Reprinted from

Séminaire de Théorie des Nombres, Paris 1987-88

Edited by Catherine Goldstein

Progress in Mathematics, Volume 81

Birkhäuser
Boston • Basel • Berlin

Séminaire de Théorie des Nombres
Paris 1987-88

ARITHMETIC OF 3 AND 4 BRANCH POINT COVERS

A bridge provided by noncongruence subgroups of $SL_2(\mathbb{Z})$

M.D. FRIED*

Abstract : The method of choice nowadays for achieving a group G as a Galois group of a regular extension of $\mathbb{Q}(x)$ goes under the heading of *rigidity*. It works essentially, only, to produce Galois extensions of $\mathbb{Q}(x)$ ramified over 3 points. The three *rigidity* conditions ((0.1) below) imply that G is generated in a very special way by two elements. Generalization of *rigidity* that considers extensions with any number r of branch points has been around even longer than *rigidity* (§ 5.1). Of the three conditions, the generalization of the *transitivity condition*, 0.1 c), requires only the addition of an action of the Hurwitz monodromy group H_r (a quotient of the Artin braid group). But it also adds a 4th condition that in many situations amounts to asking for a $\mathbb{Q}$–point on the Hurwitz space associated the data for the generators of G. Theorem 1 below –our main theorem– is that in the case $r = 4$ this is equivalent to finding a $\mathbb{Q}$–point on a curve derived from a quotient of the upper half plane by a subgroup of $PSL_2(\mathbb{Z})$.

Although the description of this curve is quite explicit, there is one big problem : while it is sometimes a modular curve (§ 4), more often it is not. For this exposition we apply the theory to a simple example that illustrates the main points that arise in the arithmetic of 4 branch point covers (§ 5.2 and 5.3). The group is just A_5 in this case, but this allows us to compare the generalizations of *rigidity* with the historical progenitor of this, Hilbert's method for realizing alternating groups as Galois groups (§ 5.3).

Description of the main results.

The theory of the arithmetic of covers of the sphere arises in many diophantine investigations. The most well known, of course, is a version of the inverse problem of Galois theory : does every finite group G arise as the group of a Galois extension $L/\mathbb{Q}(x)$ with $\bar{\mathbb{Q}} \cap L = \mathbb{Q}$ (i.e. $L/\mathbb{Q}(x)$ is a regular extension) ?

For this lecture we use the dual theory of finite covers $\phi : X \longrightarrow \mathbb{P}^1$ of projective nonsingular curves. We shall consistently assume in this notation that $\mathbb{P}^1$ is identified with $\mathbb{C} \cup \infty = \mathbb{P}^1_x$, a copy of the complex plane uniformized by x, together with a point at ∞. Such a cover corresponding to the field extension $L/\mathbb{Q}(x)$ would have the property that it is defined over $\mathbb{Q}$ (§ 1.1) and the induced map on the function field level recovers the field extension $L/\mathbb{Q}(x)$. It is valuable, as we shall see in the key example of the paper, to consider covers $\phi : X \longrightarrow \mathbb{P}^1$ that may not be Galois.

Branch points and monodromy groups : Denote the degree of such an extension by n. The branch points of the cover are the values of x for which the cardinality of the fiber $\phi^{-1}(x)$ is inferior to n. We will consistently denote the branch points of the cover by $x_1,...,x_r$ (almost always assuming that each is a genuine branch point). The key parameter in all investigations is r.

From Riemann's existence theorem, degree n extensions L of $\mathbb{C}(x)$ ramified over r places $x_1,...,x_r$ are in one–one correspondence – up to a natural equivalence – with the degree n equivalence classes of connected covers of $\mathbb{P}^1_x \backslash \{x_1,...,x_r\}$. These are in turn in one–one correspondence with equivalence classes of transitive permutation representations $T : \pi_1 \longrightarrow S_n$ on the set $\{1,2,...,n\}$ where π_1 denotes the fundamental group of $\mathbb{P}^1_x \backslash \{x_1,...,x_r\}$. The Galois group of the normal closure of the extension $L/\mathbb{C}(x)$ is identified with the *monodromy group of the cover*, the group $G = T(\pi_1)$.

Rigidity when $r = 3$: Excluding solvable groups, most of the success in achieving groups as Galois groups has come through the arithmetic theory of covers in the case $r = 3$. The apparatus that reduces this to a computation related to a description of the cover through Riemann's existence theorem has been named *rigidity* following Thompson's usage in [T] (the name has the unfortunate aspect of potential confusion with the concept of *rigidifying data*, a tool that does appear in the proofs of results that generalize rigidity. We do only an exposition on *rigidity* so no problems are likely to occur). The *rigidity test* starts with an r–tuple $\mathbf{C} = (\mathbf{C}_1,...,\mathbf{C}_r)$ of conjugacy classes of G (§ 1.2). Our version (§ 5.1) includes the faithful permutation representation $T : G \longrightarrow S_n$ of the monodromy group of the cover as part of the data of the statement. For the

moment we use a stronger set of conditions on $(\mathbf{C}, T)$ than is necessary – it is still more general than used by most practitioners – in order to simplify our exposition on the distinction between $r = 3$ and $r > 3$. A little more notation will help to keep the key statements relatively memorable.

Denote the normalizer of G in S_n by $N_{S_n}(G)$. We denote the subgroup of this that maps $\{\mathbf{C}_1,...,\mathbf{C}_r\}$ into itself (by conjugation) by $N_{S_n}(\mathbf{C})$. The group generated by the entries of $\sigma_1,...,\sigma_r$ is $G(\sigma)$. Recall that a conjugacy class of a group is said to be rational if it is closed under putting elements to powers relatively prime to the orders of elements in the class.

If the following hold, then G is the Galois group of a regular extension of $\mathbb{Q}(x)$ ramified at any r points $x_1,...,x_r \in \mathbb{Q}$:

(0.1) a) $G = N_{S_n}(G)$;

b) each of the classes $\mathbf{C}_1,...,\mathbf{C}_r$ is rational; and

c) G acts transitively by conjugation on the following set of r–tuples

$$\{(\tau_1,...,\tau_r) \mid G(\tau) = G,\ \tau_i \in \mathbf{C}_i \text{ and } \tau_1 \cdots \tau_r = 1\}.$$

Condition (0.1 a) is not necessary, but weakening it is no triviality. Dealing with some version of (0.1 a) (as [Fr, 2] illustrates using the theory of complex multiplication) is a necessity. There have been successful attempts to finesse around consideration of (0.1 a) for special cases in Hilbert's original paper [Hi] and in Shih's use of modular curves to realize $PSL_2(\mathbb{Z}/p)$ as a Galois group wh[illegible] 2, 3 or 7 is a quadratic nonresidue modulo p [Sh]. Our example in [illegible]direct approach to weakening (0.1. a).

[illegible]ints of $x_1,...,x_r$ are to be in $\mathbb{Q}$, then (0.1. b) is necessary. Our n[illegible]statement in § 5.1 (Prop. 5.2 and Prop. 5.4) relaxes the condition on the branch points being in $\mathbb{Q}$, but the replacement condition will now be an absolute necessity. Finally, no one yet has shed any serious light on relaxation of (0.1 c).

What is surprising is how very often the conditions are satisfied in *the case that* $r = 3$ (e.g., Belyi [Be], Feit [F] among others, many papers of Malle and

Matzat some of which are included in [Ma,1], and Thompson [T]). They are almost never satisfied when r exceeds 3 (e.g. no example has been found when G is a noncyclic simple group).

Suppose that even every finite *simple* group is generated by three elements τ_1, τ_2, τ_3 that give conjugacy classes that satisfy the necessary condition analogous to (0.1 b) and the mysterious condition (0.1 c). If all that were of concern were the inverse Galois theory problem, then it *might* make sense to concentrate all research efforts on relaxation of condition (0.1 a). The hypotheses, however, of these statements don't hold : generators of groups with such handy properties don't always exist; and few of the other applications allow the investigator to be so picky about the choice of generators (as in [DFr] and [FR,2 and 3], we are referring to applications to Hilbert's irreducibility theorem and Siegel's theorem, ranks of elliptic curves and values of rational functions over finite fields).

Generalizations of rigidity for $r > 3$: Fortunately there are generalizations of *rigidity* that hold quite frequently for $r \geq 4$ ([Fr,1 : Theorem 5.1] and [Fr,3 : Theorem 1.5]). Matzat has used versions of these [Ma,1] to realize several simple groups as Galois groups (among them the Matthew group of degree 24 [Ma,2]). Increasing r improves the possibility of satisfying all three of the conditions (0.1), as explained in [Fr,2; Remark 2.2]. But there are two serious points. First : the generalization of (0.1 c) (condition 5.5 c)) works by asking for transitivity of a group that contains the *Hurwitz monodromy group* H_r *of degree* r (a quotient of the Artin braid group; (§ 3.1). The calculations for this applied to one of the classical sequences of simple groups can be quite formidable (e.g., Ex. 2.3 of [Fr,3] to realize all of the A_n's as Galois groups of 4 branch point covers of $\mathbb{P}^1$). For any one group, Matzat, for example, has put together a computer program to test this transitivity, but experience with the calculations is still more of an art than a science.

A later paper will consider the series of groups

$$PSL_2(\mathbb{Z}/p),\ p \equiv \pm 1 \bmod 24, \text{ and } 7 \text{ a quadratic nonresidue modulo } p.$$

For the other primes this is Shih's result [Sh]. While the calculations aren't quite complete, it doesn't seem that it is possible to achieve the groups of this series with covers of fewer than 4 branch points. And for each of these primes there does exist (C, T) with $r = 4$ satisfying the analog of the 3 conditions of (0.1)

(conditions 5.5. a–c). Why this doesn't quite finish the job of realizing these groups as Galois groups comes from our second point. The analog of (0.1) includes a condition d) which we now explain.

Parametrization of the covers associated to (C,T) : The collection of equivalence classes of covers associated to (C,T) is naturally parametrized by the associated *Hurwitz space* $\mathscr{H}(C)$ (with T understood from the context). This arises as a cover of $\mathbb{P}^r\backslash D_r$ coming from a representation of the Hurwitz monodromy group (§ 3.2). Here D_r is the classical discriminant locus in the respective spaces. We note this existence of the Noether cover $(\mathbb{P}^1)^r \to \mathbb{P}^r$, Galois with group S_r. When the analogs of the conditions 0.1) hold, $\mathscr{H}(C)$ (with its maps to $\mathbb{P}^r$) is defined over $\mathbb{Q}$. The extra condition d) for $r>3$ demands that there be a $\mathbb{Q}$ point on a connected component of the pullback of $\mathscr{H}(C)$ to $(\mathbb{P}^1)^r$. Below we refer to this space as $\mathscr{H}(C)'$. If all of the conditions (0.1) hold (with the Hurwitz monodromy action added to (0.1 c)), then condition d) is necessary (and sufficient) when the conjugacy classes in C are distinct.

The problem with this is clear : the space $\mathscr{H}(C)$ is a production of such great abstraction that the diophantine reduction seems impossible to effect. The main result of this paper is an alternative description of (5.5 d) in the case that $r=4$.

THEOREM 1 (special case of Conclusion 4.2). *There is a curve cover* $\psi_C' : Y_C' \to \mathbb{P}^1$ *ramified over just* $0,1,\infty$, *such that* $\mathscr{H}(C)'$ *has a* $\mathbb{Q}$*–point if and only if*

$$Y_C'(\mathbb{Q}) - \psi_C'^{-1}(0,1,\infty)$$

is nonempty. Furthermore, Y_C' *is identified with the projective normalization of a quotient of the upper half plane by a subgroup* H_C *of* $PSL_2(\mathbb{Z})$ *(of finite index), in such a way that it identifies the covered copy of* $\mathbb{P}^1$ *with the classical* λ*–line* $\mathbb{P}^1_\lambda$. *Finally, there is an explicit description of the branch cycles of the cover* ψ_C' *given by an action of the Hurwitz monodromy group* H_4.

There is an analogous curve cover $\psi_C \to \mathbb{P}^1$ in which $\mathbb{P}^1$ is identified with the classical j–line. Conclusion 4.2 is more general than Theorem 1 in that the former uses this cover as a replacement for that with Y_C'. This gives a necessary statement replacing condition (5.5 d) even when the 4 conjugacy classes of C are not distinct (when they are distinct, $Y_C = Y_C'$).

Congruence and noncongruence subgroups : A part of the proof of Conclusion 4.2 consists of showing that special values of C, Y_C can be identified with the classical curve $Y_0(n)$ that arises from the quotient of the upper half plane by the subgroup called $\Gamma_0(n)$. Thus modular curves arise. But in general the curves Y_C belong to noncongruence subgroups of $PSL_2(\mathbb{Z})$. Indeed, recently Diaz, Donagi and Harbater [DDH] have actually shown that *every* curve defined over the algebraic closure of $\mathbb{Q}$ occurs as Y_C' for some choice of C. Their choice, however, of C has nothing to do with the classical modular curve arithmetic.

