

# Real Hilbertianity and the Field of Totally Real Numbers

MICHAEL D. FRIED<sup>\*†</sup>, DAN HARAN<sup>\*‡</sup>  
AND HELMUT VÖLKLEIN<sup>\*•</sup>

ABSTRACT. We use moduli spaces for covers of the Riemann sphere to solve regular embedding problems, with prescribed extendability of orderings, over PRC fields. As a corollary we show that the elementary theory of  $\mathbb{Q}^{\text{tr}}$  is decidable. Since the ring of integers of  $\mathbb{Q}^{\text{tr}}$  is undecidable, this gives a natural undecidable ring whose quotient field is decidable.

## Introduction

The theory and use in [F] of moduli spaces of covers of the Riemann sphere with prescribed ramification data has been further developed in [FV1]. There the main theme is that  $K$ -rational points of the moduli spaces correspond to covers defined over  $K$ . Furthermore, [FV2] notes a correspondence between existence of  $K$ -rational points on certain related spaces and the solvability of regular embedding problems over  $K$ . Thus, using moduli spaces allows us to prove solvability of regular embedding problems over fields  $K$  suitably large for such varieties to have the requisite  $K$ -rational points.

This principle appears in [FV2] to show that the absolute Galois group of a countable Hilbertian PAC field of characteristic 0 is free. The natural extension of this to the (larger) class of Hilbertian PRC fields appears in [FV3].

Recall [FJ, p. 129] that  $K$  is **PAC** (**p**seudo **a**lgebraically **c**losed) if every absolutely irreducible variety  $V$  defined over  $K$  has a  $K$ -rational point. Furthermore [P2],  $K$  is **PRC** (**p**seudo **r**eal **c**losed) if every absolutely irreducible

---

1991 *Mathematics Subject Classification*. Primary 12D15, 12E25, 12F12, 11G25.

\* Support from the Institute for Advanced Study at Hebrew University, 1991–92.

† Supported by NSA grant MDA 14776 and BSF grant 87-00038.

‡ Supported by Max-Planck-Institut für Mathematik, Bonn, 1992–93.

• Supported by NSA grant MDA 904-89-H-2028.

This paper is in final form and no version of it will be submitted for publication elsewhere.

variety  $V$  defined over  $K$  has a  $K$ -rational point, provided that  $V$  has a non-singular point over each real closure of  $K$ . The latter condition on  $V$  is equivalent to the following one: the function field  $K(V)$  of  $V$  is a **totally real** extension of  $K$ , that is, every ordering on  $K$  extends to  $K(V)$ .

The field  $\mathbb{Q}^{\text{tr}}$  of all totally real algebraic numbers is the fixed field of all involutions in the absolute Galois group  $G(\mathbb{Q})$  of  $\mathbb{Q}$ . From Pop [P],  $\mathbb{Q}^{\text{tr}}$  is PRC. By Weissauer's theorem [FJ, Proposition 12.4] every proper finite extension of  $\mathbb{Q}^{\text{tr}}$  is Hilbertian. Also, by Prestel's extension theorem [P2, Theorem 3.1] every algebraic extension of  $\mathbb{Q}^{\text{tr}}$  is PRC. Hence, the absolute Galois group of a proper finite extension of  $\mathbb{Q}^{\text{tr}}$  is known [FV3]. The field  $\mathbb{Q}^{\text{tr}}$ , however, is not Hilbertian. For example,  $Z^2 - (a^2 + 1)$  is reducible over  $\mathbb{Q}^{\text{tr}}$  for every  $a \in \mathbb{Q}^{\text{tr}}$ .

In [FHV] we cover also the case of  $\mathbb{Q}^{\text{tr}}$ . The key observation is that  $\mathbb{Q}^{\text{tr}}$  satisfies a certain weakening of the Hilbertian property. This allows specializing Galois extensions of  $K(x)$  whose Galois group is generated by *real* involutions to obtain Galois extensions of  $K$  with the same Galois group. As a result we determine the absolute Galois group of  $\mathbb{Q}^{\text{tr}}$ .

In the present paper we extend the methods and results of [FV3]. This solves regular embedding problems over a PRC field  $K$  so that the orderings of  $K$  extend to prescribed subfields (Theorem 5.2). Thus, Theorem 5.3 gives new information about the absolute Galois group of the field  $K(x)$  of rational functions over  $K$ .

The first 5 sections setup the proof of Theorem 5.2. We need an approximation theorem for varieties over PRC fields (section 1), supplements about the moduli spaces (section 2), group-theoretic lemmas (section 3), and the determination of the real involutions in Galois groups over  $\mathbb{R}(x)$  (section 4).

In section 6 we define the concept of totally real Hilbertian, and show that  $\mathbb{Q}^{\text{tr}}$  has this property. Section 7 combines these results to determine the absolute Galois group of a countable totally real Hilbertian PRC field satisfying these properties: it has no proper totally real algebraic extensions; and its space of orderings has no isolated points. This group is the free product of groups of order 2, indexed by the Cantor set  $X_\omega$  (Theorem 7.6). In particular,  $G(\mathbb{Q}^{\text{tr}}) = \text{Aut}(\tilde{\mathbb{Q}}/\mathbb{Q}^{\text{tr}})$  is isomorphic to this group.

As a corollary we introduce the notion of *real Frobenius fields*:  $\mathbb{Q}^{\text{tr}}$  is an example (Corollary 8.3). Following the Galois stratification procedure of [FJ, Chap. 25] and [HL] we show that the elementary theory of real Frobenius fields allows elimination of quantifiers in the appropriate language. In particular,  $\mathbb{Q}^{\text{tr}}$  is primitive recursively decidable (Theorem 10.1). On the other hand the ring of integers of  $\mathbb{Q}^{\text{tr}}$  is undecidable (A. Prestel pointed us to Julia Robinson's proof of this [R2].) Thus we obtain a natural example of an undecidable ring with a decidable quotient field. Compare this with the possibility that  $\mathbb{Q}$  is decidable (cf. Robinson [R1, p. 951]). Furthermore, we give (Corollary 10.5) a system of axioms for the theory of  $\mathbb{Q}^{\text{tr}}$ .

**Affirmations.** We are grateful to Moshe Jarden for numerous suggestions

that led to an improved presentation of this paper.

F. Pop told us the characterization of  $G(\mathbb{Q}^{\text{tr}})$  also follows from his “ $\frac{1}{2}$  Riemann existence theorem.” His method uses rigid analytic geometry, versus our use of the classical Riemann existence theorem. We look forward to seeing a written account.

This paper corresponds to a portion of the talk of the first author at the Tempe conference on Arithmetic Geometry, March 1993. Appropos the theme of the Tempe conference, this paper uses profinite ideas of Iwasawa for characterizing absolute Galois groups of fields. The remainder of the talk discussed regular realizations of dihedral groups. It considered the dihedral groups  $D_{p^n}$  of order  $2p^n$  with  $p$  an odd prime and realization of these as Galois groups over  $\mathbb{Q}(x)$  with a bounded numbers of branch points [DF2, section 5.2]. The talk emphasized the relation with rational points on modular curves. Extension of these ideas with a general group  $G$  replacing  $D_p$  will appear under the title **Modular stacks and the Inverse Galois Problem**.

### 1. Ordered fields and an approximation theorem for PRC fields

Let  $K$  be a field of characteristic 0, and let  $G(K)$  be its absolute Galois group. Recall [P1, §6] that the set of orderings  $X(K)$  of  $K$  is a boolean topological space in its natural Harrison topology. This topology is given by a subbase consisting of sets of the form  $H(c) = \{P \in X(K) \mid c \in P\}$ , for  $c \in K^\times$ . Here  $P$  denotes the positive elements in an ordering.

By Artin-Schreier theory [L, XI,§2], the real closures of  $K$  (inside a fixed algebraic closure  $\tilde{K}$  of  $K$ ) are the fixed fields of the involutions in  $G(K)$ . This identifies the set  $\hat{\mathcal{X}}$  of real closures of  $K$  with a topological subspace of  $G(K)$ . It is a boolean space, since the set of involutions is closed in  $G(K)$ . Observe that  $\overline{H}(z) = \{R \in \hat{\mathcal{X}} \mid z \in R\}$  is open in  $\hat{\mathcal{X}}$ , for each  $z \in \tilde{K}^\times$ .

For each  $R \in \hat{\mathcal{X}}$  let  $\pi(R)$  be the restriction of the unique ordering of  $R$  to  $K$ . Then  $\pi(R_1) = \pi(R_2)$  if and only if  $R_1$  and  $R_2$  are conjugate by an automorphism of  $\tilde{K}$  over  $K$ . The map  $\pi: \hat{\mathcal{X}} \rightarrow X(K)$  is continuous:  $\pi^{-1}(H(c)) = \overline{H}(\sqrt{c})$ . Moreover, there exists a closed subset  $\mathcal{X}$  of  $\hat{\mathcal{X}}$  such that  $\pi: \mathcal{X} \rightarrow X(K)$  is a homeomorphism [HJ1, Corollary 9.2]. The corresponding closed subset of involutions in  $G(K)$  contains exactly one representative from each conjugacy class of involutions. Having fixed such  $\mathcal{X}$ , identify  $X(K)$  with it.

REMARK 1.1. *Comments on orderings.*

- (a) If  $K$  is PRC, then every clopen subset of  $X(K)$  is of the form  $H(c)$  for a suitable  $c \in K^\times$  [P2, Proposition 1.3].
- (b) Let  $R$  be a real closed field, and let  $a \in R$ ,  $c \in R^\times$ . If either  $c < 0$  or  $a > 0$ , then the system  $Y^2 + cZ^2 = a$ ,  $Y \neq 0$  has a solution in  $R$ .
- (c) For  $\mathbf{X} = (X_1, \dots, X_n)$  put  $\|\mathbf{X}\|^2 = \sum_{i=1}^n X_i^2$ . Let  $K$  be an ordered field, and let  $\mathbf{a}, \mathbf{b}, \mathbf{c} \in K^n$  and  $\nu \in K^\times$ . From the triangle inequality (over the real closure of  $K$ ), if  $\|\mathbf{a} - \mathbf{b}\|^2, \|\mathbf{b} - \mathbf{c}\|^2 < (\frac{\nu}{2})^2$  then  $\|\mathbf{a} - \mathbf{c}\|^2 < \nu^2$ .

