ACTA ARITHMETICA
LVI (1990)

Rigidity and real residue class fields

by

MICHAEL D. FRIED* (Irvine, Ca.) and PIERRE DEBES (Paris)

Introduction and acknowledgements. Consider a cover $\phi\colon X \to P_x^1$ of the Riemann sphere (uniformized by x) by a projective nonsingular curve X with $r > 2$ branch points. Assume that both the curves and the map are defined over Q. Generalizing Serre [Se] we consider not necessarily Galois covers with any number r of branch points (not necessarily in R). We show how to compute the action of complex conjugation on the fiber in X over a real value of $x_0 \in P_x^1$. It is an "exceptional cover" for which all of the residue class fields above x_0 are real. The group of the Galois closure of such an exceptional cover must be a quotient of a universal group generated by elements of order 2.

Serre was interested primarily in applications to groups as Galois groups, so he considered only the case that x_0 is not equal to a branch point of the cover. Siegel's theorem [S] gives explicit necessary conditions for an affine curve to have infinitely many integral points. As motivation for allowing x_0 to be a branch point we give immediate application to a converse of Siegel's theorem phrased in terms of "complete Siegel families".

Sprindžuk too was often motivated by Siegel's theorem. His papers were not similar in style to ours, but both authors were influenced in the direction of the topics here by [Sp]. Finally, we would like to acknowledge that there are a number of papers in the literature in addition to [Se] that have considered the continuous action of complex conjugation on paths (e.g., [KN]). It is inevitable therefore that some of our results repeat older observations.

Acknowledgements. In addition to the correction of a considerable number of typos, we thank the referee for pointing out that similar versions of the formulas of §2.1, with a different arrangement of the branch points, appear in [H].

§0. Framework for the main results

Consider the rational function field $C(x)$ in one variable and a fixed copy of the complex plane with a point at ∞ uniformized by a variable x. Denote

1980 *Mathematics Subject Classification*: 12F05, 14H40, 14D20, 14E20, 20F36.

* Appreciated support from NSF grant DMS-8702150 and Institut Henri Poincaré.

the latter by $\mathbf{P}^1_x$. From Riemann's existence theorem, degree n extensions E of $\mathbf{C}(x)$ ramified over r places $x_1, \dots, x_r$ are in one-one correspondence – up to a natural equivalence – with the degree n connected covers of $\mathbf{P}^1_x \setminus \{x_1, \dots, x_r\}$. These are in turn in one-one correspondence with equivalence classes of transitive permutation representations $T\colon \pi_1 \to S_n$ on the set $\{1, 2, \dots, n\}$ where π_1 denotes the fundamental group of $\mathbf{P}^1_x \setminus \{x_1, \dots, x_r\}$.

The Galois group of the normal closure of the extension $E/\mathbf{C}(x)$ is identified with the *monodromy group of the cover*, the group $G = T(\pi_1)$. If a Galois cover $X \to \mathbf{P}^1_x$ is known to be defined over $\mathbf{Q}$, then its monodromy group can be realized as a Galois group over $\mathbf{Q}$; by application of Hilbert's irreducibility theorem G is the Galois group of some residue class field extension $E_{x_0}/\mathbf{Q}$ with x_0 a rational specialization of x. For nonsolvable groups, this idea has been an essential part of any success on the inverse Galois theory problem. In this paper we investigate the real embeddings of these residue class fields. In particular, when are they totally real? In terms of covers this would be asking when such a cover can have fibers consisting of only real points.

Generalization of Serre's observations. This work originated with a question of Serre [Se]. A given group G is easily realized as the monodromy group of a cover. Indeed, since π_1 is isomorphic to a free group on $r-1$ generators (cf. §1.1), for sufficiently large r, G is $T(\pi_1)$. But the problem is to get the cover corresponding to the permutation representation to be defined over $\mathbf{Q}$, the purpose of "rigidity theory". After discussing the rigidity assumptions, Serre asks about local properties (over $\mathbf{R}$ and $\mathbf{Q}_p$) of the residue class extensions provided by a rigid situation. He shows for example that for 3 real branch points and $G \neq S_3$ these extensions cannot be totally real.

We consider any number $r = r_1 + 2r_2$ of branch points with r_1 of them real and $2r_2$ of them in complex conjugate pairs. Then we give necessary conditions (§1) on a group G for there to be a cover with monodromy group G to have totally real fibers (Theorem 1.1). For the statement of the following simplified version we 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.

THEOREM 0.0. *Assume that a cover $X \to \mathbf{P}^1_x$ and each of its r branch points are defined over $\mathbf{Q}$. Consider $x_0 \in \mathbf{P}^1_x \setminus \{x_1, \dots, x_r\}$. If the fiber consists of just real points, then the monodromy group G is generated by $r-1$ elements $\alpha_1, \dots, \alpha_{r-1}$ of order 2. Furthermore, if the Galois closure $\hat{X} \to \mathbf{P}^1_x$ is also defined over $\mathbf{Q}$ (i.e., the smallest Galois cover factoring through $X \to \mathbf{P}^1_x$, and $\hat{X}$ is irreducible over the closure of $\mathbf{Q}$) the elements $\alpha_1\alpha_2, \alpha_2\alpha_3, \dots, \alpha_{r-2}\alpha_{r-1}$ are in rational conjugacy classes of G.*

Other examples and corollaries of §1: if a group of odd order is the Galois group of a regular extension $E/\mathbf{Q}(x)$, then the extension has no real branch points. Also, Theorem 2.4 (§2.3) shows the effect of complex conjugation on the fiber of a cover over a real point in the general case: condition (1.3) of Theorem 1.1.

The proof of Theorem 1.1 (as a combination of Theorem 2.4 and of §2.4) appears in §2. Here two aspects of complex conjugation are considered: action on the points in a fiber of a cover defined over $\mathbf{R}$; and through its action on π_1, as an automorphism of G. The simple formulation of Theorem 0.0 comes through some miraculous group theoretic manipulations. The "branch cycle argument" from [Fr 1] concludes the proof (§2.4). Below we will denote the element that gives this action by $c_{x_0} = c$.

"Rigidity" and exceptions to Theorem 1.1 for $r = 4$. No rigidity assumptions are involved in the first part of the paper. These come up in §3 to study the converse of Theorem 1.1. That is, when can we actually realize a group satisfying the necessary conditions of Theorem 1.1 as a Galois group of a totally real extension of $\mathbf{Q}$?

We have been suppressing the dependence of all statements on data given by a collection of r conjugacy classes, $\mathbf{C} = (C_1, \dots, C_r)$, of the group G which contain respective inertia group generators corresponding to the points $x_1, \dots, x_r$ for the Galois closures of one of the covers under investigation. In §3.2 we state generalizations of the classical "rigidity assumption" (as discussed in [Se]). All of the results of this paper and the "rigidity results" depend on $\mathbf{C} = (C_1, \dots, C_r)$. But this brings up the difficulty that also appears in [FrT]. In addition to the new rigidity assumption on $\mathbf{C}$, transitivity of the straight Hurwitz monodromy group on straight Nielsen classes (Prop. 3.3), one needs a $\mathbf{Q}$-point on a certain algebraic variety $\mathscr{H}(\mathbf{C})$ associated to G (and $\mathbf{C}$). In the case $r = 3$ this is a rational variety, and so it has lots of $\mathbf{Q}$-points.

In the case $r = 3$ there is just one centerless group, S_3, that has conjugacy classes $\mathbf{C}$ that satisfy the necessary conditions of Theorem 1.1 (Prop. 1.2). In contrast to this, Proposition 3.6 and Theorem 3.7 show that all of the groups S_n and A_n, $n \geqslant 4$ are exceptions to Theorem 1.1 in the case that $r = 4$ in the following weak sense. To each of these groups G there is an associated $\mathbf{C}$ with this property: there is a curve cover $Y_G \to \mathbf{P}^1_x$ ramified over $\{0, 1, \infty\}$ and defined over $\mathbf{Q}$ such that the totally real field conclusion holds for $\mathbf{C}$ if and only if there is a $\mathbf{Q}$-point $\boldsymbol{m} \in Y_G$, not lying over of the branch points of the cover.

When $n = 4$ $(G = S_4)$ and 5 $(G = S_5)$ the curve Y_G is of genus 0, and we show that it has infinitely many rational points (Theorem 3.7). Thus S_4 (resp., S_5) is achieved as a Galois group of a regular extension of $\mathbf{Q}(t)$ with infinitely many totally real specializations giving S_4 (resp., S_5) as a totally real extension of $\mathbf{Q}$. Actually, this is true for all n between 4 and 9. But showing that Y_G is of genus 0 in the respective cases takes up some space. For other values of n, the genus of the curve exceeds 0. (Indeed, for values of n that are prime, the genus of Y_G is a quadratic function of n.) This happens, also, when you modify the initial set of α's. Since we cannot devine the existence of rational points on these curves unless they are of genus 0, this is a serious obstruction when $r = 4$ to getting all S_n's as Galois groups of regular extensions with infinitely many real specializations. Finding real points on these curves, however, is another matter.

The theory of §2 shows exactly how to describe such real points. This is a special case of our next topic.

Real points on $\mathscr{H}(\mathbf{C})$. The formulas that are satisfied by the element c_{x_0} that plays the role of complex conjugation on the data for a cover $X \to \boldsymbol{P}^1_x$ in Theorem 2.4 can be inspected without having the cover defined over $\boldsymbol{R}$. In fact, the existence of c_{x_0} is an if and only if condition for the corresponding cover to be defined over $\boldsymbol{R}$. This shows dramatically in terms of the parameter space $\mathscr{H}(\mathbf{C})$ and its presentation as a cover of $\boldsymbol{P}^r$ minus the standard discriminant locus D_r (§3.3).

THEOREM 0.1 (Theorem 4.4 of §4.2). *There is a constructive partition $\mathscr{H}_1, \ldots, \mathscr{H}_v$ of the points of $\mathscr{H}(\mathbf{C})$ lying over $\boldsymbol{P}^r(\boldsymbol{R}) \backslash D_r$ with the following property: each of the $\mathscr{H}_i$'s, as a set of complex valued points on the manifold $\mathscr{H}(\mathbf{C})$ is connected; and for each $\mathbf{m} \in \mathscr{H}_i$ we may apply Theorem 2.4 to explicitly test for the existence of a collection of c's playing the role of complex conjugation on the fibers of the cover—up to equivalence—that corresponds to $\mathbf{m}$. This test does not depend on the choice of base point that we use to apply Theorem 2.4, and $\mathscr{H}_i$ passes this test if and only if all of the points of $\mathscr{H}_i$ correspond to covers defined over $\boldsymbol{R}$.*

Nonexistence of a $\boldsymbol{Q}_p$ analog. This brings up the problem of $\boldsymbol{Q}_p$ analogues of these results for rational primes p. There are tools: Neukirch [N] has checked local behavior for Galois extensions $K/\boldsymbol{Q}$ whose groups are of odd order; and Grothendieck's lifting theorems (for tamely ramified covers [Gro]) consider the primes relatively prime to the order of the group. But in a later paper we will show there is no *naive* $\boldsymbol{Q}_p$ analogue for these results; this uses that there is no nontrivial Hecke operator theory for the curves associated to the upper half plane by a *noncongruence subgroup* (cf. §3.6 prior to Theorem 3.7) of $\mathrm{SL}_2(\boldsymbol{Z})$ due to Atkin [A].

Application to a converse of Siegel's theorem. We conclude by considering residue class fields of points over the branch points $x_1, \ldots, x_r$ of the cover. The effect of complex conjugation here is a corollary of Theorem 2.4 together with data from *markings* on the disjoint cycles of a branch cycle attached to the specific ramified point of interest (Theorem 4.2).

A version of Siegel's theorem [S] says that an affine curve X defined over $\boldsymbol{Q}$ has infinitely many integral points only if the curve is of genus 0 and it has either one point or two real conjugate points at infinity. The above gives an explicit criterion for the "general" real member of a family of affine covers to satisfy the "real conjugate points" condition. This is the source of the definition of Siegel families in §4.3. For "complete" Siegel families we then discuss criteria for a natural converse of Siegel's theorem. The families themselves and the criteria for the converse are put in terms of combinatorial data that goes along with Riemann's existence theorem. We conclude with examples that display relevant properties of Siegel families. For example, for families over $\boldsymbol{Q}$, as a corollary to Theorem 1.1, §4.3 gives a computation for whether the residue class field over the point at ∞ in a cover from a Siegel family is constant as a function of the family parameters.

§1. Covers with real fibers

§1.1. Notations and background tools. Let $\phi\colon X \to \boldsymbol{P}^1_x$ be a finite cover of the projective line of degree n by an irreducible projective nonsingular curve. This cover is ramified over a finite set of points $x_1, \ldots, x_r$ called the *branch points of the cover*. For $x_0 \notin \{x_1, \ldots, x_r\}$ consider a labeling of the points $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ of $\phi^{-1}(x_0)$. There is a natural transitive action $T\colon \pi_1 \to S_n$, called the *monodromy action*, of the fundamental group π_1 of $\boldsymbol{P}^1_x \backslash \{x_1, \ldots, x_r\}$ on $\{1, 2, \ldots, n\}$ identified respectively with the $\boldsymbol{p}$'s given as follows.

For $[\gamma]$ the homotopy class of a path γ based at x_0, $T([\gamma])$ is the element of S_n that maps i to j where $\boldsymbol{p}_j$ is the terminal point of the unique lift of γ (through ϕ) which has initial point $\boldsymbol{p}_i$, $i \in \{1, 2, \ldots, n\}$. Up to conjugation by an element of S_n this action is independent of the choices of x_0, the representative of $[\gamma]$ and the labeling of the $\boldsymbol{p}$'s.

The group $G = T(\pi_1)$ is called the *monodromy group* of the cover. Consider π_1: it is the free group on r generators $[\gamma_1], \ldots, [\gamma_r]$ with the one relation $[\gamma_1] \ldots [\gamma_r] = 1$ where $\gamma_1, \ldots, \gamma_r$ can be taken as "loops" around $x_1, \ldots, x_r$ based at x_0 with special properties (as in the Figures of §2.1 and §2.2). Therefore the homomorphic image G is generated by r elements $\sigma_i = T([\gamma_i]) \in S_n$, $i = 1, \ldots, r$, that satisfy $\sigma_1 \ldots \sigma_r = 1$. The r-tuple $(\sigma_1, \ldots, \sigma_r)$ is called a *branch cycle description* of the cover.

Galois action on branch points. Let $K \subset \boldsymbol{C}$ be a field of definition of the cover $\phi\colon X \to \boldsymbol{P}^1_x$. 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 $K(\boldsymbol{P}^1_x) = K(x)$ (i.e., if $\widehat{K(X)} \cap \bar{K} = K$). 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 $\widehat{K(X)}$.

We also need a group theoretic definition extending the definition of rational conjugacy class of a group (see Main Results, above).