An example where $G = A_5$ appears in [FrT] to show how one might investigate (for the inverse Galois theory problem) the infinitely many totally nonsplit extensions of any given finite simple group. Here we use it for three straight forward reasons : to show in practice the distinction between the curves Y_C and Y_C' ; to consider by example weakenings of condition (0.1 a); and to compare our results with the beginnings of this subject in [Hi].

1.– **Basic data for covers.**

One way to give an (irreducible) algebraic curve is to give a polynomial (irreducible) in two variables $f(x,y) \in \mathbb{C}[x,y]$ where $\mathbb{C}$ denotes the complex numbers. Then the curve is

$$\{x,y) | f(x,y) = 0\} \stackrel{\text{def}}{=} X.$$

This curve, however, may have singular points : points $(x_0, y_0) \in X$ for which $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial x}$ evaluated at (x_0, y_0) are both 0. Furthermore, we are missing the points at infinity obtained by taking the closure of X in the natural copy of projective 2–space $\mathbb{P}^2$ that contains the affine space $\mathbb{A}^2$ with variables x and y (and these points, too, might be singular).

The x–coordinate projection : After this we assume that our algebraic curves X don't have these defects; they will be projective nonsingular curves, so we may not be able to regard them as given by a single polynomial in 2–space. But the essential ingredient of this presentation, represented by the x–coordinate, will still be there.

That is, we have a covering map

$$\{x,y)|\, f(x,y) = 0\} \longrightarrow \mathbb{P}^1_x \stackrel{\text{def}}{=} \mathbb{C} \cup \infty \quad \text{or} \quad X \longrightarrow \mathbb{P}^1_x$$

given by projection of the point (x,y) onto its first coordinate. When the context is clear we will identify $\mathbb{P}^1_x$ with $\mathbb{P}^1$. We use this extra decoration by coordinate when it clarifies the context. The *monodromy group* of this cover is defined to be the Galois group G of the Galois closure of the field extension $\mathbb{C}(X)/\mathbb{C}(x)$ where $\mathbb{C}(X)$ denotes the quotient field of the ring $\mathbb{C}[x,y]/(f(x,y))$. In the sequel we will denote this Galois closure by $\widehat{\mathbb{C}(X)}$ or by the geometric version $\hat{X}$, the smallest Galois cover of $\mathbb{P}^1_x$ that factors through $X \longrightarrow \mathbb{P}^1_x$.

Note that in this situation G automatically comes equipped with a transitive permutation representation $T: G \longrightarrow S_n$. Denote the stabilizer in G of an integer (say, 1) by $G(T)$. Also, T is *primitive* (i.e., there are no proper groups between G and $G(T)$) if and only if there are no proper fields between $\mathbb{C}(X)$ and $\mathbb{C}(x)$ (equivalently, no proper covers fitting between $X \longrightarrow \mathbb{P}^1_x$).

1.1.– Branch points and the classical $PSL_2(\mathbb{C})$ action : The first parameter for dealing with covers is the number r of branch points of a given cover : the number of distinct points x of $\mathbb{P}^1$ for which the fiber of X above x has fewer actual points than the degree of the map. We deal not with one polynomial at a time, but rather with a parametrized family of them. But clearly it is natural to assume that all members of the family have the same number of branch points. The Hurwitz monodromy groups H_r are the key for putting these covers into families. In § 2 for $r = 3$ and in § 3 for $r = 4$ we introduce these groups and their basic properties. Although § 2.1 uses nothing more than the transitive action of $PSL_2(\mathbb{C})$ on distinct triples of points of $\mathbb{P}^1_x$, the notation used here is the main tool for the rest of the paper.

In classical algebraic geometry it has become a habit and a tradition to regard the parameter variety $\mathscr{H}$ for a family of covers with r branch points as

the source for a quotient $\mathscr{H}/PSL_2(\mathbb{C})$. Consider covers $\phi_i : X_i \longrightarrow \mathbb{P}^1_x$, i = 1,2, associated to two points $m_1, m_2 \in H$. The action is the one that equivalences m_1 and m_2 if and only if there exists $\alpha \in PSL_2(\mathbb{C})$ such that $\alpha \circ \phi_1 = \phi_2$. In § 2.3–2.4 we display the arithmetic and geometric subtleties that would make it a disaster to do this even in the case of families of 3 branch point covers. Here are some of the negatives for forming the quotient frivolously :

(1.1 a) there are technical difficulties in giving $\mathscr{H}/PSL_2(\mathbb{C})$ the structure of an algebraic variety and in visualizing its properties;

b) taking the quotient often destroys subtle finite group actions that are valuable for using the parameter space as a moduli space;

c) there are few quotable sources on the enriched family of covers structure; and

d) forming the quotient often wipes out the possibility of dealing with problems of considerable consequence.

Our first 3 branch point example in § 2.3 should go a long way to make our case for (1.1 d). It is the other points, of course, that cause the lengthy preambles to this subject with so many down to earth applications.

1.2.– Riemann's existence theorem and Nielsen classes : The classical discussion of maps of degree n from curves of genus g to projective 1–space gives us data for a natural collection of covers. We call the data a *Nielsen class* (below), and it is this that we shall regard as being fixed in the consideration of any family of covers.

Suppose that we are given a finite set $x = \{x_1,...,x_r\}$ of distinct points of $\mathbb{P}^1_x$. For any element $\sigma \in S_n^r$ denote the group generated by its coordinate entries by $G(\sigma)$. Consider $\phi : X \longrightarrow \mathbb{P}^1_x$, ramified only over x up to the relation that regards $\phi : X \longrightarrow \mathbb{P}^1_x$ and $\phi' : X' \longrightarrow \mathbb{P}^1_x$ as equivalent if there exists a homeomorphism $\lambda : X \longrightarrow X'$ such that $\phi' \circ \lambda = \phi$. These equivalence classes are in one–one correspondence with

(1.2) $\{\sigma = (\sigma_1,...,\sigma_r) \in S_n^r \mid \sigma_1...\sigma_r = 1,\ G(\sigma)$ is a transitive subgroup of $S_n\}$

modulo the relation that regards σ and σ' as equivalent if there is $\gamma \in S_n$ with $\gamma\sigma\gamma^{-1} = \sigma'$. This correspondence goes under the heading of Riemann's existence theorem [Gro]. The collection of ramified points $\boldsymbol{x}$ will be called the branch points of the cover $\phi : X \longrightarrow \mathbb{P}^1_{\boldsymbol{x}}$. (In most practical situations we shall mean that there truly is ramification over each of the points x_i, $i = 1,...,r$).

Riemann's existence theorem for families : Riemann's existence theorem generalizes through a combinatorial group situation to consider the covers above, not one at a time, but as topologized collections of families. That is, the branch points $\boldsymbol{x}$ run over the set $(\mathbb{P}^1)^r \backslash \Delta_r$ with Δ_r the r–tuples with two or more coordinates equal. In § 2 and § 3, respectively, we will introduce the coordinates for these families in the cases $r = 3$ and 4.

Suppose that $T : G \longrightarrow S_n$ is any faithful transitive permutation representation of a group G. Let $\mathbf{C} = (\mathbf{C}_1,...,\mathbf{C}_r)$ be an r–tuple of conjugacy classes from G. It is understood in our next definition that we have fixed the group G before introducing conjugacy classes from it.

DEFINITION 1.1. *The Nielsen class of* $\mathbf{C}$ *is* $Ni(\mathbf{C}) \stackrel{\text{def}}{=}$

$$\{r \in G^r \mid G(r) = G \textit{ and there is } \mathbf{C} \in S_r \textit{ with } \tau_{(i)\beta} \in C_i,\ i = 1,...,r\}.$$

Relative to canonical generators $\bar{\sigma}_1,...,\bar{\sigma}_r$ of the fundamental group $\pi_1(\mathbb{P}^1_{\boldsymbol{x}} - \boldsymbol{x}, x_0)$, we say that a cover ramified only over $\boldsymbol{x}$ is in $Ni(\mathbf{C})$ if the classical representation of the fundamental group sends the respective canonical generators to an r–tuple $\sigma \in Ni(\mathbf{C})$.

2.– Families for $r = 3$ and the Hurwitz monodromy group H_3.

2.1.– Complete families for $r = 3$ from transport of structure : It is clear that the fundamental group of $\mathbb{P}^3 \backslash D_3$ is of order 12 once it is shown that the fundamental group of $(\mathbb{P}^1)^3 \backslash \Delta_3$ is of order 2. But for any point $(x_1, x_2, x_3) = \boldsymbol{x}$ there is a unique element $\beta = \beta_{\boldsymbol{x}} \in PSL_2(\mathbb{C})$ that maps $(0, 1, \infty)$ to $\boldsymbol{x}$:

$$\beta(0) = x_1,\ \beta(1) = x_2,\ \text{and } \beta(\infty) = x_3.$$

Thus $\mathbb{P}^3\setminus\Delta_3$ is a principal homogeneous space for $PSL_2(\mathbb{C})$. They therefore have the same fundamental groups. As is well known, $SL_2(\mathbb{C})$ has trivial fundamental group. Thus the cover $SL_2(\mathbb{C})\longrightarrow PSL_2(\mathbb{C})$ displays the representative permutation representation.

Below we will use this in the manner of [Fr 1, p. 42]. Let $\phi : X\longrightarrow \mathbb{P}^1_x$ be any cover with three distinct branch points and order these as $(x_1^0, x_2^0, x_3^0) = x^0$. Denote $(\mathbb{P}^1)^3\setminus\Delta_3$ (resp., $\mathbb{P}^3\setminus D_3$) by $\mathcal{U}^3$ (resp., $\mathcal{U}_3$). Also, denote the natural map $PSL_2(\mathbb{C})\longrightarrow \mathrm{Aut}(\mathbb{P}^1_x)$ by $\mathcal{A}$. Form an irreducible family of covers from this data by transport of structure :

$$\begin{array}{ccccc} \mathcal{I} & \xrightarrow{\Phi} & \mathcal{U}^3\times\mathbb{P}^1_x & \xrightarrow{pr_1} & \mathcal{U}^3 \\ \downarrow & & \downarrow & & \downarrow \\ PSL_2(\mathbb{C})\times X & \xrightarrow{(Id,\mathcal{A})\circ Id\times\phi} & PSL_2(\mathbb{C})\times\mathbb{P}^1_x & \xrightarrow{pr_1} & PSL_2(\mathbb{C}), \end{array} \tag{2.1}$$

where the down map on the far right takes x to $\beta_x\circ\beta_{x^0}^{-1}$. The down maps indicate that the usual *family* notation (i.e. $\mathcal{I}$ denotes a *total* space) for the items in the bottom row is given in the top row. That is, with the identification of $\mathcal{U}^3\times\mathbb{P}^1_x$ and $PSL_2(\mathbb{C})\times\mathbb{P}^1_x$ based on x^0, $\mathcal{I}$ is the fiber product in the leftmost square of diagram (2.1). For each $x\in\mathcal{U}^3$ the points of $\mathcal{I}$ over $x\times\mathbb{P}^1_x$ give a cover of $\mathbb{P}^1_x$ equivalent to the cover $\beta_x\circ\beta_{x^0}^{-1}\circ\phi : X\longrightarrow\mathbb{P}^1_x$.

Let $Ni(\mathbf{C})$ be the Nielsen class and G the monodromy group of $\phi : X\longrightarrow\mathbb{P}^1_x$. Then $\mathcal{U}^3$ is the space $\mathcal{H}(\mathbf{C})_T$ (cf. § 3.2) much of the time. Indeed, consider the straight absolute Nielsen classes of $\mathbf{C}$:

$$SNi(\mathbf{C}) = \{\sigma\in Ni(\mathbf{C})\mid \sigma_i\in \mathbf{C}_i,\ i=1,2,3\}.$$

The normalizer of G in S_n, $N_T(G)$ acts by conjugation on the r–tuples of elements in G. The subset that stabilizes $Ni(\mathbf{C})$ is denoted by $N_T(\mathbf{C})$. Form the quotient of $SNi(\mathbf{C})$ by the subgroup of $N_T(\mathbf{C})$ that leaves this set stable to

get the absolute straight Nielsen classes, $SNi(\mathrm{C})_T^{ab}$. Note that the quotient of H_3 by the subgroup stabilizing each element of $SNi(\mathrm{C})_T^{ab}$ is itself a quotient of S_3 (and therefore is of order 1,2, 3 or 6).