PROPOSITION 1.2. *Let  $K$  be a PRC field, and let  $V \subseteq \mathbb{A}^n$  be an absolutely irreducible affine variety defined over  $K$ . Let  $\mathcal{X}$  be a closed set of real closures of  $K$ , one for each ordering of  $K$ . Let  $\mathcal{X}_1, \dots, \mathcal{X}_m$  be disjoint clopen subsets of  $\mathcal{X}$  that cover  $\mathcal{X}$ . Let  $\mathbf{x}_1, \dots, \mathbf{x}_m$  be nonsingular points on  $V$  such that  $\mathbf{x}_j \in V(R)$  for every  $R \in \mathcal{X}_j$ , for  $j = 1, \dots, m$ . Let  $\nu_1, \dots, \nu_m \in K^\times$ . Then there is  $\mathbf{x} \in V(K)$  such that for each  $1 \leq j \leq m$*

$$(1) \quad \|\mathbf{x} - \mathbf{x}_j\|^2 < \nu_j^2 \text{ in } R, \quad \text{for every } R \in \mathcal{X}_j.$$

PROOF. Fix  $j$  and put  $L = K(\mathbf{x}_j)$ . Let  $R \in \mathcal{X}_j$ . Then  $L \subseteq R$ . As  $K$  is dense in  $R$  [**P2**, Proposition 1.4], there is  $\mathbf{a}_j \in K^n$  such that

$$(2) \quad \|\mathbf{x}_j - \mathbf{a}_j\|^2 < \left(\frac{\nu_j}{2}\right)^2 \text{ in } R.$$

This  $\mathbf{a}_j$  depends on  $R$ , but if  $R' \in \mathcal{X}_j$  is sufficiently close to  $R$ , then (2) holds also with  $R'$  instead of  $R$ . Indeed, the restriction  $\mathcal{X}_j \rightarrow X(L)$  is continuous, and (2) describes a basic open set in  $X(L)$ . Use compactness of  $\mathcal{X}_j$  to partition  $\mathcal{X}_j$  into smaller clopen subsets (and thereby increase  $m$ ). Associate with each of them the original point  $\mathbf{x}_j$  such that (2) holds with suitable  $\mathbf{a}_j$  for all  $R \in \mathcal{X}_j$ .

By Remark 1.1(a), for each  $j$  there is  $c_j \in K^\times$  such that  $\mathcal{X}_j = H(c_j)$ . Suppose that  $V$  is defined by  $f_1(\mathbf{X}), \dots, f_r(\mathbf{X}) \in K[X_1, \dots, X_n]$ . These together with the additional polynomials

$$f_{r+j}(\mathbf{X}, \mathbf{Y}, \mathbf{Z}) = \left(\frac{\nu_j}{2}\right)^2 - \|\mathbf{X} - \mathbf{a}_j\|^2 - Y_j^2 - c_j Z_j^2, \quad j = 1, \dots, m$$

define an absolutely irreducible variety  $W \subseteq \mathbb{A}^{n+2m}$  of dimension  $\dim V + m$ .

Indeed, by induction on  $m$  we may assume that  $m = 1$ . Let  $\mathbf{x}$  be the generic point of  $V$  over  $\tilde{K}$ , that is, the image of  $\mathbf{X}$  in the integral domain  $\tilde{K}[V] = \tilde{K}[\mathbf{X}]/(f_1, \dots, f_r)$ . Let  $u = \left(\frac{\nu_1}{2}\right)^2 - \|\mathbf{x} - \mathbf{a}_1\|^2$ , and let  $y_1$  be transcendental over  $\tilde{K}(V)$ . Observe that  $u \neq 0$ , since, by (2),  $\left(\frac{\nu_1}{2}\right)^2 - \|\mathbf{x}_1 - \mathbf{a}_1\|^2 \neq 0$ . Therefore  $f_{r+1}(\mathbf{x}, y_1, Z_1) = u - y_1^2 - c_1 Z_1^2$  is irreducible over  $\tilde{K}(V)(y_1)$ . Let  $z_1$  be its root in the algebraic closure  $M$  of  $\tilde{K}(V)(y_1)$ . Clearly

$$\tilde{K}[W] = \tilde{K}[\mathbf{X}, Y_1, Z_1]/(f_1, \dots, f_r, f_{r+1}) \cong \tilde{K}[V][y_1, z_1] \subseteq M.$$

It follows that  $\tilde{K}[W]$  is an integral domain, and  $\text{tr.deg.}(W) = \text{tr.deg.}(V) + 1$ . Thus  $W$  is absolutely irreducible and  $\dim W = \dim V + 1$ .

Let  $R \in \mathcal{X}$ . With no loss, assume  $R \in \mathcal{X}_1$ , and hence  $R \notin \mathcal{X}_2, \dots, \mathcal{X}_m$ . Thus,  $c_1$  is positive, and  $c_2, \dots, c_m$  are negative in  $R$ . Apply (2) and Remark 1.1(b) to complete the  $\mathbf{x}_1$  to a point  $(\mathbf{x}_1, \mathbf{y}, \mathbf{z}) \in W(R)$  with  $y_j \neq 0$  for each  $1 \leq j \leq m$ . In particular,  $\frac{\partial f_{r+j}}{\partial Y_j}(\mathbf{x}_1, \mathbf{y}, \mathbf{z}) \neq 0$ :  $(\mathbf{x}_1, \mathbf{y}, \mathbf{z})$  is a nonsingular point on  $W$ .

By the PRC property of  $K$  there exists a point  $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in W(K)$ . Clearly  $\mathbf{x} \in V(K)$ , and for each  $j$  we have  $\|\mathbf{x} - \mathbf{a}_j\|^2 \leq \left(\frac{\nu_j}{2}\right)^2$  in  $R$ , for each  $R \in \mathcal{X}_j$ . This and (2) imply (1), by Remark 1.1(c).  $\square$

Applying Proposition 1.2 to  $V = \mathbb{A}^1$  yields the Block Approximation Lemma of [P3, p. 354]:

**COROLLARY 1.3.** *Let  $K$  be a PRC field. Let  $H_1, \dots, H_m$  be disjoint clopen subsets of  $X(K)$ , and let  $x_1, \dots, x_m \in K$ , and  $\nu_1, \dots, \nu_m \in K^\times$ . Then there is  $x \in K$  such that for every  $j$   $(x - x_j)^2 \leq_P \nu_j^2$  for every  $P \in H_j$ .*

**DEFINITION 1.4.** Let  $\tilde{K}$  be algebraically closed with  $\iota \in \text{Aut}(\tilde{K})$  of order 2.

- (a) For  $c \in \tilde{K}$  let  $|c|_\iota^2 = c \cdot \iota(c)$ .
- (b) For  $\mathbf{z} \in \tilde{K}^n$  let  $\|\mathbf{z}\|_\iota^2 = \sum_{i=1}^n |z_i|_\iota^2$ .
- (c) For a  $\tilde{K}$ -linear morphism  $f: \mathbb{A}^n \rightarrow \mathbb{A}^m$  given by a matrix  $A = (a_{ij}) \in M_{m \times n}(\tilde{K})$  let  $\|f\|_\iota^2 = \sum_{i,j} |a_{ij}|_\iota^2$ .

In the above definition, the fixed field  $R$  of  $\iota$  is real closed, and  $\|c|_\iota^2, \|\mathbf{z}\|_\iota^2, \|f\|_\iota^2$  are nonnegative elements of  $R$ . If  $\mathbf{z} \in R^n$  then  $\|\mathbf{z}\|_\iota^2 = \|\mathbf{z}\|^2$ . Also, in the unique ordering of  $R$ , for all  $\mathbf{z} \in \tilde{K}^n$  the Schwartz inequality gives

$$(3) \quad \|f(\mathbf{z})\|_\iota^2 \leq \|f\|_\iota^2 \cdot \|\mathbf{z}\|_\iota^2.$$

**REMARK 1.5.** The space  $X(\mathbb{Q}^{\text{tr}})$  is homeomorphic to  $X_\omega = \{0, 1\}^{\aleph_0}$ , the universal Boolean space of weight  $\aleph_0$  (cf. the concluding Remark of [FV3]). In particular it has no isolated points.

**LEMMA 1.6.** *If  $K$  is a finitely generated field, then the set  $X^a(K)$  of archimedean orderings on  $K$  is dense in  $X(K)$ .*

**PROOF.** By induction on the number of generators of  $K/\mathbb{Q}$  it suffices to show the following. Let  $K/K_0$  be a simple extension of countable fields, let  $P \in X(K)$ , and let  $P_0 = \text{res}_{K_0} P \in X(K_0)$ . If  $P_0$  is in the closure of  $X^a(K_0)$ , then  $P$  is in the closure of  $X^a(K)$ .

The restriction  $X(K) \rightarrow X(K_0)$  is open [ELW, 4.bis], hence we may assume that  $P_0$  is archimedean. If  $K/K_0$  is algebraic, then  $P$  is also archimedean. Otherwise  $K$  is the field of rational functions in one variable  $t$  over  $K_0$ . Replace  $(K_0, P_0)$  by its real closure (cf. [C, Lemma 8]) to assume that  $K_0$  is real closed.

By [C, Corollary 9(c)], every neighborhood  $U$  of  $P$  in  $X(K)$  contains a set of the form  $\{Q \in X(K) \mid a < t < b \text{ in } Q\}$ , where  $a, b \in K_0$  and  $a < b$  in  $P_0$ . As  $P_0$  is archimedean, we can embed  $K_0$  into  $\mathbb{R}$ . Since  $K_0$  is countable, there is  $c \in \mathbb{R} \setminus K_0$  in the interval  $(a, b)$  in  $\mathbb{R}$ . This  $c$  is then transcendental over  $K_0$ . The  $K_0$ -embedding  $K \rightarrow \mathbb{R}$  given by  $t \mapsto c$  induces an archimedean ordering  $Q$  on  $K$ , and  $a < t < b$  in  $Q$ . Thus  $Q \in U$ .  $\square$

For a subset  $I$  of a group  $G$  let  $\text{Con}_G(I) = \bigcup_{\sigma \in G} I^\sigma$ . We say that  $I$  is a **conjugacy domain**, if  $I$  is closed under the conjugation, that is,  $I = \text{Con}_G(I)$ .

**DEFINITION 1.7.** Let  $F/E$  be a Galois extension of fields with  $F$  not formally real. We say an involution  $\epsilon \in G(F/E)$  is **real** if its fixed field  $F(\epsilon)$  in  $F$  is formally real. Equivalently,  $\epsilon$  is the restriction of an involution in the absolute Galois group  $G(E)$  of  $E$ . Let  $I(F/E)$  be the set of real involutions of  $G(F/E)$ .

Furthermore, assume that  $E$  is a totally real extension of a field  $K$ , and let  $P \in X(K)$ . Denote the involutions  $\epsilon \in G(F/E)$  for which  $P$  extends to an ordering of  $F(\epsilon)$  by  $I_P(F/E)$ . For  $X \subseteq X(K)$ , let  $I_X(F/E) = \bigcup_{P \in X} I_P(F/E)$ . If  $F$  is the algebraic closure of  $E$ , write  $I_P(E)$  for  $I_P(F/E)$ , etc.

REMARK 1.8. (a) If  $E = K$ , then  $I_P(F/E)$  is a conjugacy class in  $G(F/E)$ . In the general case  $I_P(F/E)$  is a conjugacy domain in  $G(F/E)$ ; in fact,

$$I_P(F/E) = \bigcap_{\substack{Q \in X(E) \\ Q \supseteq P}} I_Q(F/E).$$

(b) If  $M/N$  is a finitely generated extension of fields, then the restriction map of orderings  $X(M) \rightarrow X(N)$  is closed and open [ELW, Theorem 4.1 and 4.bis]. In particular, let  $I$  be a set of involutions in  $G(F/E)$ , and assume that  $F/K$  is finitely generated. Then so is  $F(\epsilon)/K$ , for every involution  $\epsilon \in G(F/E)$ . Hence the set  $\{P' \in X(K) \mid I_P(F/E) = I\}$  is closed and open in  $X(K)$ .

