SYBILLA BECKMANN

Galois groups of fields of definition of solvable branched coverings

Compositio Mathematica, tome 66, nº 2 (1988), p. 121-144

<http://www.numdam.org/item?id=CM_1988__66_2_121_0>

Compositio Mathematica 66: 121–144 (1988)
© Kluwer Academic Publishers, Dordrecht – Printed in the Netherlands

Galois groups of fields of definition of solvable branched coverings

SYBILLA BECKMANN*
Department of Mathematics, Yale University, Box 2155 Yale Station, New Haven, CT 06520, USA

Received 5 August 1986; accepted in revised form 8 December 1987

Introduction

The guiding problem of this paper is: Given only the topological description of a branched covering of the Riemann sphere, determine its field of moduli and small fields of definition.

The main result of this paper (Theorem 7.3) describes the factor groups in a subinvariant series for the galois group (over $\mathbb{Q}$) of small fields of definition of a solvable branched covering of $\mathbb{P}^1_{\mathbb{C}}$. These factor groups are either abelian or subgroups of symplectic groups. Furthermore, the only information needed to describe these factor groups is the topological description of the covering and a chief series for its galois group. (See 7.2 for group theoretic definitions.)

Theorem 7.3 is proven by inducting on a chief series for the galois group of the covering. Since this galois group is solvable, each step in the induction consists of "going up by" a $(\mathbb{Z}/\ell)^n$ covering.

The theory of abelian varieties comes into play because $(\mathbb{Z}/\ell)^n$ unramified coverings of a curve correspond to ℓ-torsion points on the Jacobian of the curve. The symplectic groups in Theorem 7.3 come from the Weil pairing. The Weil pairing is also used to prove that "the arithmetic galois group acts on the geometric galois group via the cyclotomic character" (Proposition 5.6). A similar result in Section 6 (Prop. 6.1) says that "the arithmetic galois group acts on branch cycles via the cyclotomic character". Both results are generalizations of a result due to Belyi [Bel] and Fried [Fr]. Proposition 6.1 is also a consequence of the proof of a result of Matzat ([M2] Satz 2.2).

Preliminary, technical "descent" and "lifting" results are cohomological in nature. Some of these results can be found in [M1], presented in a different form.

Aside from intrinsic appeal, one reason to study the "guiding problem" above is due to its connection to the "Inverse Galois Problem" via Hilbert's

Irreducibility Theorem (see [L DG]). The Inverse Galois Problem is to determine which groups occur as galois groups of finite extensions of $\mathbb{Q}$. One knows that every solvable group (see [Sh] and [N]), and many other groups occur (see e.g., [Bel2], [M2], [Th] and [Ft]). The reader may wish to consult [G], [Ha] and [M3], which contain surveys and further references.

This paper is essentially the first half of my University of Pennsylvania Ph.D. thesis [B].

1. Definitions

In this section we define the field of moduli and fields of definition of branched coverings, as well as models for curves and for coverings.

The reader should consult [C + H] for useful results on fields of moduli and fields of definition.

1.1. Definition: A *branched covering* is a pair of nonsingular, irreducible, complex projective, algebraic curves $\mathscr{C}$ and $\mathscr{D}$, and a finite, dominant morphism $\mathscr{C} \to \mathscr{D}$ (see [H], Ch.1 for terminology).

Two branched coverings $\mathscr{C} \to \mathscr{D}$ and $\mathscr{C}' \to \mathscr{D}$ are called *equivalent* if there is an isomorphism $\mathscr{C} \to \mathscr{C}'$ making a commutative triangle

$$\begin{tikzcd}
\mathscr{C} \arrow[r] \arrow[dr] & \mathscr{C}' \arrow[d] \\
& \mathscr{D}
\end{tikzcd}$$

■

Let $\mathscr{C} \to \mathscr{D}$ be a branched covering. Then there are only finitely many points P of $\mathscr{C}$, such that there is a neighborhood of P (in the classical, metric topology) on which $\mathscr{C} \to \mathscr{D}$ looks like $z \mapsto z^n$ for some $n > 1$. These points of $\mathscr{C}$ are called *ramification points*. Their images in $\mathscr{D}$ are called *branch points*. (See [H], ch. IV for algebraic definitions).

1.2. Definitions: Let $\mathscr{C} \to \mathscr{D}$ be a branched covering. Then $\mathscr{C} \to \mathscr{D}$ is called *galois* (or *regular*) if the order of the group of deck transformations of $\mathscr{C} \to \mathscr{D}$ is equal to the degree of the map $\mathscr{C} \to \mathscr{D}$.

If $\mathscr{C} \to \mathscr{D}$ is galois, we let $\mathrm{gal}(\mathscr{C}/\mathscr{D})$ denote the group of deck transformations of $\mathscr{C} \to \mathscr{D}$, and we call this group the *galois group* of $\mathscr{C} \to \mathscr{D}$.

Let G be a finite group. A *G-galois branched covering* is a branched covering $\mathscr{C} \to \mathscr{D}$, which is galois with galois group isomorphic to G, together with a fixed isomorphism of G with $\mathrm{gal}(\mathscr{C}/\mathscr{D})$. An isomorphism of G with $\mathrm{gal}(\mathscr{C}/\mathscr{D})$ is called a *G-action* on $\mathscr{C} \to \mathscr{D}$.

We write $\mathscr{C} \xrightarrow{G} \mathscr{D}$ for a G-galois branched covering $(\mathscr{C} \to \mathscr{D}, \Phi)$ when we do not want to refer explicitly to the G-action $\Phi\colon G \to \mathrm{gal}(\mathscr{C}/\mathscr{D})$.

Two G-galois branched coverings are called *equivalent* if the corresponding coverings are equivalent and the G-actions on them are compatible. ■

Let $\mathscr{C} \to \mathscr{D}$ be a branched covering. Let C and D denote the field of rational functions on $\mathscr{C}$ and $\mathscr{D}$ respectively. Then there is an inclusion $D \subset C$. By [H], Ch. I, Cor. 6.12, the equivalence class of $\mathscr{C} \to \mathscr{D}$ is uniquely determined by the field extension C/D.

1.3. Definitions: Let $\mathscr{C}$ be an algebraic curve over $\mathbb{C}$ with function field $C \supset \mathbb{C}$. Let $B \subset \mathbb{C}$ be a field. Suppose there is a field $B(\mathscr{C}) \subset C$ such that
1) $B \subset B(\mathscr{C})$, and B is algebraically closed in $B(\mathscr{C})$
2) $B(\mathscr{C}) \cdot \mathbb{C} = C$ ($\cdot$ denotes compositum in C)
3) $\mathrm{aut}(C/B(\mathscr{C})) \approx \mathrm{aut}(\mathbb{C}/B)$.
Then the pair consisting of the field $B(\mathscr{C})$, and a fixed isomorphism $\alpha\colon \mathrm{aut}(\mathbb{C}/B) \to \mathrm{aut}(C/B(\mathscr{C}))$ such that (restriction of $\mathbb{C}) \circ \alpha =$ identity, is called a *model for $\mathscr{C}$ over B*. ($\mathrm{aut}(\mathbb{C}/B)$ stands for the automorphisms of $\mathbb{C}$ leaving B elementwise fixed.)

Let $P \in \mathscr{C}$ be a point. The point P corresponds to a discrete valuation ring R which contains $\mathbb{C}$ and whose fraction field is C. The *field of definition of P with respect to the model* $(B(\mathscr{C}), \alpha)$ is the fixed field in $\mathbb{C}$ of

$$\{\sigma \in \mathrm{aut}(\mathbb{C}/B) \mid \alpha(\sigma)(R) = R\}.$$ ■

1.4. Convention: Unless otherwise stated, we will always use the standard model $(\mathbb{Q}(x), \alpha)$ for $\mathbb{P}^1_{\mathbb{C}}$ over $\mathbb{Q}$, where $\alpha(\sigma)(x) = x$ for $\sigma \in \mathrm{aut}(\mathbb{C}/\mathbb{Q})$.

1.5. Definitions: Let $\mathscr{C} \to \mathscr{D}$ be a branched covering. Let C/D be the corresponding extension of function fields. Let F be an algebraic closure of C.

Fix a model $(B(\mathscr{D}), \alpha)$ for $\mathscr{D}$ over a field $B \subset \mathbb{C}$. Let K be a field with $B \subset K \subset \mathbb{C}$. Let $K(\mathscr{D}) = K \cdot B(\mathscr{D})$ (where $\cdot$ denotes compositum in F).

Then K is called a *field of definition of the branched covering $\mathscr{C} \to \mathscr{D}$* if there is a field $K(\mathscr{C})$, with $K(\mathscr{D}) \subset K(\mathscr{C}) \subset F$, and $K(\mathscr{C})/K(\mathscr{D})$ algebraic, such that K is algebraically closed in $K(\mathscr{C})$ and $K(\mathscr{C}) \cdot \mathbb{C} = C$.

If G is a finite group and if $\mathscr{C} \xrightarrow{G} \mathscr{D}$ is a G-galois branched covering, then K is a *field of definition of the G-galois branched covering $\mathscr{C} \xrightarrow{G} \mathscr{D}$* if, in addition to the above conditions, $K(\mathscr{C})/K(\mathscr{D})$ is galois with galois group isomorphic to G.

The field extension $K(\mathscr{C})/K(\mathscr{D})$ is called a *model for the branched covering* $\mathscr{C} \to \mathscr{D}$ *over* K (with respect to $(B(\mathscr{D}), \alpha)$).

If $\mathscr{C} \xrightarrow{G} \mathscr{D}$ is G-galois, then the field extension $K(\mathscr{C})/K(\mathscr{D})$, together with a G-action on $K(\mathscr{C})$ (an isomorphism of G with $\text{gal}(K(\mathscr{C})/K(\mathscr{D}))$), is called a *model for the G-galois branched covering* $\mathscr{C} \xrightarrow{G} \mathscr{D}$ *over* K (with respect to $(B(\mathscr{D}), \alpha)$).

The *field of moduli of the branched covering* $\mathscr{C} \to \mathscr{D}$ (with respect to $(B(\mathscr{D}), \alpha)$) is the fixed field in $\mathbb{C}$ of $\{\sigma \in \text{aut}(\mathbb{C}/B) \mid \text{There exists an extension } \Sigma \text{ of } \alpha(\sigma) \text{ to an automorphism of } F \text{ such that } \Sigma(C) = C\}$.