PROPOSITION 2.1. *In the notation of section* 2.1 *assume that*

$$|SNi(\mathrm{C})_T^{ab}| = 1. \tag{2.2}$$

Thus H_3 *acts on* $Ni(\mathrm{C})_T^{ab}$ *through a transitive permutation representation of* S_3. *Then, as covers of* $\mathcal{U}_3$, $\mathcal{H}(\mathrm{C})$ *is isomorphic to* $\mathcal{U}^3$ *(resp.,* $\mathcal{U}_3$*) if and only if this is the regular representation (resp., the trivial representation).*

2.2.– **Most 3 branch point families derive from transport of structure** : A version of Proposition 2.1 appears in [BFr,1; § 4]. This analyzes when there exists a total representing family like that of (2.1) in the case when either (2.2) doesn't hold or when the action of H_3 isn't through the regular representation of S_3. Below we will use a converse. That is, suppose that

$$\mathcal{J} \xrightarrow{\Phi} \mathcal{H} \times \mathbb{P}^1_x \xrightarrow{pr_1} \mathcal{H}$$

is any family of 3 branch point covers with $\mathcal{J}$ and $\mathcal{H}$ irreducible nonsingular complex manifolds. We assume that all morphisms are smooth. Also, for each $m \in \mathcal{H}$, restriction of $pr_1 \circ \Phi$ to the fiber $\mathcal{J}_m$ gives a 3 branch point cover $\mathcal{J}_m \to \mathbb{P}^1_x$.

As above consider the following natural maps : $\mathcal{U}^3 \to \mathcal{U}_3$; and $\Psi_{\mathcal{H}} : \mathcal{H} \to \mathcal{U}_3$ by $m \in \mathcal{H}$ goes to the unordered collection of branch points of the corresponding cover. Any connected component $\mathcal{H}'$ of the fiber product $\mathcal{H} \times_{\mathcal{U}_3} \mathcal{U}^3$ has over it a connected component $\mathcal{J}'$ that gives a family of 3 branch point covers. Suppose that $m' \in \mathcal{H}'$, that x' is the image of projection of m' on $\mathcal{U}^3$, and that $\mathcal{J}_{m'} = X \to \mathbb{P}^1_x$ is the corresponding cover. Apply the transport of structure construction to canonically form a family of three branch

point covers over $\mathcal{U}^3$ having the fiber $X \to \mathbb{P}^1_x$ over x'. Then take a connected component of its pulback to $\mathcal{H}'$.

PROPOSITION 2.2. *Consider an irreducible family $\mathcal{F}'$ of 3 branch point covers over $\mathcal{H}'$ which has $\mathcal{J}_{m'} = X \to \mathbb{P}^1_x$ as a fiber. Then all covers $X' \to \mathbb{P}^1_x$ that appear in such a family have X' analytically isomorphic to X. Furthermore all such families are in one-one correspondence with the elements of the set*

$$\mathrm{Hom}(\pi_1(\mathcal{H}', m'), \mathrm{Aut}(X/\mathbb{P}^1_x)).$$

In particular :

(2.3) *if $\mathcal{H}' = \mathcal{U}^3$ and $(|\mathrm{Aut}(X/\mathbb{P}^1_x)|, 2) = 1$,*

then $\mathcal{F}'$ is uniquely determined by a single member of the family. In this case the total space $\mathcal{T}'$ of the family is analytically isomorphic to an open subset of $X \times (\mathbb{P}^1)^3$.

Proof : Form a locally constant sheaf of groups $\mathcal{A}\mathcal{U}\mathcal{T}(X/\mathbb{P}^1_x)$ on $\mathcal{H}'$ as follows. For $m \in \mathcal{H}'$ there is a unique element $\beta \in \mathrm{PSL}_2(\mathbb{C})$ that acts on $\mathbb{P}^1_x$ to map the (ordered) branch points of $\phi : \mathcal{J}_{m'} = X \to \mathbb{P}^1_x$ to those of $\mathcal{J}_{m'} \to \mathbb{P}^1_x$. From the transport of structure argument this last cover is equivalent to the cover $\beta \circ \phi : X \to \mathbb{P}^1_x$. Thus identify $\mathrm{Aut}(X/\mathbb{P}^1_x)$ to $\mathrm{Aut}(\mathcal{J}_{m'}/\mathbb{P}^1_x)$ by the identity map : an element $\gamma \in \mathrm{Aut}(X/\mathbb{P}^1_x)$ has the property that $\phi \circ \gamma = \phi$, and this automatically implies that $\beta \circ \phi \circ \gamma = \beta \circ \phi$.

A well–known theory identifies bundles over $\mathcal{H}'$ with constant fiber X and transition functions in $\mathcal{A}\mathcal{U}\mathcal{T}(X/\mathbb{P}^1_x)$ with the elements of $\mathrm{Hom}(\pi_1(\mathcal{H}', m'), \mathrm{Aut}(X/\mathbb{P}^1_x))$ (e.g., [Gu; p. 184–189]). If the groups $\pi_1(\mathcal{H}', m')$ and $\mathrm{Aut}(X/\mathbb{P}^1_x)$ have relatively prime order this set consists of just one element. This happens if (2.3) holds. The family in this case must be the very one that we formed by transport of structure. □

2.3.– Arithmetic constraints in placing branch points : we do an example. Here is the data for the Nielsen class : $r = 3$; $G = \mathbb{Z}/5 \times^{S} (\mathbb{Z}/5)^*$; $T : G \longrightarrow S_5$ is the standard degree 5 affine action on the affine line over $\mathbb{Z}/5$; and C_1 is the class of (0,2), C_2 is the class of (0,3) and C_3 is the class of (1,1). Representatives $\sigma \in Ni(\mathrm{C})_T^{ab}$ of the Nielsen class are easy to write out. First consider those where $\sigma_i \in C_i$, $i = 1, 2, 3$. Up to conjugation by elements of G there's only one : ((0,2),(2,3),(1,1)). Thus there are 6 total elements of $Ni(\mathrm{C})_T^{ab}$. Suppose that $X \longrightarrow \mathbb{P}^1_x$ is a cover in this Nielsen class where the branch points are x_1, x_2, x_3, corresponding in order to the three conjugacy classes as we have given them. The proof of next lemma is called the *branch cycle argument* in [Fr,1; § 5].

LEMMA 2.3. *If x_1, x_2, x_3 are in a field F disjoint from $\mathbb{Q}(i)$, then every field of definition of (X,ϕ) that contains x_1, x_2, x_3 also contains $\mathbb{Q}(i)$. In particular, (X,ϕ) can't be defined over $\mathbb{Q}$ if the branch points are $0, 1, \infty$.*

Proof : For simplicity assume F to be inside $\hat{\mathbb{Q}}$, an algebraic closure of the rationals. Let $\hat{\phi} : \hat{X} \longrightarrow \mathbb{P}^1_x$ be the Galois closure of the cover, and suppose that $\hat{F}$ is a field of definition of $(\hat{X},\hat{\phi})$ (note the momentary switch below in notation from subscript i to subscript j). Then giving data about inertial groups of points $\hat{m}_i \in \hat{X}$ lying over x_i, $i = 1,2,3$, is tantamount to giving an embedding $\psi_j : \hat{F}(\hat{X}) \longrightarrow \hat{F}(i)(((x-x_j)^{\frac{1}{2}}))$, $j = 1,2$, and $\psi_j : \hat{F}(\hat{X}) \longrightarrow \hat{F}(e^{\frac{2\pi i}{5}})(((x-x_j)^{\frac{1}{5}}))$, $j = 3$ (ordinarily we could only say that the embedding was into the power series fields over $\bar{\mathbb{Q}}$, but the simplicity of this situation allows considerable precision). Also, the inertia groups are given by the restriction of the automorphisms $\bar{\sigma}_j$ that respectively take $(x-x_j)^{\frac{1}{k}}$ to $e^{\frac{2\pi i}{k}}(x-x_j)^{\frac{1}{k}}$, with k the inertia index corresponding to j.

If we assume that F does not contain $\mathbb{Q}(i)$, then there exists an element $\tau \in G(\bar{\mathbb{Q}}/F)$ with the property that $\tau(i) = -i$. Act on the Puiseux expansions about x_1 by acting trivially on $(x-x_1)^{\frac{1}{4}}$ and extend the action by applying τ to the coefficients. With no loss we may assume that the restriction of τ to the

embedding of $F(X)$ is trivial. But an application of $\tau^{-1} \circ \bar{\sigma}_1 \circ \tau \circ \psi_1$ to the conjugate of an element α of $F(X)$ whose initial Puiseux expansion term (around x_1) is $i^t(x-x_1)^{\frac{1}{4}}$ gives an element whose initial expansion is $i^{t-1}(x-x_1)^{\frac{1}{4}}$. Since the effect of this on $F(\hat{X})$ must be conjugate to the effect of $\bar{\sigma}_1 \circ \psi_1$, conclude that σ_1^{-1} is conjugate within the group G to σ_1. This is a contradiction. □

2.4.– Resolution of the subtleties when $r = 3$. One must not assume that the little solvable group of Lemma 2.3 is difficult to achieve as a Galois group of a regular extension of $\mathbb{Q}(x)$. The problem is only that we took the branch points to be in $\mathbb{Q}$. We explain this further.

Let $X \longrightarrow \mathbb{P}^1_x$ be the cover of Lemma 2.3. Consider an element $\lambda \in (\bar{\mathbb{Q}}/\mathbb{Q})$ whose restriction to $\mathbb{Q}(i)$ is the generator of $G(\mathbb{Q}(i)/\mathbb{Q})$. Denote the effect of applying λ to the coefficients of the equations for (X,ϕ) by a subscript λ. The argument of Lemma 2.3 shows that $\phi^\lambda : X^\lambda \longrightarrow \mathbb{P}^1_x$ isn't equivalent to $X \longrightarrow \mathbb{P}^1_x$. But it also shows that the former cover is the only one in the Nielsen class that has the branch point 0 (resp., 1) associated to the conjugacy class C_2 (resp., C_1). Thus for some $\phi : X \longrightarrow X'$ we have a commutative diagram

$$\begin{array}{ccc} X & \longrightarrow & X^\lambda \\ \downarrow \phi & & \downarrow \phi^\lambda \\ \mathbb{P}^1_x & \longrightarrow & \mathbb{P}^1_x \end{array}$$

where ψ^0 is the linear fractional transformation that takes 1 to 0, 0 to 1, and leaves ∞ fixed.

Suppose that we take x_1 and x_2 to be i and $-i$ (or more generally conjugates in the field extension $\mathbb{Q}(i)$). Then we see that $\phi^\lambda : X^\lambda \longrightarrow \mathbb{P}^1_x$ is equivalent to $X \longrightarrow \mathbb{P}^1_x$. It is easy now, with the *Weil cocycle condition* (see [Fr,1; p. 34–35], [Sh; Part 1] or [We]), to conclude that both covers are equivalent to a cover defined over $\mathbb{Q}$. Indeed, at the level of function fields there is a canonical exact sequence of Galois groups :

$$(2.4) \qquad 1 \longrightarrow G(\mathbb{C}(\hat{X})/\mathbb{C}(x))) \longrightarrow G(\widehat{\mathbb{Q}(X)}/\mathbb{Q}(x)) \longrightarrow G(\hat{\mathbb{Q}}/\mathbb{Q}) \longrightarrow 1,$$

where $\widehat{\mathbb{Q}(X)}$ is the Galois closure of the extension $\mathbb{Q}(X)/\mathbb{Q}$ and $\hat{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in $\widehat{\mathbb{Q}(X)}$. The first group – which is G – is identified with the same group obtained by replacing $\mathbb{C}$ by $\hat{\mathbb{Q}}$ and the map from the middle to the end is restriction of elements to the subfield $\hat{\mathbb{Q}}$. Thus, the middle group is a subgroup of the normalizer of G in S_n. Since this normalizer is just G itself in this example, conclude that $\hat{\mathbb{Q}} = \mathbb{Q}$ and the group G has been realized as a Galois group over $\mathbb{Q}$. This less than astounding example is here to aid with the example of § 5.3.

3.– Families for $r = 4$ and the Hurwitz monodromy group H_4

3.1.– The Hurwitz monodromy group H_r. Generators $Q_1,\ldots,Q_{r-1}$ of H_r satisfy the following relations :

(3.1 a) $Q_iQ_{i+1}Q_i = Q_{i+1}Q_iQ_{i+1}$, $i = 1,\ldots,r-2$;

b) $Q_iQ_j = Q_jQ_i$, $1 \le i < j-1 \le r-1$; and

c) $Q_1Q_2\cdots Q_{r-1}Q_{r-1}\cdots Q_1 = 1$.

Relations (3.1 a) and b) alone give the Artin braid group $B(r)$. It is relation (3.1 c) that indicates involvement with projective algebraic geometry. The Artin braid group is the fundamental group of $\mathbb{A}^r - D_r$ while the Hurwitz monodromy group is the fundamental group of $\mathbb{P}^r - D_r$. Here D_r is the classical discriminant locus in the respective spaces. Embed $\mathbb{A}^r$ in $\mathbb{P}^r$ by regarding $\mathbb{A}^r$ as the space of monic polynomials of degree r and $\mathbb{P}^r$ as the space of all nonzero polynomials of degree at most r up to the equivalence by multiplication by a nonzero constant. This embedding gives the natural surjective homomorphism from the braid group to the monodromy group.