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

$$(1.1) \quad \text{the set } \bigcup_{i=1}^{r} C_i \text{ contains all powers } \tau_i^k,\ i = 1, \ldots, r$$

and k relatively prime to N.

Note that unions of rational sets of conjugacy classes are also rational sets of conjugacy classes. An alternative statement to (1.1) is the following:

(1.2) for $k \in (\mathbf{Z}/N)^*$, there exists $\beta \in S_r$ such that $\tau_i^k \in C_{(i)\beta}$, $i = 1, \ldots, r$.

Consider the orbits of the action of $G(\bar{K}/K)$ on the branch points $x_1, \ldots, x_r$ 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 $\bigcup_{j \in O(i)} C_j$ of the conjugacy classes attached to this orbit of the branch points. Denote this by $O(C_i)$, the *orbit of* C_i under $G(\bar{K}/K)$.

§1.2. Necessary conditions for real residue classes. Consider a cover $\phi\colon X \to \boldsymbol{P}_x^1$ as in §1.1. When convenient we denote $\boldsymbol{P}_x^1$ by $\boldsymbol{P}^1$. From now on assume that this cover is defined over $\boldsymbol{R}$. Then the branch points $x_1, \ldots, x_r$ consist of r_1 real points and r_2 pairs of complex conjugate points with $r = r_1 + 2r_2$.

We now inspect the possibility that a fiber of this cover will consist only of real points. For simplicity we assume that $r_1 \neq 0$. Modification for the case $r_1 = 0$ appears in a remark after Theorem 1.1. Of course it is possible to rephrase Theorem 1.1 entirely in terms of function fields (examples of §1.3). Denote the normalizer of G in S_n by $N_{S_n}(G)$.

THEOREM 1.1. *Assume in addition to the above that for some real point* $x_0 \in \boldsymbol{P}^1(\boldsymbol{R})$, *not a branch point, the fiber* $\phi^{-1}(x_0)$ *consists of n real points. Then* $r_1 \geqslant 2$ *and the monodromy group G can be generated by* $r_1 + r_2 - 1$ *elements* $\alpha_1, \ldots, \alpha_{r_1 - 1}, \tau_1, \ldots, \tau_{r_2}$ *with the following properties:*

(1.3) *the* α_i*'s are each of order 2 and therefore* $\alpha_1, \alpha_1\alpha_2, \alpha_2\alpha_3, \ldots$ $\ldots, \alpha_{r_1-2}\alpha_{r_1-1}, \alpha_{r_1-1}$, *respectively denoted* $\sigma_1, \ldots, \sigma_{r_1}$, *are each distinct from* 1 *and each is conjugate to its inverse in* G.

Denote the respective conjugacy classes in G of the elements $\sigma_1, \ldots, \sigma_{r_1}$, $\tau_1, \ldots, \tau_{r_2}$ *and* $\tau_1^{-1}, \ldots, \tau_{r_2}^{-1}$ *by the set*

$$S = \{C_1, \ldots, C_{r_1}, D_1, \ldots, D_{r_2}, D_1^{-1}, \ldots, D_{r_2}^{-1}\}.$$

If, further, the cover is g-regular over $\boldsymbol{Q}$, *then in addition to* (1.3)

(1.4) *each* $G(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ *orbit of S is a rational set of (nontrivial) conjugacy classes.*

Remark. (a) *Theorem* 0.0. Theorem 0.0 in the prior discussion of results is the special case $r = r_1$ ($r_2 = 0$) and the assumption that the branch points are rational (the $G(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ orbits of the conjugacy classes are each of length 1).

(b) *Dropping the g-regular assumption.* In the last statement of the theorem we have only to replace the list of conjugacy classes in G by the same list of conjugacy classes in $\hat{G} = G(\widehat{\boldsymbol{Q}(X)}/\boldsymbol{Q}(x))$. Note that $\hat{G} \subset N_{S_n}(G)$. Proposition 2.6 gives a necessary condition for g-regularity in terms of an explicit subgroup $\bar{G}$ of $N_{S_n}(G)$. This is also a sufficiency test for the g-regular assumption if in addition, $\bar{G} = G$ [Fr 1; p. 33, Prop. 2].

(c) *If* $r_1 = 0$. Then condition (1.3) is empty. The rest remains the same.

§1.3. Examples and corollaries. First we consider the special case of $r = 3$. This example is considered by Serre [Se], in a "rigid" situation (cf. § 3) and with the extra hypothesis $r = r_1$. Here we complement his work by not assuming any "rigidity" hypotheses hold. In particular, unlike Serre, we allow that G has a center.

PROPOSITION 1.2. *Let G be a group different from any of* $\boldsymbol{Z}/n \times^s \boldsymbol{Z}/2$ *with* $n = 2, 3, 4$ *or* 6. *Suppose that* $E/\boldsymbol{Q}(x)$ *is a regular Galois extension with group G and* $r = 3$ *branch points. Then the residue class field extensions* $E_{x_0}/\boldsymbol{Q}$ *with group G and* $x_0 \in \boldsymbol{Q}$ *cannot be totally real. The only centerless group among the exceptions is for* $n = 3$ *(i.e.,* S_3*).*

Proof. Since $r = 3$ is odd, r_1 which is at least 2 from Theorem 1.1, must be 3. The branch points are real and the group G is generated by two elements α_1 and α_2 of order 2. A group generated by two elements of order two must be the dihedral group of degree the order of the product of the two elements (denoted σ_2). Thus $2 \cdot \operatorname{ord}(\sigma_2) = |G|$.

From (1.4), the powers σ_2^k (identified with $(k; 0) \in \boldsymbol{Z}/n \times^s \boldsymbol{Z}/2$) with $(k, n) = 1$ should either be conjugate to α_1, σ_2 or $\sigma_3 = \alpha_2$ (respectively identified with (0; 1), (1; 0) and (1; 1)). Since the two elements on the end are of order 2, this implies that $k = \pm 1$. Thus $\varphi(n) < 3$ where φ is the Euler phi-function. This won't be true unless the dihedral group is of degree at most 6. The only possibilities are $n = 2, 3, 4$ or 6, thereby giving the very groups that were excluded. ∎

In § 3.3 and § 3.4 there is an extensive discussion of some of the many more exceptions to the conclusion of Proposition 1.2 in the case $r = 4$. In particular, S_n and A_n are exceptions to versions of Serre's example for each $n > 4$. We conclude this subsection with a discussion of condition (1.3). First note that it forces the group to be of even order.

COROLLARY 1.3. *The Galois group of a regular Galois extension* $E/\boldsymbol{Q}(x)$ *with at least one real branch point is of even cardinality.*

Proof. Choose a rational number x_0 for which the Galois group $G(E_{x_0}/\boldsymbol{Q})$ of the residue class field is isomorphic to G (i.e., apply Hilbert's irreducibility theorem). If E_{x_0} is totally real, since $r_1 \neq 0$, Theorem 1.1 implies that $r_1 \geqslant 2$. From (1.3) there is at least one element of order 2. Thus G is even. If E_{x_0} is not totally real, then complex conjugation is an element of order 2 of $G(E_{x_0}/\boldsymbol{Q})$. ∎

Now assume that all branch points are real: $r = r_1$. Then (1.3) is fairly restrictive:

(1.5) G is generated by $r - 1$ elements $\alpha_1, \ldots, \alpha_{r-1}$ of order 2.

Proposition 1.4. *Condition* (1.5) *is equivalent to the following statement. The group G contains a subgroup H of index at most 2 where H is generated by $r-2$ elements $\beta_1, \ldots, \beta_{r-2}$ with this property*:

(1.6) *there exists β_0 of order 2 such that $\beta_0\beta_k\beta_0 = \beta_k^{-1}$, $k = 1, \ldots, r-2$.*

Proof. First assume that (1.5) holds. Let β_0 be α_1 and let β_i be $\alpha_1\alpha_{i+1}$, $i = 1, \ldots, r-2$. Since $(\beta_0\beta_k)^2 = 1$, conclude that (1.6) holds. Furthermore $G = H \cup H\alpha_1$ because the group generated by the β_i's, $i \neq 0$, contains all of the products $\alpha_i\alpha_j$, $1 \leqslant i, j \leqslant r-1$. The converse is clear by defining α_1 to be β_0 and α_i to be $\beta_0\beta_{i-1}$, $i = 2, \ldots, r-1$. ■

Remark. There are two possibilities corresponding to (1.6): either $\beta_0 \in H$ and $G = H$ or $\beta_0 \notin H$ and $G = H \times^s \langle\beta_0\rangle$.

There is another easy characterization of (1.5). Denote the free group on generators $b_1, \ldots, b_{r-2}$ by $F(\boldsymbol{b})$. Let J be the automorphism of $F(\boldsymbol{b})$ defined by $J(b_k) = b_k^{-1}$, $k = 1, \ldots, r-2$. This provides an action of $\boldsymbol{Z}/2$ on $F(\boldsymbol{b})$ by regarding J as the generator of $\boldsymbol{Z}/2$. Denote the semidirect product $F(\boldsymbol{b}) \times^s \boldsymbol{Z}/2$ by $D_{\infty,r}$. The groups generated by $r-1$ elements of order 2 are the quotients of $D_{\infty,r}$.

§ 2. Proof and generalization of Theorem 1.1

The notations are those of § 1, especially § 1.1. Consider a cover $\phi\colon X \to \boldsymbol{P}_x^1$ with r branch points $x_1, \ldots, x_r$ defined over $\boldsymbol{R}$. As there abbreviate $\boldsymbol{P}_x^1$ to $\boldsymbol{P}^1$ when there can be no confusion.

§ 2.1. Complex conjugation on fundamental groups. Complex conjugation provides a topological automorphism of the points of X that extends the action of complex conjugation on $\boldsymbol{P}^1$. We use this in our opening lemma. In the proof E will denote the function field of X over $\boldsymbol{R}$, and $\hat{E}$ the Galois closure of $E/\boldsymbol{R}(x)$.

Lemma 2.1. *Let γ be a path in $\boldsymbol{P}^1\backslash\{x_1, \ldots, x_r\}$ based at $x_0 \in \boldsymbol{R} \cup \infty$. Label the points of X above x_0 as $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$. Denote the usual representation associated to the cover by $T\colon \pi_1 \to S_n$ where we have identified the integers $\{1, \ldots, n\}$ with the points of the fiber X_{x_0}. Then complex conjugation induces an automorphism $c_{x_0} = c$ of X_{x_0}. This satisfies*

$$cT(\gamma)c = T(\bar{\gamma}). \tag{2.1}$$

Proof. Suppose that f_u and f_l are bi-continuous maps that render the following diagram commutative:

$$\begin{tikzcd} X \arrow[r, "f_u"] \arrow[d, "\phi"] & X \arrow[d, "\phi"] \\ \boldsymbol{P}_x^1 \arrow[r, "f_l"] & \boldsymbol{P}_x^1 \end{tikzcd} \tag{2.2}$$

It is a standard deduction that if f_l fixes x_0, then $T(f_l \circ \gamma) = f_* \circ T(\gamma) \circ f_*^{-1}$ where f_* denotes the action induced by f_u on the fiber over x_0. We apply this to the case where both f_l and f_u are given by complex conjugation to get the desired formula.

Alternative proof. (Using Puiseux expansions.) The branch cycles relative to a given set of paths are computed by their actions on the points $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ through liftings of the paths that start at the various points. We, however, wish to identify the effect of complex conjugation in a residue class field with a process related to analytic continuation. It is perhaps safer to see this on the level of functions.

Consider functions $f_1, \ldots, f_n$ of $\hat{E}$ where the f_i's are a complete set of conjugates (under $G(\hat{E}/\boldsymbol{R}(x))$) and such that f_1 is a local uniformizing parameter at each place of $\hat{E}$ above x_0. In particular, $f_1(\boldsymbol{p}_i)$ generates the residue class field of the point $\boldsymbol{p}_i$ over $\boldsymbol{R}(x_0)$. With no loss identify $f_1 = f_1(x; x_0)$ with a Puiseux expansion about x_0. The conjugates of f_1 are therefore the complete set of Puiseux expansions that result from analytically continuing f_1 around the lifts to $\hat{X}$ of closed paths on $\boldsymbol{P}_x^1\backslash\{x_1, \ldots, x_r\}$ that are based at x_0. Since x_0 is real, the effect of complex conjugation in the residue class field is obtained by acting on the coefficients of the Puiseux expansions of the f_i's. This gives c_{x_0}.

The process of analytic continuation is given by rearrangement of power series, an essentially algebraic process. Denote the path around x_j by $\mathscr{P}_j$, $j = 1, \ldots, r$. Suppose that when you continue f_k around $\mathscr{P}_j$ the result is f_l. Then, when you continue $\bar{f}_k$ around $\bar{\mathscr{P}}_j$, the result is $\bar{f}_l$. This is what the formula says. ■

Remark. From Lemma 2.1 it is immediate that c_{x_0} is an element of $N_{S_n}(G)$, the normalizer of G in S_n.

Real branch points. This is the start of a discussion in which we give specific generators of π_1 and we study how complex conjugation acts on them. Since there is a considerable distinction between the effect on the generators that go around real branch points and those that go around complex (not real) branch points, we start with the case where $X \to \boldsymbol{P}_x^1$ and the branch points $x_1, \ldots, x_r$ of the cover are both defined over $\boldsymbol{R}$. Assume that these are arranged in order on the "circle" $\boldsymbol{R} \cup \infty$. Then a point $x_0 \in \boldsymbol{R} \cup \infty$ lies in one of the segments

$$(x_1, x_2), (x_2, x_3), \ldots, (x_{r-1}, x_r), (x_r, x_1).$$

Let ϱ_i be a counterclockwise rectangle about x_i as shown in Figure 1, $i = 1, \ldots, r$.

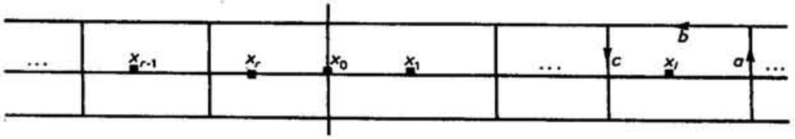

Fig. 1. Convenient paths in the case of real branch points ($u_l = abc$ and $\varrho_l = u_l\bar{u}_l^{-1}$)

Define closed paths based at x_0 as follows using the u_i's—top counterclockwise halves of ϱ_i's whose respective initial–end points are on the x-axis—of Figure 1:

$$\gamma_r = \varrho_r, \quad \gamma_{r-1} = u_r \varrho_{r-1} (u_r)^{-1}, \quad \gamma_{r-2} = u_r u_{r-1} \varrho_{r-2} (u_r u_{r-1})^{-1}, \quad \dots$$

$$\dots, \quad \gamma_2 = u_r \dots u_3 \varrho_2 (u_r \dots u_3)^{-1}, \quad \gamma_1 = (u_1)^{-1} \varrho_1 u_1.$$

Note that in expressing γ_1 we have used that $u_r u_{r-1} \dots u_1$, which is homotopic on the r-punctured sphere to the top of the band, is also homotopic there to the trivial path based at x_0. Then the γ_i's are generators of π_1 which satisfy $\gamma_1 \dots \gamma_r = 1$. Denote the effect of applying complex conjugation to each point of a path γ by $\bar{\gamma}$.