The *field of moduli of the G-galois branched covering* $(\mathscr{C} \to \mathscr{D}, \Phi)$ (with respect to $(B(\mathscr{D}), \alpha)$) is the fixed field in $\mathbb{C}$ of $\{\sigma \in \text{aut}(\mathbb{C}/B) \mid \text{There exists an extension } \Sigma \text{ of } \alpha(\sigma) \text{ to an automorphism of } F \text{ such that } \Sigma(C) = C \text{ and } \Sigma \circ \Phi(g) \circ \Sigma^{-1} = \Phi(g) \text{ for all } g \in G\}$. (Where we have also used Φ: $G \to \text{gal}(C/D)$ to denote the G-action on C/D.) ■

The field of moduli of $\mathscr{C} \to \mathscr{D}$ (resp. $\mathscr{C} \xrightarrow{G} \mathscr{D}$) is the fixed field of those automorphisms of $\mathbb{C}$ over B which take $\mathscr{C} \to \mathscr{D}$ (resp. $\mathscr{C} \xrightarrow{G} \mathscr{D}$) to an equivalent branched covering (resp. G-galois branched covering).

Let G be a finite group, and let $\mathscr{C} \xrightarrow{G} \mathbb{P}^1_{\mathbb{C}}$ be a G-galois branched covering. Let $P_1, P_2, \ldots, P_r \in \mathbb{P}^1_{\mathbb{C}}$ be the branch points of $\mathscr{C} \to \mathbb{P}^1_{\mathbb{C}}$. Pick a base point $P \in \mathbb{P}^1_{\mathbb{C}} - \{P_1, \ldots, P_r\}$.

Fix a standard homotopy basis $\alpha_1, \ldots, \alpha_r$ of $\pi_1(\mathbb{P}^1_{\mathbb{C}} - \{P_1, \ldots, P_r\}, P)$ (i.e., α_i is represented by a loop at P which winds once around P_i counterclockwise, and winds around no other P_j). By basic topology, $\mathscr{C} \xrightarrow{G} \mathbb{P}^1_{\mathbb{C}}$ gives rise to the equivalence class of an r-tuple of elements of G, $(g_1, g_2, \ldots, g_r)$, which generate G and for which $g_1 \cdot g_2 \cdot \cdots \cdot g_r = 1$. Here $(g_1, \ldots, g_r)$ is equivalent to $(g_1', \ldots, g_r')$ if they are uniformly conjugate.

1.6. Definition: The data consisting of: a standard homotopy basis $\alpha_1, \alpha_2, \ldots, \alpha_r$ for $\pi_1(\mathbb{P}^1_{\mathbb{C}} - \{P_1, \ldots, P_r\}, P)$, together with the equivalence class of an r-tuple of elements of G, $(g_1, g_2, \ldots, g_r)$, which generate G and for which $g_1 \cdot g_2 \cdot \cdots \cdot g_r = 1$ is called a *topological description* (of $\mathscr{C} \xrightarrow{G} \mathbb{P}^1_{\mathbb{C}}$). (This is the same as what is called a *description* of a G-galois cover in [C + H]). ■

The Riemann Existence Theorem says that a topological description determines an *algebraic* branched covering. In other words, every topological branched covering of $\mathbb{P}^1_{\mathbb{C}}$ is equivalent to a branched covering given by polynomial equations. See [F], Proposition 1.2 and [GAGA], Proposition 15 and its corollary.

2. Sections and descent of models

Throughout this section, let G be a finite group and let $\mathscr{C} \xrightarrow{G} \mathscr{D}$ be a G-galois branched covering. Let C/D be the corresponding field extension. Fix a field $K \subset \mathbb{C}$ and a model $(K(\mathscr{D}), \alpha)$ for $\mathscr{D}$ over K.

If L is a field with $\mathbb{C} \supset L \supset K$, then $L(\mathscr{D})$ will always mean the fixed field in D of $\alpha(\mathrm{aut}(\mathbb{C}/L))$, so $L(\mathscr{D}) = L \cdot K(\mathscr{D})$.

If $L \subset \mathbb{C}$ is a field then $\bar{L}$ denotes the algebraic closure of L in $\mathbb{C}$.

2.1. Definitions: Let L be a field with $\mathbb{C} \supset L \supset K$. Assume that $L(\mathscr{C})/L(\mathscr{D})$, $K(\mathscr{C})/K(\mathscr{D})$ are models for $\mathscr{C} \xrightarrow{G} \mathscr{D}$ over L and K respectively with $L(\mathscr{C}) \supset K(\mathscr{C})$. We say that $L(\mathscr{C})/L(\mathscr{D})$ *extends* (or *is compatible with*) $K(\mathscr{C})/K(\mathscr{D})$ if $L(\mathscr{C})$ is the compositum of L and $K(\mathscr{C})$ and the G-actions on $L(\mathscr{C})/L(\mathscr{D})$ and $K(\mathscr{C})/K(\mathscr{D})$ are compatible. We shall also say that $L(\mathscr{C})/L(\mathscr{D})$ is *the extension of* $K(\mathscr{C})/K(\mathscr{D})$ *to* L and that $L(\mathscr{C})/L(\mathscr{D})$ *descends to* K. ■

Let L be a field with $\mathbb{C} \supset L \supset K$, and L galois over K. Assume there is a model $L(\mathscr{C})/L(\mathscr{D})$ for $\mathscr{C} \xrightarrow{G} \mathscr{D}$ over L.

2.2. Definition: Assume that $L(\mathscr{C})$ is galois over $K(\mathscr{D})$. Let $P_{L/K}$: gal $(L(\mathscr{C})/K(\mathscr{D})) \to$ gal (L/K) be the natural homomorphism. A homomorphism

$$\hat{o}\colon \mathrm{gal}\,(L/K) \to \mathrm{gal}\,(L(\mathscr{C})/K(\mathscr{D}))$$

for which $P_{L/K} \circ \hat{}\ =$ identity, is called a *section* for $(L(\mathscr{C}), K(\mathscr{D}))$. ■

Sections are cohomological objects. If there is some section for $(L(\mathscr{C}), K(\mathscr{D}))$, then one can define an action of gal(L/K) on $G =$ gal$(L(\mathscr{C})/L(\mathscr{D}))$. One can show that there is a one-to-one correspondence between the pointed sets {sections for $(L(\mathscr{C}), K(\mathscr{D}))$}/equivalence and H^1(gal (L/K), G) (see [B], Lemma 2.2.5). Here, two sections are called equivalent if they differ by an inner automorphism of G.

The following lemma is essentially Lemma 4.1 of [M1].

2.3. Lemma: (*Criterion for $L(\mathscr{C})/L(\mathscr{D})$ to descend to K*). *Assume that $L(\mathscr{C})$ is galois over $K(\mathscr{D})$. Then the model $L(\mathscr{C})/L(\mathscr{D})$ descends to K if and only if there is a section* $\hat{}$ *for* $(L(\mathscr{C}), K(\mathscr{D}))$ *such that*

$$\hat{\sigma} g \hat{\sigma}^{-1} = g$$

for all $\sigma \in$ gal(L/K), $g \in G =$ gal$(L(\mathscr{C})/L(\mathscr{D}))$.

Proof: ← Let $K(\mathscr{C})$ be the fixed field in $L(\mathscr{C})$ of $\mathrm{gal}(L/K)\hat{}$. Since $\mathrm{gal}(L/K)$ commutes with G,

$$\mathrm{gal}(L(\mathscr{C})/K(\mathscr{D})) \approx G \oplus \mathrm{gal}(L/K)\hat{}.$$

Thus $K(\mathscr{C})/K(\mathscr{D})$ is galois with group G, and $L(\mathscr{C})$ is the compositum of $L(\mathscr{D})$ and $K(\mathscr{C})$.

→ If $L(\mathscr{C})/L(\mathscr{D})$ descends to K then there is a field $K(\mathscr{C}) \subset L(\mathscr{C})$ such that $K(\mathscr{C})/K(\mathscr{D})$ is a model for $\mathscr{C} \xrightarrow{G} \mathscr{D}$ over K and $L(\mathscr{C})$ is the compositum of $K(\mathscr{C})$ and L. Therefore the map

$$\varphi\colon \mathrm{gal}(L(\mathscr{C})/K(\mathscr{D})) \to \mathrm{gal}(L/K) \oplus \mathrm{gal}(K(\mathscr{C})/K(\mathscr{D}))$$

defined by

$$\varphi(\varrho) = (\varrho|_L, \varrho|_{K(\mathscr{C})})$$

is an isomorphism. Define

$$\hat{}\colon \mathrm{gal}(L/K) \to \mathrm{gal}(L(\mathscr{C})/K(\mathscr{D}))$$

by

$$\hat{\sigma} = \varphi^{-1}(\sigma, 1) \quad \text{for } \sigma \in \mathrm{gal}(L/K).$$

Then $\hat{}$ is a section for $(L(\mathscr{C}), K(\mathscr{D}))$ and $\hat{\sigma} g \hat{\sigma}^{-1} = g$ whenever $\sigma \in \mathrm{gal}(L/K)$, $g \in \mathrm{gal}(L(\mathscr{C})/L(\mathscr{D}))$. ■

Note that Lemma 2.3 requires $L(\mathscr{C})/K(\mathscr{D})$ to be galois. The following lemma gives a criterion for this to occur. See [M1], before Satz 1.1, for a different way of phrasing this criterion.

2.4. LEMMA: *There is a model $\bar{K}(\mathscr{C})/\bar{K}(\mathscr{D})$ for $\mathscr{C} \xrightarrow{G} \mathscr{D}$ over $\bar{K}$ such that $\bar{K}(\mathscr{C})$ is galois over $K(\mathscr{D})$, if and only if K contains the field of moduli of $\mathscr{C} \to \mathscr{D}$, considered as a covering without its group action.*

Proof: → Suppose there is a model $\bar{K}(\mathscr{C})/\bar{K}(\mathscr{D})$ such that $\bar{K}(\mathscr{C})$ is galois over $K(\mathscr{D})$. Fix an algebraic closure $\mathfrak{F}$ of C. Recall that C/D is the function field extension corresponding to $\mathscr{C} \xrightarrow{G} \mathscr{D}$.

Let $\sigma \in \mathrm{aut}(\mathbb{C}/K)$ and let Σ be any extension of $\alpha(\sigma)$ to an automorphism of $\mathfrak{F}$.

Since $\bar{K}(\mathscr{C})$ is galois over $K(\mathscr{D})$, $\Sigma(\bar{K}(\mathscr{C})) = \bar{K}(\mathscr{C})$. Since C is the compositum of $\bar{K}(\mathscr{C})$ and $\mathbb{C}$, it follows that $\Sigma(C) = C$.

$\leftarrow$ Assume that K contains the field of moduli of $\mathscr{C} \to \mathscr{D}$ (without the group action). The field of moduli of $\mathscr{C} \xrightarrow{G} \mathscr{D}$ is contained in a finite extension of K. Therefore there is a model $\bar{K}(\mathscr{C})/\bar{K}(\mathscr{D})$ for $\mathscr{C} \xrightarrow{G} \mathscr{D}$ over $\bar{K}$ (see [C + H] Prop. 2.8). We may assume $\bar{K}(\mathscr{C}) \subset \mathfrak{F}$.