LEMMA 1.9. *Let  $(K, P) \subseteq (K', P')$  be an extension of ordered fields. Let  $x$  be transcendental over  $K'$ , and put  $E = K(x)$  and  $E' = K'(x)$ . Furthermore, let  $F/E$  and  $F'/E'$  be Galois extensions with  $F' = F \cdot E$ . Assume that  $F$ , and hence also  $F'$ , is not formally real. Then  $I_P(F/E) = \text{Con}_{G(F/E)} \text{res}_F I_{P'}(F'/E')$ .*

PROOF. We have  $I_P(F/E) = \bigcap_{\substack{Q \in X(E) \\ Q \supseteq P}} I_Q(F/E)$ . Also,

$$I_{P'}(F'/E') = \bigcap_{\substack{Q' \in X(E') \\ Q' \supseteq P'}} I_{Q'}(F'/E').$$

As  $E$  and  $K'$  are linearly disjoint over  $K$ , each extension  $Q$  of  $P$  to  $E$  extends to an ordering  $Q'$  of  $E'$  that extends  $P'$ . Thus it suffices to show

$$I_Q(F/E) = \text{Con}_{G(F/E)} \text{res}_F I_{Q'}(F'/E')$$

for each ordering  $Q$  of  $E$  and for each extension  $Q'$  of  $Q$  to  $E'$ .

Let  $\epsilon' \in I_{Q'}(F'/E')$  and  $\epsilon = \text{res}_F \epsilon'$ . There is an ordering  $R'$  of  $F'(\epsilon')$  that extends  $Q'$ . Its restriction to  $F(\epsilon)$  is an extension of  $Q$ , and hence  $\epsilon \in I_Q(F/E)$ . Since  $I_Q(F/E)$  is a conjugacy class in  $G(F/E)$ , the assertion follows.  $\square$

## 2. Moduli spaces for covers of the Riemann sphere

In this section we add remarks to the notation and results from [FV1] in the form to be used later. Let  $G$  be a finite group, and  $r \geq 3$  an integer.

**(2.1) Covers of the sphere.** Let  $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$  denote the Riemann sphere. We consider covers  $\chi: X \rightarrow \mathbb{P}^1$  of compact (connected) Riemann surfaces. Call two such covers  $\chi: X \rightarrow \mathbb{P}^1$  and  $\chi': X' \rightarrow \mathbb{P}^1$  **equivalent** if there exists an isomorphism  $\alpha: X \rightarrow X'$  with  $\chi' \circ \alpha = \chi$ . Let  $\text{Aut}(X/\mathbb{P}^1)$  denote the group of automorphisms  $\alpha$  of  $X$  with  $\chi \circ \alpha = \chi$ . We say that  $\chi$  is **Galois** if  $\text{Aut}(X/\mathbb{P}^1)$  is transitive on the fibers of  $\chi$ . From now on  $\chi$  will always denote a Galois cover. All but finitely many points of  $\mathbb{P}^1$  have the same number of inverse images under  $\chi$ . These finitely many exceptional points are called the **branch points** of  $\chi$ .

**(2.2) Punctured spheres.** Let  $a_1, \dots, a_r \in \mathbb{P}^1$  be the branch points of (the Galois cover)  $\chi: X \rightarrow \mathbb{P}^1$ , and set  $\mathbf{a} = \{a_1, \dots, a_r\}$ . Then  $\chi$  restricts to an (unramified) topological covering of the punctured sphere  $\mathbb{P}^1 \setminus \mathbf{a}$ . Choose a base point  $a_0$  on this punctured sphere, and consider the (topological) fundamental group  $\Gamma = \Pi_1(\mathbb{P}^1 \setminus \mathbf{a}, a_0)$ , based at  $a_0$  (with the composition law:  $\gamma_1 \gamma_2$  is the path  $\gamma_1$  followed by  $\gamma_2$ ).

Depending on the choice of a base point  $p_0 \in \chi^{-1}(a_0)$ , we get an epimorphism  $\iota: \Gamma \rightarrow \text{Aut}(X/\mathbb{P}^1)$  as follows. For each path  $\gamma$  representing an element  $[\gamma]$  of  $\Gamma$ , let  $p_1$  be the endpoint of the unique lift of  $\gamma$  to  $X \setminus \chi^{-1}(\mathbf{a})$  with initial point  $p_0$ . Then,  $\iota$  sends  $[\gamma]$  to the unique element  $\alpha$  of  $\text{Aut}(X/\mathbb{P}^1)$  with  $\alpha(p_0) = p_1$ .

**(2.3) Related equivalence classes of covers.** Let  $\mathcal{H}^{\text{ab}} = \mathcal{H}_r(G)^{\text{ab}}$  be the set of equivalence classes  $[\chi]$  of all Galois covers  $\chi: X \rightarrow \mathbb{P}^1$  with  $r$  branch points and with  $\text{Aut}(X/\mathbb{P}^1) \cong G$ . Let  $\mathcal{H}^{\text{in}} = \mathcal{H}_r(G)^{\text{in}}$  be the set of equivalence classes  $[\chi, h]$  of pairs  $(\chi, h)$  where  $\chi: X \rightarrow \mathbb{P}^1$  is a Galois cover with  $r$  branch points, and  $h: \text{Aut}(X/\mathbb{P}^1) \rightarrow G$  is an isomorphism. Here  $(\chi, h)$  and  $(\chi': X' \rightarrow \mathbb{P}^1, h')$  are equivalent if there is an isomorphism  $\delta: X \rightarrow X'$  with  $\chi' \circ \delta = \chi$  and  $h' \circ \delta_* = h$ , where  $\delta_*: \text{Aut}(X/\mathbb{P}^1) \rightarrow \text{Aut}(X'/\mathbb{P}^1)$  is the isomorphism  $\alpha \mapsto \delta \circ \alpha \circ \delta^{-1}$ . Let  $\Lambda: \mathcal{H}^{\text{in}} \rightarrow \mathcal{H}^{\text{ab}}$  be the map sending  $[\chi, h]$  to  $[\chi]$ .

**(2.4)  $G$ -covers.** Think of points of  $\mathcal{H}^{\text{in}}$  as equivalence classes  $[\mathbf{a}, a_0, f]$  of triples  $(\mathbf{a}, a_0, f)$ . Here  $\mathbf{a} = \{a_1, \dots, a_r\}$  is a set of  $r$  points of  $\mathbb{P}^1$ , and  $a_0 \in \mathbb{P}^1 \setminus \mathbf{a}$ , and  $f: \Gamma = \Pi_1(\mathbb{P}^1 \setminus \mathbf{a}, a_0) \rightarrow G$  is an epimorphism that does not factor through the canonical map  $\Gamma \rightarrow \Pi_1((\mathbb{P}^1 \setminus \mathbf{a}) \cup \{a_i\}, a_0)$ , for any  $i$ . (The latter condition means that the corresponding cover  $\chi$  has **exactly**  $r$  branch points). Call two such triples  $(\mathbf{a}, a_0, f)$  and  $(\tilde{\mathbf{a}}, \tilde{a}_0, \tilde{f})$  equivalent if  $\mathbf{a} = \tilde{\mathbf{a}}$  and there is a path  $\omega$  from  $a_0$  to  $\tilde{a}_0$  in  $\mathbb{P}^1 \setminus \mathbf{a}$  such that  $\tilde{f} \circ \omega_* = f$ . Here  $\omega_*: \Pi_1(\mathbb{P}^1 \setminus \mathbf{a}, a_0) \rightarrow \Pi_1(\mathbb{P}^1 \setminus \mathbf{a}, \tilde{a}_0)$  is the isomorphism  $\gamma \mapsto \omega^{-1} \gamma \omega$ .

**(2.5) Covers versus cycle descriptions.** Here is the correspondence between the above pairs and triples [FV1, §1.2]. Given  $[\chi, h] \in \mathcal{H}^{\text{in}}$ , with  $\chi: X \rightarrow \mathbb{P}^1$  as above, let  $\mathbf{a}$  be the set of branch points of  $\chi$ , and choose  $a_0 \in \mathbb{P}^1 \setminus \mathbf{a}$  and  $p_0 \in \chi^{-1}(a_0)$ . Set  $\Gamma = \Pi_1(\mathbb{P}^1 \setminus \mathbf{a}, a_0)$  as above, and define  $f: \Gamma \rightarrow G$  as  $f = h \circ \iota$ , where  $\iota: \Gamma \rightarrow \text{Aut}(X/\mathbb{P}^1)$  is the map from (2.2). Recall that  $\iota$  is canonical up to composition with inner automorphisms of  $\text{Aut}(X/\mathbb{P}^1)$ . Thus  $h$  and  $f$  determine each other up to inner automorphisms of  $G$ . This is compatible with the equivalence of pairs (resp., triples).

**(2.6) The topology on  $\mathcal{H}^{\text{in}}$ .** To specify a neighborhood  $\mathcal{N}$  of the point  $[\mathbf{a}, a_0, f]$  of  $\mathcal{H}^{\text{in}}$ , where  $\mathbf{a} = \{a_1, \dots, a_r\}$ , choose pairwise disjoint open discs  $D_1, \dots, D_r$  around  $a_1, \dots, a_r$ , with  $a_0 \notin D_1 \cup \dots \cup D_r$ . Then  $\mathcal{N}$  consists of all points  $[\tilde{\mathbf{a}}, \tilde{a}_0, \tilde{f}]$  such that  $\tilde{\mathbf{a}}$  has exactly one point in each  $D_i$ , and  $\tilde{f}$  is the composition of the canonical isomorphisms

$$\Pi_1(\mathbb{P}^1 \setminus \tilde{\mathbf{a}}, \tilde{a}_0) \cong \Pi_1(\mathbb{P}^1 \setminus (D_1 \cup \dots \cup D_r), \tilde{a}_0) \cong \Pi_1(\mathbb{P}^1 \setminus \mathbf{a}, a_0)$$

with  $f$ . These  $\mathcal{N}$  form a basis for the topology. They are connected. The sets  $\Lambda(\mathcal{N})$  form a basis for a topology on  $\mathcal{H}^{\text{ab}}$ , such that  $\Lambda: \mathcal{H}^{\text{in}} \rightarrow \mathcal{H}^{\text{ab}}$  becomes an (unramified) covering.

**(2.7)  $r$ -tuples of unordered branch points.** Let  $\mathcal{U}_r$  denote the space of all subsets of cardinality  $r$  of the Riemann sphere  $\mathbb{P}^1$ . It has a natural structure of algebraic variety defined over  $\mathbb{Q}$  [FV1, §1.1]; it is isomorphic to  $\mathbb{P}^r \setminus D$ , where  $D$ , the discriminant locus, is a hypersurface in  $\mathbb{P}^r$ . In particular,  $\mathcal{U}_r$  is an affine variety. Furthermore, if  $K$  is a subfield of  $\mathbb{C}$  and  $\mathbf{a} = \{a_1, \dots, a_r\} \in \mathcal{U}_r$  with  $a_1, \dots, a_r \neq \infty$ , then  $\mathbf{a}$  is  $K$ -rational if and only if  $\prod_{i=1}^r (X - a_i) \in K[X]$ . As a complex manifold, the topology of  $\mathcal{U}_r$  has a basis consisting of sets  $\mathcal{D}$  of the following form: Given pairwise disjoint open discs  $D_1, \dots, D_r$  on  $\mathbb{P}^1$ , let  $\mathcal{D}$  be the set of all  $\mathbf{a} \in \mathcal{U}_r$  with  $|\mathbf{a} \cap D_i| = 1$  for  $i = 1, \dots, r$ .