Lemma 2.2. *The paths $\bar{\gamma}_1, \bar{\gamma}_2, \dots, \bar{\gamma}_{r-2}, \bar{\gamma}_{r-1}, \bar{\gamma}_r$ are respectively homotopic to*

$$\gamma_1^{-1}, \quad (\gamma_3 \cdots \gamma_r)^{-1} \gamma_2^{-1} (\gamma_3 \cdots \gamma_r), \quad \dots$$

$$\dots, \quad (\gamma_{r-1} \gamma_r)^{-1} \gamma_{r-2}^{-1} (\gamma_{r-1} \gamma_r), \quad (\gamma_r)^{-1} \gamma_{r-1}^{-1} \gamma_r, \quad \gamma_r^{-1}.$$

Proof. Clearly $\bar{\gamma}_1 = \gamma_1^{-1}$ and $\bar{\gamma}_r = \gamma_r^{-1}$. Throughout use that

$$\bar{\varrho}_i = \varrho_i^{-1} \quad \text{and} \quad u_i \bar{u}_i^{-1} = \varrho_i, \quad i = 1, \dots, r. \tag{2.3}$$

Apply conjugation to $\gamma_{r-1} = u_r \varrho_{r-1} u_r^{-1}$ to get $\bar{\gamma}_{r-1} = \bar{u}_r \bar{\varrho}_{r-1} \bar{u}_r^{-1}$. With the help of (2.3) we get the desired expression for γ_{r-1}. The procedure is the same to compute

$$\bar{\gamma}_{r-2} = \overline{u_r u_{r-1}}\, \bar{\varrho}_{r-2} (\overline{u_r u_{r-1}})^{-1}$$

except to note that $u_r u_{r-1} (\overline{u_r u_{r-1}})^{-1}$ is $u_r \varrho_{r-1} \bar{u}_r^{-1}$, which is homotopic to $\gamma_{r-1} \gamma_r$. ■

Remark 2.3. In the case that x_0 is in the interval (x_i, x_{i+1}) the statement of Lemma 2.2 would go through with $(\gamma_1, \dots, \gamma_r)$ replaced by

$$(\gamma_{i+1}, \gamma_{i+2}, \dots, \gamma_r, \gamma_1, \dots, \gamma_i).$$

Now define σ_i to be $T(\gamma_i)$, $i = 1, \dots, r$, so that $(\sigma_1, \dots, \sigma_r) \in S_n^r$ is a branch cycle description of the cover $X \to \boldsymbol{P}_x^1$. Lemmas 2.1 and 2.2 give us an element $c_{x_0} = c \in N_{S_n}(G)$ such that

$$c \sigma_1 c = \sigma_1^{-1}, \quad c \sigma_2 c = (\sigma_3 \dots \sigma_r)^{-1} \sigma_2^{-1} (\sigma_3 \dots \sigma_r), \quad \dots \tag{2.4}$$

$$\dots, \quad c \sigma_{r-1} c = (\sigma_r)^{-1} \sigma_{r-1}^{-1} \sigma_r, \quad c \sigma_r c = \sigma_r^{-1}.$$

§ 2.2. Adjustments for complex branch points. For a cover defined over $\boldsymbol{R}$ some of the branch points are real and the remainder occur in complex conjugate pairs. Exactly as in § 2.1 we get the existence of $c_{x_0} = c$ playing the role of complex conjugation. It is defined in terms of its effect on branch cycles.

We follow the notation of § 1.1 with r_1 the number of real points (including the possibility of ∞) among the r branch points. As in § 2.1 it is convenient to label the real branch points $x_1, \dots, x_{r_1}$, from left to right (as in Figure 2) in such a way that x_0 falls between x_{r_1} and x_1. Of course, this may mean that we must relabel the conjugacy classes also (cf. Hurwitz monodromy action, § 3.1). We have also chosen to use an idealized picture in which the pairs of complex conjugate points, $x_{r_1+1}, \bar{x}_{r_1+1}, \dots, x_{r_1+r_2}, \bar{x}_{r_1+r_2}$, are placed left to right in the band of rectangles (the barred points below the real circle) with the rectangles surrounding them composing part of the band. It will be clear from the comments below that is goes through *mutatis mutandis* with the complex points anywhere so long as the paths for the complex conjugate pairs of points are chosen symmetrically with respect to the real circle and so that the order of the paths is the same as that of our idealized picture.

Consider any description

$$\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_{r_1}, \sigma_{r_1+1,1}, \sigma_{r_1+1,2}, \dots, \sigma_{r_1+r_2,1}, \sigma_{r_1+r_2,2})$$

of the branch cycles for a cover $\phi\colon X \to \boldsymbol{P}_x^1$ defined over $\boldsymbol{R}$ and having the x's above as branch points, where the subscript labeling has been chosen to indicate that the entries correspond in order to the given branch points.

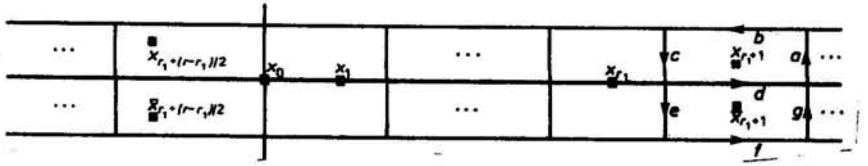

Fig. 2. A band about $\boldsymbol{P}_x^1(\boldsymbol{R})$ containing $x_1, \dots, x_r$ ($\varrho_{r_1+1,1} = abcd$ and $\varrho_{r_1+1,2} = d^{-1}efg$)

In Figure 2, x_0 is the intersection of the left side of the rectangle around x_1 with the x-axis (where the surrounding band is sufficient to encompass the complex conjugate points, labeled with $r_1+1, \dots, r$; these start from the right and continue around to the left). Use the u's along the top of the band, and ϱ_i (resp., $\varrho_{i,1}$ and $\varrho_{i,2}$) the counterclockwise path around the rectangle surrounding x_i, $i = 1, \dots, r_1$ (resp., x_i and $\bar{x}_i$, $i = r_1+1, \dots, r_1+r_2$) to form γ's as was done with Figure 1 in § 2.1.

Consider the paths

$$\gamma_1, \dots, \gamma_{r_1}, \gamma_{r_1+1,1}, \gamma_{r_1+1,2}, \dots, \gamma_{r_1+r_2,1}, \gamma_{r_1+r_2,2},$$

chosen in this order so that product is homotopic to 1, given by

$$u_{r_1+r_2} \dots u_{j+1} \varrho_j (u_{r_1+r_2} \dots u_{j+1})^{-1} = \gamma_j, \quad j = 1, \dots, r_1,$$

$$u_{r_1+r_2} \dots u_{j+1} \varrho_{j,1} (u_{r_1+r_2} \dots u_{j+1})^{-1} = \gamma_{j,1},$$

$$u_{r_1+r_2} \dots u_{j+1} \varrho_{j,2} (u_{r_1+r_2} \dots u_{j+1})^{-1} = \gamma_{j,2}, \quad j = r_1+1, \dots, r_1+r_2.$$

Denote $\gamma_{j,1} \gamma_{j,2}$ by $\gamma_{j,.}$, $j = r_1+1, \dots, r_1+r_2$; and denote the product $\gamma_{r_1+1,.} \cdots \gamma_{r_1+r_2,.}$ by $\gamma_.$. As in Lemma 2.2 of § 2.1, applying complex conjugation to the γ's gives these results: $\bar{\gamma}_1, \dots, \bar{\gamma}_{r_1}$ are respectively homotopic to

$$(2.5a)\quad \gamma_1^{-1},\ (\gamma_3\ldots\gamma_{r_1}\gamma_{\cdot})^{-1}\gamma_2^{-1}(\gamma_3\ldots\gamma_{r_1}\gamma_{\cdot}),\ \ldots$$

$$\ldots,\ (\gamma_{r_1}\gamma_{\cdot})^{-1}\gamma_{r_1-1}^{-1}\gamma_{r_1}\gamma_{\cdot},\quad \gamma_{\cdot}^{-1}\gamma_{r_1}^{-1}\gamma_{\cdot};$$

and $\bar{\gamma}_{r_1+1,1}$, $\bar{\gamma}_{r_1+1,2}$, $\ldots$, $\bar{\gamma}_{r_1+r_2,1}$, $\bar{\gamma}_{r_1+r_2,2}$ are respectively homotopic to

$$(2.5b)\quad (\gamma_{r_1+2,\cdot}\cdots\gamma_{r_1+r_2,\cdot})^{-1}\gamma_{r_1+1,2}^{-1}(\gamma_{r_1+2,\cdot}\cdots\gamma_{r_1+r_2,\cdot}),$$

$$(\gamma_{r_1+2,\cdot}\cdots\gamma_{r_1+r_2,\cdot})^{-1}\gamma_{r_1+1,1}^{-1}(\gamma_{r_1+2,\cdot}\cdots\gamma_{r_1+r_2,\cdot}),\quad \ldots,$$

$$\gamma_{r_1+r_2,2}^{-1},\gamma_{r_1+r_2,1}^{-1}.$$

Now define σ's in the notation above to be $T(\gamma)$'s, to get a branch cycle description of the cover $X \to \boldsymbol{P}_x^1$. Similarly to the above notation denote $\sigma_{j,1}\sigma_{j,2}$ by $\sigma_{j,\cdot}$, $j = r_1+1, \ldots, r_1+r_2$; and denote the product $\sigma_{r_1+1,\cdot}\ldots\sigma_{r_1+r_2,\cdot}$ by $\sigma_{j,\cdot}$.

Application of Lemma 2.1 and the computation above gives (in analogy with Lemma 2.2) an element $c_{x_0} = c \in N_{S_n}(G)$ such that

$$(2.6a)\quad c\sigma_1 c = \sigma_1^{-1},\quad c\sigma_2 c = (\sigma_3\ldots\sigma_{r_1}\sigma_{\cdot})^{-1}\sigma_2^{-1}(\sigma_3\ldots\sigma_{r_1}\sigma_{\cdot}),\ \ldots$$

$$\ldots,\quad c\sigma_{r_1-1}c = (\sigma_{r_1}\sigma_{\cdot})^{-1}\sigma_{r_1-1}^{-1}\sigma_{r_1}\sigma_{\cdot},\quad c\sigma_{r_1}c = \sigma_{\cdot}^{-1}\sigma_{r_1}^{-1}\sigma_{\cdot};$$

and

$$(2.6b)\quad c\sigma_{r_1+1,1}c = (\sigma_{r_1+2,\cdot}\cdots\sigma_{r_1+r_2,\cdot})^{-1}\sigma_{r_1+1,2}^{-1}(\sigma_{r_1+2,\cdot}\cdots\sigma_{r_1+r_2,\cdot}),$$

$$c\sigma_{r_1+1,2}c = (\sigma_{r_1+2,\cdot}\cdots\sigma_{r_1+r_2,\cdot})^{-1}\sigma_{r_1+1,1}^{-1}(\sigma_{r_1+2,\cdot}\cdots\sigma_{r_1+r_2,\cdot}),\quad \ldots,$$

$$c\sigma_{r_1+r_2,1}c = \sigma_{r_1+r_2,2}^{-1},\quad c\sigma_{r_1+r_2,2}c = \sigma_{r_1+r_2,1}^{-1}.$$

§2.3. The main theorem and condition (1.3). We now state our main theorem. In particular it includes the statement of (1.3) of Theorem 1.1.

THEOREM 2.4. *Consider a cover $\phi: X \to \boldsymbol{P}_x^1$ defined over $\boldsymbol{R}$ and having $x_1, \ldots, x_r \in \boldsymbol{C} \cup \infty$ as its branch points. With the choices of ordering on the branch points $x_1, \ldots, x_{r_1} \in \boldsymbol{R}$ made above and with respect to the paths of Figure 2, let $(\sigma_1, \ldots, \sigma_r)$ be the description of the branch cycles of the cover given above. Denote the Galois closure of the function field extension $\boldsymbol{R}(X)/\boldsymbol{R}(x)$ by $\hat{E}$, and the Galois group $G(\hat{E}/\boldsymbol{R}(x))$ by $\hat{G} \overset{\text{def}}{=} \hat{G}_{\boldsymbol{R}}$. It is a subgroup of $N_{S_n}(G)$. For each value of $x_0 \in \boldsymbol{P}^1(\boldsymbol{R})$ different from $x_1, \ldots, x_{r_1}$, there is an element $c = c_{x_0} \in G(\hat{E}/\boldsymbol{R}(x))$ such that c can be identified with the action of complex conjugation in the residue class field of a prime of $\hat{E}$ above x_0 and thereby with an element of $N_{S_n}(G)$. In the induced action of complex conjugation on the points of X this element is determined by the formulas of (2.6) up to an involution in the center of $N_{S_n}(G)$.*

Furthermore, if c is the identity (i.e., the fiber $\phi^{-1}(x_0)$ consists only of real points), $\alpha_i = \sigma_1\ldots\sigma_i$ is of order 2, $i = 1, \ldots, r_1 - 1$.

Proof. The first paragraph is an immediate consequence of Lemmas 2.1 and 2.2. The element c is identified with a generator of the decomposition group of a place of the function field $\hat{E}$ that lies over x_0. In particular, it must be an element of $\hat{G}$. Our next task is to show that the formulas that result from (2.6) in the case that $c = 1$ give the result on the α's. We inductively deduce this from (2.6): $i = 1$ is already in (2.6). The rest of the argument is mere combinatorics from (2.6) and from the formula $\sigma_1\ldots\sigma_r = 1$. Since the last $2r_2$ of the σ's, being paired up next to their inverses, disappear from the formula $\sigma_1\ldots\sigma_r = 1$, with no loss we may assume in the rest of our calculations that $r = r_1$. From the product of the σ's equal to 1, $(\sigma_1\sigma_2)^{-1} = \sigma_3\ldots\sigma_r$. Plug this into the relation $\sigma_3\ldots\sigma_r = \sigma_2^{-1}(\sigma_3\ldots\sigma_r)\sigma_2^{-1}$. This immediately gives $(\sigma_1\sigma_2)^2 = 1$. The induction continues quite easily on the same principles. ∎

Note. *Special case*. Assume that $r = 3$ and that two of the branch points are complex conjugate. Let $\boldsymbol{\sigma}$ be a description of the branch cycles of $\phi: X \to \boldsymbol{P}_x^1$ relative to the paths of Figure 2. The effect of complex conjugation on the residue class fields of the points above x_0 is given by $c = c_{x_0} \in \hat{G} \subset N_{S_n}(G)$ with these properties:

$$c\sigma_1^{-1}c = \sigma_1 \quad\text{and}\quad c\sigma_2^{-1}c = \sigma_3.$$

In particular, if $c = 1$, then $\sigma_1^2 = 1$ and $\sigma_2\sigma_3 = 1$. But this gives $\sigma_1 = 1$, contrary to our assumptions. Thus, in the case that two of the branch points are complex conjugate, c is different from 1. ∎

§2.4. The branch cycle argument and (1.3) and (1.4). We now explain the extra conditions that are forced on the conjugacy classes $\mathbf{C}$ under the assumption that the Galois closure of a cover associated to them is defined over $\boldsymbol{R}$ (resp., $\boldsymbol{Q}$). Again, we use the notation that the coordinate entries of $\mathbf{C}$ are conjugacy classes of the transitive subgroup G of S_n defined by a description $\boldsymbol{\sigma}$ of the branch cycles of a cover. As in §1.1 let N denote the least common multiple of the orders of the elements in the conjugacy classes C_i, $i = 1, \ldots, r$. For each $k \in (\boldsymbol{Z}/N)^*$ we define a unique conjugacy class C_i^k of G by putting each element of 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. Let $\sigma \in S_r$ act on $\mathbf{C}$ by permuting the coordinates. Denote the result by ${}^{\sigma}\mathbf{C}$. Recall that $N_{S_n}(G)$ acts by conjugation on $\mathbf{C}$ to give a new r-tuple of conjugacy classes. Also, $\mathbf{C} \bmod N_{S_n}(G)$ denotes the ordered collections of r-tuples of conjugacy classes $\gamma\mathbf{C}\gamma^{-1}$, $\gamma \in N_{S_n}(G)$.