Let $\sigma \in \operatorname{aut}(\mathbb{C}/K)$ and let Σ be an extension of $\alpha(\sigma)$ to an automorphism of $\mathfrak{F}$.

Since K contains the field of moduli of $\mathscr{C} \to \mathscr{D}$ (without the group action), and since C/D is galois, it follows that $\Sigma(C) = C$. Now $C = \mathbb{C} \cdot \bar{K}(\mathscr{C})$ and $\Sigma(C) = \mathbb{C} \cdot \Sigma(\bar{K}(\mathscr{C}))$, where the composita are taken inside $\mathfrak{F}$. Therefore, $\bar{K}(\mathscr{C}) = \Sigma(\bar{K}(\mathscr{C}))$. Since $\bar{K}(\mathscr{C})/\bar{K}(\mathscr{D})$ is galois, this suffices to prove that $\bar{K}(\mathscr{C})/K(\mathscr{D})$ is galois. ■

The following proposition is essentially [M1], Satz 1.1. We give the proof only for a special case.

2.5. Proposition: (Matzat) Assume there is a model $\bar{K}(\mathscr{C})/\bar{K}(\mathscr{D})$ for $\mathscr{C} \xrightarrow{G} \mathscr{D}$ over $\bar{K}$, and assume that $\bar{K}(\mathscr{C})$ is galois over $K(\mathscr{D})$. If some point P of $\mathscr{D}$ is defined over K (with respect to $(K(\mathscr{D}), \alpha)$), then there is a section for $(\bar{K}(\mathscr{C}), K(\mathscr{D}))$.

Proof: (In the case that P is not a branch point. See [M1], Satz 1.1 for the proof in general). Let A be the discrete valuation ring with fraction field $\bar{K}(\mathscr{D})$ which corresponds to the point P. Let $\mathfrak{p}$ be the maximal ideal of A. Let B be the integral closure of A in $\bar{K}(\mathscr{C})$. Since P is not a branch point, B has $n = |G|$ distinct maximal ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$.

We will now construct a section for $(\bar{K}(\mathscr{C}), K(\mathscr{D}))$. Given $\sigma \in \operatorname{gal}(\bar{K}/K)$, let σ' be an extension of σ to an element of $\operatorname{aut}(\mathbb{C}/K)$ and let Σ be any extension of $\alpha(\sigma')|_{\bar{K}(\mathscr{D})} \in \operatorname{gal}(\bar{K}(\mathscr{D})/K(\mathscr{D}))$ to an element of $\operatorname{gal}(\bar{K}(\mathscr{C})/K(\mathscr{D}))$. Since P is defined over K, $\Sigma(A) = A$ and Σ permutes $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$.

For $j = 1, \ldots, n$, let g_j be the unique element of G which takes $\mathfrak{q}_j$ to $\mathfrak{q}_1$. If $\Sigma(\mathfrak{q}_1) = \mathfrak{q}_j$, define

$$\hat{\sigma} = g_j \circ \Sigma.$$

Thus $\hat{\sigma}(\mathfrak{q}_1) = \mathfrak{q}_1$.

To see that $\hat{}$: $\operatorname{gal}(\bar{K}/K) \to \operatorname{gal}(\bar{K}(\mathscr{C})/K(\mathscr{D}))$ is a homomorphism, note that $\hat{\sigma}\hat{\tau}(\sigma\hat{\ }\tau)^{-1} \in G$ and $\hat{\sigma}\hat{\tau}(\sigma\hat{\ }\tau)^{-1}(\mathfrak{q}_1) = \mathfrak{q}_1$, so that $\hat{\sigma}\hat{\tau}(\sigma\hat{\ }\tau)^{-1} =$ identity. It is now clear that $\hat{}$ is a section. ■

3. Sections and towers of coverings

Throughout this section, let G be a finite group with a normal subgroup H. Assume that H is abelian. Let $\mathscr{C} \xrightarrow{G} \mathbb{P}^1_{\mathbb{C}}$ be a G-galois branched covering, and let $\mathscr{D} = \mathscr{C}/H$. Thus $\mathscr{C} \xrightarrow{H} \mathscr{D}$, $\mathscr{D} \xrightarrow{G/H} \mathbb{P}^1_{\mathbb{C}}$ are H-galois and G/H-galois branched coverings respectively.

Let $K \subset \mathbb{C}$ be a field and assume there are models $\bar{K}(\mathscr{C})/\bar{K}(x)$ and $K(\mathscr{D})/K(x)$ for $\mathscr{C} \xrightarrow{G} \mathbb{P}^1_{\mathbb{C}}$ over $\bar{K}$ and $\mathscr{D} \xrightarrow{G/H} \mathbb{P}^1_{\mathbb{C}}$ over K respectively. Let $\bar{K}(\mathscr{D})/\bar{K}(x)$ be the extension of $K(\mathscr{D})/K(x)$ to $\bar{K}$, and assume that $\bar{K}(\mathscr{D})$ is the fixed field of H in $\bar{K}(\mathscr{C})$.

$$\begin{tikzcd}
\bar{K}(\mathscr{C}) \arrow[d, dash, "H"'] & \\
\bar{K}(\mathscr{D}) \arrow[d, dash, "G/H"'] \arrow[dr, dash] & \\
\bar{K}(x) \arrow[dr, dash] & K(\mathscr{D}) \arrow[d, dash, "G/H"] \\
 & K(x)
\end{tikzcd}$$

Since $\bar{K}(\mathscr{D})$ is the compositum (in $\bar{K}(\mathscr{C})$) of $K(\mathscr{D})$ and $\bar{K}$, there is a unique section $\tilde{\ }$ for $(\bar{K}(\mathscr{D}), K(x))$ such that $\tilde{\sigma}$ leaves $K(\mathscr{D})$ elementwise fixed whenever $\sigma \in \operatorname{gal}(\bar{K}/K)$. Because the models for $\mathscr{D} \xrightarrow{G/H} \mathbb{P}^1_{\mathbb{C}}$ over k and $\bar{K}$ are compatible, it follows that

$$\tilde{\sigma}\bar{g}\tilde{\sigma}^{-1} = \bar{g}$$

for all $\sigma \in \operatorname{gal}(\bar{K}/K)$ and $\bar{g} \in G$.

Recall that we always use the standard model of $\mathbb{P}^1_{\mathbb{C}}$ over $\mathbb{Q}$, namely $(\mathbb{Q}(x), \alpha)$ (see Convention 1.4). Let $(K(\mathscr{D}), \beta)$ be the model for $\mathscr{D}$ over K which is compatible with $(\mathbb{Q}(x), \alpha)$.

If $\bar{K}(\mathscr{C})$ is galois over $K(x)$, then let

$$\text{res}: \operatorname{gal}(\bar{K}(\mathscr{C})/K(x)) \to \operatorname{gal}(\bar{K}(\mathscr{D})/K(x))$$

be the natural homomorphism.

In [B] sections were "lifted" by working over a field of cohomological dimension $\leqslant 1$. Here, the following trivial lemma will be used instead.

3.1. Lemma: *Assume that $\bar{K}(\mathscr{C})$ is galois over $K(\mathscr{D})$. Then*

1) *$\bar{K}(\mathscr{C})$ is galois over $K(x)$.*
2) *If some point of $\mathscr{D}$ is defined over K (with respect to $(K(\mathscr{D}), \beta)$), then there is a section $\hat{\ }$ for $(\bar{K}(\mathscr{C}), K(x))$ which is a lift of $\tilde{\ }$, i.e.*

$$\text{res} \circ \hat{\ } = \tilde{\ }. \qquad \blacksquare$$

Let G/H act on H on the left by conjugation:

$$\bar{g}(h) = ghg^{-1}$$

where $g \in G$ is any element which goes to $\bar{g}$ in G/H. Since H is abelian, this action is well defined.

3.2. LEMMA: *Assume $\bar{K}(\mathscr{C})$ is galois over $K(x)$. If there is a section $\hat{}$ for $(\bar{K}(\mathscr{C}), K(x))$ such that*
a) $(\text{res } \hat{\sigma})\bar{g}(\text{res } \hat{\sigma})^{-1} = \bar{g}$
for all $\bar{g} \in G/H$, $\sigma \in$ $\text{gal}(\bar{K}/K)$
b) $\hat{\sigma}h\hat{\sigma}^{-1} = h$
for all $h \in H$, $\sigma \in$ $\text{gal}(\bar{K}/K)$,
then
i) $\bar{K}(\mathscr{C})/\bar{K}(x)$ descends to a field J, where J/K is galois and $\text{gal}(J/K) \hookrightarrow Z^1(G/H, H)$.
ii) If c.d.$(K) \leqslant 1$ *then $\bar{K}(\mathscr{C})/\bar{K}(x)$ descends to a field J, where J/K is galois and* $\text{gal}(J/K) \hookrightarrow H^1(G/H, H)$.

REMARK: Let Φ: $\text{gal}(\bar{K}/K) \to \text{Aut}(G)$ by $\Phi(\sigma)(g) = \hat{\sigma}g\hat{\sigma}^{-1}$, $g \in G$, $\sigma \in \text{gal}(\bar{K}/K)$.In case *i*), J is the fixed field of ker Φ. In case *ii*), J is the fixed field of $\Phi^{-1}(\text{Inn } (G))$.

Proof: i) Let $h_{\sigma,g} = \hat{\sigma}g\hat{\sigma}^{-1}g^{-1}$ for $\sigma \in \text{gal}(\bar{K}/K)$, $g \in G$. We shall show that:
1) For each $\sigma \in \text{gal}(\bar{K}/K)$, $\bar{g} \mapsto h_{\sigma,g}$ (where $g \in G$ has image $\bar{g}$ in G/H) is a well-defined element of $Z^1(G/H, H)$.
2) $\sigma \mapsto (\bar{g} \mapsto h_{\sigma,g})$ is a homomorphism of $\text{gal}(\bar{K}/K)$ into $Z^1(G/H, H)$.

Proof of 1): By hypothesis a), $h_{\sigma,g} \in H$. Let $\sigma \in \text{gal}(\bar{K}/K)$, $g \in G$, $K \in H$. By hypothesis *b*) and since H is abelian,

$$h_{\sigma,kg} = h_{\sigma,g}$$

Therefore, $\bar{g} \mapsto h_{\sigma,g}$ is well-defined.

To show that $\bar{g} \mapsto h_{\sigma,g}$ is an element of $Z^1(G/H, H)$, one must show that if $\bar{g},\bar{f} \in G/H$ are represented by $g,f \in G$, then $g(h_{\sigma,f}) \cdot h_{\sigma,gf}^{-1} \cdot h_{\sigma,g} = 1$. This is an easy computation.