**(2.8) Maps to  $\mathcal{U}_r$ .** Define  $\Psi: \mathcal{H}^{\text{in}} \rightarrow \mathcal{U}_r$  and  $\bar{\Psi}: \mathcal{H}^{\text{ab}} \rightarrow \mathcal{U}_r$  by sending  $[\chi, h]$  and  $[\chi]$ , respectively, to the set of branch points of  $\chi$ . These maps are (unramified) coverings and  $\bar{\Psi} \circ \Lambda = \Psi$ . Through these coverings the spaces  $\mathcal{H}^{\text{ab}}$  and  $\mathcal{H}^{\text{in}}$  inherit a structure of complex manifold from  $\mathcal{U}_r$ .

**(2.9) The algebraic structure on covers.** Each cover  $\chi: X \rightarrow \mathbb{P}^1$  as above is an algebraic morphism of algebraic varieties over  $\mathbb{C}$ , compatible with its analytic structure (Riemann's existence theorem). An automorphism  $\beta$  of  $\mathbb{C}$  defines an automorphism  $\beta^*$  of  $\mathbb{P}^1$  by  $(x_0 : x_1) \mapsto (\beta^{-1}(x_0) : \beta^{-1}(x_1))$ . Consider the cover  $\beta(\chi): \beta(X) \rightarrow \mathbb{P}^1$  obtained from  $\chi: X \rightarrow \mathbb{P}^1$  through base change with  $\beta^*$ . Furthermore, for each  $\alpha \in \text{Aut}(X/\mathbb{P}^1)$  let  $\beta_*(\alpha) = \beta(\alpha) \in \text{Aut}(\beta(X)/\mathbb{P}^1)$  be the morphism obtained by the same base change.

**(2.10) The algebraic structure on  $\mathcal{H}^{\text{in}}$ .** The spaces  $\mathcal{H}^{\text{ab}}$  and  $\mathcal{H}^{\text{in}}$  have a unique structure of (the set of complex points of) a (reducible) algebraic variety defined over  $\mathbb{Q}$  [FV1, Theorem 1]. This variety structure is compatible with the analytic structure of  $\mathcal{H}^{\text{ab}}$  and  $\mathcal{H}^{\text{in}}$ , and it makes the maps  $\Psi$ ,  $\bar{\Psi}$  and  $\Lambda$  into algebraic morphisms defined over  $\mathbb{Q}$ . Also, each automorphism  $\beta$  of  $\mathbb{C}$ —in its natural action  $(x_1, \dots, x_n) \mapsto (\beta(x_1), \dots, \beta(x_n))$  on the complex points of (the affine pieces of) a variety defined over  $\mathbb{Q}$ —sends the point  $[\chi] \in \mathcal{H}^{\text{ab}}$  to  $[\beta(\chi)]$  and the point  $[\chi, h] \in \mathcal{H}^{\text{in}}$  to  $[\beta(\chi), h \circ \beta_*^{-1}]$ .

**(2.11) Complex conjugation acting on  $\mathcal{H}^{\text{in}}$ .** We can describe the action of complex conjugation  $c$  on the triples of (2.4) that compose  $\mathcal{H}^{\text{in}}$ . Namely,  $c$  naturally acts on paths in  $\mathbb{P}^1$ . Thus, it induces a map  $\Pi_1(\mathbb{P}^1 \setminus \mathbf{a}, a_0) \rightarrow \Pi_1(\mathbb{P}^1 \setminus c(\mathbf{a}), c(a_0))$ . Denote this map by  $\gamma \mapsto c\gamma$ .

LEMMA. *If  $\mathbf{p} = [\mathbf{a}, a_0, f] \in \mathcal{H}^{\text{in}}$ , then  $c(\mathbf{p}) = [c(\mathbf{a}), c(a_0), cf]$ . Here  $(cf)(c\gamma) = f(\gamma)$  for each  $\gamma \in \Pi_1(\mathbb{P}^1 \setminus \mathbf{a}, a_0)$ .*

PROOF. Write  $\mathbf{p}$  as  $\mathbf{p} = [\chi, h]$ . Then  $c(\mathbf{p}) = [c(\chi), h \circ c_*^{-1}]$ . It remains to show that this point is represented by the triple  $(c(\mathbf{a}), c(a_0), cf)$ . This is a straightforward consequence of the definitions (cf. [DF1, Lemma 2.1]).  $\square$



**(2.12)  $r$ -tuples of all conjugacy classes of  $G$ .** Let  $\mathbf{b} = \{b_1, \dots, b_r\} \in \mathcal{U}_r$  such that  $0 \notin \mathbf{b}$ . We can choose generators  $\gamma_1, \dots, \gamma_r$  for the fundamental group  $\Pi_1(\mathbb{P}^1 \setminus \mathbf{b}, 0)$  so that  $\gamma_1 \cdots \gamma_r = 1$  is the only relation among them. Indeed, assume that  $b_j = \zeta^j$ , for  $j = 1, \dots, r$ , where  $\zeta = e^{\frac{2\pi i}{r}}$ . Otherwise apply a homeomorphism  $\mathbb{P}^1 \rightarrow \mathbb{P}^1$  that maps 0 onto itself and  $b_j$  onto  $\zeta_j$ . Let  $\tilde{\gamma}_j$  be a path starting at 0, going up on a straight line to a neighborhood of  $b_j$ , traversing a small disk around  $b_j$  in the counterclockwise direction, and following the same straight line back to 0. Then  $\tilde{\gamma}_1, \dots, \tilde{\gamma}_r$  do not intersect except at 0. Let  $\gamma_j$  be the homotopy class of  $\tilde{\gamma}_j$ . Then  $\gamma_1, \dots, \gamma_r$  generate  $\Pi_1(\mathbb{P}^1 \setminus \mathbf{b}, 0)$  and  $\gamma_1 \cdots \gamma_r = 1$ .

Represent a point  $\mathbf{p} \in \Psi^{-1}(\mathbf{b})$  by a triple  $(\mathbf{b}, 0, f)$ . The  $r$ -tuple  $(\sigma_1, \dots, \sigma_r) = (f(\gamma_1), \dots, f(\gamma_r))$  determines the epimorphism  $f: \Pi_1(\mathbb{P}^1 \setminus \mathbf{b}, 0) \rightarrow G$ . It has the following properties:  $\sigma_1 \cdots \sigma_r = 1$ ,  $\sigma_1, \dots, \sigma_r$  generate  $G$ , and  $\sigma_j \neq 1$  for all  $j$  [FV1, §1.3]. Let  $\mathcal{E}_r$  denote the set of such  $r$ -tuples  $(\sigma_1, \dots, \sigma_r)$ . Clearly, each  $(\sigma_1, \dots, \sigma_r) \in \mathcal{E}_r$  arises in the above way from some  $\mathbf{p} \in \Psi^{-1}(\mathbf{b})$ . Let  $\mathcal{L}(G)$  be the collection of conjugacy classes  $\neq \{1\}$  of  $G$ , and let  $\mathcal{E}^{(r)}$  be all  $r$ -tuples  $(\sigma_1, \dots, \sigma_r) \in \mathcal{E}_r$  where each  $\mathcal{C} \in \mathcal{L}(G)$  is represented exactly  $r/|\mathcal{L}(G)|$  times among  $\sigma_1, \dots, \sigma_r$ .

**(2.13) When commutators generate the Schur multiplier of  $G$ .** For the rest of section 2 assume that  $r$  is a multiple of  $|\mathcal{L}(G)|$  and suitably large [FV1, Appendix], and the Schur multiplier of  $G$  is generated by commutators. We explain the latter condition. Let  $R$  be a group of maximal order with the property that  $R$  has a subgroup  $M \leq R' \cap Z(R)$  satisfying  $R/M \cong G$ . Then  $M \cap \{g^{-1}h^{-1}gh \mid g, h \in R\}$  generates  $M$ , the Schur multiplier of  $G$ .

Fix  $\mathbf{b} \in \mathcal{U}_r$  and  $\gamma_1, \dots, \gamma_r$  as above. By [FV1, §1.3] there is a (unique) connected component  $\mathcal{H}$  of  $\mathcal{H}^{\text{in}}$  containing  $\{[\mathbf{b}, 0, f] \mid (f(\gamma_1), \dots, f(\gamma_r)) \in \mathcal{E}^{(r)}\}$ . Let  $\bar{\mathcal{H}} = \Lambda(\mathcal{H})$  be its image in  $\mathcal{H}^{\text{ab}}$ . We call  $\mathcal{H}$  and  $\bar{\mathcal{H}}$  **Hurwitz spaces**. By [FV1, Thm. 1] they are absolutely irreducible algebraic varieties defined over  $\mathbb{Q}$ . Moreover, since  $\Psi: \mathcal{H} \rightarrow \mathcal{U}_r$  and  $\bar{\Psi}: \bar{\mathcal{H}} \rightarrow \mathcal{U}_r$  are finite normal covers of an affine variety,  $\mathcal{H}$  and  $\bar{\mathcal{H}}$  are affine [H, Exc. III.4.1].

**(2.14) Automorphisms of  $\mathcal{H}^{\text{in}} \rightarrow \mathcal{H}^{\text{ab}}$ .** For  $A \in \text{Aut}(G)$  (acting from the left on  $G$ ), let  $\delta_A: \mathcal{H} \rightarrow \mathcal{H}$  be the map sending the point  $[\chi, h]$  to  $[\chi, A \circ h]$ . Then  $\delta_A$  is an automorphism of the covering  $\Lambda: \mathcal{H} \rightarrow \bar{\mathcal{H}}$ . It depends only on the class of  $A$  modulo  $\text{Inn}(G)$ . In fact,  $\Lambda$  is a Galois covering, and the map  $A \mapsto \delta_A$  induces an isomorphism  $\delta: \text{Out}(G) = \text{Aut}(G)/\text{Inn}(G) \rightarrow \text{Aut}(\mathcal{H}/\bar{\mathcal{H}})$  [FV1, §6.1]. Furthermore,  $\delta_A$  is a morphism defined over  $\mathbb{Q}$  [FV1, §6.2]. In the description of  $\mathcal{H}^{\text{in}}$  in (2.4),  $\delta_A$  sends the point  $[\mathbf{a}, a_0, f]$  to  $[\mathbf{a}, a_0, A \circ f]$ . As  $\Lambda: \mathcal{H}^{\text{in}} \rightarrow \mathcal{H}^{\text{ab}}$  is an unramified covering (2.8),  $\delta_A$  has no fixed points.

For the rest of this section assume that  $G$  has trivial center. Accordingly, identify  $G$  with the subgroup  $\text{Inn}(G)$  of  $\text{Aut}(G)$  (acting from the left on  $G$ ). Let  $\mathbf{p} \in \mathcal{H}$  and let  $K \subseteq L$  be subfields of  $\mathbb{C}$  such that  $\Lambda(\mathbf{p}) \in \bar{\mathcal{H}}(K)$  and  $L = K(\mathbf{p})$ .