This all fits together in a commutative diagram of fundamental groups induced from a geometric diagram :

(3.2)
$$\begin{array}{ccc} \mathbb{A}^r\setminus\Delta_r & \longrightarrow & (\mathbb{P}^1)^r\setminus\Delta_r \\ \Psi_r\downarrow & & \downarrow\Psi_r \\ \mathbb{A}^r\setminus\Delta_r & \longrightarrow & \mathbb{P}^r\setminus D_r \end{array}$$

where the map Ψ_r can be regarded as the quotient action of S_r acting as permutations on the coordinates of $(\mathbb{P}^1)^r$. The respective fundamental groups in the upper row of (3.2) will be called here the *straight* Artin braid and Hurwitz monodromy groups :

(3.3) $SH_r = \pi_1((\mathbb{P}^1)^r \backslash \Delta_r, x^0)$ is the kernel of the homomorphism $\Psi_r^* : H_r \longrightarrow S_r$ that maps Q_i to $(i\ i{+}1)$, $i = 1,...,r$.

3.2.– **Hurwitz action gives a moduli space.** From the relations we compute that H_r acts on the absolute Nielsen classes by extension of the following formula :

$$(3.4) \qquad (\tau_1,...,\tau_r)Q_i = (\tau_1,...,\tau_{i-1},\tau_i\tau_{i+1}\tau_i^{-1},\tau_i,\tau_{i+2},...,\tau_r).$$

In the notation of Definition 1.1 we say that $\phi_T : X_T \longrightarrow \mathbb{P}^1_x$ is in the absolute Nielsen class $Ni(\mathrm{C})_T^{ab}$.

Any permutation representation of a fundamental group defines a cover of the space. In this case we denote the cover corresponding to the Nielsen class by

$$\Psi(\mathrm{C}) : \mathscr{H}(\mathrm{C})_T \longrightarrow \mathbb{P}^r \backslash D_r .$$

That is, an absolute Nielsen class $Ni(\mathrm{C})_T^{ab}$ defines a moduli space $\mathscr{H}(\mathrm{C})_T$ of covers $\phi_T : X_T \longrightarrow \mathbb{P}^1_x$ of degree equal to $\deg(T)$ in that Nielsen class. In this situation this means that each point $m \in \mathscr{H}(\mathrm{C})_T$ corresponds to exactly one equivalence class of covers of $Ni(\mathrm{C})_T^{ab}$ [Fr,1; § 4]. A representative cover $\phi_m : X_m \longrightarrow \mathbb{P}^1_x$ has coordinates $x \in (\mathbb{P}^1)^r$ as an ordering of its branch points where $\Psi_r(x) = \Psi(\mathrm{C})(m)$.

PROPOSITION 3.1. ***The algebraic set*** $\mathscr{H}(\mathrm{C})_T$ ***is irreducible if and only if it is connected and this holds if and only if*** H_r ***is transitive on*** $Ni(\mathrm{C})_T^{ab}$.

Proof : Since $\Psi(C)$ is unramified and $\mathbb{P}^r \backslash D_r$ is nonsingular, so is $\mathscr{H}(C)_T$. Thus it is irreducible as an algebraic set (i.e., an open subset of some projective variety which is defined by a prime ideal in the ring of polynomials in the ambient projective space) if and only if it is connected. From the theory of fundamental groups this last property is equivalent to the transitivity of the permutation representation. □

3.3.– H_4 as a $PSL_2(\mathbb{Z})$ extension. For applications we really want to know many explicit things about $\mathscr{H}(C)_T$, and about the function fields of its irreducible components. Unfortunately, not only is H_r a seemingly complicated group, but it isn't clear how knowing about H_r tells that much about $\mathscr{H}(C)_T$. Indeed, that is a complicated story that has much left in the telling. One can imagine, however, that if it were possible to compare $\mathscr{H}(C)_T$ with a classical heavily studied variety, then the very act of comparison would shed new light on both $\mathscr{H}(C)_T$ and the classical variety with which it is compared. This subsection and § 4 do just that, using a comparison with modular curves, when $r = 4$. As a preliminary we explain the *easy* case $r = 3$: a discussion that is totally compatible with our construction of the 3 branch point families related to diagram (2.1).

For simplicity in this beginning discussion assume that $\mathscr{H}(C)_T$ is connected. Also, here we take the field of definition to be $\mathbb{C}$. Denote the field of meromorphic functions on $\mathscr{H}(C)_T$ by $F_C = \mathbb{C}(\mathscr{H}(C)_T)$ and denote the subfield of $\mathbb{C}(x_1,...,x_r) = \mathbb{C}(\boldsymbol{x})$ invariant under the natural action of S_r by $\mathbb{C}(\boldsymbol{x})^{S_r} \stackrel{\text{def}}{=} \mathbb{C}(\boldsymbol{x}^*)$. That is, $\boldsymbol{x}^*$ is the r–tuple of symmetric functions in $\boldsymbol{x}$. We may regard $F_{\mathbb{C}}$ as a field of definition of a generic cover $\phi : X \longrightarrow \mathbb{P}^1_x$ of the family. In particular, F_C includes the coefficients of the curve X and of the graph of the covering map ϕ.

Also, $F_C/\mathbb{C}(\boldsymbol{x}^*)$ is naturally a field extension of degree equal to $|\, Ni(C)_T^{ab}|$. When $r = 3$, in considerations over $\mathbb{C}$, F_C is actually contained in $\mathbb{C}(\boldsymbol{x})$. This doesn't make arithmetic questions about 3 branch point covers trivial – not at all. But it makes them immensely easier than similar questions

when $r \geq 4$. Of course this all gets down to the sharp transitivity of $PSL_2(\mathbb{C})$ on distinct ordered triples from $\mathbb{P}^1_x$.

DEFINITION 3.2. *The dicyclic group of order* $4n$ *is characterized by having generators* τ_1, τ_2 *with* $\mathrm{ord}(\tau_1) = 2n$, $\mathrm{ord}(\tau_2) = 4$, $\tau_2^{-1}\tau_1\tau_2 = \tau_1^{-1}$ *and* $\tau_2^2 \in <\tau_1>$.

Here are the facts about H_3 in terms of the generators Q_1 and Q_2: $Q_1Q_2 = \tau_1$ and $Q_1Q_2Q_1 = \tau_2$ are generators of H_3. From relation (3.1 a), $\tau_2^2 = \tau_1^3$. Thus :

(3.5 a) $\mathrm{ord}(\tau_1) = 6$ and $\mathrm{ord}(\tau_2) = 4$; and

b) H_3 is the dicyclic group of order 12.

In the case $r = 4$ we rarely expect to have $F_C \subset \mathbb{C}(x)$. It appears, however, to be far from hopeless to make things explicit in this case.

Let $\mathcal{Q} = <(Q_1Q_2Q_3)^2, Q_1Q_3^{-1}>$.

THEOREM 3.3. *In the case that* $r = 4$ *the following hold :*

(3.6 a) H_4 *contains precisely one involution;*

b) $\mathcal{Q} \triangleleft H_4$ *and* $\mathcal{Q}$ *is the quaternion group of order* 8;

c) $H_4/\mathcal{Q} \cong PSL_2(\mathbb{I})$; *and*

d) H_4 *has precisely two conjugacy classes of subgroups isomorphic to* $\mathrm{SL}_2(\mathbb{I})$.

This is due to John Thompson who has continued to investigate interpretations of the quaternion group kernel of H_4 [FrT].

4.– Modular curves and H_4

4.1.– Geometric interpretation of H_4 using $r = 3$. Suppose that $r = 4$ and that H' is a subgroup of H_4 of finite index. This gives an unramified cover

$$\Psi_{H'} : \mathscr{H}_{H'} \to \mathbb{P}^4 \backslash D_4$$

associated to H' as in § 3.2. Consider the pullback $\mathscr{H}'$ of the fiber product $\mathscr{H} \times_{\mathscr{U}_3} \mathscr{U}^3$ that occurred at the outset of § 2.2. We perform the analogous operation here to consider a connected component $\mathscr{H}'$ of the pullback of $\mathscr{H}_{H'}$ to $(\mathbb{P}^1)^4 \backslash \Delta_4$. If we identify the four copies of $\mathbb{P}^1$, respectively, with $\mathbb{P}^1_x$ (i.e., $x = x_1$) and $\mathbb{P}^1_{x_i}$, $i = 2,3,4$, then the fiber $\mathscr{H}'_{x_2,x_3,x_4}$ of points of $\mathscr{H}'$ lying over points of the form (x,x_2,x_3,x_4) is a Zariski open subset of a projective algebraic curve that is a 3 branch point cover of $\mathbb{P}^1_x$ (ramified over x_2, x_3, x_4). Proposition 2.2 says that for each value of (x_2, x_3, x_4) this curve is analytically isomorphic to a fixed curve $C(H')$ (i.e., independent of (x_2, x_3, x_4)). Furthermore, from the construction, the natural projection of $C(H')$ to $\mathbb{P}^1_x$ is of degree equal to the index of $H' \cap SH_4$ in SH_4. Finally, if this cover has no automorphism of order 2, then these identifications force $\mathscr{H}_{H'}$ to be a Zariski open subset of $C(H') \times \mathbb{P}^1_{x_2} \times \mathbb{P}^1_{x_3} \times \mathbb{P}^1_{x_4}$.

In the case when H' is the stabilizing subgroup of an absolute class through the permutation representation given by (3.4) there is an explicit description of the branch cycles of the cover $C(H') \to \mathbb{P}^1_x$ in terms of the Q's and their action on $SNi(\mathbf{C})^{ab}_T$ [BFr; Lemma 1.6]. It is traditional (as in [BFr]) to use (a_{12}, a_{13}, a_{13}) instead of $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ for these branch cycles (as well as for the elements of H_4 that induce them) :

$$a_{12} = Q_1^{-2},\ a_{13} = Q_1 Q_2^{-2} Q_1^{-1},\ a_{14} = Q_1 Q_2 Q_3^{-2} Q_2^{-1} Q_1^{-1}. \tag{4.1}$$

As with the σ notation, denote the permutation group (acting on $SNi(\mathbf{C})_T^{a\,b}$) generated by the a's of (4.1) by $G(\boldsymbol{a})$, and the subgroup that stabilizes a specific element of $SNi(\mathbf{C})_T^{a\,b}$ by $G(\boldsymbol{a},1)$. Recall also, that there is an effective procedure to decide if $(|\operatorname{Aut}(C(H')/\mathbb{P}^1_x)|,2)=1$ since $\operatorname{Aut}(C(H')/\mathbb{P}^1_x)$ may be identified with the quotient group $N_{G(\boldsymbol{a})}(G(\boldsymbol{a},1))/G(\boldsymbol{a},1)$ of the normalizer of $G(\boldsymbol{a},1)$ in $G(\boldsymbol{a})$. Furthermore (in the case that H' does come from a permutation representation given by (3.4)), we may count the number of connected components of the fiber product

$$\mathscr{H}_{H'} \times_{\mathbb{P}^4\backslash D4}((\mathbb{P}^1)^4\backslash\Delta_4)$$

as the number of orbits of SH_4 on $SNi(\mathbf{C})_T^{a\,b}$.

The next discussion starts to turn this around by trying to realize certain subgroups H' of H_4 as the stabilizing subgroup of some absolute Nielsen class through the permutation representation given by (3.4). The examples of § 5 will be helpful to the reader, but we start by seeing that examples of such H' are related to modular curves.

4.2.– Elliptic curves and the $PSL_2(\mathbb{Z})$ quotient of H_4. The presentation of H_4 given in Theorem 3.3 shows an intimate relation between the appearance of the $PSL_2(\mathbb{Z})$ quotient and the theory of modular curves. It comes form the following diagram.

Suppose that E' and E are elliptic curves in Weierstrass normal form. Consider an integer $n\geq 1$. Fix a group A_0 that is isomorphic to a subgroup of $\mathbb{Z}/n\oplus\mathbb{Z}/n$. This latter group is isomorphic to the group of points of E of order dividing n. Now suppose that $\phi : E' \longrightarrow E$ is an isogeny whose kernel is isomorphic to A_0. On each of E' and E we may equivalence points $\boldsymbol{p}$ and $-\boldsymbol{p}$ to form the quotients $E'/<\pm 1>$ and $E/<\pm 1>$. These may be respectively identified with $\mathbb{P}^1_{x'}$ and $\mathbb{P}^1_x$ where x' and x represent the corresponding *x–coordinates* of the Weierstrass normal form. This gives a commutative diagram of algebraic curves :

$$\begin{array}{ccc} E' & \xrightarrow{\phi} & E \\ {\scriptstyle p\tau(E')}\downarrow & & \downarrow{\scriptstyle p\tau(E)} \\ \mathbb{P}^1_{x'} & \xrightarrow[\psi(f)]{} & \mathbb{P}^1_{x} \end{array} \tag{4.2}$$

where $\psi(f)$ denotes the rational function that takes x' to x.