Proof of 2): To show that $\sigma \mapsto (\bar{g} \mapsto h_{\sigma,g})$ is a homomorphism of $\text{gal}(\bar{K}/K)$ into $Z^1(G/H, H)$, one must show that $h_{\sigma\tau,g} = h_{\sigma,g} \cdot h_{\tau,g}$. This is another easy computation, using hypothesis *b*) and the fact that H is abelian.

To conclude the proof of the lemma, let J be the fixed field of the kernel of the homomorphism $\text{gal}(\bar{K}/K) \to Z^1(G/H, H)$ above. Then $\sigma \in \text{gal}(\bar{K}/J)$

iff $h_{\sigma,g} = 1$, i.e., $\hat{\sigma}g\hat{\sigma}^{-1} = g$ for all $g \in G$. (Hence the remark). By Lemma 2.3, $\bar{K}(\mathscr{C})/\bar{K}(x)$ descends to J.

ii) Now assume c.d. $(L) \leqslant 1$. As above we have a homomorphism $\mathrm{gal}(\bar{K}/K) \to H^1(G/H, H)$. Let J be the fixed field of the kernel. Then $\sigma \in \mathrm{gal}(\bar{K}/J)$ iff there is some $h_\sigma \in H$ such that for all $g \in G$,

$$h_{\sigma,g} = h_\sigma^{-1}(gh_\sigma g^{-1}) \quad \text{i.e.,}$$

$$\hat{\sigma}g\hat{\sigma}^{-1} = h_\sigma^{-1}gh_\sigma .$$

This implies that the field of moduli of $\mathscr{C} \xrightarrow{G} \mathbb{P}^1_{\mathbb{C}}$ is contained in J. By [Bel], Theorem 1, $\bar{K}(\mathscr{C})/\bar{K}(x)$ descends to J. ■

4. Unramified coverings

Throughout this section, let $\mathscr{D}$ be a curve (over $\mathbb{C}$) of genus g. Let $K \subset \mathbb{C}$ be a field over which there is a model $(K(\mathscr{D}), \alpha)$ for $\mathscr{D}$ over K. Let ℓ be a prime number.

4.1. Definition: Given branched coverings $\mathscr{C}_1 \to \mathscr{D}$, $\mathscr{C}_2 \to \mathscr{D}$, we say that $\mathscr{C}_1 \to \mathscr{D}$ *dominates* $\mathscr{C}_2 \to \mathscr{D}$ if there is a branched covering map $\mathscr{C}_2 \to \mathscr{C}_2$ making the diagram below commute:

$$\begin{tikzcd}
 & \mathscr{C}_1 \arrow[dl] \arrow[dd] \\
\mathscr{C}_2 \arrow[dr] & \\
 & \mathscr{D}
\end{tikzcd}$$

■

4.2. Lemma:

a) *There is a unique (up to equivalence) galois unramified covering $\mathscr{U}_\ell \to \mathscr{D}$ with galois group $(\mathbb{Z}/\ell)^{2g}$.*

b) *Given any galois unramified covering $\mathscr{C} \to \mathscr{D}$ with galois group $(\mathbb{Z}/\ell)^n$, it is dominated by $\mathscr{U}_\ell \to \mathscr{D}$.*

Proof: To give a galois unramified covering of $\mathscr{D}$ with galois group $(\mathbb{Z}/\ell)^n$ is to give a surjective homomorphism $\Phi: \pi_1(\mathscr{D}) \twoheadrightarrow (\mathbb{Z}/\ell)^n$.

Since $\mathscr{D}$ has genus g, $\pi_1(\mathscr{D}) = F(a_1, b_1, a_2, b_2, \ldots, a_g, b_g)/[(a_1b_1a_1^{-1}b_1^{-1}) \cdots (a_gb_ga_g^{-1}b_g^{-1})]$ ($F(a, b, c, \ldots)$ denotes the free group on a, b, c, . . .). Let ϱ: $\pi_1(\mathscr{D}) \twoheadrightarrow (\mathbb{Z}/\ell)^{2g}$ be the homomorphism determined by

$$\varrho(a_i) = (0, \ldots, 0, 1, 0, \ldots, 0) \quad 1 \text{ in the } (2i-1)\text{st slot}$$

$$\varrho(b_i) = (0, \ldots, 0, 0, 1, 0, \ldots, 0) \quad 1 \text{ in the } 2i\text{th slot.}$$

Viewing $(\mathbb{Z}/\ell)^n$ as a vector space over $\mathbb{Z}/\ell$, one sees that any surjective homomorphism of $\pi_1(\mathscr{D})$ onto $(\mathbb{Z}/\ell)^n$ factors through ϱ. ∎

If $\mathscr{C} \to \mathscr{D}$ is a branched covering with galois group $(\mathbb{Z}/\ell)^n$, then, in general, there is no hope of using Lemma 2.3 to descend a model for $\mathscr{C} \xrightarrow{(\mathbb{Z}/\ell)^n} \mathscr{D}$ over $\bar{K}$ to some smaller field. The following lemma (part c) is useful in this situation.

4.3. Lemma:

a) Let $\mathscr{U}_\ell \to \mathscr{D}$ be the galois unramified covering with galois group $(\mathbb{Z}/\ell)^{2g}$. Then the field of moduli of $\mathscr{U}_\ell \to \mathscr{D}$ (no group action) is K.

b) Let $H = (\mathbb{Z}/\ell)^n$ and let $\mathscr{C} \xrightarrow{H} \mathscr{D}$ be an H-galois branched covering. Let $\mathscr{E} \to \mathscr{D}$ be the minimal covering which dominates both $\mathscr{C} \to \mathscr{D}$ and $\mathscr{U}_\ell \to \mathscr{D}$. Then $\mathscr{E} \to \mathscr{D}$ is galois and $\operatorname{gal}(\mathscr{E}/\mathscr{D}) \approx (\mathbb{Z}/\ell)^m$ *for some $m \leqslant n + 2g$.*

c) The field of moduli of $\mathscr{E} \to \mathscr{D}$ (no group action) is K.

Proof: b) holds because the compositum of galois extensions is galois and the galois group is a subgroup of the direct sum.

a) and *c*): Let E, U, C and D be the fields over $\mathbb{C}$ corresponding to $\mathscr{E}$, $\mathscr{U}_\ell$, $\mathscr{C}$ and $\mathscr{D}$ respectively. Let F be an algebraic closure of E. Let $\sigma \in \operatorname{aut}(\mathbb{C}/K)$ and let Σ be any extension of $\alpha(\sigma) \in \operatorname{gal}(D/K(\mathscr{D}))$ to an automorphism of F.

The field extension $\Sigma(U)/D$ corresponds to an unramified cover of $\mathscr{D}$ which is galois with galois group $(\mathbb{Z}/\ell)^{2g}$. By Lemma 4.2 *a*), $\Sigma(U) = U$, hence *a*).

For *c*), it suffices to show that $\Sigma(C) \subset E$. Let $P_1, \ldots, P_m \in \mathscr{D}$ be the branch points of $\mathscr{C} \to \mathscr{D}$. By Kummer theory, there are $y_1, \ldots, y_n \in C$ such that $C = D[y_1, \ldots, y_n]$ and $y_i^\ell = f_i \in D$. Since $\mathscr{C} \to \mathscr{D}$ is branched at P_1, . . . , P_m, which are defined over K, the divisors of f_i and $\Sigma(f_i)$ are

$$a_{i1}P_1 + a_{i2}P_2 + \cdots + a_{im}P_m + \ell \cdot D_i$$

and

$$a_{i1}P_1 + a_{i2}P_2 + \cdots + a_{im}P_m + \ell \cdot \Sigma(D_i)$$

respectively, for some divisor D_i and integers a_{ij}. Thus the divisor of $\Sigma(f_i)/f_i$ is $\ell \cdot [\Sigma(D_i) - D_i]$. It follows that the cover of $\mathscr{D}$ corresponding to the field extension $D[\Sigma(y_i)/y_i, \ldots, \Sigma(y_n)/y_n]$ of D, is unramified and has galois group $(\mathbb{Z}/\ell)^s$ for some s. By Lemma 4.2, this covering is dominated by $\mathscr{U}_\ell \to \mathscr{D}$, so $\Sigma(y_i)/y_i \in U$. This proves that $\Sigma(C) \subset E$. ■

5. The action of the arithmetic galois group on unramified coverings

Throughout this section, let $\mathscr{D}$ be a curve (over $\mathbb{C}$) of genus g. Let ℓ be a prime number and let $\mathscr{U}_\ell \to \mathscr{D}$ be the unramified covering with galois group $(\mathbb{Z}/\ell)^{2g}$ (see Section 4). Let $K \subset \mathbb{C}$ be a field over which there is a model $(K(\mathscr{D}), \alpha)$ for $\mathscr{D}$ over K. Assume that some point P of $\mathscr{D}$ is defined over K (with respect to $(K(\mathscr{D}), \alpha)$).

We will see that $\mathrm{gal}(\bar{K}/K)$ acts on $\mathrm{gal}(\mathscr{U}_\ell/\mathscr{D}) \approx (\mathbb{Z}/\ell)^{2g}$ via a section. This action will be called Φ_ℓ. $\mathrm{gal}(\bar{K}/K)$ also acts on A_ℓ – the ℓ-torsion points on the Jacobian of $\mathscr{D}$ – via the well known map ϱ_ℓ: $\mathrm{gal}(\bar{K}/K) \to \mathrm{Aut}(A_\ell) \approx GL_{2g}(\mathbb{Z}/\ell)$. We show that with respect to compatible bases,

$$\Phi_\ell(\sigma) = X_\ell(\sigma) \cdot [\varrho_\ell(\sigma)^{-1}]^t$$

(where X_ℓ is the cyclotomic character and t denotes transpose). It follows that the determinant of $\Phi_\ell(\sigma)$ is $X_\ell(\sigma)^g$, i.e., that $\mathrm{gal}(\bar{K}/K)$ acts on $\mathrm{gal}(\mathscr{U}_\ell/\mathscr{D})$ via the cyclotomic character (compare to [Bel], Theorem 5.1 of [Fr], and Proposition 5.1). Furthermore, because of the Weil pairing, the image of Φ_ℓ lies in a symplectic group.

5.1. Lemma: *Let $H = (\mathbb{Z}/\ell)^{2g}$ and fix some H-action on $\mathscr{U}_\ell \to \mathscr{D}$. Then there is a model $\bar{K}(\mathscr{U})/\bar{K}(\mathscr{D})$ for $\mathscr{U}_\ell \xrightarrow{H} \mathscr{D}$ over $\bar{K}$ such that:*

1) $\bar{K}(\mathscr{U})$ is galois over $K(\mathscr{D})$.