**(2.15) Fields of definition of covers.** Write  $\mathbf{p}$  as  $\mathbf{p} = [\chi, h]$ . Then, the cover  $\chi: X \rightarrow \mathbb{P}^1$  can be defined over  $L$  (in a unique way) such that all auto-

morphisms of  $\chi$  are defined over  $L$  [FV1, Cor. 1]. Thus, there is a unique cover  $\chi_L: X_L \rightarrow \mathbb{P}_L^1$  such that base change with the embedding  $L \rightarrow \mathbb{C}$  gives  $\chi$  from  $\chi_L$  and the automorphisms of  $\chi$  from the automorphisms of  $\chi_L$ .

**(2.16) Fields of definition of automorphisms.** We recall some facts from [FV1, §6.3]. The function field  $F = L(X_L)$  is regular over  $L$ , and the extension  $F/L(x)$  induced by  $\chi$  is Galois. Here,  $x$  is the identity function on  $\mathbb{P}^1$ . The group  $G(F/L(x))$  (acting from the left on  $F$ ) is canonically isomorphic to  $\text{Aut}(X/\mathbb{P}^1)$ , via the map that sends  $\alpha \in \text{Aut}(X/\mathbb{P}^1)$  to the element  $g \mapsto g \circ \alpha^{-1}$  of  $G(F/L(x))$ . Let  $h_0: G(F/L(x)) \rightarrow G$  be the composition of this isomorphism with  $h: \text{Aut}(X/\mathbb{P}^1) \rightarrow G$ .

**(2.17) Identification of automorphisms of  $G$ .** Furthermore,  $L/K$  and  $F/K(x)$  are Galois extensions, and the centralizer of  $G(F/L(x))$  in  $G(F/K(x))$  is trivial. This implies  $h_0$  extends to a unique embedding  $h_1: G(F/K(x)) \rightarrow \text{Aut}(G)$ . [FV1, Proposition 3] says:  $H := h_1(G(F/K(x)))$  equals

$$\{A \in \text{Aut}(G) \mid \delta_A(\mathbf{p}) \text{ is conjugate to } \mathbf{p} \text{ under } G(L/K)\}.$$

**(2.18) Action by automorphisms of  $\mathbb{C}$ .** Let  $\beta$  be an automorphism of  $\mathbb{C}$ , and let  $K$  and  $K'$  be two subfields of  $\mathbb{C}$  such that  $\beta(K) \subseteq K'$ . Put  $\mathbf{p}' = \beta(\mathbf{p})$  and  $L' = K'(\mathbf{p}')$ . Then  $\beta(L) \subseteq L'$ , and  $\Lambda(\mathbf{p}') \in \mathcal{H}(K')$ . Let  $F'/L'(x)$  be the Galois extension associated to  $K'$  and the point  $\mathbf{p}'$  of  $\mathcal{H}$ , and let  $h'_1: G(F'/K'(x)) \rightarrow \text{Aut}(G)$  be the associated embedding. Then the following holds:

Let  $\beta: L(x) \rightarrow L'(x)$  be the extension of  $\beta$  (fixing  $x$ ). This map extends further to  $\beta: F \rightarrow F'$  such that canonically

$$(1) \quad F' \equiv \beta(F) \otimes_{\beta(L)} L' \equiv F \otimes_L L'.$$

Consider restriction  $\beta^*: G(F'/K'(x)) \rightarrow G(F/K(x))$ :  $\sigma \in G(F'/K'(x))$  goes to  $\beta^{-1}\sigma|_{\beta(F)}\beta$ . It is injective and it gives an isomorphism  $G(F'/L'(x)) \rightarrow G(F/L(x))$ . Further, it makes the following diagram commutative:

$$(2) \quad \begin{array}{ccc} G(F'/K'(x)) & \xrightarrow{\beta^*} & G(F/K(x)) \\ & \searrow h'_1 & \swarrow h_1 \\ & \text{Aut}(G) & \end{array}$$

PROOF (2) COMMUTES. We have  $\mathbf{p}' = [\beta(\chi), h \circ \beta_*^{-1}]$  by (2.10). The natural action of  $\beta \in \text{Aut}(\mathbb{C})$  on functions defined over  $L$  extends  $\beta$  to a map from  $F = L(X)$  to  $F' = L(\beta(X))$ . Then (1) follows from the fact that  $F$  is regular over  $L$ , and  $[F': L'(x)] = [F : L(x)] (= \deg(\chi))$ . The proof of (2) is straightforward from the definitions.  $\square$

**(2.19) Conclusion from (2.18).** In (2.18) and Lemma 1.9 we have

$$h'_1(I_{P'}(F'/E')) \subseteq h_1(I_P(F/E)) \quad \text{and} \quad \text{Con}_H h'_1(I_{P'}(F'/E')) = h_1(I_P(F/E)),$$

where  $H$  is the image of  $h_1$  in  $\text{Aut}(G)$ . If the ‘restriction’ map  $\beta^*: G(F'/K'(x)) \rightarrow G(F/K(x))$  is an isomorphism, then  $h'_1(I_{P'}(F'/E')) = h_1(I_P(F/E))$ . Indeed,

without loss of generality assume that the map  $\beta: K \rightarrow K'$  is an inclusion of fields. Hence  $\beta^* = \text{res}_F$ . In the commutative diagram (2) we may replace  $\text{Aut}(G)$  by  $H$ , so that  $h_1$  is an isomorphism. The assertions follow from the commutativity of that diagram.

### 3. Group-theoretic lemmas

For a group  $G$  and  $r \geq 0$  put  $\dot{G} = G \setminus \{1\}$ . Let  $\mathcal{L}(G)$  be the nontrivial conjugacy classes of  $G$ , and put  $l = |\mathcal{L}(G)|$ . For an  $r$ -tuple  $\sigma = (\sigma_1, \dots, \sigma_r) \in \dot{G}^r$  and  $\mathcal{C} \in \mathcal{L}(G)$ , let  $n_{\mathcal{C}}(\sigma)$  be the number of indices,  $1 \leq i \leq r$ , with  $\sigma_i \in \mathcal{C}$ . Then  $\sum_{\mathcal{C} \in \mathcal{L}(G)} n_{\mathcal{C}}(\sigma) = r$ .

**LEMMA 3.1.** *Let  $G$  be a finite group. Every sufficiently large multiple  $r$  of  $4l$  satisfies the following. Let  $\epsilon \in \text{Aut}(G)$  be of order 2 and let  $I$  be involutions in  $(G \rtimes \langle \epsilon \rangle) \setminus G$  with  $\epsilon \in I$ . Let  $e = 8 \cdot |G|!$  if  $|I| \geq 2$ , and  $e = 0$  if  $|I| = 1$ . Put  $m = r - e$ . Then there are sequences  $\sigma \in \dot{G}^e$ ,  $\tau \in \dot{G}^m$  with these properties:*

- (a1)  $\sigma_i^\epsilon = \sigma_1 \cdots \sigma_{i-1} \sigma_i^{-1} \sigma_{i-1}^{-1} \cdots \sigma_1^{-1}$ , for each  $1 \leq i \leq e$ ;
- (a2)  $\tau_j^\epsilon = \tau_{m+1-j}^{-1}$  for each  $1 \leq j \leq m$ ;
- (b)  $I = \{\epsilon, \epsilon\sigma_1, \epsilon\sigma_1\sigma_2, \dots, \epsilon\sigma_1\sigma_2 \cdots \sigma_e\}$ ;
- (c)  $(\sigma, \tau) \in \mathcal{E}^{(r)}(G)$ ; or  $\langle \sigma_1, \dots, \sigma_e, \tau_1, \dots, \tau_m \rangle = G$ ,  $\sigma_1 \cdots \sigma_e \tau_1 \cdots \tau_m = 1$ , and  $n_{\mathcal{C}}(\sigma, \tau) = r/l$  for each  $\mathcal{C} \in \mathcal{L}(G)$ .

**PROOF.** We may consider  $\epsilon \in \text{Aut}(G)$ ,  $|\epsilon| = 2$ , and one set  $I$  of involutions.

**A. Separation of  $\sigma$  from  $\tau$ .** Define an equivalence relation on  $\mathcal{L}(G)$ : the class  $[\mathcal{C}]$  is  $\{\mathcal{C}, \mathcal{C}^{-1}, \mathcal{C}^\epsilon, \mathcal{C}^{-\epsilon}\}$ . Part B constructs  $\sigma \in \dot{G}^e$  with (a1), (b),

- (c1)  $\sigma_1 \cdots \sigma_e = 1$ ; and
- (d1) for each  $[\mathcal{C}]$  there is  $\mu_{[\mathcal{C}]} \geq 0$  such that  $n_{\mathcal{C}}(\sigma) = 4\mu_{[\mathcal{C}]}$ .

Observe that  $e = \sum_{\mathcal{C} \in \mathcal{L}(G)} n_{\mathcal{C}}(\sigma) = 4 \sum_{\mathcal{C} \in \mathcal{L}(G)} \mu_{[\mathcal{C}]}$ . Also, for each  $[\mathcal{C}]$  let  $\nu_{[\mathcal{C}]}$  be a positive integer and  $m = 4 \sum_{\mathcal{C} \in \mathcal{L}(G)} \nu_{[\mathcal{C}]}$ . Part C shows there is  $\tau \in \dot{G}^m$  satisfying (a2),

- (c2)  $\langle \tau_1, \dots, \tau_m \rangle = G$  and  $\tau_1 \cdots \tau_m = 1$ , and
- (d2)  $n_{\mathcal{C}}(\tau) = 4\nu_{[\mathcal{C}]}$ , for each  $\mathcal{C}$ .

Let  $n = \frac{r}{4l}$ , and assume  $n > \mu_{[\mathcal{C}]}$  for each  $[\mathcal{C}]$ . In the last step with  $\nu_{[\mathcal{C}]} = n - \mu_{[\mathcal{C}]}$ ,

$$e + m = 4 \sum_{\mathcal{C} \in \mathcal{L}(G)} \mu_{[\mathcal{C}]} + 4 \sum_{\mathcal{C} \in \mathcal{L}(G)} \nu_{[\mathcal{C}]} = 4 \sum_{\mathcal{C} \in \mathcal{L}(G)} n = 4ln = r.$$

Substituting (c1), (c2), (d1), and (d2) in the expressions for (c) shows (c) holds. In fact,  $n_{\mathcal{C}}(\sigma, \tau) = 4n = \frac{r}{l}$  for each  $\mathcal{C} \in \mathcal{L}(G)$ .

**B. Construction of  $\sigma$ .** If  $I = \{\epsilon\}$ , let  $e = 0$  and  $\sigma = ()$ . Otherwise put  $\sigma = (\epsilon_1\epsilon_2, \epsilon_2\epsilon_3, \dots, \epsilon_e\epsilon_1)$ , where  $\epsilon_1 = \epsilon, \epsilon_2, \dots, \epsilon_e \in I$ , not necessarily distinct, but  $\epsilon_1 \neq \epsilon_2 \neq \dots \neq \epsilon_e \neq \epsilon_1$ . Then  $\sigma$  satisfies (a1) and (c1). Furthermore, if  $I = \{\epsilon_1, \dots, \epsilon_e\}$ , then  $\sigma$  also satisfies (b). To construct such  $\epsilon_1, \dots, \epsilon_e$ , let  $n' = \frac{e}{2|I \setminus \{\epsilon\}|}$ . Note:  $n'$  is an integer divisible by 4, because  $|I \setminus \{\epsilon\}| < |G|$ . Let

$\epsilon_i = \epsilon$  for odd  $i$ , and choose  $\epsilon_2, \epsilon_4, \dots, \epsilon_e$  so that each element of  $I \setminus \{\epsilon\}$  occurs in this sequence exactly  $n'$  times.