Let $G_{A_0} = G$ be the semidirect product $A_0 \times^S <-1>$ with $<-1>$ the group generated by multiplication by -1 on E' restricted to A_0. Also denote the conjugacy class of $(v;-1) \in A_0 \times^S <-1>$ in this group by C_v. Then the Nielsen class of the cover in the bottom row is given by the argument of [Fr,2; p. 155] :

$$\{\tau \in G^4 |\ G(\tau) = G \text{ and } \tau_i \in C_{v_i},\ v_i \in A_0,\ i = 1,2,3,4 \text{ and } v_4 = v_1 - v_2 + v_3\}.$$

Note that if A_0 is cyclic and n is odd, then all of the C_v's are conjugate to $(0;-1)$. Also, if we denote $\mathbb{Z} \oplus \mathbb{Z}$ by $\mathbb{Z}^2$, then G is a quotient of $G_{\mathbb{Z}^2} = \mathbb{Z}^2 \times^S <-1>$. This latter group in turn may be identified with the quotient of the free group F_4 on 4 generators $\bar{\sigma}_i$, $i = 1,2,3,4$, by the normal subgroup N generated by $\bar{\sigma}_1 \ldots \bar{\sigma}_4$ and $\bar{\sigma}_i^2$, $i = 1,2,3,4$. Indeed, consider :

(4.3) $\theta : F_4/N \to G_{\mathbb{Z}^2}$ by $\bar{\sigma}_i$, $i = 1,2,3,4$, go in order to

$$((1,1);-1),((0,1);-1),((1,0);-1),((2,0);-1).$$

Thus the images of $\bar{\sigma}_1\bar{\sigma}_2$ and $\bar{\sigma}_1\bar{\sigma}_3$ can be identified with the generators $(1,0)$ and $(0,1)$ of $\mathbb{Z}^2$ which is the normal subgroup of $G_{\mathbb{Z}^2}$ of index 2.

Replace the τ's by $\bar{\sigma}$'s in (3.4) to get an action of the braid group $B(4)$ (as below (3.3)) on F_4/N; and thereby on $G_{\mathbb{Z}^2}$. The action of $Q_1Q_2Q_3^2Q_2Q_1$ is given by conjugation by $\bar{\sigma}_1$, which induces multiplication by -1 on $\mathbb{Z}^2$.

CONCLUSION 4.1. ***The natural map above of*** $B(4)$ ***into*** $\mathrm{Aut}(\mathbb{Z}^2)$ ***gives a natural homomorphism of*** H_4 ***into*** $\mathrm{SL}_2(\mathbb{Z})/<\pm 1> \stackrel{\mathrm{def}}{=} PSL_2(\mathbb{Z})$ ***(below we show it is onto).***

Relation with $C_0(n)$: We will see that the map of Conclusion 4.1 is onto. Consider the special case with A_0 cyclic of order n. Geometrically this ties the somewhat mysterious space $\mathscr{H}(\mathbf{C})_T$ to the well known modular curve $C_0(n)$. Recall that the latter is a projective nonsingular model for the upper half plane $\mathscr{U}$ modulo the action of the $SL_2(\mathbb{Z})$ subgroup consisting of the matrices

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \bmod n \right\}.$$

Indeed, the covers $X \longrightarrow \mathbb{P}^1_x$ in the Nielsen class $Ni(\mathbf{C})_T^{ab}$ can be completed to a diagram that looks like (4.2) with X replacing $\mathbb{P}^1_{x'}$, $\hat{\psi}$ replacing ϕ, $\hat{X}$ replacing E', etc., in that the genus of the pairs of corresponding curves are the same :

$$\begin{array}{ccc} \hat{X} & \longrightarrow & \hat{X}/A_0 \\ {\scriptstyle pr(\hat{X},X)}\downarrow & & \downarrow{\scriptstyle pr(\hat{X}/A_0,\mathbb{P}^1_x)} \\ X & \longrightarrow & \mathbb{P}^1_x \end{array} \tag{4.4}$$

Here $\hat{X}$ is the Galois closure of the cover appearing in the bottom row, and $\hat{X}/A_0$ is the quotient of $\hat{X}$ by the cyclic normal subgroup of order n of the dihedral group D_{2n} that along with -1 generates this group. The unramified cover in the upper row of (4.4), and thus it corresponds to a unique point of $C_0(n)$. This gives us the sought for commutative diagram :

$$\begin{array}{ccc} \mathscr{H}(\mathbf{C})_T & \xrightarrow{\Lambda_0(n)} & C_0(n) \\ {\scriptstyle \Psi(\mathbf{C})}\downarrow & & \downarrow{\scriptstyle \psi(n)} \\ \mathbb{P}^4 - D_4 & \xrightarrow{\Lambda_0(1)} & C_0(1) \end{array} \tag{4.5}$$

where the upper row maps $m \in \mathscr{H}(\mathbf{C})_T$ to the point of $C_0(n)$ that corresponds to diagram (4.4) with $\phi_m : X_m \longrightarrow \mathbb{P}^1$ in the bottom row. The notation is that prior to Proposition 3.1.

Some classical clarifications : it is natural to identify $C_0(1)$ with the j–line $\mathbb{P}^1_j$; the map $\Lambda_0(1)$ takes an unordered collection of four distinct points $\{x_1, x_2, x_3, x_4\}$ in $\mathbb{P}^1_x$ to the isomorphism class of the elliptic curve represented by the Weierstrass equation

$$y^2 = (x-x_1)(x-x_2)(x-x_3)(x-x_4)$$

with the convention that if one of the x_i's is ∞, then we remove the factor $(x-x_i)$; and $\Psi(\mathbf{C})$ is the natural map that takes the equivalence class of a cover $X \longrightarrow \mathbb{P}^1_x$ to the unordered collection of its branch points.

The 3 **branch point cover from Proposition 2.2** : The Legendre form of an elliptic curve has the algebraic curve $y^2 = x(x-1)(x-\lambda)$ corresponding to a value of the parameter λ. This gives a natural map from the λ–line, $\mathbb{P}^1_\lambda \longrightarrow \mathbb{P}^1_j$. Denote the fiber product $C_0(n) \times_{\mathbb{P}^1_j} \mathbb{P}^1_\lambda$ (i.e., pullback over $\mathbb{P}^1_\lambda$) by $C_0(n)_\lambda$. Similarly, as in (3.2) consider the natural map Ψ_4 from the ordered distinct points $(\mathbb{P}^1)^4 \backslash \Delta_4$ of $\mathbb{P}^1_x$ to the unordered set of such points $\mathbb{P}^4 \backslash D_4$.

From Proposition 2.2, for any possible choice of $\mathbf{C}$, each connected component of the pullback of $\mathscr{H}(\mathbf{C})_T$ has attached to it a nonsingular algebraic curve $C(\mathbf{C})$ presented as a cover of $\mathbb{P}^1_x$ ramified over just the three points 0,1 and ∞. Indeed, the computation in the middle of [Fr,2; p. 156] shows that, at least when n is odd, that not just H_4, but even $G(\boldsymbol{a})$ (as in 4.1)) is transitive on this absolute Nielsen class. This curve is actually isomorphic to $C_0(n) \times_{\mathbb{P}^1_j} \mathbb{P}^1_\lambda$. In the next subsection we display a natural process by which one recovers $C_0(n)$ from $C(\mathbf{C})$. This is applied in the main examples of § 5.

4.3.– Automorphisms from branch point twists : Assume here that $r = 4$ and that $Ni(\mathbf{C})^{ab}_T$. From [BFr] (in the case $r = 4$ only) this is equivalent to the transitivity of the group $G(\boldsymbol{a})$ generated by the $\boldsymbol{a}$'s of (4.1), so that $\mathscr{H}(\mathbf{C})$ has

but one irreducible component (Proposition 3.1). Consider the curve cover $\beta : C(\mathbf{C}) \to \mathbb{P}^1_x$, ramified over x_2, x_3, x_4 given by Proposition 2.2. For this discussion alone, identify the permutations of the points x_2, x_3, x_4 with S_3 regarded as a subgroup of $PSL_2(\mathbb{C})$. That is, for $\pi \in S_3$, the automorphism ϕ_π associated to π is that which permutes x_2, x_3, x_4 according to π.

Consider the subset of those $\pi \in S_3$ for which the covers $\beta : C(\mathbf{C}) \to \mathbb{P}^1_x$ and $\phi_\pi \circ \beta : C(\mathbf{C}) \to \mathbb{P}^1_x$ are equivalent : there exists an analytic isomorphism $\mu_\pi : C(\mathbf{C}) \to C(\mathbf{C})$ such that $\beta \circ \mu_\pi = \phi_\pi \circ \beta$. This is clearly a subgroup of S_3, and we denote it by $T(\mathbf{C})$ (for *twisting* of $\mathbf{C}$). The μ_π's act on $C(\mathbf{C})$, and the ϕ_π's act on $\mathbb{P}^1_x$. Despite our concern that the notation could easily be misunderstood out of context, we denote the respective quotients by $C(\mathbf{C})/T(\mathbf{C})$ and $\mathbb{P}^1_x/T(\mathbf{C})$.

CONCLUSION 4.2 : ***The cover*** $\beta : C(\mathbf{C}) \to \mathbb{P}^1_x$ ***has a description of branch cycles given by the*** a***'s of*** (4.1) [BFr; Lemma 1.6]. ***For the special case where*** $Ni(\mathbf{C})^{a\,b}_{T}$ ***is the Nielsen class of covers in the bottom row of diagram*** (4.4), $T(\mathbf{C}) = S_3$ ***and the map*** $\lambda_0(n)$ ***of*** (4.5) ***extended to the respective pullbacks identifies*** $C(\mathbf{C})/T(\mathbf{C})$ ***with*** $C_0(n)$, $\mathbb{P}^1_x$ ***with*** $\mathbb{P}^1_\lambda$ ***and*** $\mathbb{P}^1_x/T(\mathbf{C})$ ***with*** $\mathbb{P}^1_j$. ***For the case of general*** $\mathbf{C}$, ***both*** $C(\mathbf{C})$ ***and*** $C(\mathbf{C})/T(\mathbf{C})$ ***(respectively covering*** $\mathbb{P}^1_\lambda$ ***and*** $\mathbb{P}^1_j$***) are identified with the projective normalization of the upper half plane modulo a subgroup (of finite index) of*** $PSL_2(\mathbb{Z})$. ***But only in rare circumstances would we expect this to be a congruence subgroup.***

In § 5.3 we give another example of a situation where $T(\mathbf{C})$ is not trivial so that the reader can see that the twisting automorphisms have serious application.

4.4.— Nielsen classes with markings and $C(n)$. More explicit identification of the curve $C(\mathbf{C})$ in conclusion 4.2 would be a marvelous thing, but it seems difficult. In some sense [DDH] describes all of the three branch point covers of $\mathbb{P}^1_x$ that

arise as $C(\mathrm{C})$ for some Nielsen class $Ni(\mathrm{C})_T^{a\,b}$; all that are possible by Belyi's Theorem [Be], those defined over $\bar{\mathbb{Q}}$. But their result is not so explicit as the example above in its relation to the structure of the Hurwitz monodromy group, precisely because Belyi's result is not very explicit.

There is another point, too, related to [DDH]. While that paper does imply that there exists a C that gives the modular curve $C(n)$ this way, the natural extension of the above construction does not do so. Recall that $C(n)$ is the projective nonsingular model for the upper half plane $\mathcal{U}$ modulo the action of the $SL_2(\mathbb{Z})$ subgroup consisting of the matrices

$$\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \mathbb{I} \mod n \right\}.$$

The natural way to get $C(n)$ is to consider Nielsen classes with markings – pointed Nielsen classes – the technical topic that was applied in [DFr] (after its introduction in [BFr]). Essentially the markings on a Nielsen class trace what happens to a disjoint cycle of an element representing a conjugacy class of C_i under the action of H. This therefore gives a permutation representation of H_r that extends that of the action on $Ni(\mathrm{C})_T^{a\,b}$. From this example, these markings of Nielsen classes are a generalization of the level n structures that play a traditional role in the theory of modular curves and of moduli spaces of higher dimensional abelian varieties. From the quite different construction of [DDH; Theorem p. 4] :

THEOREM 4.3. *Let H be the subgroup of $SL_2(\mathbb{Z})$ that corresponds to $\mathbb{P}^1_\lambda$. The 3 branch point curve covering $C(\mathrm{C}) \to \mathbb{P}^1_x$ as C runs over pointed Nielsen classes are in one-one correspondence with the (congruence and noncongruence) curve covering of the λ-line $\mathbb{P}^1_\lambda$ that arise from subgroups of H of finite index.*

The twisting process of Conclusion 4.2 should give us a similar statement comparing the covers $C(\mathrm{C})/T(\mathrm{C}) \to \mathbb{P}^1_x/T(\mathrm{C})$ with the covers, both congruence and noncongruence, of $\mathbb{P}^1_j$ in the cases where $T(\mathrm{C}) = S_3$. But the Nielsen classes that appear in [DDH] aren't really set up to make this comparison.