2) There is a section $\hat{}$ for $(\bar{K}(\mathscr{U}), K(\mathscr{D}))$.

Proof: By Lemma 2.4 and Proposition 2.5, it suffices to show that the field of moduli of $\mathscr{U}_\ell \to \mathscr{D}$ (without the group action) is K. This follows from Lemma 4.3 *a*). ■

Definition of Φ_ℓ: Define

$$\Phi_\ell\colon \mathrm{gal}(\bar{K}/K) \to \mathrm{Aut}\,(\mathrm{gal}(\mathscr{U}_\ell/\mathscr{D})) \approx \mathrm{Aut}((\mathbb{Z}/\ell)^{2g})$$

by $\Phi_\ell(\sigma)(h) = \hat{\sigma}h\hat{\sigma}^{-1}$ for $\sigma \in \mathrm{gal}(\bar{K}/K)$, $h \in \mathrm{gal}(\mathscr{U}_\ell/\mathscr{D}) \approx (\mathbb{Z}/\ell)^{2g}$.

Notice that $\mathrm{Aut}((\mathbb{Z}/\ell)^{2g}) \approx GL_{2g}(\mathbb{Z}/\ell)$.

Let A be the Jacobian of $\mathcal{D}$ and let A_ℓ be the group of ℓ-torsion points on A. $\mathcal{D}$ is defined over K, therefore there is a model for A over K. Let

$$\varrho_\ell\colon \mathrm{gal}(\bar{K}/K) \to \mathrm{Aut}(A_\ell) \approx GL_{2g}(\mathbb{Z}/\ell)$$

be the usual homomorphism (see [Se ℓ] p. I-4, Ex. 3).

We wish to compare Φ_ℓ and ϱ_ℓ. To do this we first pick compatible bases for $A_\ell \approx (\mathbb{Z}/\ell)^{2g}$ and $\mathrm{gal}(\mathcal{U}_\ell/\mathcal{D}) \approx (\mathbb{Z}/\ell)^{2g}$ considered as vector spaces over $\mathbb{Z}/\ell$.

Let $\{x_1, \ldots, x_{2g}\}$ be a basis for A_ℓ over $\mathbb{Z}/\ell$. $x_1, \ldots, x_{2g}$ are represented by divisors $E_1, \ldots, E_{2g}$ on $\mathcal{D}$. $E_1, \ldots, E_{2g}$ are defined over $\bar{K}$, have degree zero and $\ell \cdot E_i \sim 0$, $i = 1, \ldots, 2g$. Thus there are functions $f_1, \ldots, f_{2g} \in \bar{K}(\mathcal{D})$, such that $\ell \cdot E_i = (f_i)$.

5.2. Lemma:

$$\bar{K}(\mathcal{D})[z_1, \ldots, z_{2g}]/(z_1^\ell - f_1, \ldots, z_{2g}^\ell - f_{2g})$$

is a galois field extension of $\bar{K}(\mathcal{D})$ which corresponds to a galois unramified covering of $\mathcal{D}$ with galois group $(\mathbb{Z}/\ell)^{2g}$.

Proof: That the given ring is a field follows from the fact that $E_1, \ldots, E_{2g}$ are linearly independent. Since $(f_i) = \ell \cdot E_i$, the corresponding covering is unramified. ■

Since there is only one galois unramified covering of $\mathcal{D}$ with galois group $(\mathbb{Z}/\ell)^{2g}$ (Lemma 4.2),

$$\bar{K}(\mathcal{D})[z_1, \ldots, z_{2g}]/(z_1^\ell - f_1, \ldots, z_{2g}^\ell - f_{2g}) \approx \bar{K}(\mathcal{U}).$$

Fix a primitive ℓ-th root of unity, ζ_ℓ. There is now a natural choice of basis for $\mathrm{gal}(\bar{K}(\mathcal{U})/\bar{K}(\mathcal{D})) \approx (\mathbb{Z}/\ell)^{2g}$ (as $\mathbb{Z}/\ell$-vector spaces), namely $(h_1, \ldots, h_{2g})$, where

$$h_i(z_j) = \begin{cases} z_j & \text{if } i \neq j \\ \zeta_\ell z_j & \text{if } i = j. \end{cases}$$

Let $X_\ell\colon \mathrm{gal}(\bar{K}/K) \to (\mathbb{Z}/\ell)^*$ be the cyclotomic character, defined by $X_\ell(\sigma) = n$ if $\sigma(\zeta_\ell) = \zeta_\ell^n$.

5.3. Lemma: *With respect to compatible bases,*

$$\Phi_\ell(\sigma) = X_\ell(\sigma) \cdot [\varrho_\ell(\sigma)^{-1}]^t$$

Proof: Let $\sigma \in \text{gal}\,(\bar{K}/K)$. Suppose that $\varrho_\ell(\sigma)$ is the matrix (a_{ij}) with respect to the basis $\{x_1, \ldots, x_{2g}\}$, i.e., $\varrho_\ell(\sigma)(x_j) = a_{1j}x_1 + a_{2j}x_2 + \cdots + a_{2g,j}x_{2g}$ $(a_{ij} \in \mathbb{Z}/\ell)$. Thus $\hat{\sigma}(E_j) \sim a_{1j}E_1 + a_{2j}E_2 + \cdots + a_{2g,j}E_{2g}$, and therefore $\hat{\sigma}(z_j) = dz_1^{a_{1j}} \cdots z_{2g}^{a_{2g,j}}$, for some $d \in \bar{K}(\mathscr{D})$.

Let the matrix $(b_{ij}) = (a_{ij})^{-1}$. Then $\hat{\sigma}^{-1}(z_j) = ez_1^{b_{1j}} \cdots z_{2g}^{b_{2g,j}}$ for some $e \in \bar{K}(\mathscr{D})$. $(\hat{\sigma}h_i\hat{\sigma}^{-1})(z_j) = \hat{\sigma}(e\zeta_\ell^{b_{ij}}z_1^{b_{1j}} \cdots z_{2g}^{b_{2g,j}}) = \zeta_\ell^{X(\sigma)\cdot b_{ij}} \cdot z_j = h_j^{X(\sigma)b_{ij}}(z_j)$ (where $X = X_\ell$).

Thus $\Phi_\ell(\sigma)(h_i) = \hat{\sigma}h_i\hat{\sigma}^{-1} = h_1^{X(\sigma)b_{i1}}h_2^{X(\sigma)b_{i2}} \cdots h_{2g}^{X(\sigma)b_{i,2g}}$. With respect to the basis $\{h_1, \ldots, h_{2g}\}$ for $\text{gal}(\bar{K}(\mathscr{U})/\bar{K}(\mathscr{D}))$, $\Phi_\ell(\sigma)$ has matrix $X_\ell(\sigma) \cdot (b_{ij})^t = X_\ell(\sigma) \cdot [(a_{ij})^{-1}]^t$. ■

Let $v_\ell\colon A_\ell \times A_\ell \to \mathbb{Z}/\ell$ be the Weil pairing. The following is well-known, see [L AV] Ch. VII, or [Si] Ch. III, Sec. 8 for the case $g = 1$.

5.4. Proposition:

a) $v_\ell\colon A_\ell \times A_\ell \to \mathbb{Z}/\ell$

is a nondegenerate, bilinear, alternating form.

b) If $\sigma \in \text{gal}\,(\bar{K}/K)$, *and* $x, y \in A_\ell$, *then*

$$v_\ell(\varrho_\ell(\sigma)(x), \varrho_\ell(\sigma)(y)) = X_\ell(\sigma) \cdot v_\ell(x, y).$$

5.5. Corollary: *With respect to an appropriate basis, the image of* $\varrho_\ell\colon \text{gal}(\bar{K}/K) \to \text{Aut}(A_\ell) \approx GL_{2g}(\mathbb{Z}/\ell)$ *lies in the group of symplectic similitudes,* $GSp_g(\mathbb{Z}/\ell)$. *If K contains the* ℓ*-th roots of unity, then the image of* ϱ_ℓ *lies in the symplectic group* $Sp_g(\mathbb{Z}/\ell)$.

Where:

$$GSp_g(\mathbb{Z}/\ell) = \left\{ M \in GL_{2g}(\mathbb{Z}/\ell) \mid M^t \circ \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix} \circ M = \begin{bmatrix} 0 & \lambda I \\ -\lambda I & 0 \end{bmatrix} \right.$$

$$\left. \textit{for some } \lambda \in (\mathbb{Z}/\ell)^* \right\}$$

$$Sp_g(\mathbb{Z}/\ell) = \left\{ M \in GL_{2g}(\mathbb{Z}/\ell) \mid M^t \circ \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix} \circ M = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix} \right\}$$

where I is the $g \times g$ identity matrix.

The form $v_\ell \wedge \cdots \wedge v_\ell$, g times, is a nondegenerate alternating $2g$-linear form. $(v_\ell \wedge \cdots \wedge v_\ell)$ is defined by $(v_\ell \underbrace{\wedge \cdots \wedge}_{g\text{ times}} v_\ell)(x_1, x_2, \ldots, x_{2g-1}, x_{2g}) = \Sigma_{\tau \in P_{2g}} v(x_{\tau(1)}, x_{\tau(2)}) \cdot v(x_{\tau(3)}, x_{\tau(4)}) \cdot \cdots \cdot v(x_{\tau(2g-1)}, x_{\tau(2g)})$ where $P_{2g} = \{\tau \in S_{2g} | \tau(2k) > \tau(2k-1), \tau(2k+1) > \tau(2k-1)\}$.) Thus $(v_\ell \wedge \cdots \wedge v_\ell) \circ \varrho_\ell(\sigma) = \det \varrho_\ell(\sigma) \cdot v_\ell \wedge \cdots \wedge v_\ell$ for $\sigma \in \mathrm{gal}(\bar{K}/K)$. On the other hand, by Prop. 5.4, $(v_\ell \wedge \cdots \wedge v_\ell) \circ \varrho_\ell(\sigma) = X_\ell(\sigma)^g \cdot v_\ell \wedge \cdots \wedge v_\ell$. Therefore, $\det \varrho_\ell(\sigma) = X_\ell(\sigma)^g$.

5.6. Proposition: ("*The arithmetic galois group*, gal$(\bar{K}/K)$, *acts on the geometric galois group*, gal$(\mathcal{U}_\ell/\mathcal{D})$, *via the cyclotomic character*")

$$\det \Phi_\ell(\sigma) = X_\ell(\sigma)^g$$

if $\sigma \in \mathrm{gal}(\bar{K}/K)$.