Suppose that the cover $X \to \boldsymbol{P}^1$, defined over a field K has a description of its branch cycles associated to $\mathbf{C}$. Retain the association of x_i with the conjugacy class C_i, $i = 1, \ldots, r$. Regard $G(K(\mathbf{x})/K)$ as a subgroup of S_r through the action of its elements on the r-tuple $\mathbf{x} = (x_1, \ldots, x_r)$. Similarly, regard $G(K(\zeta_N)/K)$ as a subgroup of $(\boldsymbol{Z}/N)^*$. Here ζ_N is a primitive Nth root of 1. As earlier denote the Galois closure of the field extension $K(X)/K(x)$ by $\hat{E}$ and its Galois group by $\hat{G}$. The elements γ of $\hat{G}$ satisfy $\gamma\mathbf{C}\gamma^{-1} = {}^{\sigma}\mathbf{C}^k$ for some $\sigma \in S_r$ and $k \in (\boldsymbol{Z}/N)^*$. More precisely, consider the group

(2.7) $\bar{G} = \{\gamma \in N_{S_n}(G) \mid \gamma \mathbf{C} \gamma^{-1} = {}^{\sigma}\mathbf{C}^k, (\sigma, k) \in S_r \times (\mathbf{Z}/N)^*$ and there exists $\tau \in G(\bar{K}/K)$ with $\tau_{|K(\mathbf{x})} = \sigma, \tau_{|K(\zeta_N)} = k\}$.

Then $\hat{G} \subset \bar{G}$ [Fr 1; p. 33, Prop. 2].

Definition 2.5. The branch points $\mathbf{x}$ and the conjugacy classes $\mathbf{C}$ are said to be *Galois compatible* (over K) if for each $\tau \in G(\bar{K}/K)$, if τ permutes the x_i's as $\bar{\tau} \in S_r$, then for $k = k_\tau$ the image of τ in $G(K(\zeta_N)/K)$,

(2.8) $C_i^k = \gamma C_{(i)\bar{\tau}} \gamma^{-1}$ for some $\gamma \in \hat{G}$ (independent of i), $i = 1, \ldots, r$.

The next result is a rephrasing of the *branch cycle argument* of [Fr 1; p. 61].

Proposition 2.6. *Suppose that the cover $X \to \mathbf{P}^1$ has a description of its branch cycles associated to $\mathbf{C}$. Then Galois compatibility of $\mathbf{x}$ and $\mathbf{C}$ (over K) is a necessary condition that the field of definition of the cover actually be K. Furthermore, if the cover is g-regular* (§ 1.1), *then for each $k \in (\mathbf{Z}/N)^*$, there exists $\sigma \in G(K(\mathbf{x})/K)$ $(\subseteq S_r)$ such that $\mathbf{C}^k \equiv {}^{\sigma}\mathbf{C}$.*

With this we show that we have completed the necessary ingredients for the proof for Theorem 1.1. The proof of Theorem 2.4 gives (1.3) by applying complex conjugation as given by -1. In order to get (1.4) note that the g-regularity assumption just means that $\hat{G} = G$. Thus we choose any k relatively prime to N and consider whether $O(C_i)$ contains C_i^k. For any $\tau \in G(\bar{K}/K)$ apply (2.8) to conclude that this is so. Since this works for any k with the stated properties, we are done.

This section concludes with an example that will appear again in § 4.1. It is a warmup, too, to the definition of Nielsen class in the next section.

Example 2.7. *Comparison of all real branch points with complex conjugate branch points.* As in § 1.1, consider covers ϕ: $X \to \mathbf{P}^1$ which have associated to them a description of the branch cycles $\boldsymbol{\sigma}$ with $r = 3$, group $G = A_4$, and conjugacy classes $\mathbf{C}$ given as follows: C_1 is the conjugacy class of a 3-cycle; C_2 is the conjugacy class of elements inverse to those of C_1; and C_3 the conjugacy class of a product of two 2-cycles. Inside of A_4 the 3-cycles form two conjugacy classes: a 3-cycle and its inverse are in different conjugacy classes. These are permuted by the action of $N_{S_4}(G) = S_4$. Thus from Proposition 2.6, if our cover is defined over $\mathbf{R}$ (resp., $\mathbf{Q}$), and if it has real branch points (since $\mathbf{R}(\mathbf{x}) = \mathbf{R}$), then its Galois closure must contain $\mathbf{C}$ (resp., be defined over $\mathbf{Q}(\zeta_3)$, $\zeta_3 = e^{2\pi\sqrt{-1}/3}$).

Suppose that C_1 is represented by (1 2 4). Compute the complete list of possible branch cycle descriptions, up to equivalence, that have representatives in the respective order of C_1, C_2, C_3. In § 3.1 this will be called an *absolute straight Nielsen class.* This list consists of exactly one element represented by

$$\boldsymbol{\sigma} = ((1\,2\,4), (1\,2\,3), (1\,3)(2\,4)).$$

It is easy to see that there is a natural family of covers defined over $\mathbf{Q}$ containing exactly once a representative cover of each equivalence class of covers. Indeed, these are parametrized by the covering of $\mathbf{P}^3 \backslash D_3 = \mathscr{U}^3$ which has function field F equal to the fixed field in $\mathbf{Q}(x_1, x_2, x_3)$ of the automorphism that switches x_1 and x_2: $F = \mathbf{Q}(x_1 x_2, x_1 + x_2, x_3)$. Any $\mathbf{Q}$-rational point of this rational variety gives us one of the desired covers ϕ: $X \to \mathbf{P}_x^1$. Because it suits applications in § 4.3 so well, we intend to consider such a cover where x_3, the branch point corresponding to C_3, is ∞. For the rest of the example consider the two possibilities for the placement of the other branch points.

Case 1. *x_1 and x_2 are real.* We compute $c_{x_0} = c$ according to Theorem 2.4. There are 3 cases depending on the interval in which we choose x_0. But in each case these are determined by the property that c conjugates a pair of elements from the entries of $\boldsymbol{\sigma}$ to their inverses. This gives these possibilities for c:

(2 4) for $x_0 \in (\infty, x_1)$; (1 2) for $x_0 \in (x_1, x_2)$; and (1 3) for $x_0 \in (x_2, \infty)$.

Case 2. *x_1 and x_2 are complex conjugate.* From Theorem 2.4 there is only one possibility for c. It conjugates each of (1 2 4) and (1 2 3) to the inverse of the other, and it conjugates (1 3)(2 4) to itself. Thus $c = (1\,2)(3\,4)$. ∎

§ 3. Rigidity and a converse to Theorem 1.1

If in Theorem 2.4 for some choice of x_0 the element c is the identity (i.e., complex conjugation acts trivially on the fiber of the cover) we refer to the cover, and its associated group G, in Theorem 2.4 as *exceptional.* We have already listed what happens in the case when $r = 3$ in § 1.3. There are results for each of the fields $K = \mathbf{R}$ and $K = \mathbf{Q}$ in Theorem 2.4. Denote the exceptional list of groups having associated $\mathbf{C}$ for which c_{x_0} comes out to be 1 satisfying condition (1.3) (resp., also, (1.4)) by $\mathscr{E}_{\mathbf{R},r}$ (resp. $\mathscr{E}_{\mathbf{Q},r}$). For example, Proposition 1.2 shows that there are just four groups in $\mathscr{E}_{\mathbf{Q},3}$.

The problems that we consider in this section start with describing some of the groups (with associated conjugacy classes $\mathbf{C}$) that appear in $\mathscr{E}_{\mathbf{Q},4}$ $(r = 4)$. In particular, $\mathscr{E}_{\mathbf{Q},4}$ contains S_n and A_n for each $n \geqslant 4$. Then we want to consider some of these examples for whether there are actual covers ϕ: $X \to \mathbf{P}^1$ associated to this data that are defined over $\mathbf{Q}$ that satisfy the hypotheses of Theorem 1.1. In this case we would realize the given group as a totally real Galois extension of $\mathbf{Q}$. For simplicity we consider only the case where the cover has all of its branch points real (i.e., $r_1 = r$ in § 2). Our special case of concentration is S_5 in the case $r = 4$. Here is a reminder of the conditions in terms of generators.

For covers and branch points over $\mathbf{R}$ the following hold for exceptional $\boldsymbol{\sigma}$:

(3.1a) G is generated by α_i, $i = 1, \ldots, r-1$, all of order 2; and

(3.1b) $\sigma_i = \alpha_{i-1}\alpha_i$, $i = 2, \ldots, r-1$, and $\sigma_r = \alpha_{r-1}$.

For covers and branch points over $\mathbf{Q}$, there would be one further condition:

(3.1c) σ_i is in a rational conjugacy class of G, $i = 1, \ldots, r$ (and $\sigma_1^2 = \sigma_r^2 = 1$).

Of necessity we must now recall some basics related to the problem.

§ 3.1. Nielsen classes and Hurwitz monodromy groups. This is the classical discussion of maps of degree n from curves of genus g to projective 1-space. It gives us more discrete data for a cover, called a *Nielsen class*, that we shall regard as being fixed in the consideration of any family of covers. Suppose that $\{x_1, \dots, x_r\}$ consists of distinct points of $\boldsymbol{P}_x^1$. For any element $\boldsymbol{\sigma} \in S_n^r$ denote the group generated by its coordinate entries by $G(\boldsymbol{\sigma})$.

Consider ϕ: $X \to \boldsymbol{P}_x^1$, ramified only over $\boldsymbol{x}$, up to the relation that regards ϕ: $X \to \boldsymbol{P}_x^1$ and ϕ': $X' \to \boldsymbol{P}_x^1$ as equivalent if there exists a homeomorphism λ: $X \to X'$ such that $\phi' \circ \lambda = \phi$. These equivalence classes are in one-one correspondence with

$$\{\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_r) \in S_n^r |\ \sigma_1 \dots \sigma_r = 1,\ G(\boldsymbol{\sigma}) \text{ is a transitive subgroup of } S_n\}$$

modulo the relation that regards $\boldsymbol{\sigma}$ and $\boldsymbol{\sigma}'$ as equivalent if $\gamma \boldsymbol{\sigma} \gamma^{-1} = \boldsymbol{\sigma}'$ for some $\gamma \in S_n$. This correspondence goes under the heading of Riemann's existence theorem [Gro]. (In most practical situations we shall mean that there truly is ramification over each of the branch points x_i, $i = 1, \dots, r$.)

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: the branch points $\boldsymbol{x}$ run over the set $(\boldsymbol{P}_x^1)^r \backslash \Delta_r$ with Δ_r the r-tuples with two or more coordinates equal. The key definition is of a Nielsen class. This is part and parcel of the formulations of "rational rigidity" and its generalizations (§ 3.2).

Suppose that T: $G \to S_n$ is any faithful transitive permutation representation of a group G. Let $\mathbf{C} = (C_1, \dots, C_r)$ 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. Denote the subgroup of S_n that permutes the entries of $\mathbf{C}$ (a subgroup of the normalizer of G) by $N_{S_n}(\mathbf{C})$.

Definition 3.1. The *Nielsen class* of $\mathbf{C}$ is

$$\{\boldsymbol{\tau} \in G^r |\ G(\boldsymbol{\tau}) = G, \text{ there exists } \beta \in S_r \text{ with } \tau_{(i)\beta} \in C_i,$$
$$i = 1, \dots, r \text{ and } \tau_1 \dots \tau_r = 1\}.$$

Denote this by $\mathrm{Ni}(\mathbf{C})$. The *straight Nielsen class* is defined the same way, except that it does not include the permutation of the conjugacy classes:

$$\mathrm{SNi}(\mathbf{C}) \overset{\text{def}}{=} \{\boldsymbol{\tau} \in G^r |\ G(\boldsymbol{\tau}) = G,\ \tau_i \in C_i,\ i = 1, \dots, r \text{ and } \tau_1 \dots \tau_r = 1\}.$$

The quotient of $\mathrm{Ni}(\mathbf{C})$ by $N_{S_n}(\mathbf{C})$ is denoted $\mathrm{Ni}(\mathbf{C})_T^{\mathrm{ab}}$, and it is called the *absolute Nielsen class* of $\mathbf{C}$. Similarly there are *absolute straight Nielsen classes* by replacing $N_{S_n}(\mathbf{C})$ by the appropriate subgroup.

Consider canonical generators $\gamma_1, \dots, \gamma_r$ of the fundamental group $\pi_1(\boldsymbol{P}_x^1 - \boldsymbol{x}, x_0)$ (e.g., those used in the proof of Lemma 2.2). We say that a cover ramified only over $\boldsymbol{x}$ is in $\mathrm{Ni}(\mathbf{C})$ if the classical representation of the fundamental group sends the respective canonical generators to an r-tuple $\boldsymbol{\sigma} \in \mathrm{Ni}(\mathbf{C})$.