5.– Generalizations of rigidity and examples

5.1.– Generalization of rigidity and (0.1) : The topic is how to check if there are covers in a given Nielsen class that are actually defined over $\mathbb{Q}$. Although the results that we state here are essentially in [Fr,1], it is the attention drawn to the special case of $r = 3$ by [T] that brought their significance to the mathematical public. There is a technically valuable game that compares the Galois and nonGalois situations. Even if one is ultimately interested in Galois extensions, many times it is better to start with a nonGalois cover and go to the Galois closure. The strong *rigidity* conditions may be harder to satisfy in the nonGalois situation than in the corresponding Galois situation. But if they do hold, that implies the vanishing of an obstruction for the field of definition that isn't easily checked from the Galois situation.

Galois action on branch points : Let $K \subset \mathbb{C}$ be a field of definition of the cover $\phi : X \to \mathbb{P}^1_x$. The cover is said to be g–regular over K if the Galois closure $\widehat{K(X)}$ of the function field extension $K(X)/K(x)$ is a regular extension of $K(\mathbb{P}^1_x) = K(x)$ (i.e., if $K(X) \cap \bar{K} = K$). Informally we say that there is no extension of constants. More generally, however, we must deal with the group $\hat{G} = G(\widehat{K(X)}/K(x))$. This is also a subgroup of S_n. It contains G identified as $G(\widehat{K(X)}/\hat{K}(x))$, with $\hat{K}$ the algebraic closure of K in $\widehat{K(X)}$ (as in § 2.4). We also need a group theoretic definition extending the definition of rational conjugacy class of a group.

DEFINITION. *Let G be a group and let C_i be the conjugacy class of σ_i, $i = 1,...,r$. Denote the order of σ_i by e_i, $i = 1,...,r$. Denote the least common multiple of the e_i's by N. The set $\{C_1,...,C_r\}$ is said to be a rational set of conjugacy classes of G if*

(5.1) *the set $\bigcup_{i=1}^{r} C_i$ contains all powers σ_i^k, $i = 1,...,r$ and k relatively prime to N.*

Note that unions of rational sets of conjugacy classes are also rational. An alternative statement to (5.1) is the following :

(5.2) for $k \in (\mathbb{Z}/N)^*$, there exists $\beta \in S_r$ such that $\sigma_i^k \in \mathbf{C}_{(i)\beta}$, $i = 1,...,r$.

Consider the orbits of the action of $G(\bar{K}/K)$ on the branch points $x_1,...,x_r$ of the cover. We denote the orbit of x_i by $O(i)$, where the notation implies that we use the integer subscripts in place of the points themselves. Below we need to consider the union $\bigcup_{j \in O(i)} \mathbf{C}_j$ of the conjugacy classes attached to this orbit of the branch points. Denote by $O(\mathbf{C}_i)$ this orbit of $\mathbf{C}_i$ under $G(\bar{K}/K)$.

In many applications it is natural to make a basic assumption about the conjugacy classes $\mathbf{C}$ in the transitive subgroup G of S_n defined by a description σ of the branch cycles of a cover. With N as above for each $k \in (\mathbb{Z}/N)^*$ we define a unique conjugacy class $\mathbf{C}_i^k$ of G by putting each element of $\mathbf{C}_i$ to the power k. Put each coordinate of $\mathbf{C}$ to the power k to consider a new r–tuple $\mathbf{C}^k$ of conjugacy classes of G. Also, let $\sigma \in S_r$ act on $\mathbf{C}$ by permuting the coordinates. Denote the result by ${}^{\sigma}\mathbf{C}$. Also, $\mathbf{C} \bmod N_{S_n}(G)$ denotes the ordered collections of r–tuples of conjugacy classes $\gamma \mathbf{C} \gamma^{-1}$, $\gamma \in N_{S_n}(\mathbf{C})$. Two special conditions are used below in Proposition 5.4 (the a) part implies b)) :

(5.3 a) for each $k \in (\mathbb{Z}/N)^*$, $\mathbf{C}^k \equiv \mathbf{C} \bmod N_{S_n}(G)$; and

b) for each $k \in (\mathbb{Z}/N)^*$, there exists $\sigma \in S_r$ such that $\mathbf{C}^k \equiv {}^{\sigma}\mathbf{C} \bmod N_{S_n}(G)$.

Suppose that the cover $X \to \mathbb{P}^1$ is in the Nielsen class $Ni(\mathbf{C})_T^{ab}$ (§ 1.2). Retain the association of x_i with the conjugacy class $\mathbf{C}_i$, $i = 1,...,r$. Regard $G(K(\zeta_N)/K)$ as a subgroup of the units of the ring $\mathbb{Z}/N$. Here ζ_N is a primitive Nth root of 1. If (5.3 b) holds regard $G(K(\zeta_N)/K)$ (acting through integers) as permutations on the coordinates of $\mathbf{C}$ modulo $N_{S_n}(G)$. If a number field K is

a field of definition of the cover, as earlier, denote the Galois closure of the field extension $K(X)/K(x)$ by $\widehat{K(X)}$. Its Galois group, $\hat{G}$ is a subgroup of $N_{S_n}(G)$.

DEFINITION 5.1. *For each* $\tau \in G(\bar{\mathbb{Q}}/K)$ *denote the image of* τ *in* $G(K(\zeta_N)/K)$ *by* $k = k_\tau$. *The branch points* x *and conjugacy classes* C *are said to be Galois compatible (over* K*) if for each* $\tau \in G(\bar{\mathbb{Q}}/K)$, *if* τ *permutes the* x_i*'s as* $\bar{\tau} \in S_r$, *then*

(5.4) $\quad C_i^k = \gamma C_{(i)\bar{\tau}} \gamma^{-1}$ *for some* $\gamma \in \hat{G}$ *(independant of* i*),* $i = 1,...,r$.

The next result is a special case of the branch cycle argument [Fr,1; p. 61].

PROPOSITION 5.2. *Suppose that the cover* $X \longrightarrow \mathbb{P}^1$ *is in* $Ni(C)_T^{ab}$. *If the cover is defined over* $\mathbb{Q}$, *then* x *and* C *are Galois compatible over* $\mathbb{Q}$. *In particular,* (5.3) b) *holds. If the cover is g-regular over* $\mathbb{Q}$, *then* $O(C_i)$ *is rational,* $i = 1,...,r$.

$\mathbb{Q}$–points on Hurwitz spaces : The point of the Hurwitz monodromy action is this (see [Fr,1], [Fr,3], [DFr] for details). Suppose that $SH(r)$ acts transitively on the straight Nielsen classes (§ 3.2), that $\mathrm{Cen}_{S_n}(G)$ is trivial, and that each of the conjugacy classes of C is rational. Then the Hurwitz space cover $\Psi(C) : \mathscr{H}(C)_T \longrightarrow \mathscr{U}_r$ prior to Proposition 3.1 (including the total space of representing covers for the points of $\mathscr{H}(C)_T$) is defined over $\mathbb{Q}$. For $r > 3$ we improve upon condition (0.1) with the following statement (note that a) and b) are the same as in (0.1) :

(5.5
a) $G = N_{S_n}(G)$;
b) each of the classes $C_1,...,C_r$ is rational;
c) SH_r is transitive on the absolute straight Nielsen classe $SNi(C)_T^{ab}$ defined by C (expression (3.4)); and
d) there exists a $\mathbb{Q}$–point on the Hurwitz space $\mathscr{H}(C)_T$.

Our next result is an analogue of *rigidity* as it is based directly on conditions (5.5). It is an immediate corollary of the following Proposition 5.4 whose hypotheses are much weaker because it uses just condition 5.3 b).

PROPOSITION 5.3. *Assume that* $Ni(\mathrm{C})_T^{ab}$ *is a Nielsen class for which one of the following holds. Either* G *is in its regular representation and* G *has no center; or*

(5.6) *the centralizer,* $\mathrm{Cen}_{S_n}(G)$ *of* G *of* S_n *is trivial.*

If the conditions (5.5) *hold, then* G *is the Galois group of a regular extension of* $\mathbb{Q}(x)$.

To state the next general proposition precisely we need to consider another variety which fits in a sequence of covers

$$\mathscr{H}(\mathrm{C})_T \longrightarrow \mathscr{H}_q \longrightarrow \mathscr{U}_r \tag{5.7}$$

where the map $\mathscr{H}(\mathrm{C})_T \longrightarrow \mathscr{H}_q$ is Galois (e.g., it is of degree 1 under the hypotheses of Proposition 5.3). We explain the construction of $\mathscr{H}_q$ in the comments after the statement of the result. The field K_M is the fixed field in $\mathbb{Q}(\zeta_N)$ of the integers k for which the expression (5.3 a) holds

$$\mathrm{C}^k \equiv \mathrm{C} \bmod N_{S_n}(G).$$

PROPOSITION 5.4. *Let* $Ni(\mathrm{C})_T^{ab}$ *be a Nielsen class for which* (5.3 b) *and* (5.5 c) *hold. Assume also that either* G *is in its regular representation and* G *has no center or* (5.6) *holds. Then the cover* $\mathscr{H}(\mathrm{C})_T \longrightarrow \mathscr{H}_q$ *is defined over* K_M, *and the cover* $\mathscr{H}_q \longrightarrow \mathscr{U}_r$ *is defined over* $\mathbb{Q}$. *Suppose that the cover* $\phi : X \longrightarrow \mathbb{P}^1_x$ *corresponds to the point* $m \in \mathscr{H}(\mathrm{C})_T$ *(as in Proposition 3.1) and let* x (resp., m_q) *be the image of* m *in* $\mathbb{P}^r$ (resp., $\mathscr{H}_q$). *Then the cover is defined over* $\mathbb{Q}$ *if and only if*

(5.8 a) m_q *is a* $\mathbb{Q}$*-point; and*

b) x *and* C *are Galois compatible over* $\mathbb{Q}$.

If in addition (5.5 a) *holds then* $G(\widehat{\mathbb{Q}(X)}/\mathbb{Q}(x))$ *is isomorphic to* G, *and* G *has been realized as the Galois group of a regular extension of* $\mathbb{Q}(x)$.

Comments on the proof : This is a special case of Proposition 1.5 of [Fr,3] (and most of it is from [Fr1, Thm. 5.1]). Without assuming that 5.5 a) holds we may only assert that, for $\bar{G} = \{\gamma \in N_{S_n}(G) |$ there exists $k \in (\mathbb{Z}/N)^*$, $\sigma \in S_r$ with (5.4) holding :

$$G \subset G(\widehat{\mathbb{Q}(X)}/\mathbb{Q}(x)) \subset \bar{G}.$$

This will figure in the examples that follow. In § 5.2 we will also see a method that sometimes allows us to check for condition 5.5 d).

Here is the construction of $\mathscr{H}_q$ starting from the result of Proposition 1.5 of [Fr,3] that says that $\mathscr{H}(\mathbf{C})_T \to \mathscr{U}_r$ is defined over K_M. As in § 2.2 consider a connected component $\mathscr{H}'$ of the fiber product $\mathscr{H} \times_{\mathscr{U}_r} \mathscr{U}^r$. We form $\mathscr{H}_q$ using the same ideas that appear in the discussion of *branch point twists* in § 4.3. From (5.3 b) it is easy to show that to each $\tau \in G(K_M/\mathbb{Q})$ there exists $\bar{\tau} \in S_r$ (acting on $\mathscr{U}^r$ by permutation of coordinates) and $\Psi_{\bar{\tau}} : (\mathscr{H}')^\tau \to \mathscr{H}'$ that makes the following diagram commutative :

$$\begin{array}{ccc} (\mathscr{H}')^\tau & \xrightarrow{\Psi_\tau} & \mathscr{H}' \\ {\scriptstyle (\Psi_{\mathbf{C}})^\tau}\downarrow & & \downarrow{\scriptstyle \Psi_{\mathbf{C}}} \\ \mathscr{U}^r & \xrightarrow{\bar{\Psi}} & \mathscr{U}^r \end{array}.$$

As usual the superscript τ is application of τ to the coefficients of the polynomials describing the varieties. Then $\mathscr{H}_q$ is the variety that results from applying Weil's cocycle condition to this (cf. the proof of Prop. 1.5 of [Fr,3] for details). □

5.2.– Unirational Hurwitz spaces and the group A_5 : As an application of the theory of § 5.1 we start by considering the geometry and arithmetic of degree 5 covers $X \longrightarrow \mathbb{P}^1_x$ (and their Galois closures $\hat{X} \longrightarrow \mathbb{P}^1_x$) whose monodromy group is A_5 and for which the representation T is the standard representation of degree 5.