Proof: By Lemma 5.3, $\Phi_\ell(\sigma) = X_\ell(\sigma) \cdot [\varrho_\ell(\sigma)^{-1}]^t$. Since $\Phi_\ell(\sigma)$ is a linear transformation on a $2g$-dimensional vector space,

$$\det \Phi_\ell(\sigma) = X_\ell(\sigma)^{2g} \cdot \det \varrho_\ell(\sigma)^{-1} = X_\ell(\sigma)^{2g} \cdot X_\ell(\sigma)^{-g} = X_\ell(\sigma)^g. \quad \blacksquare$$

6. The action of the arithmetic galois groups on branch cycles

Throughout this section, let H be a finite group (possibly not abelian) and let $\mathcal{C} \xrightarrow{H} \mathcal{D}$ by an H-galois branched covering. Let $K \subset \mathbb{C}$ be a field over which there is a model $(K(\mathcal{D}), \alpha)$ for $\mathcal{D}$ over K. Assume that:

1) K contains the field of moduli of $\mathcal{C} \to \mathcal{D}$ (without its group action).
2) The branch points of $\mathcal{C} \to \mathcal{D}$ are defined over K. (There is a version of Proposition 6.1 that doesn't require this condition, see [M2]).

In this section we prove that the arithmetic galois group, gal$(\bar{K}/K)$, acts on the decomposition groups of ramification points of $\mathcal{C} \to \mathcal{D}$ via the cyclotomic character (Prop. 6.1). In the case $\mathcal{D} = \mathbb{P}^1_{\mathbb{C}}$, this was shown in [Bel] and [Fr] (see [C + H], Cor. 2.2). Proposition 6.1 is a consequence of the proof of Satz 2.2 of [M2], but we include the proof here for completeness. The proof of Proposition 6.1 is also similar to Fried's "Branch Cycle Argument" ([Fr], in the proof of Theorem 5.1).

Compare Proposition 6.1 to Proposition 5.6, which says that the arithmetic galois group acts on the galois group of the $(\mathbb{Z}/\ell)^{2g}$ unramified cover of $\mathscr{D}$ (g = genus of $\mathscr{D}$), via the cyclotomic character.

By Lemma 2.4 and Proposition 2.5, there is a model $\bar{K}(\mathscr{C})/\bar{K}(\mathscr{D})$ of $\mathscr{C} \xrightarrow{H} \mathscr{D}$ over $\bar{K}$ such that:

a) $\bar{K}(\mathscr{C})$ is galois over $K(\mathscr{D})$

b) there is a section $\hat{}$ for $(\bar{K}(\mathscr{C}), K(\mathscr{D}))$.

Let $P \in \mathscr{D}$ be a branch point of $\mathscr{C} \xrightarrow{H} \mathscr{D}$, and let $Q \in \mathscr{C}$ be a ramification point over P. Let $h \in H = \text{gal}\,(\mathscr{C}/\mathscr{D})$ generate the decomposition group of Q, i.e., $\langle h \rangle = \{k \in H | k(Q) = Q\}$.

Suppose that h has order e. Let

$$X\colon \text{gal}\,(\bar{K}/K) \to (\mathbb{Z}/e)^*$$

be the cyclotomic character, i.e., $X(\sigma) = r$ if $\sigma(\zeta_e) = \zeta_e^r$ (ζ_e is a primitive e-th root of unity).

6.1. Proposition: (*Matzat, Fried, Belyi, "The arithmetic galois group acts on branch cycles through the cyclotomic character."*)

Let $\sigma \in \text{gal}\,(\bar{K}/K)$. *Recall that h generates the decomposition group of a ramification point of* $\mathscr{C} \to \mathscr{D}$. *Then*

$$\hat{\sigma} h \hat{\sigma}^{-1} \sim h^{X(\sigma)}$$

where $\tilde{}$ *denotes conjugacy in H.*

Let A be the discrete valuation ring containing $\bar{K}$, with fraction field $\bar{K}(\mathscr{D})$, corresponding to the branch point $P \in \mathscr{D}$. Let $\mathfrak{p}$ be the maximal ideal of A.

Let B be the integral closure of A in $\bar{K}(\mathscr{C})$. Let $\mathfrak{q}$ be the maximal ideal of B corresponding to the ramification point Q (so $\mathfrak{q}$ lies over $\mathfrak{p}$).

Since the point P is defined over K, there is $s \in \mathfrak{p}$ which generates the maximal ideal of A, and for which $\hat{\sigma}(s) = s$.

By considering the fixed field of $\langle h \rangle$ in $\bar{K}(\mathscr{C})$, and using Kummer theory, one can show that:

6.2. Lemma: *There is* $t \in B$ *such that*

1) $h(t) = \zeta_e t$ *for some primitive* e-th *root of unity* ζ_e

2) $B_{\mathfrak{q}} \cdot \mathfrak{q} = (t)$

3) $t^e = u \cdot s$ *for some* $u \in B_{\mathfrak{q}}^*$ (*= units of* $B_{\mathfrak{q}}$) (*where s is as above*).

Proof of Proposition 6.1: Let $\sigma \in \operatorname{gal}(\bar{K}/K)$. Since $\hat{\sigma}(\mathfrak{p}) = \mathfrak{p}$ and $\hat{\sigma}(B) = B$, $\hat{\sigma}$ permutes the maximal ideals of B lying over $\mathfrak{p}$. Let $\mathfrak{q}_0 = \hat{\sigma}(\mathfrak{q})$.

Pick $k \in H = \operatorname{gal}(\bar{K}(\mathscr{C})/\bar{K}(\mathscr{D}))$ such that $k(\mathfrak{q}) = \mathfrak{q}_0$. Since $\langle h \rangle$ is the decomposition group of $\mathfrak{q}$, $\langle khk^{-1} \rangle$ is the decomposition group of $\mathfrak{q}_0$.

Let t, u be as in Lemma 6.2 and let $t_0 = k(t)$, $u_0 = k(u)$. Then

1) $h(t) = \zeta_e t;\quad (khk^{-1})(t_0) = \zeta_e t_0$

2) $B_{\mathfrak{q}} \cdot \mathfrak{q} = (t);\quad B_{\mathfrak{q}0} \cdot \mathfrak{q}_0 = (t_0)$

3) $t^e = u \cdot s$ for some $u \in B^*_{\mathfrak{q}}$;

$t_0^e = u_0 \cdot s$ for some $u_0 \in B^*_{\mathfrak{q}}$

(recall that $\mathfrak{p} = (s)$, so $k(s) = s$).

Let $\hat{\mathcal{O}}$, $\hat{\mathcal{O}}_0$ denote the completions of $B_{\mathfrak{q}}$, $B_{\mathfrak{q}0}$ respectively. Then $\hat{\mathcal{O}} \approx \bar{K}[\![t]\!]$, $\hat{\mathcal{O}}_0 \approx \bar{K}[\![t_0]\!]$ (by [Se LF], Ch. II, Sec. 4, Prop. 5, since $B/\mathfrak{q} \approx \bar{K} \approx B/\mathfrak{q}_0$), so $B_{\mathfrak{q}} \subset \bar{K}[\![t]\!]$ and $B_{\mathfrak{q}0} \subset \bar{K}[\![t_0]\!]$.

Since $\hat{\sigma}$ and k both give homomorphisms from $B_{\mathfrak{q}}$ into $B_{\mathfrak{q}0}$, taking $\mathfrak{q}^n$ to $\mathfrak{q}_0^n$ for all positive integers n, they can be extended uniquely to homomorphisms of $\bar{K}[\![t]\!]$ into $\bar{K}[\![t_0]\!]$, which we still call $\hat{\sigma}$ and k. Similarly, h can be extended uniquely to an automorphism of $\bar{K}[\![t]\!]$.

Since the e-th roots of the constant term in the formal power series expansion for u are contained in $\bar{K}$, there is $v \in \bar{K}[\![t]\!]$ such that $v^e = u$.

We shall show that $h(v) = v$. Note that $h(t) = \zeta_e t$ and $h(s) = s$, therefore $h(u) = h(t^e/s) = u$. Since $v^e = u$, $h(v) = \zeta_e^a v$ for some integer a. If $v = d_0 + d_1 t + d_2 t^2 + \ldots$, $d_i \in K$, then $d_0 \neq 0$. Since $h(d_0) = d_0$, we have $a \equiv 0 \bmod e$ and $h(v) = v$.

Let $y = t/v$ (v is a unit, so $t/v \in \bar{K}[\![t]\!]$). Then $y^e = t^e/v^e = (u \cdot s)/u = s$ and $h(y) = \zeta_e t/v = \zeta_e y$.

Let $y_0 = k(y)$. Then $y_0^e = s$ and $(khk^{-1})(y_0) = \zeta_e y_0$.

Since $y^e = s$ and $\hat{\sigma}(s) = s$, and since $\hat{\sigma}\colon \bar{K}[\![t]\!] \to \bar{K}[\![t_0]\!]$, therefore $\hat{\sigma}(y) = \zeta_e^d \cdot y_0$ for some $d \in \mathbb{Z}/e$. Let $c \in \mathbb{Z}/e$ so that $\hat{\sigma}(\zeta_e^c \cdot y) = y_0$. $(\hat{\sigma}h\hat{\sigma}^{-1})(y_0) = (\hat{\sigma}h)(\zeta_e^c \cdot y) = \hat{\sigma}(\zeta_e^c \cdot \zeta_e \cdot y) = \hat{\sigma}(\zeta_e) y_0 = (khk^{-1})^{X(\sigma)}(y_0)$.

$\hat{\sigma}(\mathfrak{q}) = \mathfrak{q}_0$, $\hat{\sigma}\langle h \rangle \hat{\sigma}^{-1} = \langle khk^{-1} \rangle$, therefore $\hat{\sigma}h\hat{\sigma}^{-1} = (khk^{-1})^b$ for some $b \in (\mathbb{Z}/e)^*$. Since $(khk^{-1})^p(y_0) = (khk^{-1})^q(y_0)$ if and only if $p \equiv q \bmod e$, the above calculation shows that

$$\hat{\sigma}h\hat{\sigma}^{-1} = (khk^{-1})^{X(\sigma)} = kh^{X(\sigma)}k^{-1}. \qquad \blacksquare$$

7. The main theorem

As usual, fix the standard model $(\mathbb{Q}(x), \alpha)$ for $\mathbb{P}^1_{\mathbb{C}}$ over $\mathbb{Q}$ (see Convention 1.4).

The following lemma is the inductive step needed to prove Theorem 7.3.