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

(3.2a) $Q_i Q_{i+1} Q_i = Q_{i+1} Q_i Q_{i+1}$, $\quad i = 1, \dots, r-2;$

(3.2b) $Q_i Q_j = Q_j Q_i$, $\quad 1 \leqslant i < j-1 \leqslant r-1;$

(3.2c) $Q_1 Q_2 \dots Q_{r-1} Q_{r-1} \dots Q_1 = 1.$

Relations (3.2a) and (3.2b) alone give the Artin braid group B_r. It is relation (3.2c) that indicates involvement with projective algebraic geometry. The Artin braid group is the fundamental group of $\boldsymbol{A}^r - D_r$ while the Hurwitz monodromy group is the fundamental group of $\boldsymbol{P}^r - D_r$. Here D_r is the classical discriminant locus in the respective spaces. The natural embedding of $\boldsymbol{A}^r$ in $\boldsymbol{P}^r$ 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 commutative diagram:

(3.3)
$$\begin{tikzcd}
\boldsymbol{A}^r \backslash \Delta_r \arrow[r] \arrow[d, "\Psi_r"'] & (\boldsymbol{P}^1)^r \backslash \Delta_r \arrow[d, "\Psi_r"] \\
\boldsymbol{A}^r \backslash D_r \arrow[r] & \boldsymbol{P}^r \backslash D_r
\end{tikzcd}$$

where the map Ψ_r can be regarded as the quotient action of S_r acting as permutations on the coordinates of $(\boldsymbol{P}^1)^r$. The respective fundamental groups in the upper row of (3.3) will be called here the *straight Artin braid* and *Hurwitz monodromy groups*:

(3.4) $SH_r = \pi_1((\boldsymbol{P}^1)^r \backslash \Delta_r, \boldsymbol{x}_0)$ is the kernel of the homomorphism Ψ_r^*: $H_r \to S_r$ that maps Q_i to $(i\ i+1)$, $i = 1, \dots, r-1$.

Production of a moduli space. In our final topic we consider how Hurwitz monodromy action on Nielsen classes defines a moduli space. From the relations we compute that H_r acts on the absolute Nielsen classes by extension of the following formula:

(3.5)
$$(\tau_1, \dots, \tau_r) Q_i = (\tau_1, \dots, \tau_{i-1}, \tau_i \tau_{i+1} \tau_i^{-1}, \tau_i, \tau_{i+2}, \dots, \tau_r).$$

In the notation above we say that ϕ_T: $X_T \to \boldsymbol{P}_x^1$ is in the absolute Nielsen class $\mathrm{Ni}(\mathbf{C})_T^{\mathrm{ab}}$.

Exercise. Let $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_r)$ be an r-tuple of elements of G with $\sigma_1 \dots \sigma_r = 1$. There exists $Q \in SH_r$ such that the r-tuple given by applying Q to the r-tuple $(\sigma_1^{-1}, \dots, \sigma_r^{-1})$ is the r-tuple with entries the right hand terms in formula (2.4) of § 2.1.

Solution. Take Q for example to be

$$(Q_{r-1} Q_{r-2} \dots Q_1)(Q_{r-1} Q_{r-2} \dots Q_2) \dots (Q_{r-1} Q_{r-2}) Q_1. \ \blacksquare$$

Any permutation representation of a fundamental group defines a cover of the space. Denote the cover corresponding to the action of H_r on $\mathrm{Ni}(\mathbf{C})_T^{\mathrm{ab}}$ by

(3.6)
$$\Psi(\mathbf{C})\colon \mathscr{H}(\mathbf{C})_T \to \boldsymbol{P}^r \backslash D_r.$$

That is, an absolute Nielsen class $\mathrm{Ni}(\mathbf{C})_T^{\mathrm{ab}}$ defines a *moduli space* $\mathscr{H}(\mathbf{C})_T$ of covers $\phi_T\colon X_T \to \boldsymbol{P}_x^1$ of degree equal to $\deg(T)$ in that Nielsen class [Fr 1; § 4]. For each point $\boldsymbol{m} \in \mathscr{H}(\mathbf{C})_T$ choose a point $\boldsymbol{x} \in (\boldsymbol{P}^1)^r \setminus \Delta_r$ such that $\boldsymbol{x}^* = \Psi_r(\boldsymbol{x}) = \Psi(\mathbf{C})(\boldsymbol{m})$. The cardinality of $\Psi(\mathbf{C})^{-1}(\boldsymbol{x}^*)$ is $|\mathrm{Ni}(\mathbf{C})_T^{\mathrm{ab}}|$. Thus $\boldsymbol{m}$ corresponds to exactly one equivalence class of covers of $\mathrm{Ni}(\mathbf{C})_T^{\mathrm{ab}}$. A representative cover $\phi_{\boldsymbol{m}}\colon X_{\boldsymbol{m}} \to \boldsymbol{P}_x^1$ has coordinates $\boldsymbol{x} \in (\boldsymbol{P}^1)^r$ for its branch points. We often drop the decorative subscript T.

PROPOSITION 3.2. *The algebraic set $\mathscr{H}(\mathbf{C})_T$ is irreducible if and only if it is connected, and this holds if and only if H_r is transitive on* $\mathrm{Ni}(\mathbf{C})_T^{\mathrm{ab}}$.

Proof. Since $\Psi(\mathbf{C})$ is unramified and $\boldsymbol{P}^r \setminus D_r$ is nonsingular, so is $\mathscr{H}(\mathbf{C})_T$. 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. ∎

§ 3.2. Generalizations of rigidity. The topic is how to check if there are covers in a given Nielsen class that are actually defined over $\boldsymbol{Q}$ (or $\boldsymbol{R}$). 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 non-Galois situations. Even if ultimate interest is in Galois extensions, it can be better to start with a non-Galois cover and go to the Galois closure. The strong "rigidity" conditions may be harder to satisfy in the non-Galois situation. But if they do hold, this implies the vanishing of an obstruction for the field of definition that is not easily checked from the Galois situation.

The point of the Hurwitz monodromy actions is this ([Fr 1,3,4] or [DFr] for details). Suppose that SH_r acts transitively on the straight Nielsen classes (§ 3.1), that $\mathrm{Cen}_{S_n}(G)$ is trivial, and that each of the conjugacy classes of $\mathbf{C}$ is rational. Then the cover (3.6), with the total space of representing covers for points of $\mathscr{H}(\mathbf{C})_T$, is defined over $\boldsymbol{Q}$.

$\boldsymbol{Q}$-points on Hurwitz spaces. In particular, existence of covers in the Nielsen class $\mathrm{Ni}(\mathbf{C})_T^{\mathrm{ab}}$ defined over $\boldsymbol{Q}$ is equivalent to existence of $\boldsymbol{Q}$-points on the Hurwitz space $\mathscr{H}(\mathbf{C})$. Two special assumptions appear in the next proposition (the first implies the second):

(3.7a) for each $k \in (\boldsymbol{Z}/N)^*$, $\mathbf{C}^k = \mathbf{C} \bmod N_{S_n}(G)$;

(3.7b) for each $k \in (\boldsymbol{Z}/N)^*$, there exists $\sigma \in S_r$ such that $\mathbf{C}^k \equiv {}^{\sigma}\mathbf{C} \bmod N_{S_n}(G)$.

Note that (3.7b) is a consequence of Galois compatibility of $\boldsymbol{x}$ and $\mathbf{C}$ over $\boldsymbol{Q}$ as in (2.8).

PROPOSITION 3.3. *Suppose that the cover $X \to \boldsymbol{P}_x^1$ corresponds to the point $\boldsymbol{m} \in \mathscr{H}(\mathbf{C})_T$ (as in Prop. 3.2). Assume that SH_r is transitive on the absolute straight Nielsen classes $\mathrm{SNi}(\mathbf{C})_T^{\mathrm{ab}}$ defined by $\mathbf{C}$ (§ 1.2). Assume also that one of the following holds: either G is in its regular representation and G has no center; or*

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

Then (3.7b) holds if and only if the intersection of all fields of definition of all covers $X \to \boldsymbol{P}_x^1$ in the Nielsen class $\mathrm{Ni}(\mathbf{C})$ is $\boldsymbol{Q}$. In the case that (3.7a) holds, the cover (3.6) is defined over $\boldsymbol{Q}$ and the field of definition of the cover $X \to \boldsymbol{P}_x^1$ is $\boldsymbol{Q}(\boldsymbol{m})$.

§ 3.3. S_n and A_n are in $\mathscr{E}_{\boldsymbol{Q},4}$. We discuss groups generated by elements of order 2.

DEFINITION 3.4. A finite group G is said to be *$(m_1, \dots, m_t)$-generated* if it is generated by elements $\{\alpha_1, \dots, \alpha_t\}$ with $\mathrm{ord}(\alpha_i) = m_i$, $i = 1, \dots, t$. We shorten this expression to m^t-generated if the m_i's are a constant function of i.

In seeking to find the exceptional groups in Theorem 2.4 we apply this definition to consider groups that are 2^{r-1}-generated for suitably small values of r. Of course all noncyclic simple groups are 2^{r-1}-generated for suitable values of r, but it is not exactly clear what value this would be; nor given a small value of r for which it is so, is it clear that we can find suitable generators α_i, $i = 1, \dots, r-1$ so that (3.1c) holds. Proposition 3.6 says that $r = 4$ works for S_n and for A_n. The referee suggested [F] for a proof of the following result.

LEMMA 3.5. *Consider an element $\sigma \in A_n$ with $n \geqslant 2$. Suppose that the disjoint cycle decomposition of σ has the shape $(s_1) \dots (s_u)$ (counting the cycles of length 1) with $s_1 \leqslant s_2 \leqslant \dots \leqslant s_u$. If $s_i = s_{i+1}$ for some i, or if one of the s_i's is odd, then the conjugacy class of σ is rational. Note that it may be rational even if neither is satisfied.*

PROPOSITION 3.6. *For $n \geqslant 4$, S_n and A_n are both 2^3-generated, and both are in $\mathscr{E}_{\boldsymbol{Q},4}$.*

Proof. We chose S_n and A_n because in the former case all conjugacy classes are rational, and in the latter case Lemma 3.5 shows nearly all of them to be so. Suppose that we have obtained the dihedral group D_{n-1} of order $2(n-1)$ as a subgroup of S_{n-1}. Since D_{n-1} has an $(n-1)$-cycle in S_{n-1}, the group $\langle D_{n-1}, (1\,n) \rangle$ must be S_n: it is a doubly transitive group containing a 2-cycle. There are two cases to deal with here: n odd and n even. In the former case use

$$\alpha_1 = (1\,2)(3\,4) \dots (n-2\;\; n-1) \quad \text{and} \quad \alpha_2 = (2\,3)(4\,5)(6\,7) \dots (n-3\;\; n-2)$$

as generators of D_{n-1}; and in the latter case use

$$\alpha_1 = (1\,2)(3\,4) \dots (n-3\;\; n-2) \quad \text{and} \quad \alpha_2 = (2\,3)(4\,5)(6\,7) \dots (n-2\;\; n-1).$$

This finishes our discussion of S_n by taking $\alpha_3 = (2\;n)$ in (3.1).

The modified principle for A_n is based on the lemma that a primitive subgroup of A_n containing a 3-cycle must be all of A_n (e.g., [Car; p. 163 # 15]).

We consider separately each of the residue classes of n modulo 4, with the most difficult of these, $n \equiv 0 \bmod 4$, coming last. The α's here are as in (3.1).

Case 1. $n \equiv 1 \bmod 4$. Take the α's as follows:

$$\begin{aligned} \alpha_1 &= (1\,2)(3\,4)\ldots(n-2\;\, n-1),\\ \alpha_2 &= (1\,2)(4\,5)\ldots(n-1\;\, n),\\ \alpha_3 &= (2\,3)(4\,5)\ldots(n-1\;\, n). \end{aligned} \tag{3.8}$$

We will repeatedly use a simple principle: if α and α' are of order 2, $\operatorname{ind}(\alpha)+\operatorname{ind}(\alpha') = m-1$ and $\langle \alpha, \alpha' \rangle$ is transitive on m integers, then $\alpha\alpha'$ is an m-cycle on these integers. Apply this to (3.8) to conclude that $\alpha_1\alpha_3$ is an n-cycle; $\alpha_1\alpha_2$ is an $(n-2)$-cycle (on $\{3, \ldots, n\}$); and $\alpha_2\alpha_3$ is the 3-cycle $(1\,3\,2)$. Let $G = G(\boldsymbol{\alpha})$ be the group generated by the α's.

Note that conjugation of $(1\,3\,2)$ by $\alpha_3\alpha_1$ gives $(1\,3\,5)$. Also, $\alpha_1\alpha_2$ is an $(n-3)$-cycle on $\{3, \ldots, n\}$. Thus the subgroup of G that stabilizes 2 is transitive on the remainder of the integers. In particular, G is doubly transitive, and therefore primitive: $G = A_n$. To conclude that $A_n \in \mathscr{E}_{\boldsymbol{Q},4}$ we check that $\alpha_1\alpha_2$ and $\alpha_2\alpha_3$ are rational conjugacy classes. But both have repeated 1-cycles. Lemma 3.5 concludes this case.

Case 2. $n \equiv 3 \bmod 4$. This case has a twist that shows in our choice of α's:

$$\begin{aligned} \alpha_1 &= (1\,2)(3\,4)\ldots(n-4\;\, n-3),\\ \alpha_2 &= (2\,3)(4\,5)\ldots(n-5\;\, n-4)(n-3\;\, n-1),\\ \alpha_3 &= (n-3\;\, n-2)(n-1\;\, n). \end{aligned} \tag{3.9}$$

Here $\alpha_1\alpha_2$ (resp., $(\alpha_1\alpha_3)^2$) is an $(n-2)$-cycle (resp., 3-cycle) on $\{1, 2, \ldots, n-3, n-1\}$ (resp., $\{n-4, n-3, n-2\}$). As in Case 1, G is doubly transitive and therefore equal to $A_n \in \mathscr{E}_{\boldsymbol{Q},4}$.

Case 3. $n \equiv 2 \bmod 4$. This is even easier than the previous cases with the α's as follows:

$$\begin{aligned} \alpha_1 &= (1\;2)(3\,4)\ldots(n-3\;\, n-2),\\ \alpha_2 &= (n-4\;\, n-3)(n-1\;\, n),\\ \alpha_3 &= (2\,3)(4\,5)\ldots(n-4\;\, n-3)(n-2\;\, n-1). \end{aligned} \tag{3.10}$$

Here $\alpha_1\alpha_3$ is an $(n-1)$-cycle on $\{1, 2, \ldots, n-1\}$, and $(\alpha_2\alpha_3)^2$ is a 3-cycle on $\{n-2, n-1, n\}$. Conclude as previously.

Case 4. $n \equiv 0 \bmod 4$. Here we take the α's in a slightly more complicated way:

$$\begin{aligned} \alpha_1 &= (1\,2)(3\,4)\ldots(n-1\;\, n),\\ \alpha_2 &= (2\,3)(4\,5)\ldots\left(\frac{n}{2}\;\frac{n}{2}+1\right),\\ \alpha_3 &= \left(\frac{n}{2}+1\;\,\frac{n}{2}+3\right)\left(\frac{n}{2}+4\;\,\frac{n}{2}+5\right)\ldots(n\;\,1). \end{aligned} \tag{3.11}$$

Since $(\alpha_1\alpha_3)^2$ is the 3-cycle $\left(\frac{n}{2}\;\frac{n}{2}+1\;\,\frac{n}{2}+3\right) \overset{\text{def}}{=} \lambda$, our main difficulty is to show that the group G generated by the α's is primitive.