Let  $g \in G$ , and let  $n_g(\boldsymbol{\sigma})$  be the number of indices  $1 \leq i \leq e$  for which  $\sigma_i = g$ . From the above,  $4|n_g(\boldsymbol{\sigma})$ . Moreover,  $\sigma_{2i-1}^\epsilon = \epsilon(\epsilon\epsilon_{2i})\epsilon = \sigma_{2i-1}^{-1} = \sigma_{2i}$ , for each  $1 \leq i \leq e/2$ . Hence,  $n_g(\boldsymbol{\sigma}) = n_{g^{-1}}(\boldsymbol{\sigma}) = n_{g^\epsilon}(\boldsymbol{\sigma}) = n_{g^{-\epsilon}}(\boldsymbol{\sigma})$ . This yields (d1).

**C. Construction of  $\boldsymbol{\tau}$ .** For each  $[\mathcal{C}]$  let  $\nu_{[\mathcal{C}]}$  be a positive integer. Choose  $k$  and  $\mathbf{g} = (g_1, \dots, g_k) \in \dot{G}^k$  such that  $n_{\mathcal{C}}(\mathbf{g}) = \nu_{[\mathcal{C}]}$ , for each  $\mathcal{C}$ . In particular,  $\mathbf{g}$  contains an entry from each  $\mathcal{C} \in \mathcal{L}(G)$ . A proper subgroup of  $G$  misses some conjugacy classes of  $G$  [FJ, Lemma 12.4]. Therefore,  $G = \langle g_1, \dots, g_k \rangle$ . Furthermore,  $k = \sum_{\mathcal{C} \in \mathcal{L}(G)} \nu_{[\mathcal{C}]} = \frac{m}{4}$ . Put

$$\boldsymbol{\tau} = (g_1, g_1^{-1}, \dots, g_k, g_k^{-1}, g_k^\epsilon, g_k^{-\epsilon}, \dots, g_1^\epsilon, g_1^{-\epsilon}).$$

This choice satisfies (a2) and (c2), and, for each  $\mathcal{C}$ ,

$$n_{\mathcal{C}}(\boldsymbol{\tau}) = n_{\mathcal{C}}(\mathbf{g}) + n_{\mathcal{C}^{-1}}(\mathbf{g}) + n_{\mathcal{C}^\epsilon}(\mathbf{g}) + n_{\mathcal{C}^{-\epsilon}}(\mathbf{g}) = 4\nu_{[\mathcal{C}]}. \quad \square$$

LEMMA 3.2. *Let  $1 \rightarrow G \rightarrow H \xrightarrow{\pi} C \rightarrow 1$  be an exact sequence of finite groups, and let  $I$  be a set of involutions in  $H \setminus G$ . There exists a commutative diagram*

$$(1) \quad \begin{array}{ccccccc} 1 & \longrightarrow & \tilde{G} & \longrightarrow & \tilde{H} & \xrightarrow{\tilde{\pi}} & C & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \parallel & & \\ 1 & \longrightarrow & G & \longrightarrow & H & \xrightarrow{\pi} & C & \longrightarrow & 1 \end{array}$$

with exact rows and surjective vertical maps such that the Schur multiplier of  $\tilde{G}$  is generated by commutators and  $C_{\tilde{H}}(\tilde{G}) = 1$ . Finally, every involution in  $I$  lifts to at least two involutions in  $\tilde{H}$ .

PROOF. Choose a presentation  $1 \rightarrow \mathcal{R} \rightarrow \mathcal{F} \rightarrow H \rightarrow 1$ , where  $\mathcal{F}$  is the free product of a free group of finite rank with finitely many groups of order 2, say  $\langle \delta_1 \rangle, \dots, \langle \delta_e \rangle$ , such that  $\{\delta_1, \dots, \delta_e\}$  maps onto  $I$ . The inverse image  $\mathcal{F}_1$  of  $G$  in  $\mathcal{F}$  contains no conjugates of  $\delta_1, \dots, \delta_e$ . By the Kurosh Subgroup Theorem [M, Theorem VII.5.1 and Proposition VII.5.3] it is a free of finite rank. Let  $\mathcal{N} = [\mathcal{F}_1, \mathcal{R}]$  be the group generated by commutators  $[f, r]$  with  $f \in \mathcal{F}_1, r \in \mathcal{R}$ . Set  $F = \mathcal{F}/\mathcal{N}$ ,  $F_1 = \mathcal{F}_1/\mathcal{N}$ , and  $R = \mathcal{R}/\mathcal{N}$ . Then  $1 \rightarrow R \rightarrow F_1 \rightarrow G \rightarrow 1$  is a central extension.

Schur multiplier theory [Hu, Kap.5, §23] shows  $R$  is the direct product of the Schur multiplier  $M(G) = R \cap (F_1)'$  and a free abelian group  $A$ . Let  $A_0$  be the intersection of all the  $F$ -conjugates of  $A$ . Then  $A_0 \triangleleft F$ . Since  $(R : A) = |M(G)| < \infty$ , also  $(F : A_0) < \infty$ . Set  $\tilde{H} = F/A_0$ ,  $\tilde{G} = F_1/A_0$ , and  $S = R/A_0$ , to get diagram (1). The image  $\tilde{I}$  of  $\{\delta_1, \dots, \delta_e\}$  in  $\tilde{H}$  maps onto  $I$ . Notice that  $S$  is the direct product of  $S \cap (\tilde{G})' \cong M(G)$  and  $A/A_0$ . As in the proof of [FV3, Lemma 2] the Schur multiplier of  $\tilde{G}$  is generated by commutators.

Replace  $G, H$ , and  $I$  by  $\tilde{G}, \tilde{H}$ , and  $\tilde{I}$ , to assume that the Schur multiplier of  $G$  is generated by commutators. Let  $T$  be a non-abelian finite simple group with trivial Schur multiplier. For example, take  $T = \text{SL}_2(8)$  [Hu, Satz 25.7].

Form the regular wreath product  $\tilde{H}$  of  $H$  with  $T$  (e.g., [Hu, Def. 15.6]). Thus  $\tilde{H} = T^j \rtimes H$ , with  $j = |H|$ , and  $H$  acts on  $T^j$  by permuting the factors in its regular representation. Let  $\tilde{G}$  be  $T^j \rtimes G \leq \tilde{H}$ . Clearly,  $C_{\tilde{H}}(T^j) = 1$ , and hence  $C_{\tilde{H}}(\tilde{G}) = 1$ . If  $\epsilon \in I$  and  $\tau \in T^j$ , then  $\tau^{-1}\epsilon\tau$  is an involution in  $\tilde{H}$  that maps to  $\epsilon$ . This proves the last assertion of the lemma.

Since  $M(T) = 1$ , every central extension of  $T$  splits. This implies that every representation group of  $\tilde{G}$  has a normal subgroup isomorphic to  $T^j$  such that the quotient by this subgroup is a representation group of  $G$ . Therefore,  $M(\tilde{G}) \equiv M(G)$  is generated by commutators.  $\square$

LEMMA 3.3. *Let  $\pi: H \rightarrow \bar{H}$  be an epimorphism of finite groups, and let  $I_1, \dots, I_m \subseteq H$  and  $\bar{I}_1, \dots, \bar{I}_m \subseteq \bar{H}$  be sets of involutions such that  $\pi(I_j) = \bar{I}_j$ . Then there exists a finite group  $\tilde{H}$ , a surjection  $\rho: \tilde{H} \rightarrow H$ , and sets of involutions  $\tilde{I}_1, \dots, \tilde{I}_m \subseteq \tilde{H}$  such that  $\rho(\tilde{I}_j) = I_j$  for every  $j$ , and every automorphism  $\bar{\alpha}$  of  $\bar{H}$  that satisfies  $\bar{\alpha}(\bar{I}_j) = \bar{I}_j$  for all  $j$ , lifts to an automorphism  $\tilde{\alpha}$  of  $\tilde{H}$  (that is,  $(\pi \circ \rho) \circ \tilde{\alpha} = \bar{\alpha} \circ (\pi \circ \rho)$ ) that satisfies  $\tilde{\alpha}(\tilde{I}_j) = \tilde{I}_j$  for all  $j$ . Moreover, if the  $I_j$  are conjugacy domains in  $H$ , then the  $\tilde{I}_j$  can be taken conjugacy domains in  $\tilde{H}$ .*

PROOF. Let  $K$  be a set of cardinality  $\text{Ker}(\pi)$ . Consider the free product

$$\tilde{H} = \left( \prod_{\substack{\bar{h} \in \bar{H} \\ k \in K}} \langle x_{\bar{h},k} \rangle \right) * \left( \prod_{\substack{\bar{\epsilon} \in \bar{I} \\ k \in K}} \langle \tilde{\epsilon}_{\bar{\epsilon},k,1} \rangle \right) * \left( \prod_{\substack{\bar{\epsilon} \in \bar{I} \\ k \in K}} \langle \tilde{\epsilon}_{\bar{\epsilon},k,2} \rangle \right) * \cdots * \left( \prod_{\substack{\bar{\epsilon} \in \bar{I} \\ k \in K}} \langle \tilde{\epsilon}_{\bar{\epsilon},k,m} \rangle \right),$$

of cyclic groups. Here  $\langle x_{\bar{h},k} \rangle \equiv \mathbb{Z}$  and  $\langle \tilde{\epsilon}_{\bar{\epsilon},k,j} \rangle \equiv \mathbb{Z}/2\mathbb{Z}$ , and let  $\tilde{I}_j = \{\tilde{\epsilon}_{\bar{\epsilon},k,j} \mid \bar{\epsilon} \in \bar{I}_j, k \in K\}$ . (Of course,  $\tilde{H}$  is not yet finite.) Define a surjection  $\rho: \tilde{H} \rightarrow H$  by mapping  $\{x_{\bar{h},k} \mid k \in K\}$  onto  $\{h \in H \mid \pi(h) = \bar{h}\}$  and  $\{\tilde{\epsilon}_{\bar{\epsilon},k,j} \mid \bar{\epsilon} \in \bar{I}_j\}$  onto  $\{\epsilon \in I_j \mid \pi(\epsilon) = \bar{\epsilon}\}$ . Then  $\rho(\tilde{I}_j) = I_j$ . Every automorphism  $\bar{\alpha}$  of  $\bar{H}$  that satisfies  $\bar{\alpha}(\bar{I}_j) = \bar{I}_j$  for all  $j$ , lifts to an automorphism  $\tilde{\alpha}$  of  $\tilde{H}$  defined by  $x_{\bar{h},k} \mapsto x_{\bar{\alpha}(\bar{h}),k}$  and  $\tilde{\epsilon}_{\bar{\epsilon},k,j} \mapsto \tilde{\epsilon}_{\bar{\alpha}(\bar{\epsilon}),k,j}$ . Clearly  $\tilde{\alpha}(\tilde{I}_j) = \tilde{I}_j$ . If  $I_j$  and  $\bar{I}_j$  are conjugacy domains, we can replace  $\tilde{I}_j$  by the conjugacy domain that it generates in  $\tilde{H}$ .