Hilbert's *trick*: Hilbert [Hi] considered the groups A_n, $n = 5,6, \ldots$ in his famous paper applying the Hilbert irreducibility theorem to realize groups as Galois groups over $\mathbb{Q}$. The *trick* is to realize S_n as a 3 branch point Galois cover $\hat{X} \longrightarrow \mathbb{P}^1_x$ (given by Nielsen class $Ni(\mathbf{C})$) defined over $\mathbb{Q}$, and then to consider the quotient $\hat{X}/A_n = Y$. The Nielsen class for Hilbert was that with $\mathbf{C}$ given by C_1 the class of 2–cycle, C_2 the class of an n–1–cycle and C_3 the class of an n–cycle.

By necessity two of the conjugacy classes in $\mathbf{C}$ (say C_1 and C_2) must be represented by elements of $S_n \backslash A_n$. This implies that the degree two cover $Y \longrightarrow \mathbb{P}^1_x$ is ramified only over the branch points x_1 and x_2 corresponding to these two classes. If in addition the two conjugacy classes are distinct, the respective points y_1 and y_2 on Y over the branch points are easily shown to be $\mathbb{Q}$–rational. A genus 0 curve with a rational point (actually any odd degree rational divisor) is isomorphic to $\mathbb{P}^1_y$ for some element y of the function field. This last observation, fittingly, is due to Hilbert and Hurwitz.

There are other siutations where one may use Hilbert's idea, and difficulties around condition (0.1 a) offer motivation to do so. When it is possible to realize the automorphism group $\mathrm{Aut}(G)$ of a sporadic simple group G as the Galois group of a 3 branch point cover over $\mathbb{Q}$, this may work if $\mathrm{Aut}(G)/G$ is small. Matzat [Ma,1] has used this to realize a number of the sporadic groups as Galois groups. In addition, sometimes this trick can work even when the big group is realized by a Nielsen class consisting of 4 branch point covers. We used this in [Fr,3; Ex. 2.3] to introduce 5 independent transcendental parameters into realizations of A_n as a Galois group over $\mathbb{Q}$. We reviewed Hilbert's idea (as did Shih [Sh]) in [Fr,1; p. 70] in order to point out the difficulties in obtaining the information provided by it in a more direct manner. Although our example is

mainly designed to show the practical use of the twisting automorphisms of Conclusion 4.2, it can also be viewed as continuing the discussion of [Fr,1].

Nielsen classes given by 3–cycles : We consider the absolute Nielsen class of A_5 where $r = 4$, $T: A_5 \longrightarrow S_5$ is the natural injection and $\mathbf{C} = \mathbf{C}_{3^4}$ has $C_1 = C_2 = C_3 = C_4$, each the conjugacy class of a 3–cycle. Let $X \longrightarrow \mathbb{P}^1_x$ be a cover in the Nielsen class $Ni(\mathbf{C}_{3^4})^{ab}_T$. In order to apply the result of § 5.1 we first show that H_4 is transitive on the elements of this Nielsen class.

Clearly $N_T(\mathbf{C}_{3^4}) = S_5$. Thus with no loss we may assume that any representative σ of an element of $Ni(\mathbf{C}_{3^4})^{ab}_T$ has $\sigma_1 = (123)$ and that σ_2 has either 1, 2 or 3 integers in its 3–cycle in common with $\{1,2,3\}$. If the third holds then $\sigma_2 = \sigma_1^{-1}$ and $\sigma_3 = (145)$; if the second holds, then we may assume $\sigma_2 = (214)$; and if the first, $\sigma_2 = (145)$. With this data we have uniquely determined a given Nielsen class.

List 5.5 :

$X_1 : \sigma_2 = (132), \sigma_3 = (145), \sigma_4 = (154)$; $X_2 : \sigma_2 = (145), \sigma_3 = (154), \sigma_4 = (132)$;
$X_3 : \sigma_2 = (145), \sigma_3 = (215), \sigma_4 = (243)$; $X_4 : \sigma_2 = (145), \sigma_3 = (321), \sigma_4 = (354)$;
$X_5 : \sigma_2 = (145), \sigma_3 = (432), \sigma_4 = (415)$; $X_6 : \sigma_2 = (145), \sigma_3 = (543), \sigma_4 = (521)$;
$X_7 : \sigma_2 = (214), \sigma_3 = (245), \sigma_4 = (532)$; $X_8 : \sigma_2 = (214), \sigma_3 = (325), \sigma_4 = (543)$;
$X_9 : \sigma_2 = (214), \sigma_3 = (435), \sigma_4 = (245)$.

Replace X_i by the integer i, $i = 1,...,9$, to give a degree 9 representation of H_4. Here is the effect of the generators Q_i, $i = 1,2,3$, on $Ni(\mathbf{C}_{3^4})^{ab}_T$:

(5.9) $Q_1 = (25364)(798)$, $Q_2 = (14985)(367)$ and $Q_3 = (25364)(798)$.

The action of H_4 is clearly transitive.

The cover $\beta : C(\mathbf{C}_{3^4}) \longrightarrow \mathbb{P}^1_x$: Our next computation shows that the 3 branch point cover associated to $Ni(\mathbf{C}_{3^4})$ is not of genus 0. In particular, the pullback

$\mathscr{H}'$ of $\mathscr{H}(\mathbf{C}_{3^4})$ over $\mathscr{U}^4$ is not a unirational variety. But, because we are repeating the same conjugacy class many times, we see in Theorem 5.6 that $\mathscr{H}(\mathbf{C}_{3^4})$ itself is a $\mathbb{Q}$–unirational variety. In particular it has lots of rational points to satisfy condition (5.5 d).

Apply Conclusion 4.2 to the action of the Q_i's on List 5.5 to get

$$a_{12} = Q_1^{-2} = (26543)(798)$$
$$a_{13} = Q_1 Q_2^{-2} Q_1^{-1} = (19627)(385)$$
$$a_{14} = (a_{12}a_{13})^{-1} = (84591)(376).$$

In particular, a_{12} and a_{13} generate a group that is transitive on the straight absolute Nielsen classes $SNi(\mathbf{C}_{3^4})_T^{ab}$. From the comment at the end of § 4.1, the transitivity of the a_{1j}'s on the Nielsen classes (which are the straight Nielsen classes in this case) implies that the fiber product

$$\mathscr{H}' \stackrel{\text{def}}{=} \mathscr{H}(\mathbf{C}_{3^4}) \times_{\mathbb{P}^4\setminus D_4} (\mathbb{P}^1)^4 \setminus \Delta_4$$

is irreducible. Since the degree of the cover of Δ_4 is 9, Proposition 2.2 implies that $\mathscr{H}'$ is isomorphic to an open subset of $C(\mathbf{C}_{3^4}) \times (\mathbb{P}^1)^3$. From the Riemann–Hurwitz formula, compute the genus g of $C(\mathbf{C}_{3^4})$ from the formula

$$2(9 + g - 1) = \sum_{i=2}^{4} \mathbf{ind}(a_{1i}) = 18, \text{ or } g = 1.$$

Unirationality of $\mathscr{H}(\mathbf{C}_{3^4})$: We leave to the reader the final lemma of preparation.

Ramification Lemma : ***Assume that we have covers*** $X_i \longrightarrow \mathbb{P}^1_x$, ***with*** $p_i \in X_i$ ***ramified of order*** e_i ***over*** $x_0 \in \mathbb{P}^1_x$, $i = 1,2$. ***Then in the normalization*** Y ***of the fiber product*** $X_1 \times_{\mathbb{P}^1_x} X_2$ ***there are*** $gcd(e_1, e_2)$ ***points above the point*** (p_1, p_2)

and each of them has ramification order over x_0 ***equal to*** $lcm(e_1, e_2)$. ***Furthermore, each of these points in*** Y ***has ramification order*** $lcm(e_1, e_2)/e_1$ ***over*** p_1.

Our next result shows that all of the conditions of (5.5), except (5.5.a), are satisfied.

THEOREM 5.6. ***With*** C_i ***the conjugacy class of a*** 3***-cycle in*** A_5, $i = 1,2,3,4$, ***the parameter space*** $\mathscr{H}(C_{3^4})$ ***is a unirational variety over*** $\mathbb{Q}$. ***In particular, its*** $\mathbb{Q}$ ***points are Zariski dense.***

Proof : Refer back to the discussion prior to Conclusion 4.2 with $C = C_{3^4}$. In this case the group $T(C)$ is S_3. Here is why. Let $\phi : X \longrightarrow \mathbb{P}^1_x$ be any cover in the Nielsen class corresponding to a point of $C(C)$ lying above x. Now let $\alpha : \mathbb{P}^1_x \longrightarrow \mathbb{P}^1_x$ be any linear fractional transformation that permutes 0,1 and ∞. Then $\alpha \circ \phi : X \longrightarrow \mathbb{P}^1_x$ is in the same Nielsen class, and it has 3 of its branch points equal to 0,1 and ∞. In the case of C_{3^4} we already have noted that this cover is therefore represented by a point of $C(C)$ which has a representing cover of $\mathbb{P}^1_x$ whose 4th branch point is $\alpha(x)$.

Also $\mathscr{H}(C_{3^4})$ is in this case identified with the quotient of an action of S_4 on $\mathscr{H}'$, with $T(C_{3^4})$ identified with a copy of S_3 inside this S_4. Thus we are done if we show that $C(C_{3^4})/T(C_{3^4}) \times (\mathbb{P}^1)^3$ is unirational. This is equivalent to show that $C(C_{3^4})/T(C_{3^4})$ is rational over $\mathbb{Q}$.

But $C(C)/T(C) \longrightarrow \mathbb{P}^1_x/T(C)$ is a cover of degree 9. If we show that $C(C)/T(C)$ is of genus 0, as it has a rational class of odd (9) degree (see *Hilbert's trick* above) it is a $\mathbb{Q}$–rational curve. It is enough to show that the cover $C(C) \longrightarrow C(C)/T(C)$ is ramified, in which case $C(C)/T(C)$ is of genus less than 1 (i.e., 0). It suffices also, to replace $T(C)$ by the subgroup generated by (13), which is regarded as leaving 1 fixed and permuting 0 and ∞. Then $\mathbb{P}^1_x/\langle(13)\rangle$ is identified with $\mathbb{P}^1_y$, $y = x + 1/x$. Note that $C(C)$ is identified with the normalization of the fiber product

(5.10) $$C(\mathbf{C})/<(13)> \times_{\mathbb{P}^1_x/<(13)>} \mathbb{P}^1_x .$$

In the fiber product (5.10) the only possible branch points of $C(\mathbf{C})/<(13)> \longrightarrow \mathbb{P}^1_y$ can be identified with the images of $0, 1, \infty$, or -1 in the cover $\mathbb{P}^1_x \longrightarrow \mathbb{P}^1_y$. The images of 1 and -1 are respectively 2 and -2, and both 0 and ∞ go to ∞. The consideration of -1 comes from its being the other ramified point of $\mathbb{P}^1_x \longrightarrow \mathbb{P}^1_y$. It is clear that the disjoint cycle structure of the branch cycle over ∞ is the same as that for $C(\mathbf{C}) \longrightarrow \mathbb{P}^1_x$ over ∞ (or 0). For the other 2 points, however, the disjoint cycle structure of the branch cycle is potentially a bit more complicated. Here we have only to consider ramification over $-2 \in \mathbb{P}^1_x$ in order to draw our conclusion. But in Theorem 5.9 we will need analysis of the more complicated ramification over the other point too.

Consider the point $-1 \in \mathbb{P}^1_x$. Since there is no ramification in the cover $C(\mathbf{C}) \longrightarrow \mathbb{P}^1_x$ the Ramification Lemma (above) tells us that the points of $C(\mathbf{C})/<(13)>$ over -2, are ramified of order either 1 or 2. The maximum that this contributes to the index is 4. And then there are 4 points of order 2 ramified over -2 and one point, p_0, unramified. By the Ramification Lemma, the point of $C(\mathbf{C})$ corresponding to $(p_0, -1)$ is ramified over p_0. Thus $C(\mathbf{C}) \longrightarrow C(\mathbf{C})/<(13)>$ is ramified. This proves the result. □

5.3.– Further inspection of condition (5.5 a) : From Theorem 5.6 we conclude the following about the Nielsen class $Ni(\mathbf{C}_{34})_T$. There exist (a great many) covers $\phi : X \longrightarrow \mathbb{P}^1_x$ defined over $\mathbb{Q}$ in this Nielsen class. Furthermore, from the comments following Proposition 5.4, we have

(5.11) $$A_5 \subset G(\widehat{\mathbb{Q}(X)}/\mathbb{Q}(x)) \subset S_5 .$$

That is, in this case $N_{S_n}(G) = S_5 = \bar{G}$ (defined after (5.8)).

For the possibility of analyzing the necessity of condition (5.5 a), and for considering how to incorporate Hilbert's *trick* in the general theory, it behooves us to be able to answer a natural question in this simple case.