Suppose that

$$\{1, \ldots, n\} = V_1 \cup \ldots \cup V_t$$

is a partition of the integers from $1, \ldots, n$ into a system of imprimitivity for G: this is a disjoint union, and G acts as permutations of $V_1, \ldots, V_t$. Here is the principle we need for our next computation. If $\tau \in G$ is the 3-cycle $(a_1\,a_2\,a_3)$, then $\{a_1, a_2, a_3\} \subset V_i$ for some integer i. Indeed, because τ is transitive on the a's, the set of a's must consist of a union of any of the V's that it actually moves together with a subset of one of the V's. If τ moves any V_i the cardinality of the a's would have to be at least 4. Thus the only other possibility is that τ moves none of the V's.We use this principle by conjugating λ by various of the α's to get 3-cycles that show that one of the V's contains all of the integers.

Consider these elements in G, with $\alpha_{1,i} = \alpha_1\alpha_i$, $i = 2, 3$:

$$\alpha_{1,2} = \left(1\,3\,5\ldots\frac{n}{2}-1\;\,\frac{n}{2}+1\;\,\frac{n}{2}+2\;\,\frac{n}{2}\;\,\frac{n}{2}-2\ldots4\;2\right)\left(\frac{n}{2}+3\;\,\frac{n}{2}+4\right)\ldots(n-1\;\,n),$$

$$\alpha_{1,3} = (3\,4)\ldots\left(\frac{n}{2}-1\;\,\frac{n}{2}\right)\left(\frac{n}{2}+1\;\,\frac{n}{2}+2\;\,\frac{n}{2}+3\;\,\frac{n}{2}+5\;\ldots n-1\;1\;2\;n\;\,n-2\ldots\frac{n}{2}+4\right).$$

Note that the square of $\alpha_{1,3}$ (resp., $\alpha_{1,2}$) fixes $n/2$ (resp., $n/2+3$) and has $n/2+1$ and $n/2+3$ (resp., $n/2$ and $n/2+1$) next to each other in a cycle

$$\left(\frac{n}{2}+1\;\,\frac{n}{2}+3\;\,\frac{n}{2}+7\;\ldots\;a\;\ldots\frac{n}{2}+10\;\,\frac{n}{2}+6\right)$$

with $a = 1$ or 2 depending on whether $n/4$ is congruent to 0 modulo 2 (resp., $(\ldots n/2-7\;\; n/2-3\;\; n/2+1\;\; n/2\;\; n/2-4\ldots)$). Thus, repeated conjugates of λ by these cycles show that all of these integers are in the same V. This by itself gives $n/2+1$ integers in V.

Thus the group is primitive and since it contains a 3-cycle it is all of A_n. ∎

In Proposition 3.6 there are groups that would be exceptions to the general situation excluded by Theorem 2.4 under the condition that they arise as the geometric monodromy groups of Galois covers over K ($K = \boldsymbol{R}$ or $\boldsymbol{Q}$) with appropriate branch cycle conditions. Suppose that G is one of these groups with appropriate branch cycle generators $\boldsymbol{\sigma}$. In § 3.4 (Theorem 3.7) we apply this to explicit cases of Proposition 3.6. The reader will note that the theory is not restricted to $\boldsymbol{R}$ or $\boldsymbol{Q}$, but for simplicity we stick to these cases.

§ 3.4. Exceptional covers in Proposition 3.6. Take $\alpha_1, \alpha_2, \alpha_3$ from the first paragraph of the proof of Proposition 3.6. Here $G = S_n$. Let

$$\sigma_1 = \alpha_1, \quad \sigma_2 = \alpha_1\alpha_2, \quad \sigma_3 = \alpha_2\alpha_3 \quad \text{and} \quad \sigma_4 = \alpha_3,$$

as we already have done. The representatives of the Nielsen class have the property that if a cover $X \to \boldsymbol{P}_x^1$ (of degree n) in this Nielsen class is defined over

$\boldsymbol{Q}$, then there would be (lots of) points $x_0 \in \boldsymbol{P}_x^1(\boldsymbol{R})$ distinct from the branch points of the cover such that the points of X over x_0 are all real. Because the group is S_n, it is immediate that the Galois closure $\hat{X} \to \boldsymbol{P}_x^1$ is geometrically irreducible and has group S_n. Thus it would realize this Nielsen class with $r = 4$ as an exception over $\boldsymbol{Q}$ to the general complex residue class property of Theorem 2.4.

What we will see is that all of the example Nielsen classes of Proposition 3.6 are tantalizingly close to being exceptions over $\boldsymbol{Q}$. The obstruction to completing this, for each n, lies in finding $\boldsymbol{Q}$-rational points on a curve Y_n for which we have a great deal of information about its presentation as a 3-branch point cover of the sphere defined over $\boldsymbol{Q}$ (Theorem 3.7). Indeed, the curve can be described as a quotient of the upper half plane by a "noncongruence subgroup" of $\mathrm{SL}(2, \boldsymbol{Z})$, similar to the examples of [Fr 4; Theorems 5.6 and 5.9]. What we demonstrate is that for $n = 4$ and 5 the curve Y_n is a genus 0 curve. The values of n for which this curve is of genus 0 are $4 \leqslant n \leqslant 9$ (cf. § 0).

Suppose that $\mathscr{H}(\mathrm{C})_T$ is the parameter space of covers in this Nielsen class (Part 3 below). We show that the group SH_4 acts transitively on the absolute straight Nielsen classes. With this, the cover $X \to \boldsymbol{P}_x^1$ above is defined over $\boldsymbol{Q}(\boldsymbol{m})$ with $\boldsymbol{m} \in \mathscr{H}(\mathrm{C})_T$ the point corresponding to the equivalence class of the cover. Thus we are reduced to finding a (any) rational point on $\mathscr{H}(\mathrm{C})_T$.

Our first task is to conveniently display the straight absolute Nielsen classes when $n = 5$. The following discussion has three parts leading up to Theorem 3.7.

Part 1. *Preparation for the listing.* Multiplications of elements in left-right notation tend to be more transparent if the shapes of the first elements being multiplied are easily visualized. Although the notation of Proposition 3.6 has them in a different order, we therefore choose representatives of the Nielsen class to have σ_1 a 4-cycle, σ_2 a 2-cycle, σ_3 a 3-cycle, and σ_4 a product of two 2-cycles. For example, replace the σ's above in the given order by

$$\sigma_4 \sigma_1 \sigma_4^{-1}, \sigma_4, \sigma_2, \sigma_3.$$

Now let us look at any 4-tuple $\boldsymbol{\tau}$ in the straight Nielsen class. Conjugating by an element of S_n allows us to assume that $\tau_1 = (1\,2\,3\,4)$. If we follow this by conjugation by a power of τ_1 we may assume that $\tau_2 = (1\,a)$ with the choices for a divided into the case $a = 5$ and the cases $a = 2$ or 3.

Consider the values of $a \neq 5$, all of which turn out to give representatives. First: $\tau_1 \tau_2 = (1\;2 \ldots a-1)(a\;a+1 \ldots 4)$ and $\tau_3 \tau_4$ is the inverse of this. If 5 disappears from the product of τ_3 and τ_4, then 5 appears in τ_3 in the 3-cycle.

For the case $a = 3$, $\tau_3 = (5\,2\,1)$ and $\tau_4 = (2\,5)(3\,4)$. For $a = 2$ we consider the appearance of 1 in τ_3 or τ_4. If it appears in the 3-cycle of τ_3, then by conjugation by $(2\,3\,4)$ we may assume that the 3rd integer in the 3-cycle is 2. Wherever it is, $\tau_3 \tau_4$ is forced to send 1 to 2 or to send 2 to 1, contrary to what $\tau_1 \tau_2$ does.

Part 2. *Notation for the display.* For a moment exclude the case $a = 5$. In the display below there is a *leader notation* $L_{1,a}$ (for $a = 2$ or 3). This indicates that we are displaying a *representative* for the values of τ_3 and τ_4 that goes along with the corresponding values of τ_1 and τ_2. Recall that since the product of all of the τ's is 1, the product of τ_3 and τ_4 is the inverse of $(1 \ldots a-1)(a \ldots 4)$. From the combinatorics above, we obtain the complete list of possibilities for τ_3 and τ_4 that should appear in the line $L_{c,a}$ by conjugating (just) τ_3 and τ_4 by

$$\{(1 \ldots a-1)^r (a \ldots 4)^s \mid r \in \boldsymbol{Z}/(a-1) \text{ and } s \in \boldsymbol{Z}/(5-a)\}.$$

For the case $a = 5$ the conjugation is by the powers of $(1\,2\,3\,4\,5)$, but there is also an additional notation in place of the c for a parameter b, which is just 3 in the case $n = 5$.

Part 3. *Quotation of* [Fr 4] (or [FrT]). We briefly review the results of § 4.1 of [Fr 4] (or § 3.2 of [FrT]). The 4 conjugacy classes defining the Nielsen class of S_5 with which we deal are all distinct. This simplifies considerably the theory of such families of covers. In particular, transitivity of SH_4 on the list described by Part 2 above is equivalent to transitivity of the subgroup generated by the following set of elements (§ 3.1):

$$a_{1,2} = Q_1^2, \quad a_{1,3} = Q_1^{-1} Q_2^2 Q_1, \quad a_{1,4} = Q_1^{-1} Q_2^{-1} Q_3^2 Q_2 Q_1. \tag{3.12}$$

If we show transitivity of the group generated by these elements, then Proposition 3.3 implies that any cover $X \to \boldsymbol{P}_x^1$ in this Nielsen class is defined over $\boldsymbol{Q}(\boldsymbol{m})$ where $\boldsymbol{m}$ is the point of the Hurwitz space ($\mathscr{H}(\mathrm{C})_T$ of Proposition 3.2) that corresponds to the cover. Furthermore, there is a cover

$$\psi_n\colon Y_n \to \boldsymbol{P}_x^1, \quad \text{ramified over just } 0, 1, \infty$$

defined over $\boldsymbol{Q}$ such that $\mathscr{H}(\mathrm{C})_T(\boldsymbol{Q})$ is nonempty if and only if

$$Y_n(\boldsymbol{Q}) - \{\psi_n^{-1}(0), \psi_n^{-1}(1), \psi_n^{-1}(\infty)\} \tag{3.13}$$

is nonempty. Finally, this cover has these further properties:

(3.14a) it can be identified with the projective normalization of the upper half plane modulo a subgroup (of finite index) of $\mathrm{PSL}(2, \boldsymbol{Z})$; and

(3.14b) a description of the branch cycles of the cover is given by the collection $a_{1,i}$, $i = 2, 3, 4$ in their permutation action on the straight Nielsen classes described by Part 3.

In particular (3.14b) allows us to explicitly compute the genus of Y_n from the Riemann–Hurwitz formula. Of course, as already explained, we will do this only for the cases $n = 4$ and 5. In another paper we will explicitly list all of the Nielsen classes and show that the action of SH_4 on the straight Nielsen classes described by Part 3 is transitive. In the next result we state this tentatively.

THEOREM 3.7. *If the action of SH_4 on the straight Nielsen classes is transitive, then the curve cover $\psi_n\colon Y_n \to \boldsymbol{P}_x^1$ defined over $\boldsymbol{Q}$ with properties* (3.13) *and* (3.14) *exists. For any n for which expression* (3.13) *is nonempty, S_n is the*

Galois group of a regular extension of P^1_x over Q with the branch cycles given by the proof of Proposition 3.6. In particular this cover has many totally real specializations (i.e., is an exception to the conclusion of Proposition 3.6). In the case that $n = 4$, the cover $\psi_4: Y_4 \to P^1_x$ is of degree 6 and Y_4 is isomorphic to P^1 over Q. In particular (3.13) is nonempty. The cover ψ_5: $Y_5 \to P^1_x$ (i.e., $n = 5$) is of degree 10 and it has a description of its branch cycles given by the following elements in S_{10}:

$$(1\ 2\ 3)(4\ 5)(6\ 7\ 8\ 9\ 10), \quad (1\ 7\ 6)(2\ 4\ 3)(5\ 9) \quad \textit{and} \quad ((1\ 4\ 9\ 10)(8\ 5\ 3\ 7))^{-1}.$$

Thus Y_5 is also of genus 0 and again (3.13) is nonempty.

Proof. We need only find the action of $a_{1,j}$, $j = 2$, 3 and 4 on representatives of the list of straight Nielsen classes as described in Part 3 to reduce the theorem to a computation. Since the a's are a description of the branch cycles of a cover, we compute $a_{1,4}$ as the inverse of the product of $a_{1,2}$ and $a_{1,3}$. First: $n = 5$ following the notation of Part 2.

Here is an expansion of the list of absolute Nielsen classes, including the actual results of conjugating the pairs (τ_3, τ_4):

$L_{1,2}$: $\tau_3 = (5\,2\,3)$, $\tau_4 = (2\,5)(3\,4)$; $\tau_3 = (5\,3\,4)$, $\tau_4 = (3\,5)(2\,4)$;
$\tau_3 = (5\,4\,2)$, $\tau_4 = (4\,5)(2\,3)$;

$L_{1,3}$: $\tau_3 = (5\,2\,1)$, $\tau_4 = (2\,5)(3\,4)$; $\tau_3 = (5\,1\,2)$, $\tau_4 = (1\,5)(3\,4)$;

$L_{3,5}$: $\tau_3 = (1\,5\,3)$, $\tau_4 = (3\,4)(1\,2)$; $\tau_3 = (2\,1\,4)$, $\tau_4 = (4\,5)(2\,3)$;
$\tau_3 = (3\,2\,5)$, $\tau_4 = (1\,5)(3\,4)$; $\tau_3 = (4\,3\,1)$, $\tau_4 = (1\,2)(4\,5)$;
$\tau_3 = (5\,4\,2)$, $\tau_4 = (2\,3)(5\,1)$.