7.1. Lemma: *Let G be a finite group with a normal subgroup $H = (\mathbb{Z}/\ell)^n$ for some prime number ℓ and some integer n. Let $\mathscr{C} \xrightarrow{G} \mathbb{P}^1_{\mathbb{C}}$ be a G-galois branched covering. Let $\mathscr{D} = \mathscr{C}/H$ and let g be the genus of $\mathscr{D}$.*

Let $L \in \mathbb{C}$ be a field over which $\mathscr{D} \xrightarrow{G/H} \mathbb{P}^1_{\mathbb{C}}$ is defined. Fix a model $L(\mathscr{D})/L(x)$. Assume that

a) *L contains the ℓ-th roots of unity*

b) *the branch points of $\mathscr{C} \to \mathbb{P}^1_{\mathbb{C}}$ are defined over L.*

Then there are finite extensions

$$J \supset M \supset M^u \supset M^b \supset L,$$

each galois over the next, satisfying the following:

1) $\mathscr{C} \xrightarrow{G} \mathbb{P}^1_{\mathbb{C}}$ is defined over J.

2a) M^b is the compositum (in $\mathbb{C}$) of the fields of definition (with respect to $L(\mathscr{D})$) of the branch points of $\mathscr{C} \to \mathscr{D}$, or M^b is the field of definition of some point of $\mathscr{D}$ if there are no branch points.

2b) $\mathrm{gal}(M^b/L)$ is a subquotient of $G/H \oplus \cdots \oplus G/H$ r times, where r is either the number of branch points of $\mathscr{C} \to \mathbb{P}^1_{\mathbb{C}}$, or is 1 if there are none.

3a) M^u is a field of definition of $\mathscr{U}_\ell \xrightarrow{(\mathbb{Z}/\ell)^{2g}} \mathscr{D}$ ($\mathscr{U}_\ell$ as in Lemma 4.2), and $\mathrm{gal}(M^u/M^b) \subset Sp_g(\mathbb{Z}/\ell)$.

3b) The image of $\mathrm{gal}(M^u/M^b)$ in $Sp_g(\mathbb{Z}/\ell) \subset GL_{2g}(\mathbb{Z}/\ell)$ commutes with the image of G/H in $GL_{2g}(\mathbb{Z}/\ell)$ obtained by letting G/H act on $\mathrm{gal}(\mathscr{U}_\ell/\mathscr{D})$ by conjugation

4) $\mathrm{gal}(M/M^u) \subset (\mathbb{Z}/\ell)^{2gn}$.

5) $\mathrm{gal}(J/M) \subset Z^1(G/H, H) \oplus Z^1(G/H, \mathrm{gal}(\mathscr{U}_\ell/\mathscr{D}))$ (G/H acts on H and $\mathrm{gal}(\mathscr{U}_\ell/\mathscr{D})$ by conjugation).

$$\begin{tikzcd}
J \arrow[dr, dash, "\text{subgr. of } Z^1(G/H, H) \oplus Z^1(G/H, (\mathbb{Z}/\ell)^{2g})"] & & & \\
& M \arrow[dr, dash, "\text{subgr. of } (\mathbb{Z}/\ell)^{2gn}"'] & & \\
& & M^u \arrow[dr, dash, "\text{subgr. of } Sp_g(\mathbb{Z}/\ell)"] & \\
& & & M^b \arrow[dr, dash, "\text{subq. of } G/H \oplus \cdots \oplus G/H"'] & \\
& & & & L
\end{tikzcd}$$

Remark: The Z^1's can be replaced by H^1's if one works over a field of cohom. dim. $\leqslant 1$ (using Lemma 3.2). See [B].

Proof: Let M^b be defined as in 2a). Then 2b) holds.

Let $\mathscr{E} \to \mathscr{D}$ be the minimal covering which dominates both $\mathscr{C} \to \mathscr{D}$ and $\mathscr{U}_\ell \to \mathscr{D}$. By Lemma 4.2, $\mathscr{U}_\ell \to \mathbb{P}^1_{\mathbb{C}}$ is galois. Since the compositum of galois extensions is galois, $\mathscr{E} \to \mathbb{P}^1_{\mathbb{C}}$ is galois. Let $\mathfrak{H} = \mathrm{gal}\,(\mathscr{E}/\mathbb{P}^1_{\mathbb{C}})$ and fix an $\mathfrak{H}$-action on $\mathscr{E} \to \mathbb{P}^1_{\mathbb{C}}$.

By Lemma 4.3, the field of moduli of $\mathscr{E} \to \mathscr{D}$ is contained in M^b. Lemmas 2.4 and 3.1 apply to yield a model $\bar{L}(\mathscr{E})/\bar{L}(x)$ for $\mathscr{E} \xrightarrow{\mathfrak{H}} \mathbb{P}^1_{\mathbb{C}}$ over $\bar{L}$ such that:
1) $\bar{L}(\mathscr{E})$ is galois over $M^b(x)$.
2) There is a section $\hat{}$ for $(\bar{L}(\mathscr{E}), M^b(x))$.
3) $\hat{\sigma}$ leaves $M^b(\mathscr{D}) = M^b \cdot L(\mathscr{D})$ elementwise fixed.

Let $\bar{L}(\mathscr{C})$, $\bar{L}(\mathscr{U})$, $\bar{L}(\mathscr{D})$ be the subfields of $\bar{L}(\mathscr{E})$ corresponding to $\mathscr{C}$, $\mathscr{U}$, $\mathscr{D}$ respectively.

By Lemma 4.2, $\hat{\sigma}$ takes $\bar{L}(\mathscr{U})$ to itself whenever $\sigma \in \mathrm{gal}(\bar{L}/M^b)$.

Let Φ_ℓ: $\mathrm{gal}(\bar{L}/M^b) \to \mathrm{Aut}(\mathrm{gal}(\mathscr{U}_\ell/\mathscr{D})) \approx GL_{2g}(\mathbb{Z}/\ell)$ be defined, as in Section 5, by $\Phi_\ell(\sigma)(f) = \hat{\sigma}f\hat{\sigma}^{-1}$, $\sigma \in \mathrm{gal}(\bar{L}/M^b)$, $f \in \mathrm{gal}(\mathscr{U}_\ell/\mathscr{D}) \approx (\mathbb{Z}/\ell)^{2g}$. By Lemmas 5.3 and 5.5, the image of Φ_ℓ lies in the symplectic group $Sp_g(\mathbb{Z}/\ell)$.

Let M^u be the fixed field of the kernel of Φ_ℓ. Thus 3a) holds (by Lemma 2.3).

Since $\hat{\sigma}\bar{g}\hat{\sigma}^{-1} = \bar{g}$ for $\sigma \in \mathrm{gal}(\bar{L}/M^b)$, $\bar{g} \in G/H$, the image of Φ_ℓ in $\mathrm{Aut}(\mathrm{gal}(\mathscr{U}_\ell/\mathscr{D}))$ commutes with the image of G/H in $\mathrm{Aut}(\mathrm{gal}(\mathscr{U}_\ell/\mathscr{D}))$. Hence 3b).

$\mathrm{gal}(\mathscr{E}/\mathscr{U}_\ell)$ is generated by all the decomposition groups of $\mathscr{E} \to \mathscr{D}$. Since $\mathrm{gal}(\mathscr{E}/\mathscr{D})$ is abelian, Proposition 6.1 implies that

$$(*)\ \hat{\sigma}k\hat{\sigma}^{-1} = k$$

for all $\sigma \in \mathrm{gal}(\bar{L}/M^b)$, $k \in \mathrm{gal}(\mathscr{E}/\mathscr{U}_\ell)$.

For 4), let

$$\eta\colon \mathrm{gal}(\bar{L}/M^u) \to \mathrm{Hom}\,(\mathrm{gal}(\mathscr{U}_\ell/\mathscr{D}), \mathrm{gal}(\mathscr{E}/\mathscr{U}_\ell))$$

$$\subset \mathrm{Hom}\,((\mathbb{Z}/\ell)^{2g}, (\mathbb{Z}/\ell)^n) \approx (\mathbb{Z}/\ell)^{2gn}$$

be defined by

$$(**)\ \eta(\sigma)(\bar{h}) = k_{\sigma,h}$$

where

$$k_{\sigma,h} = \hat{\sigma}h\hat{\sigma}^{-1}h^{-1}$$

for $\sigma \in \operatorname{gal}(\bar{L}/M^u)$, $h \in \operatorname{gal}(\mathscr{E}/\mathscr{D})$, $h \to \bar{h} \in \operatorname{gal}(\mathscr{U}_\ell/\mathscr{D})$. Note that $k_{\sigma,h} \in \operatorname{gal}(\mathscr{E}/\mathscr{U}_\ell)$.

If $h \in \operatorname{gal}(\mathscr{E}/\mathscr{D})$, $j \in \operatorname{gal}(\mathscr{E}/\mathscr{U}_\ell)$, then by (*), $k_{\sigma,hj} = \hat{\sigma}(hj)\hat{\sigma}^{-1}(j^{-1}h^{-1}) = \hat{\sigma}h\hat{\sigma}^{-1}h^{-1} = k_{\sigma,h}$. Therefore (**) is well defined.

Let h_1, $h_2 \in \operatorname{gal}(\mathscr{E}/\mathscr{D})$. Then it is easy to see that

$$k_{\sigma,h_1h_2} = k_{\sigma,h_1} \cdot k_{\sigma,h_2},$$

since $\operatorname{gal}(\mathscr{E}/\mathscr{U}_\ell)$ is abelian. Let $\sigma, \tau \in \operatorname{gal}(\bar{L}/M^u)$, $h \in \operatorname{gal}(\mathscr{E}/\mathscr{D})$. A calculation (using that $\operatorname{gal}(\mathscr{E}/\mathscr{U}_\ell)$ is abelian) shows that $\eta(\sigma\tau) = \eta(\sigma) \cdot \eta(\tau)$.

The above calculations show that η is a well defined homomorphism.

Let M be the fixed field of the kernel of η. Then 4) holds.

For 5) and 1), let $\sigma \in \operatorname{gal}(\bar{L}/M)$ and $h \in \operatorname{gal}(\mathscr{E}/\mathscr{D})$. Then $\hat{\sigma}h\hat{\sigma}^{-1} = h$. By Lemma 3.2, $\bar{L}(\mathscr{E})/\bar{L}(x)$ descends to a field J, where J/M is galois and $\operatorname{gal}(J/M) \hookrightarrow Z^1(G/H, \operatorname{gal}(\mathscr{E}/\mathscr{D}))$ (G/H acts on $\operatorname{gal}(\mathscr{E}/\mathscr{D})$ by conjugation). $\operatorname{gal}(\mathscr{E}/\mathscr{D}) \subset \operatorname{gal}(\mathscr{U}_\ell/\mathscr{D}) \oplus \operatorname{gal}(\mathscr{C}/\mathscr{D})$, therefore $\operatorname{gal}(J/M) \hookrightarrow Z^1(G/H, \operatorname{gal}(\mathscr{U}_\ell/\mathscr{D})) \oplus Z^1(G/H, H)$ so 5) and 1) hold. ■

7.2. Definitions: Let G be a finite group. Consider a chain of subgroups

$$(*)\ G_m \subset \cdots \subset G_1 \subset G_0 = G.$$

If $G_{i+1} \lhd G_i$, then (*) is called a *subinvariant series.*

If (*) is a subinvariant series such that each G_i is a maximal normal subgroup of G_{i-1}, then (*) is called a *composition series.*

If each G_i is maximal among normal subgroups of G contained in G_{i-1}, then (*) is called a *chief series.*

The groups G_i/G_{i+1} are called *factor groups.* ■

Let G be a finite, solvable group. Then G has a chief series

$$\{1\} = G_m \subset \cdots \subset G_1 \subset G_0 = G,$$

and each factor group G_i/G_{i+1} is elementary abelian (i.e., $(\mathbb{Z}/\ell)^n$, ℓ prime). See Theorem 9.2.4 of [Hall].