Thus  $\tilde{H}$  satisfies the requirements of the lemma, except that it is not finite. To make  $\tilde{H}$  finite, replace it by its quotient  $\tilde{H}/N$ , and  $\rho$  by the induced quotient map, where  $N$  is a characteristic subgroup of finite index in  $\tilde{H}$ , contained in  $\text{Ker}(\rho)$ . For example, take  $N$  to be the intersection of all normal subgroups  $M$  of  $\tilde{H}$  with  $\tilde{H}/M \equiv H$ .  $\square$

#### 4. Points over ordered fields

Let  $G$  be a finite group with a trivial center such that the Schur multiplier of  $G$  is generated by commutators. Identify  $G$  with the subgroup  $\text{Inn}(G)$  of  $\text{Aut}(G)$ . Fix a sufficiently large integer  $r$  that satisfies (2.13) and the assertions of Lemma 3.1. Associate with  $G$  and  $r$  the moduli spaces  $\mathcal{H}^{\text{in}}$  and  $\mathcal{H}^{\text{ab}}$  from (2.3).

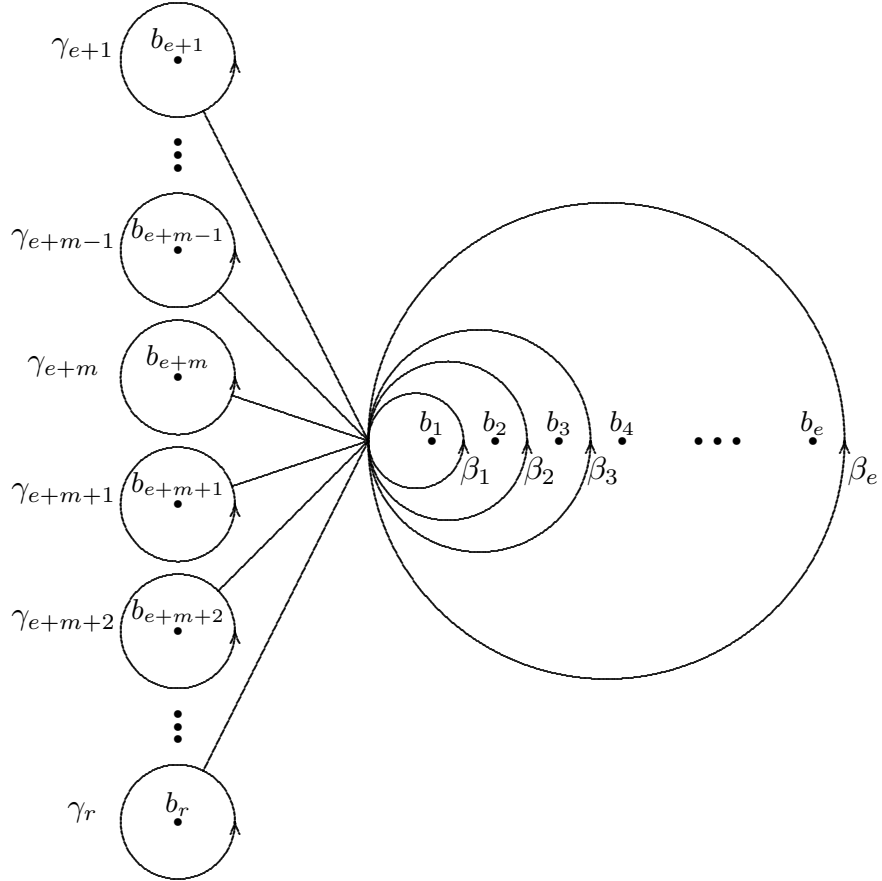
Our aim is to choose Hurwitz spaces  $\mathcal{H}$  and  $\tilde{\mathcal{H}}$  and some points  $\mathbf{q} = [\mathbf{b}, 0, f_0]$  on  $\mathcal{H}$  as in (2.4). First, let  $e = 8 \cdot |G|!$  and  $m = \frac{r-e}{2}$ , so  $r = e + 2m$ . Define the

base point  $\mathbf{b} = \{b_1, \dots, b_r\}$  in  $\mathcal{U}_r$  by

$$b_1 = 1, \dots, b_e = e, \text{ and } b_{e+j} = -3 + (2m+1-2j)\sqrt{-1}, \text{ for } j = e, \dots, 2m.$$

Next, fix generators of  $\Pi_1(\mathbb{P}^1 \setminus \mathbf{b}, 0)$ . For each  $1 \leq j \leq r$  let  $D_j$  be the disc of diameter  $\frac{1}{2}$  around  $b_j$  (so that  $D_1, \dots, D_r$  are disjoint). Define loops  $\gamma_1, \dots, \gamma_r$  in the complex plane with the initial and final point 0 in the following way:

- (1)  $\gamma_1 = \beta_1$ ,  $\gamma_2 = \beta_1^{-1}\beta_2$ ,  $\dots$ ,  $\gamma_e = \beta_{e-1}^{-1}\beta_e$ , where  $\beta_j$  is the circle in the counterclockwise direction with diameter  $[0, b_j + \frac{1}{2}]$  on the real axis;
- (2) for  $e < j \leq r$  the path  $\gamma_j$  goes on a straight line from 0 towards  $b_j$ , then travels on a circle of diameter  $\frac{1}{2} < \rho < 1$  in the counterclockwise direction around  $b_j$ , and returns on a straight line to 0.



These loops are homotopic to the loops those from (2.12). Therefore they represent generators of the fundamental group  $\Pi_1(\mathbb{P}^1 \setminus \bigcap D_j, 0)$ , subject only to the relation  $\gamma_1 \cdots \gamma_r = 1$ . If  $\mathbf{a}$  is an  $r$ -tuple with  $|\mathbf{a} \cap D_j| = 1$  for  $j = 1, \dots, r$ , then  $\gamma_1, \dots, \gamma_r$  also represent generators of  $\Gamma = \Pi_1(\mathbb{P}^1 \setminus \mathbf{a}, 0)$ . Indeed,  $\Pi_1(\mathbb{P}^1 \setminus \bigcap D_j, 0) \cong \Gamma$  via the inclusion  $\mathbb{P}^1 \setminus \bigcap D_j \rightarrow \mathbb{P}^1 \setminus \mathbf{a}$ . Furthermore, for such  $\mathbf{a}$ , we may use  $\gamma_1, \dots, \gamma_r$  also to represent free generators of  $\tilde{\Gamma} = \Pi_1(\mathbb{P}^1 \setminus (\mathbf{a} \cup \{\infty\}), 0)$ . The canonical epimorphism  $\lambda_*: \tilde{\Gamma} \rightarrow \Gamma$  induced by the inclusion  $\lambda: \mathbb{P}^1 \setminus (\mathbf{a} \cup \{\infty\}) \rightarrow \mathbb{P}^1 \setminus \mathbf{a}$  maps the class of  $\gamma_j$  in  $\tilde{\Gamma}$  onto the class of  $\gamma_j$  in  $\Gamma$ . Using  $\mathbf{b}$  and  $\gamma_1, \dots, \gamma_r$ , define the Hurwitz spaces  $\mathcal{H}$  and  $\tilde{\mathcal{H}}$  and the maps  $\Lambda$ ,  $\Psi$ , and  $\bar{\Psi}$  as in (2.13).

Finally, assume  $G$  has a non-inner automorphism  $\epsilon$  of order 2. Let  $G \rtimes \langle \epsilon \rangle$  be the subgroup of  $\text{Aut}(G)$  generated by  $G$  and  $\epsilon$ . In particular, the centralizer of  $G$  in  $G \rtimes \langle \epsilon \rangle$  is trivial. Let  $I \subseteq G \rtimes \langle \epsilon \rangle \setminus G$  be a set of involutions, with  $\epsilon \in I$  and  $|I| \geq 2$ . Lemma 3.1 (with  $m$  replaced by  $2m$ ) produces an  $r$ -tuple  $(\sigma_1, \dots, \sigma_r) \in \mathcal{E}^{(r)}(G)$  (see (2.12)) with the following properties:

- (3)  $\sigma_j^\epsilon = \sigma_1 \cdots \sigma_{j-1} \sigma_j^{-1} \sigma_{j-1}^{-1} \cdots \sigma_1^{-1}$ , for each  $1 \leq j \leq e$ ;
- (4)  $\sigma_{e+j}^\epsilon = \sigma_{e+(2m+1-j)}^{-1}$  for  $j = 1, \dots, 2m$ ;
- (5)  $I = \{\epsilon, \epsilon\sigma_1, \epsilon\sigma_1\sigma_2, \dots, \epsilon\sigma_1\sigma_2 \cdots \sigma_e\}$ .

Fix (for each  $\epsilon$  and each  $I$ ) such an  $r$ -tuple  $(\sigma_1, \dots, \sigma_r)$ . As  $\sigma_1 \cdots \sigma_r = 1$ , there is a unique epimorphism  $f_0: \Pi_1(\mathbb{P}^1 \setminus \mathbf{b}, 0) \rightarrow G$  with  $f_0(\gamma_j) = \sigma_j$ , for  $j = 1, \dots, r$ .

**DEFINITION 4.1.** The point  $\mathbf{q} = [\mathbf{b}, 0, f_0] \in \mathcal{H}$  is called **the basic point associated with  $G$ ,  $\epsilon$ , and  $I$** . The neighborhood

$$\mathcal{N} = \{\mathbf{p} = [\mathbf{a}, 0, f] \in \mathcal{H}^{\text{in}} \mid |\mathbf{a} \cap D_j| = 1, f(\gamma_j) = f_0(\gamma_j) = \sigma_j, \text{ for } j = 1, \dots, r\}$$

of  $\mathbf{q}$  in  $\mathcal{H}$  is called **the basic neighborhood of  $\mathbf{q}$** .

**REMARK 4.2.** *Properties of a basic neighborhood.*

- (a) A priori,  $\mathcal{N}$  is a neighborhood of  $\mathbf{q}$  in  $\mathcal{H}^{\text{in}}$  (see (2.6)). Yet,  $\mathcal{N}$  is connected. Hence,  $\mathcal{N} \subseteq \mathcal{H}$ .
- (b) The point  $\mathbf{b}$  is  $\mathbb{Q}$ -rational (2.7). Hence  $\mathbf{q}$  is algebraic over  $\mathbb{Q}$ .
- (c) Let  $\mathbf{p} \in \mathcal{N}$ , and let  $\mathbf{a} = \{a_1, \dots, a_r\} = \Psi(\mathbf{p})$ . Then without loss of generality  $a_j \in D_j$ , for  $j = 1, \dots, r$ . If  $\mathbf{a}$  is  $\mathbb{R}$ -rational (i.e.,  $(X - a_1) \cdots (X - a_r) \in \mathbb{R}[X]$ ), then  $a_1 < \cdots < a_e$  are real, and  $a_{e+(2m+1-j)}$  is the complex conjugate of  $a_{e+j}$ , for  $j = 1, \dots, m$ .
- (d) Let  $c$  be the complex conjugation. As  $\mathcal{H}$  is an affine variety, we may embed it in a fixed affine space  $\mathbb{A}^n$ . Then the complex topology on it is given by the norm  $\| - \|_c$  defined in Definition 1.4. There are only finitely many choices of  $\epsilon$  and  $I$ . Hence there are only finitely many basic points associated with  $G$ . Thus there is a positive rational number  $\nu$  (that depends only on  $G$ ) such that if  $\mathbf{q}$  is a basic point,  $\mathbf{p} \in \mathcal{H}$ , and  $\|\mathbf{p} - \mathbf{q}\|_c^2 < \nu^2$ , then  $\mathbf{p}$  is in the basic neighborhood  $\mathcal{N}$  of  $\mathbf{q}$ .