Denote the elements under $L_{1,2}$ by x_i, $i = 1, 2, 3$, in the order of their listing; under $L_{1,3}$ by x_4 and x_5; and those under $L_{3,5}$ by x_i, $i = 6, \ldots, 10$. For each of these denote $(x_i)Q_1^{-1}$ by y_i, $i = 1, \ldots, 10$. The essential part of the computation is the effect of Q_1^2 (resp., Q_2^2) on the x's (resp., y's). For example, the practical effect of previous comments is that

$$Q_1^2 = (x_1\,x_2\,x_3)(x_4\,x_5)(x_6\,x_7\,x_8\,x_9\,x_{10}).$$

Here are the y's:

y_1: $((1\,2), (2\,1\,3\,4), (5\,2\,3), (2\,5)(4\,3))$ y_2: $((1\,2), (2\,1\,3\,4), (5\,3\,4), (3\,5)(4\,2))$
y_3: $((1\,2), (2\,1\,3\,4), (5\,4\,2), (4\,5)(2\,3))$ y_4: $((1\,3), (3\,2\,1\,4), (5\,2\,1), (2\,5)(3\,4))$
y_5: $((1\,3), (3\,2\,1\,4), (5\,1\,2), (1\,5)(3\,4))$ y_6: $((1\,5), (5\,2\,3\,4), (1\,5\,3), (3\,4)(1\,2))$
y_7: $((1\,5), (5\,2\,3\,4), (2\,1\,4), (4\,5)(2\,3))$ y_8: $((1\,5), (5\,2\,3\,4), (3\,2\,5), (1\,5)(3\,4))$
y_9: $((1\,5), (5\,2\,3\,4), (4\,3\,1), (1\,2)(4\,5))$ y_{10}: $((1\,5), (5\,2\,3\,4), (5\,4\,2), (2\,3)(1\,5))$

Apply Q_2^2: y_1 goes to $((1\,2), ?, (2\,1\,3\,4)(5\,2\,3)(2\,1\,3\,4)^{-1}, (2\,5)(4\,3))$; which has $(5\,4\,1)$ in the 3rd position; and conjugation by $(2\,5\,4\,1)^{-1}$ gives y_7. Continue in this way to get

$$Q_2^2 = (y_1\,y_7\,y_6)(y_2\,y_4\,y_3)(y_5\,y_9).$$

Translate this back to the x's to get that the cover ψ_5: $Y_5 \to P^1_x$ has a description of its branch cycles given by

$$a_{1,2} = (1\,2\,3)(4\,5)(6\,7\,8\,9\,10),$$
$$a_{1,3} = (1\,7\,6)(2\,4\,3)(5\,9),$$
$$a_{1,4} = ((1\,4\,9\,10)(7\,8\,5\,3))^{-1}.$$

From the Riemann–Hurwitz formula, the genus of Y_5 is 0. Since each of the disjoint cycles of σ_i, $i = 1, 2, 3$ is of a distinct length, the points above the branch points—all of them—are rational. This shows that Y_5 has a lot of rational points. From the renown Hilbert–Hurwitz observation, Y_5 is isomorphic to P^1.

Finally, we quickly traverse the similar calculations for the case $n = 4$ by displaying the analogs of the calculations above for (τ_3, τ_4). There are just two listings:

$L_{1,2}$: $\tau_3 = (4\,3\,2)$, $\tau_4 = (3\,4)$; $\tau_3 = (4\,2\,3)$, $\tau_4 = (2\,4)$; and
$L_{2,4}$: $\tau_3 = (4\,3\,2)$, $\tau_4 = (1\,4)$; $\tau_3 = (3\,2\,1)$, $\tau_4 = (4\,3)$;
$\tau_3 = (2\,1\,4)$, $\tau_4 = (3\,2)$; $\tau_3 = (1\,4\,3)$, $\tau_4 = (2\,1)$.

Denote the elements under $L_{1,2}$ by x_i, $i = 1, 2$, in the order of their listing; under $L_{2,4}$ by x_i, $i = 3, \ldots, 6$. For each of these denote $(x_i)Q_1^{-1}$ by y_i, $i = 1, \ldots, 6$. As above the essential part of the computation is the effect of Q_1^2 (resp., Q_2^2) on the x's (resp., y's). We easily compute that

$$Q_1^2 = (x_1\,x_2)(x_3\,x_6\,x_5\,x_4).$$

Here are the y's:

y_1: $((1\,3), (1\,2\,3), (4\,3\,2), (3\,4))$ y_2: $((1\,3), (1\,2\,3), (4\,2\,3), (2\,4))$
y_3: $((3\,4), (1\,2\,3), (4\,3\,2), (1\,4))$ y_4: $((3\,4), (1\,2\,3), (3\,2\,1), (4\,3))$
y_5: $((3\,4), (1\,2\,3), (2\,1\,4), (3\,2))$ y_6: $((3\,4), (1\,2\,3), (1\,4\,3), (2\,1))$

The effect of Q_2^2 on the y's is $(y_1\,y_5\,y_3)$. Translate this back to the x's to get that the cover ψ_4: $Y_4 \to P^1_x$ has a description of its branch cycles given by

$$a_{1,2} = (1\,2)(3\,6\,5\,4), \quad a_{1,3} = (1\,5\,3), \quad \text{and} \quad a_{1,4} = ((1\,2\,5\,4)(3\,6))^{-1}.$$

The genus of Y_4 is therefore 0 by the Riemann–Hurwitz formula, and (as in the case of $n = 5$) all of the points above the three branch points are rational. Thus the curve is isomorphic to P^1. ■

§4. Points on $\mathscr{H}(\mathbf{C})$ giving R-covers and Siegel families

Consider a collection of conjugacy classes $\mathbf{C}$ of a group G (with a permutation representation T: $G \to S_n$) and the associated Nielsen classes

$\mathrm{Ni}(\mathbf{C})_T^{ab}$. In §4.1 and §4.2 we give general results that show the following things:

(4.1a) How to effectively compute the effect of complex conjugation on the points of a fiber $\phi^{-1}(x_i)$ of a cover $\phi\colon X \to \boldsymbol{P}_x^1$ where x_i is one of the branch points of the cover;

(4.1b) How to effectively locate all of the points on the parameter space $\mathscr{H}(\mathbf{C})$ which correspond to covers over $\boldsymbol{R}$ in the Nielsen class associated to a group G.

Siegel's theorem. The remainder of the paper applies the results of §4.1–4.2 to consider a converse to the following version of Siegel's Theorem [S]. Let $\phi\colon X \to \boldsymbol{P}_x^1$ be a cover of projective nonsingular curves with both X and the graph of ϕ defined over $\boldsymbol{Q}$. Suppose that $\mathscr{A}$ is a fractional ideal of $\boldsymbol{Q}$. If there are infinitely many $\boldsymbol{Q}$ points of X that lie over the points $\mathscr{A} \subset \boldsymbol{P}_x^1$, then

(4.2a) X is of genus 0 and it has 1 or 2 points over $x = \infty$; and

(4.2b) if there are two points over ∞, they are real conjugates over $\boldsymbol{Q}$.

If there is just one point over ∞ in (4.2), a rough converse to Siegel's theorem is obvious. But if option (4.2b) holds there are serious questions for this. Our goal is to use Theorem 2.4 to consider properties of all complete families of curve covers of genus 0 for which there is some possibility that members of the family will have property (4.2b). We reduce this to a computational test with Hurwitz monodromy action – illustrated by two examples. This combined with a sufficient condition for the family to be defined over $\boldsymbol{Q}$ gives the necessary ingredients for a reasonable definition of *Siegel family of covers over* $\boldsymbol{Q}$ (with $r \geqslant 3$ branch points). In particular, if $\mathscr{H}$ is the parameter space for such a family, it is guaranteed that the natural degree 2 cover $\mathscr{H}_\infty \to \mathscr{H}$ defined by the points over infinity in the covers of the family has the following property: for a real point $\boldsymbol{m} \in \mathscr{H}$, the (two) points of $\mathscr{H}_\infty$ above $\boldsymbol{m}$ are defined over a real quadratic extension of $\boldsymbol{Q}(\boldsymbol{m})$. We have left it to the examples to illustrate how the following subtle computation would be checked:

Question 4.1. In the above notation, when is it true that for "general" real $\boldsymbol{m} \in \mathscr{H}$, the (two) points of $\mathscr{H}_\infty$ above $\boldsymbol{m}$ are conjugate over a real quadratic extension of $\boldsymbol{Q}(\boldsymbol{m})$?

The fullest converse would show how to guarantee the existence of a member of a $\boldsymbol{Q}$-Siegel family that affirmatively satisfies the questions of list (4.7). For (4.7a) and (4.7b) our computations are instructive. Therefore it is primarily in dealing with question (4.7c) that the remaining problems arise in giving a converse to Siegel's theorem.

§4.1. Real points on fibers over branch points. Use the notation of the previous sections for a cover (as general as previously) $\phi\colon X \to \boldsymbol{P}_x^1$ that is defined over $\boldsymbol{R}$ and has the usual notation $x_1, \ldots, x_r$ for its list of branch points.

Assume that G and the Nielsen class (associated to $\mathbf{C}$) are fixed for the discussion. We now state an analogue of Theorem 2.4 that tells us the effect (as a permutation) of complex conjugation on the points of the fiber $\phi^{-1}(x_i)$. Again, compatible with the ingredients for Theorem 2.4, we assume a naming of the branch points so that $x_1, \ldots, x_{r_1}$ are the real points, and these appear in clockwise order around the "circle" $\boldsymbol{P}^1(\boldsymbol{R})$. Recall that the Hurwitz monodromy action (§3.1) allows us to reorder the entries in $\mathbf{C}$ without changing the Nielsen class that is involved in the definition.

Also, for simplicity, as in the proof of Theorem 2.4, we assume that we have chosen a point $x_0 \in \boldsymbol{P}^1(\boldsymbol{R})$ that lies between x_1 and x_{r_1} and that we have $c_{x_0} = c \in N_{S_n}(G)$ so as to satisfy the formulas of (2.6). It is the action of complex conjugation on the fiber $\phi^{-1}(x_{r_1})$ that we now describe. Write out σ_{r_1} as a product of disjoint cycles: $\lambda_1 \lambda_2 \ldots \lambda_s$. These disjoint cycles are in one-one correspondence with the points of the fiber $\phi^{-1}(x_{r_1})$ in the following sense. Consider a path γ_{r_1} homotopic to the path that gives the branch cycle σ_{r_1}, with γ_{r_1} of the form $\varrho\delta\varrho^{-1}$ where δ surrounds a (suitably small) closed disc D about x_{r_1} and ϱ is along the real line. A point $\boldsymbol{p} \in \phi^{-1}(x_{r_1})$ corresponds to the disjoint cycle λ_j whose entries represent exactly the points above x_0 for which the unique lift of γ_{r_1} starting at such a point meets the unique connected component of $\phi^{-1}(D)$ containing $\boldsymbol{p}$ (e.g., [Fr 2; p. 146]).

Theorem 4.2. *In the association described above label the points of $\phi^{-1}(x_{r_1})$ by $y_1, \ldots, y_s$ so that y_i corresponds to the disjoint cycle λ_i, $i = 1, \ldots, s$. Consider the action of complex conjugation given by* (2.6): $c\sigma_{r_1}c = \sigma_{r_1}^{-1}$. *This implies that c maps the set of integers that appear in a disjoint cycle λ_j to the set of integers that appear in another disjoint cycle λ_k. Thus c induces a permutation of the integers $y_1, \ldots, y_s$ which we denote by c_y. It is c_y that gives the action of complex conjugation on the points $y_1, \ldots, y_s$.*

Proof. The action of complex conjugation on the points $y_1, \ldots, y_s$ extends naturally (and compatibly) to the connected components of $\phi^{-1}(D)$. It also extends to the lifts of γ_{r_1} (as it maps γ_{r_1} to its inverse). It is now clear that the lifts of the paths that meet a specific connected component V of $\phi^{-1}(D)$ are taken by complex conjugation to the lifts of paths that meet the effect of complex conjugation on V. When translated in terms of the points of $y_1, \ldots, y_s$, this is what the theorem says. ∎

Example 4.3. (*Example* 2.7 *continued.*) In Example 2.7 we had the following data: $r = 3$, $G = A_4$, and C_1 is the conjugacy class of a 3-cycle; C_2 is the conjugacy class of elements inverse to those of C_1; and C_3 the conjugacy class of a product of two 2-cycles. Assume that a cover $\phi\colon X \to \boldsymbol{P}^1$ is in this Nielsen class, and that x_{r_1} is ∞ and that it corresponds to the conjugacy class labeled as C_3. We want to check the effect of complex conjugation on the (two) points of the cover over ∞. First in the case that all 3 branch points are real (Case 1 of Example 2.7): if we assume that $x_0 \in (\infty, x_1)$, the computations were that conjugation by c gives (2 4). Thus it does not move the two disjoint cycles in a representative of the Nielsen class, so the points are real.

But in Case 2 of Example 2.7, under the assumption that the other two branch points are complex conjugate, the two disjoint cycles were permuted. Indeed the representative for C_3 was $(1\,3)(2\,4)$ and c turned out to be $(1\,2)(3\,4)$. That is, the points over ∞ in the cover under these hypotheses are complex conjugate. A moment's reflection reveals that this in particular implies that the residue class fields of the points over ∞ in this Nielsen class are nonconstant as a function of the parameter space. ∎

§4.2. Points on the Hurwitz space that give *R*-covers. Continue the notation from §4.1. Consider $x_0 \in \boldsymbol{P}^1(\boldsymbol{R})\backslash\{x_1, \ldots, x_r\}$. Here we explicitly use that the existence of $c_{x_0} = c \in N_{S_n}(G)$ satisfying formulas (2.6) is a necessary condition for the cover $\phi\colon X \to \boldsymbol{P}_x^1$ to be defined over $\boldsymbol{R}$. Under the hypotheses of Proposition 3.3 (cf. [DFr; Theorem 1.7]) the latter is equivalent to having $\boldsymbol{m} \in \mathscr{H}(\mathbf{C})$ corresponding to this cover defined over $\boldsymbol{R}$ (i.e., with real coordinates). What we show here is that existence of c is also a sufficient condition for the cover to be defined over $\boldsymbol{R}$, and therefore that the corresponding point of the Hurwitz space is real. This gives a satisfying combinatorial description of the real points of $\mathscr{H}(\boldsymbol{R})$. Thus it is a shame that there are no $\boldsymbol{Q}_p$ versions (cf. §0) in light of the seriousness of checking if $\mathscr{H}(\boldsymbol{R})$ has rational points (e.g., as in §3.4).

THEOREM 4.4. *We assume that the hypothesis* (∗) *of Proposition* 3.3 *holds. Suppose that a cover* $\phi\colon X \to \boldsymbol{P}^1$ *has only real and complex conjugate pairs of branch points as in* §2. *Let* $\boldsymbol{\sigma}$ *be a branch cycle description relative to a set of paths given as in Figure* 2. *Now we may ask (relative to a point* $x_0 \in \boldsymbol{P}^1(\boldsymbol{R})$) *if there exists* $c_{x_0} = c \in N_{S_n}(G)$ *that satisfies formula* (2.6). *Then* $\phi\colon X \to \boldsymbol{P}^1$ *is defined over* $\boldsymbol{R}$ *if and only if such a c exists, and this does not depend on the choice of* x_0.

There is a constructive partition $\mathscr{H}_1, \ldots, \mathscr{H}_v$ *of the points of* $\mathscr{H}(\mathbf{C})$ *over* $\boldsymbol{P}^r(\boldsymbol{R})\backslash D_r$ *with the following property: each of the* $\mathscr{H}_i$*'s, as a set of complex valued points on the manifold* $\mathscr{H}(\mathbf{C})$, *is connected; each of the* $\mathscr{H}_i$*'s corresponds to one element of the Nielsen class; and each* $\boldsymbol{m} \in \mathscr{H}_i$ *corresponds to a cover in the Nielsen class defined over* $\boldsymbol{R}$ *if and only if the element of the Nielsen class that corresponds to* $\mathscr{H}_i$ *has a corresponding c that satisfies* (2.6).