Question 5.7. *As* $\phi : X \longrightarrow \mathbb{P}^1_x$ *runs over all covers in the Nielsen class* $Ni(\mathbf{C}_{3^4})_T$ *does the middle term of* (5.11) *achieve both of the groups* A_5 *and* S_5 *?*

If the answer to the question is affirmative, we will say that $Ni(\mathbf{C}_{3^4})_T$ achieves A_5 and S_5. This is the conclusion of Theorem 5.9. The idea for treating this is already in [BFr; p. 95]. Instead of considering the action of H_4 on absolute Nielsen classes, we consider the action on just the Nielsen classes $Ni(\mathbf{C}_{3^4})_T$ themselves. A complete list of these can be obtained by adding to List 5.5 the effect of conjugation the elements of List 5.5 by (45) :

List 5.8.

$X_{10} : \sigma_2 = (132), \sigma_3 = (154), \sigma_4 = (145)$; $X_{11} : \sigma_2 = (154), \sigma_3 = (145), \sigma_4 = (132)$;
$X_{12} : \sigma_2 = (154), \sigma_3 = (214), \sigma_4 = (253)$; $X_{13} : \sigma_2 = (154), \sigma_3 = (321), \sigma_4 = (345)$;
$X_{14} : \sigma_2 = (154), \sigma_3 = (532), \sigma_4 = (514)$; $X_{15} : \sigma_2 = (154), \sigma_3 = (453), \sigma_4 = (421)$;
$X_{16} : \sigma_2 = (215), \sigma_3 = (254), \sigma_4 = (432)$; $X_{11} : \sigma_2 = (215), \sigma_3 = (324), \sigma_4 = (453)$;
$X_{18} : \sigma_2 = (215), \sigma_3 = (534), \sigma_4 = (254)$.

Just as in the previous computation we check the Hurwitz monodromy action on the union of List 5.5 and List 5.8. If the resulting $a_{1,j}$'s of Conclusion 4.2 generate a transitive group, we obtain a cover $C(\mathbf{C}_{3^4})' \longrightarrow \mathbb{P}^1_\lambda$ ramified over $0,1,\infty$. We note from (5.12) below that this holds. Of course, $C(\mathbf{C}_{3^4})'$ is a degree 2 cover of $C(\mathbf{C}_{3^4})$ (defined over $\mathbb{Q}$). From this point we assume that $\mathbf{C} = \mathbf{C}_{3^4}$. Then as before we form the quotient $C(\mathbf{C})'/T(\mathbf{C})$. By the previous ideas if we put the *last* 3 branch points at arbitrary rational numbers x_2, x_3, x_4, we consider the cover $C(\mathbf{C})'/T(\mathbf{C}) \longrightarrow C(\mathbf{C})/T(\mathbf{C})$. For each rational point $p \in C(\mathbf{C})/T(\mathbf{C})$, we showed in § 5.2 that we get a cover $X \longrightarrow \mathbb{P}^1_x$ in this Nielsen class defined over $\mathbb{Q}$.

Extending this we determine that the algebraic closure of $\mathbb{Q}$ in $\widehat{\mathbb{Q}(X)}$ is $\mathbb{Q}(p')$ where p' is a point of $C(\mathbf{C})'$ lying above p. From Hilbert's irreducibility theorem this will give a degree 2 extension of $\mathbb{Q}$ for most values of p in $\mathbb{Q}$. Thus this Nielsen class achieves S_5. To see that it achieves A_5 we

have only to see if $C(\mathbf{C})'/T(\mathbf{C})$ has a $\mathbb{Q}$–point. Here are the computation for the Q's :

$$Q_1 = (1\ 10)(2\ 5\ 3\ 6\ 4)(7\ 9\ 8)(11\ 14\ 12\ 15\ 13)(16\ 18\ 17)$$
$$Q_2 = (2\ 11)(14\ 18\ 8\ 5)(10\ 13\ 9\ 17\ 14)(3\ 15\ 16)(12\ 6\ 7)$$
$$Q_3 = (1\ 10)(2\ 5\ 3\ 6\ 4)(7\ 9\ 8)(11\ 14\ 12\ 15\ 13)(16\ 18\ 17).$$

From this we get the a's as previously :

$$a_{12} = Q_1^{-2} = (2\ 6\ 5\ 4\ 3)(7\ 9\ 8)(11\ 15\ 14\ 13\ 12)(16\ 18\ 17)$$
$$a_{13} = Q_1 Q_2^{-2} Q_1^{-1} = (1\ 18\ 15\ 11\ 7)(10\ 9\ 6\ 2\ 16)(3\ 8\ 14)(12\ 17\ 5) \tag{5.12}$$
$$a_{14} = (a_{12}a_{13})^{-1} = (7\ 12\ 6)(18\ 1\ 8\ 4\ 5)(16\ 15\ 3)(9\ 10\ 17\ 13\ 14).$$

Transitivity of the a's on the elements of $Ni(\mathbf{C}_{34})_T$ is now clear. Also the Riemann–Hurwitz formula gives the genus of $C(\mathbf{C}_{34})'$ as g' with

$$2(18 + g' - 1) = \sum_{i=2}^{4} \mathrm{ind}(a_{1i}) = 36, \text{ or } g' = 1.$$

THEOREM 5.9. ***There is a group of automorphisms of*** $T(\mathbf{C})'$ ***acting on*** $C(\mathbf{C})'$ ***as*** S_3 ***extending the action of*** $T(\mathbf{C})$ ***on*** $C(\mathbf{C})$. ***The quotient*** $C(\mathbf{C})'/T(\mathbf{C})'$ ***is a genus zero curve. In addition this curve has a*** $\mathbb{Q}$***-rational point. In the notation above*** $Ni(\mathbf{C}_{34})_T$ ***achieves both*** A_5 ***and*** S_5 .

Proof : Consider the formation of $C(\mathbf{C})'$. A representing cover is from an equivalence class of covers of $X \to \mathbb{P}^1_x$ with the following property with respect to a base point $x_0 \in \mathbb{P}^1_x \backslash \{x_1, ..., x_r\}$, a set of canonical homotopy classes of paths $\mathcal{P}_1, ..., \mathcal{P}_r$ for the fundamental group of $\mathbb{P}^1_x \backslash \{x_1, ..., x_r\}$; and a labeling $\{p_1, ..., p_n\}$ ($n = 5$ in this case) of the points of the cover over x_0 :

(5.13) the description $(\tau_1, ..., \tau_r)$ of the branch cycles of the cover produced by this data generates $G = A_5$ and the cover is in the Nielsen class $\mathbf{C}$.

The G orbit of this data is given by conjugation by G on the resulting branch cycles descriptions. It is an easy observation that these G–orbits are independent of the choice of $\mathcal{P}_1,...,\mathcal{P}_r$. Furthermore, since parallel transport of the points above x_0 around a closed path in $\mathbb{P}^1_x\backslash\{x_1,...,x_r\}$ permutes these points by an element of G, we may equivalence the labelings of the points over suitable base points. We shall call two such compatible labelings transportaties equivalent. Furthermore, over the curve $C(\mathbf{C})'$ we may form a local system of compatible transport equivalent labelings. Thus the G equivalence classes of covers are well defined. The construction of [Fr1; § 4] produces the corresponding Hurwitz space representing these G–orbits and $C(\mathbf{C})'$ is the result of the Hurwitz monodromy action on $Ni(\mathbf{C}_{3^4})^G_T$. Each of the two points of $C(\mathbf{C})'$ lying above a given point $m \in C(\mathbf{C})$ corresponds to one of the two possible G equivalence classes of covers that produce the equivalence class of covers of m.

Following the argument of Theorem 5.6, let $\phi : X \longrightarrow \mathbb{P}^1_x$ be any cover in the Nielsen class corresponding to a point of $C(\mathbf{C})'$ lying above x. If $\alpha : \mathbb{P}^1_x \longrightarrow \mathbb{P}^1_x$ is any linear fractional transformation that permutes 0,1 and ∞, then the G equivalence class of $\alpha \circ \phi : X \longrightarrow \mathbb{P}^1_x$ corresponds to a point of $C(\mathbf{C})'$ lying over $\alpha(x)$.

Follow exactly the computation of the proof of Theorem 5.6, at the point of the discussion that considers "the point $-1 \in \mathbb{P}^1_x$". Here conclude (as in the notation there) that there must be k points of $C(\mathbf{C})'/<(13)>$ ramified of order 2 over the image of $-2 \in \mathbb{P}^1_y$ of -1, and $18-2k$ points unramified over -2.

In a like manner we use the Ramification Lemma prior to Theorem 5.6 to analyze the disjoint cycle structure lengths $(s_1)(s_2)...(s_t)$ (with the s's in nonincreasing order) of the branch cycle τ for the cover $C(\mathbf{C})'/<(13)> \longrightarrow \mathbb{P}^1_y$ over $2 \in \mathbb{P}^1_y$. The s's give a possible disjoint cycle structure of $(3)(3)(5)(5)$ for $a_{1,3}$ when τ has the following form :

(5.14) $\qquad (3)(3)(5)(5),\ (6)(5)(5),\ (3)(3)(10)$ or $(6)(10)$.

Apply the Riemann–Hurwitz formula as previously to conclude that the genus of $C(\mathbf{C})'/<(13)>$ is a most $\frac{26+k}{2}-17$ and this maximum occurs under

three circumstances : when $k = 8$ and τ has type (6)(10); when $k = 9$ and τ has type (3)(3)(10) ; or when $k = 9$ and τ has type (6)(5)(5). In any of these cases $C(\mathbf{C})'/T(\mathbf{C})$ is of genus 0. But it is a degree 18 cover of $\mathbb{P}^1_x/T(\mathbf{C})$. Nevertheless we can look in the divisors that have support over the branch locus of the cover $C(\mathbf{C})'/T(\mathbf{C}) \to \mathbb{P}^1_x/T(\mathbf{C})$ to find a $\mathbb{Q}$ divisor of odd degree. Indeed, since it is only the last three cases of (5.14) that can possibly occur, we note that any of the nonrepeated lengths of the disjoint cycles for τ in the last 3 cases of (5.14) correspond to a point over $2 \in \mathbb{P}^1_y$ that must be $\mathbb{Q}$–rational. □

Manuscrit reçu le 13 septembre 1988.
Corrigé le 31 janvier 1989

(*) p. 77 : Stay in France supported by NSF grant DMS–8702150 and Institut Henri Poincaré.

BIBLIOGRAPHY

[Be] G.V. Belyi.– *On Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk. SSSR, Ser. Mat. 43 (1979), 267–276.

[BFr] R. Biggers and M. Fried.– *Moduli spaces of covers and the Hurwitz monodromy group*, J. für die reine und Angew. Math. 335 (1982), 87–121.

[DDH] S. Diaz, R. Donagi and D. Harbater.– *Every curve is a Hurwitz space*, preprint.

[DFr] P. Debes and M. Fried.– *Arithmetic variation of fibers in families of curves Part I : Hurwitz monodromy criteria for rational points on all members of the family;* preprint.

[F] W. Feit.– $\hat{A}_5$ *and* $\hat{A}_7$ *as Galois groups over number fiels*, J. of Alg. 104 (1986), 231–260.

[Fr,1] M. Fried.– *Fields of definition of function fields and Hurwitz families...*, Comm. in Alg. 5(1) (1977), 17–82.

[Fr,2] M. Fried.– *Galois group and complex multiplication*, TAMS 235 (1978), 141–163.

[Fr,3] M. Fried.– *Rigidity and applications of the classification of simple groups to monodromy Part I-Super rational connectivity with examples; Part II-Applications of connectivity*; Davenport and Hilbert–Siegel problems.

[FrT] M. Fried and J.G. Thompson.– *The Hurwitz monodromy group* H_4 *and modular curves*, preprint.

[Gro] A. Grothendieck.– *Géométrie formelle et géométrie algébrique*, Séminaire Bourbaki t. 11, 182 (1958/59).

[Gu] R.C. Gunning.– *Lectures on Riemann Surfaces*, Princeton Math. Notes (1966).

[Hi] D. Hilbert.– *Uber die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. Reine Angew. Math. 110 (1892), (Ges. Abh. II, 264–286).

[Ma,1] H. Matzat.– *Konstructive Galoistheorie*, Lecture Notes in Math–Springer Verlag 1284 (1986).

[Ma,2] H. Matzat.– *Rationality Criteria for Galois Extensions*, preprint.

[Sh] K. Shih.– *On the construction of Galois extensions of function fields and number fields*, Matematische Annalen 207 (1974), 99–120.

[T] J.G. Thompson.– *Some finite groups which appear as* Gal L/K *where* $K \subseteq \mathbb{Q}(\mu_n)$, J. of Alg. 98 (1984), 437–499.

[W] A. Weil.– *The field of definition of a variety*, Amer. J. Math. 78 (1956), 509–524.

Mike Fried
Department of Mathematics
201 Walker Hall
University of Florida
Gainesville, Fl 32611
and
Department of Mathematics
UC Irvine
Irvine, California 92717