821-839.

[Fr] M. FRIED, Fields of definition of function fields and Hurwitz families—Groups as Galois groups, *Comm. Algebra* **5** (1977), 17-82.

[Fu] W. FULTON, Hurwitz schemes and irreducibility of algebraic curves, *Ann. Of Math. (2)* **90** (1969), 542-575.

[EGAIII] A. GROTHENDIECK AND J. DIEUDONNÉ, Étude cohomologique des faisceaux coherents, *Inst. Hautes Études Sci. Publ. Math.* **11** (1961) and **17** (1963).

[SGAI] A. GROTHENDIECK, "Revêtements étales et Groupe Fondamental," Lecture Notes in Mathematics, Vol. 224, Springer-Verlag, New York/Berlin, 1971.

[H] R. HARTSHORNE, "Algebraic Geometry," Springer-Verlag, New York/Berlin, 1977.

[Has] H. HASSE, "Zahlentheorie," Akademie-Verlag, Berlin, 1963.

[L DG] S. LANG, "Fundamentals of Diophantine Geometry," Springer-Verlag, New York/Berlin, 1985.

[M] H. MATSUMURA, "Commutative Algebra," 2nd ed., Benjamin/Cumming, Reading, MA, 1980.

[Mat] B. H. MATZAT, Konstruktion von Zahl- und Funktionenkorpern mit vorgegebener Galoisgruppe, *J. Reine Angew. Math.* **349** (1984), 179–220.

[N] M. NAGATA, "Local Rings," Interscience Tracts in Pure and Applied Mathematics, Vol. 13. Wiley, New York, 1962.

[GAGA] J.-P. SERRE, Géometric algébrique et géometric analytique, *Ann. Inst. Fourier (Grenoble)* **VI** (1956), 1–42.

[S LF] J.-P. SERRE, "Local Fields," Springer-Verlag, New York, Berlin, 1979.

[Z-S] O. ZARISKI AND P. SAMUEL, "Commutative Algebra," Vol. 1, Van Nostrand, Princeton, 1958.

Printed in Belgium