Proof. Since (∗) holds, Proposition 3.3 says that the cover of the first paragraph of the introduction has a minimal field of definition K that makes K a *field of moduli* for the cover. That is, if $\tau \in \operatorname{Aut}(\boldsymbol{C}/\boldsymbol{Q})$ and if $\phi^\tau\colon X^\tau \to \boldsymbol{P}^1$ is equivalent to $\phi\colon X \to \boldsymbol{P}^1$ as a cover, then τ is fixed on K. (An application of Weil's cocycle condition; beginning of the proof of [Fr 1; Theorem 5.1].) Here the superscript τ indicates the effect of applying τ to the coefficients of the equations describing these curves.

If K is contained in $\boldsymbol{R}$ then Theorem 2.4 shows the existence of c. Suppose conversely that c exists satisfying (2.6). The proof of Theorem 2.4 actually shows that the left side of (2.6) consists of a branch cycle description of the cover obtained by applying complex conjugation to the coefficients of $\phi\colon X \to \boldsymbol{P}^1$ (as well as to the points over x_0) relative to paths homotopic to the original paths with which the branch cycles were computed to be the right side of (2.6). Two covers with equivalent branch cycle descriptions with respect to the same homotopy classes of paths are equivalent covers. Thus $\phi\colon X \to \boldsymbol{P}^1$ is equivalent to $\phi^c\colon X^c \to \boldsymbol{P}^1$. But this contradicts the field of moduli property of the field of definition K of the cover, unless c is fixed on K. That is the cover is defined over $\boldsymbol{R}$. Since being defined over $\boldsymbol{R}$ has nothing to do with the base point x_0 with which we started the inspection of (2.6), the result does not depend on this choice. Nevertheless, it would be instructive for the reader to check that if c_{x_0} exists for x_0 selected in one of the intervals of $\boldsymbol{P}^1\backslash\{x_1, \ldots, x_r\}$ it exists as well for x_0 selected in any other of these intervals.

Now we come to the description of the partition $\mathscr{H}_1, \ldots, \mathscr{H}_v$. Let I be all of the ways to write r as a sum of the form $r_1 + 2r_2$. We use I to consider first a partition of a subset of $(\boldsymbol{P}^1)^r\backslash\Delta_r = \mathscr{U}_r$ (§3.1). For $(r_1, r_2) \in I$ denote the subset of $\mathscr{U}_r$ consisting of r_1 real points and $2r_2$ pairs of complex conjugate points by $\mathscr{U}_{r_1,r_2}$. Let V be one of the finite number of connected components of $\mathscr{U}_{r_1,r_2}$. Denote the image of V under Ψ_r in $\boldsymbol{P}^r\backslash D_r$ by W. Now consider the connected components $\mathscr{H}(\mathbf{C})$ that lies over W. For any one of these, the setup for expression (2.6) gives a specific representing Nielsen class relative to the paths considered for Theorem 2.4. Thus we may check for this Nielsen class if there is a c that works in (2.6). If there is, then all points of the component of $\mathscr{H}(\mathbf{C})$ that lies over Wconsists of real points. We are now reduced to running over all pairs $(r_1, r_2) \in I$, all choices and orderings of the coordinates associated with the r_1 real points, and all representatives of the Nielsen class, to check for the existence of c in each of these cases. This concludes the algorithm for labeling the real points of $\mathscr{H}(\mathbf{C})$. ∎

§4.3. Definition of Siegel families. We will be fixing the ramification type over ∞ of our covers $X \to \boldsymbol{P}_x^1$. In particular, our concern is with covers with two points over ∞, both ramified over their images of order an integer m. Thus the cover is of degree $2m = n$. We call such a cover an (m, m)-cover thereby reserving the right to generalize to other situations without having to drastically change notation. Suppose that $\mathbf{C} = (C_1, \ldots, C_r)$ is a collection of conjugacy classes in a group G for which the covers $X \to \boldsymbol{P}_x^1$ in the Nielsen class $\mathrm{Ni}(\mathbf{C})_T^{\mathrm{ab}}$ are of genus 0 and for which C_r is the conjugacy class of an element σ_r in $G \subset S_n$ with

(4.3) σ_r is a product of two disjoint m-cycles (of (m, m)-type).

We consider just the subspace of the Hurwitz space $\mathscr{H}(\mathbf{C})$ consisting of representatives of the covers $X \to \boldsymbol{P}_x^1$ which happen to be (m, m)-covers. For most examples—just a few simple exceptions are excluded—$C_i \neq C_r$ for $i \neq r$. In this case there can be no confusion about which branch point has the (m, m)-type of branching. The space representing just the (m, m)-type covers will be denoted $\mathscr{H}(\mathbf{C}_\infty)$. We refer to a representative of the conjugacy class C_r as a *Siegel cycle.*

Consider the set

$$(4.4)\quad \mathrm{Ni}(\mathbf{C}_\infty) \overset{\mathrm{def}}{=} \{\tau \in G^r \mid G(\tau) = G,\ \tau_r = \sigma_r, \text{ with } \beta \in S_{r-1} \text{ so that } \tau_{(i)\beta} \in C_i,\ i = 1, \dots, r,\ \tau_1 \dots \tau_r = 1\}.$$

Also, denote the subgroup of the normalizer of G in S_n that centralizes σ_r and that permutes the conjugacy classes $C_1, \dots, C_{r-1}$ by $N(\mathbf{C}_\infty)$. From [DFr; § 14] $\mathscr{H}(\mathbf{C}_\infty)$ is naturally a cover of A^n of degree equal to the quotient of $\mathrm{Ni}(\mathbf{C}_\infty)$ by the natural conjugating action of $N(\mathbf{C}_\infty)$. Denote this set by $\mathrm{Ni}(\mathbf{C}_\infty)_T^{\mathrm{ab}}$. Below denote this family by $\mathscr{S}(\mathbf{C}_\infty)$.

Definition 4.5. Consider a family $\mathscr{S}(\mathbf{C}_\infty)$ of covers of (m, m)-type (of genus 0). It is said to be a *Siegel family* (of covers) if the following properties hold:

(4.5a) $\mathscr{S}(\mathbf{C}_\infty)$ is defined over $\boldsymbol{R}$;

(4.5b) a Zariski dense subset $\mathscr{W}$ of $\mathscr{H}(\mathbf{C}_\infty)$ has associated covers defined over $\boldsymbol{R}$;

(4.5c) for a Zariski dense subset of $\boldsymbol{m} \in \mathscr{W}$ a cover representing $\boldsymbol{m}$ has the property that the two points over ∞ are both real; and

(4.5d) C_r is rational in the smallest group containing G and $N(\mathbf{C}_\infty)$.

The main point that we make here is that Theorems 4.2 and 4.4 give an explicit test for a given Nielsen class (with a choice of conjugacy class as C_r) whether the corresponding family of covers is a Siegel family. Just being a Siegel family is not sufficient to provide us with curves that give a converse to Siegel's theorem stated in the introduction. The next definition adds to the properties of Definition 4.5 to further this goal.

Definition 4.6. Suppose that $\mathscr{S}(\mathbf{C}_\infty)$ is a family of Siegel covers of (m, m)-type. We say that it is a *$\boldsymbol{Q}$-Siegel family* if the following properties hold:

(4.6a) $\mathscr{S}(\mathbf{C}_\infty)$ is defined over $\boldsymbol{Q}$;

(4.6b) $\mathscr{H}(\mathbf{C}_\infty)$ has a Zariski dense set of $\boldsymbol{Q}$ points; and

(4.6c) for a Zariski dense subset of $\boldsymbol{m} \in \mathscr{H}(\mathbf{C}_\infty)(\boldsymbol{Q})$ a cover $\phi_{\boldsymbol{m}}\colon X_{\boldsymbol{m}} \to \boldsymbol{P}_x^1$ representing $\boldsymbol{m}$ has the property that the two points over ∞ are real conjugates over $\boldsymbol{Q}$.

§ 4.4. Examples and questions about Siegel families. Those families that satisfy the generalized "rigidity condition" (of Prop. 3.3) will be said to be *rigid Siegel families*. For these families we can be certain that they are defined over $\boldsymbol{Q}$, and thus members of them are part of a potential converse to Siegel's theorem. Such rigid $\boldsymbol{Q}$-families include those given by Example 4.3 and the main example of [DFr]. But we have left one of the most exciting problems untouched by restricting consideration to just the rigid families.

The list of *Siegel families* is sufficiently explicit to allow serious consideration of the following questions about the parameter space $\mathscr{H}$ of one of the families:

(4.7a) Is $\mathscr{H}(\boldsymbol{Q})$ Zariski dense in $\mathscr{H}$?;

(4.7b) If the answer to a) is positive, for sufficiently general $\boldsymbol{m} \in \mathscr{H}(\boldsymbol{Q})$ and $\phi_{\boldsymbol{m}}\colon X_{\boldsymbol{m}} \to \boldsymbol{P}_x^1$ the corresponding cover, is $X_{\boldsymbol{m}}(\boldsymbol{Q})$ nonempty?; and

(4.7c) If the answer to b) is positive, for $\mathscr{A}$ any fractional ideal of $\boldsymbol{Q}$, is $\phi_{\boldsymbol{m}}^{-1}(\mathscr{A})$ infinite?

It is only for rigid Siegel families that we would expect effective answers to these at this time. The main example of [DFr] passed all these tests affirmatively. But as yet no general procedure tests a specific Siegel family for property (4.7c) even if (4.7a) and (4.7b) hold.

We conclude the paper with an example. For this family we will show that questions (4.7a) and (4.7b) are answered affirmatively. As already discussed (cf. [DFr]) (4.7c) is tougher.

Example 4.7. *A $\boldsymbol{Q}$-Siegel family with $r = 4$.* The point of this example is to show Theorems 4.2 and 4.4 in action. We take G to be S_4, $r = 4$ and the Nielsen class has a representative given by the following 4-tuple:

$$(4.8)\quad (\sigma_1 = (1\,2),\ \sigma_2 = (2\,3),\ \sigma_3 = (2\,1\,4),\ \sigma_4 = (1\,3)(2\,4)).$$

Then a cover $X \to \boldsymbol{P}_x^1$ given with this branch cycle description is of genus 0, and we assume that the element σ_4 indicates the ramification structure over ∞. We assume the setup exactly as around formula (2.6). We have a family of covers $\mathscr{S}(\mathbf{C}_\infty)$ of $(2, 2)$-type, as given by (4.3). First note that there is no c that satisfies formula (2.6). In this case such a c would conjugate the 4-tuple of (4.8) to

$$(4.9)\quad (\sigma_1 = (1\,2),\ \sigma_2' = (1\,3),\ \sigma_3' = (2\,3\,4),\ \sigma_4 = (1\,3)(2\,4)).$$

But, such a c would commute with the group generated by σ_1 and σ_4. Therefore c would by either the identity or $(1\,2)(3\,4)$: a clear contradiction.

Representatives of the straight Nielsen classes consist of just 3 elements:

(4.10) the two elements above and $((1\,3), (1\,2), (2\,1\,4), (1\,3)(2\,4))$.

As in the proof of Theorem 3.7, we establish the basic properties of this family by computing the effect of $a_{1,2}$ and $a_{1,3}$ on these absolute straight Nielsen classes. Labeled in this order the effect of Q_1 on them is $(1\,3\,2)$. Thus Q_1^2 is $(1\,2\,3)$. Now Q_2^2 has the effect of $(1\,2)$. Compute easily that the curve Y that corresponds to this cover, in the discussion around (3.13) is of genus 0 and it has lots of $\boldsymbol{Q}$-points. Finally, if we try to find c relative to the Nielsen class representative listed in (4.10) we get that c exists and is equal to 1. Conclusion, this is a Siegel family according to Definition 4.5, but only some of the regions described in Theorem 4.4 correspond to real points. Furthermore, we have verified all of the properties of (4.6) for it to be a Q-Siegel family, except for (4.6c). This is similar—read, just as tricky—as the analogous question was for Example 4.3.

Consider the Hurwitz monodromy group action on the straight Nielsen class representatives given in (4.8)-(4.10) together with the conjugates of these by $(1\,2)(3\,4)$. We equivalence two of these elements only if one comes from the other by conjugation by an element that is in the group of centralizers of σ_4 that do not permute the two orbits of σ_4. A check shows that the Hurwitz monodromy action is transitive on these 6 classes, and we conclude as in Example 4.3. ■

Editorial Note: The paper was originally intended for the Sprindžuk's memorial volume, but has been delayed in the refereeing process.

References

[A] R. Atkin, *Nonexistence of a nontrivial Hecke operator theory for noncongruence subgroups*, Report presented to second author by J. G. Thompson, Spring 1988.

[Car] R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order*, Dover Publications, 1937.

[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*, Crelles Journal 409 (1990), 106–137.

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

[Fr 2] — *Galois groups and complex multiplication*, Trans. Amer. Math. Soc. 235 (1978), 141–163.

[Fr 3] — *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*, preprints.

[Fr 4] —*Arithmetic of 3 and 4 branch point covers: A bridge provided by noncongruence subgroups of* $SL_2(Z)$, Progress in Math. Birkhäuser 81 (1990), 77–117.

[FrT] M. Fried and J. G. Thompson, *The Hurwitz monodromy group* $H(4)$ *and modular curves*, preprint.

[F] G. Frobenius, *Über die Charaktere der alternierenden Gruppe*, Sitzungsber. Königl. Preuss. Akad. Wiss. Berlin (1901), 303–315.

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

[H] A. Hurwitz, *Über Riemann'sche Flächen mit gegebenen Verzweigungspunkten*, Math. Ann. 39 (1891), 1–61.

[KN] W. Krull and J. Neukirch, *Die Struktur der absoluten Galoisgruppe über dem Körper* $R(t)$, ibid. 193 (1971), 197–209.

[N] J. Neukirch, *On solvable number fields*, Invent. Math. 53 (1979), 135–164.

[Se] J. P. Serre, *Groupes de Galois sur* Q, Séminaire Bourbaki, 40ème année (1987-1988), n° 689.

[S] C. L. Siegel, *Über einige Anwendungen diophantischer Approximation*, Abhand. Preuss. Akad., Phys.-Math. 1 (1929), 14–67.

[Sp] V. G. Sprindžuk, *Reducibility of polynomials and rational points on algebraic curves*, Soviet Math. Dokl. 21 (1980), 331–334.

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

DEPARTMENT OF MATHEMATICS
UC IRVINE
Irvine, Ca. 92717, U.S.A.

INSTITUT HENRI POINCARÉ
"PROBLÈMES DIOPHANTIENS"
11rue Pierre et Marie Curie
75231 Paris Cedex 5, France

Received on 23.8.1988
and in revised form on 25.7.1989 (1860)