7.3. Theorem: *Let G be a finite, solvable group. Let $\mathscr{C} \xrightarrow{G} \mathbb{P}^1_{\mathbb{C}}$ be a G-galois branched covering with topological description $(h_1, \ldots, h_r)$.*

Let $\{1\} = G_m \subset \cdots \subset G_1 \subset G_0 = G$ be a chief series for G and let $G_i/G_{i+1} \approx (\mathbb{Z}/\ell_i)^{n_i}$, where ℓ_i is a prime number (see above).

Let a_{ij} be the order of the image of h_j in G/G_i. Let

$$g_\iota = 1 - |G/G_i| + (1/2)|G/G_i| \cdot \sum_{j=1}^{r} (1 - 1/a_{ij}).$$

Then there are fields

$$L_m \supset \cdots \supset L_1 \supset L_0,$$

where $L_0 = \mathbb{Q}(\zeta_n) \cdot$ (*field of def. of branch points of* $\mathscr{C} \to \mathbb{P}^1_{\mathbb{C}}$) *with* $n = |G|$, *and fields*

$$L_{\iota+1} \supset M^u_{\mathrm{i}} \supset M^b_i \supset L_i$$

$i = 0, \ldots, m - 1$, *such that*

1) L_m *is a field of definition of* $\mathscr{C} \xrightarrow{G} \mathbb{P}^1_{\mathbb{C}}$.
2) M^b_i/L_i *is galois and* $\mathrm{gal}(M^b_i/L_i) \approx (\mathbb{Z}/\ell_{i-1})^{s_i}$ *for some* $s_i \leqslant (r + 1)n_{i-1}$.
3) M^u_ι/M^b_i *is galois and* $\mathrm{gal}(M^u_i/M^b_i) \subset Sp_{g_i}(\mathbb{Z}/\ell_i)$
4) L_{i+1}/M^u_i *is galois and* $\mathrm{gal}(L_{i+1}/M^u_i) \approx (\mathbb{Z}/\ell_i)^{t_i}$ *for some* $t_i \leqslant |G/G_i| \cdot (n_i + 2g_i) + 2g_in_i$.

$$\begin{tikzcd}
L_{i+1} \arrow[dr, dash, "(\mathbb{Z}/\ell_i)^{t_i}"'] & & & \\
& M^u_i \arrow[dr, dash, "\text{subgroup of } Sp_{g_i}(\mathbb{Z}/\ell_i)"] & & \\
& & M^b_i \arrow[dr, dash, "(\mathbb{Z}/\ell_{i-1})^{S_i}"'] & \\
& & & L_i
\end{tikzcd}$$

7.4. Remark: Let $\mathscr{C}_i = \mathscr{C}/G_i$. Then the genus of $\mathscr{C}_i$ is g_i (Riemann–Hurwitz).

$$\mathscr{C} = \mathscr{C}_m \to \cdots \to \mathscr{C}_{i+1} \xrightarrow{(\mathbb{Z}/\ell_i)^{n_i}} \mathscr{C}_i \to \cdots \to \mathscr{C}_0 = \mathbb{P}^1_{\mathbb{C}}$$

$$\mathrm{gal}(\mathscr{C}_i/\mathbb{P}^1_{\mathbb{C}}) = G/G_i.$$

7.5. Remark: Here is the essence of the theorem:

Given only the topological description of a solvable branched covering of $\mathbb{P}^1_{\mathbb{C}}$ and a chief series for its galois group, Theorem 7.3 gives information on the factor groups in a subinvariant series for the galois group of some field of definition of the covering.

Proof of the Theorem: The theorem follows immediately from Remark 7.4, by applying Lemma 7.1 inductively.

Note that Lemma 7.1 gives somewhat finer information than what is stated in the theorem. ■

7.6. Corollary: ("*The arithmetic galois group is an extension of abelian groups and subquotients of symplectic groups*").

Let L be the field of definition of the branch points of $\mathscr{C} \xrightarrow{G} \mathbb{P}^1_{\mathbb{C}}$. *Let M be the galois closure, over L, of the field of moduli of* $\mathscr{C} \xrightarrow{G} \mathbb{P}^1_{\mathbb{C}}$.

Then $\mathrm{gal}(M/L)$ *is an extension of abelian groups and subquotients of symplectic groups.*

7.7. Remark: By using Lemma 7.1, 3b) and Schur's Lemma, one can show that if $(\mathbb{Z}/\ell_i)^{2g_i}$ is an irreducible G/G_i module for each $i = 0, \ldots, m$, then $\mathscr{C} \xrightarrow{G} \mathbb{P}^1_{\mathbb{C}}$ is defined over a *solvable* extension of the field of definition of its branch points. One can show that this is in general not the case: There are solvable branched coverings of $\mathbb{P}^1_{\mathbb{C}}$ with rational branch points, which are not defined over any solvable extension of $\mathbb{Q}$.

For example, let $\mathscr{E} \xrightarrow{\mathbb{Z}/2} \mathbb{P}^1_{\mathbb{C}}$ be the covering corresponding to the field extension

$$\begin{tikzcd}
\mathbb{C}(x)[y]/(y^2 - x(x-1)(x-\lambda)) \quad \text{where } \lambda \in \mathbb{Q}. \arrow[d, dash] \\
\mathbb{C}(x)
\end{tikzcd}$$

Then $\mathscr{E}$ is an elliptic curve. Choose λ so that $\mathscr{E}$ does not have complex multiplication (e.g., $\lambda = 3$ because then $j \notin \mathbb{Z}$). Let $\mathscr{U}_\ell \to \mathscr{E}$ be the galois unramified covering of $\mathscr{E}$ with galois group $(\mathbb{Z}/\ell)^2$ (see Lemma 4.2). The covering $\mathscr{U}_\ell \to \mathbb{P}^1_{\mathbb{C}}$ is galois with a solvable galois group, call it G_ℓ. By using [Se PG], Thm. 2, and the methods of this chapter, one can show that $\mathscr{U}_\ell \xrightarrow{G_\ell} \mathbb{P}^1_{\mathbb{C}}$ (with some group action) is not defined over any solvable extension of $\mathbb{Q}$. In fact, the galois group of the galois closure (over $\mathbb{Q}$) of the field of moduli of $\mathscr{U}_\ell \xrightarrow{G_\ell} \mathbb{P}^1_{\mathbb{C}}$ contains $PSL_2(\mathbb{Z}/\ell)$ as a subgroup if ℓ is sufficiently large. If $\lambda = 3$, then $\ell = 13$ is works, by [Se PG] Prop. 19.

Acknowledgement

This research was partially supported by NSF grant DMS 8512904.

I want to thank the entire mathematics department of the University of Pennsylvania for their support. For inspiration, helpful conversations and many hours spent on my behalf, I would like to thank my thesis advisor, David Harbater, as well as Ted Chinburg, Robert Coleman, Steve Diaz, Sankar Dutta, Eduardo Friedman, Herman Gluck, Will Kazez, Ken Ribet and Steve Shatz.

References

[B] S. Beckmann: *Fields of definition of solvable branched coverings*, University of Pennsylvania Ph.D. thesis (1986).

[Bel] G.V. Belyi: On Galois extensions of a maximal cyclotomic field, *Math. USSR Izv.* 14 (1980) 247–256.

[Bel2] G.V. Belyi: On extensions of the maximal cyclotomic field having a given classical Galois group, *J. reine u. angew. Math.* 341 (1983) 147–156.

[C + H] K. Coombes and D. Harbater: Hurwitz families and arithmetic Galois groups, *Duke Math. J.* 52, no. 4 (1985) 821–839.

[Ft] W. Feit, $\tilde{A}_5$ and $\tilde{A}_7$ are Galois groups over number fields, preprint (1986).

[Fr] M. Fried, Fields of definition of function fields and Hurwitz families – Groups as Galois groups, *Comm. Alg.* 5 (1977) 17–82.

[F] W. Fulton, Hurwitz schemes and irreducibility of algebraic curves, *Ann. Math.*, ser. 2, 90 (1969) 542–575.

[G] D. Gorenstein, Classifying the finite simple groups, *Bulletin of AMS*, 14, no. 1 (1986) 1–98.

[Hall] M. Hall, Jr., *The Theory of Groups*, Chelsea, NY (1976).

[Ha] D. Harbater, Galois coverings of the arithmetic line, to appear in *Proc. of the NY Number Thy.* Conf. of 1985, LNM?, Springer.

[H] R. Hartshorne, *Algebraic Geometry*, Springer, NY (1977).

[L AV] S. Lang, *Abelian Varieties*, Interscience, NY (1959).

[L DG] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, NY (1985).

[M1] B. Matzat, Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgrouppe, *J. reine u. angew. Math.* 349 (1984) 179–220.

[M2] B. Matzat, Zwei Aspekte konstruktiver Galoistheorie, *J. Algebra* 96 (1985) 449–531.

[M3] B. Matzat, Über das Umkehrproblem der galoisschen Theorie, Karlsruhe (1985), preprint.

[N] J. Neukirch, On Solvable Number Fields, *Inventiones Math.* 53 (1979) 135–164.

[Sh] I.R. Šafarevič, Construction of fields of algebraic numbers with given solvable galois group, *Izv. Akad. Nauk. SSSR. Ser. Math.* 18 (1954) 525–578; AMS Transl., Ser. 2, 4 (1956) 185–237.

[GAGA] J.-P. Serre, Géometrie algebrique et géometrie analytique, *Ann. de L'Inst. Fourier* VI (1956) 1–42.

[Se ℓ] J.-P. Serre, *Abelian ℓ-adic Representations and Elliptic Curves*, W.A. Benjamin, NY (1968).

[Se LF] J.-P. Serre, *Local Fields*, Springer, NY (1979).

[Se PG] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Inv. Math.* 15 (1972) (259–331).

[Si] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, NY (1986).

[Th] J. Thompson, Some finite groups which appear as Gal (L/K) where $K \subset \mathbb{Q}(\mu_n)$, *J. Alg.* 89 (1984) 437–499.