**LEMMA 4.3.** *Let  $\mathbf{p} \in \mathcal{N}$  such that  $\Psi(\mathbf{p})$  is  $\mathbb{R}$ -rational. Then  $\delta_\epsilon(\mathbf{p}) = c(\mathbf{p})$ , where  $c$  is complex conjugation.*

**PROOF.** Write  $\mathbf{p}$  as  $[\mathbf{a}, 0, f]$ . Then  $\mathbf{a} = \Psi(\mathbf{p})$ . We have  $\delta_\epsilon(\mathbf{p}) = [\mathbf{a}, 0, \epsilon \circ f]$  by (2.14) and  $c(\mathbf{p}) = [c(\mathbf{a}), 0, cf] = [\mathbf{a}, 0, cf]$  by (2.11). It remains to show that  $cf = \epsilon \circ f$ .

Observe that  $c\beta_j = \beta_j^{-1}$ , for  $j = 1, \dots, e$ . Recursively:

$$(6) \quad c\gamma_1 = \gamma_1^{-1}, \quad c\gamma_2 = \gamma_1\gamma_2^{-1}\gamma_1^{-1}, \dots, \quad c\gamma_e = \gamma_1 \cdots \gamma_{e-1}\gamma_e^{-1}\gamma_{e-1}^{-1} \cdots \gamma_1^{-1}.$$

Furthermore,

$$(7) \quad c\gamma_{e+j} = \gamma_{e+(2m+1-j)}^{-1}, \text{ for } j = 1, \dots, 2m.$$

Recall that  $(cf)(c\gamma) = f(\gamma)$ . Combine (6) and (7) with (3) and (4) to get  $cf(\gamma_j) = f(c\gamma_j) = \sigma_j^\epsilon = (\epsilon \circ f)(\gamma_j)$ , for each  $1 \leq j \leq r$ .  $\square$

**PROPOSITION 4.4.** *Let  $(K, P)$  be an ordered field and  $\iota$  an involution in  $G(K)$  inducing  $P$  on  $K$ . Assume  $\tilde{K} \subseteq \mathbb{C}$ . Let  $\lambda \in G(\mathbb{Q})$  and  $\mathbf{p} \in \mathcal{H}(\tilde{K})$  with*

$$(8) \quad \|\mathbf{p} - \lambda(\mathbf{q})\|_\iota^2 < \nu^2 \text{ in } \tilde{K}(\iota),$$

and  $\bar{\mathbf{p}} = \Lambda(\mathbf{p})$  is  $K$ -rational. Let  $h_1: G(F/K(x)) \rightarrow \text{Aut}(G)$  be the embedding corresponding to  $\mathbf{p}$  over  $K$  with  $F/K(x)$  Galois as given in (2.17). Put  $L = K(\mathbf{p})$  and let  $H$  be the image of  $h_1$ . The following hold:

- (a)  $\delta_\epsilon(\mathbf{p}) = \iota(\mathbf{p})$ ;
- (b)  $P$  does not extend to  $L$ ; in particular,  $P$  does not extend to  $F$ ;
- (c)  $G \rtimes \langle \epsilon \rangle \leq H$ , and therefore  $I \subseteq H$ ;
- (d)  $h_1(I_P(F/K(x))) = \text{Con}_H(I)$ .

**PROOF.** By (2.14),  $\delta_\epsilon(\mathbf{p}) \neq \mathbf{p}$ . Therefore (a) implies  $\iota(\mathbf{p}) \neq \mathbf{p}$ . Hence  $L \not\subseteq \tilde{K}(\iota)$ , and this implies (b). Furthermore, the criterion of (2.17) implies that  $\epsilon \in H$ . Since  $G \leq H$ ,  $G \rtimes \langle \epsilon \rangle \leq H$ . So it suffices to prove (a) and (d).

**Part I.** *Reduction to  $K$  with archimedean orderings dense in  $X(K)$ .* Let  $K_0$  be a finitely generated subfield of  $K$ , containing the finitely generated subfield  $\mathbb{Q}(\bar{\mathbf{p}})$  of  $K$ . Let  $P_0$  be the restriction of  $P$  to  $K_0$ . This ordering is induced from the restriction  $\iota_0 \in G(K_0)$  of  $\iota$ . Let  $F_0/K_0(x)$  be the Galois extension and  $(h_1)_0: G(F_0/K_0(x)) \rightarrow \text{Aut}(G)$  the embedding corresponding to  $\mathbf{p}$  over  $K_0$ . We may assume that  $F = F_0 \cdot K$  from (2.18). If  $K_0$  is sufficiently large, then the restriction map  $\text{res}_{F_0}: G(F/K(x)) \rightarrow G(F_0/K_0(x))$  is an isomorphism. If we can show that the assertions hold for  $K_0, P_0, \iota_0, (h_1)_0$ , then, by (2.19) and since  $\iota_0(\mathbf{p}) = \iota(\mathbf{p})$ , they also hold for  $K, P, \iota, h_1$ . Lemma 1.6(a) shows the set of archimedean orderings on  $K_0$  is dense in  $X(K_0)$ . So we may assume that  $K$  enjoys this property.

**Part II.** *Reduction to  $P$  archimedean.* By Remark 1.8, if  $P'$  is an (archimedean) ordering of  $K$  sufficiently near to  $P$ , then  $I_P(F/K(x)) = I_{P'}(F/K(x))$ . We may assume an involution  $\iota' \in G(K)$ , so near to  $\iota$ , induces  $P'$  that

$$\|\mathbf{p} - \lambda(\mathbf{q})\|_\iota^2 = \|\mathbf{p} - \lambda(\mathbf{q})\|_{\iota'}^2 \quad \text{and} \quad \iota(\mathbf{p}) = \iota'(\mathbf{p}).$$

Thus we may replace  $P$  by  $P'$  and  $\iota$  by  $\iota'$ .

**Part III.** *Reduction to  $K = \mathbb{R}$  and  $\lambda = 1$ .* Assume that  $P$  is archimedean. Extend  $\lambda^{-1}$  to an automorphism  $\beta$  of  $\mathbb{C}$ , and let  $\iota' = \beta\iota\beta^{-1}$ . Then  $\beta(\tilde{K}(\iota)) = (\beta(\tilde{K}))(\iota')$  is a real closure of  $(\beta(K), \beta(P))$ . Hence it is also archimedean. Thus we may assume that  $(\beta(\tilde{K}))(\iota') \subseteq \mathbb{R}$ . Hence  $\beta\iota\beta^{-1} = \iota' = \text{res}_{\beta(\tilde{K})} c$ , where  $c$  is complex conjugation on  $\mathbb{C}$ .

Since  $\mathbf{q}$  is algebraic over  $\mathbb{Q}$ ,  $\beta\lambda(\mathbf{q}) = \mathbf{q}$ . So, application of  $\beta$  to (8) yields

$$(8') \quad \|\beta(\mathbf{p}) - \mathbf{q}\|_c^2 < \nu^2 \text{ in } \mathbb{R}.$$



As  $\bar{\mathbf{p}}$  is  $K$ -rational,  $\iota(\bar{\mathbf{p}}) = \bar{\mathbf{p}}$ . Thus,  $c(\beta(\bar{\mathbf{p}})) = \beta(\bar{\mathbf{p}})$  and  $\beta(\bar{\mathbf{p}})$  is  $\mathbb{R}$ -rational. Also, as  $\delta_\epsilon$  is defined over  $\mathbb{Q}$ , it commutes with  $\beta$ . Therefore (a) is equivalent to

$$(a') \quad \delta_\epsilon(\beta(\mathbf{p})) = c(\beta(\mathbf{p})).$$

Finally, let  $F'/\mathbb{R}(x)$  be the Galois extension and  $h'_1: G(F'/\mathbb{R}(x)) \rightarrow \text{Aut}(G)$  the embedding corresponding to  $\beta(\mathbf{p})$  over  $\mathbb{R}$ , and let  $H'$  be the image of  $h'_1$ . Then by (2.19), condition (d) follows from

$$(d') \quad h'_1(I_{P'}(F'/\mathbb{R}(x))) = \text{Con}_{H'}(I),$$

where  $P'$  is the unique ordering of  $\mathbb{R}$ . Thus, replacing  $K$  by  $\mathbb{R}$  and  $\mathbf{p}$  by  $\beta(\mathbf{p})$ , we may assume that  $K = \mathbb{R}$  and  $\lambda = 1$ .

**Part IV.**  $K = \mathbb{R}$  and  $\lambda = 1$ . By Remark 4.2(d) we have  $\mathbf{p} \in \mathcal{N}$ . Write  $\mathbf{p}$  as  $[\mathbf{a}, 0, f]$ . Then  $\mathbf{a} = \Psi(\mathbf{p}) = \bar{\Psi}(\bar{\mathbf{p}})$  is  $\mathbb{R}$ -rational. Lemma 4.3 gives assertion (a).

**Part V.** *Proof of (d).* By (c)—follows from (a)—we have  $G \rtimes \langle \epsilon \rangle \leq H$ . Check:

$$|G \rtimes \langle \epsilon \rangle| = 2 \cdot |G| = 2 \cdot [F : \mathbb{C}(x)] = [F : \mathbb{R}(x)] = |H|.$$

So  $H = G \rtimes \langle \epsilon \rangle$ .

Write  $\mathbf{p}$  in the form  $\mathbf{p} = [\chi, h]$ , with  $\chi: X \rightarrow \mathbb{P}^1$  (2.1). Fix a point  $y \in \chi^{-1}(0)$ . Let  $Y_0 = \mathbb{P}^1 \setminus (\mathbf{a} \cup \{\infty\})$ , and let  $\psi: \hat{Y}_0 \rightarrow Y_0$  be the universal unramified covering of  $Y_0$ . Fix a point  $\hat{y} \in \psi^{-1}(0)$ . Put  $Y = \chi^{-1}(Y_0) \subseteq X$ . As  $\chi: Y \rightarrow Y_0$  is unramified, there exists a unique covering  $\varphi: \hat{Y}_0 \rightarrow Y$  such that  $\chi \circ \varphi = \psi$  and  $\varphi(\hat{y}) = y$ . Let  $\hat{F}$  be the field of algebraic meromorphic functions on  $\hat{Y}_0$  (in the sense of [KN, p. 199]). Then the field extension  $\hat{F}/\mathbb{C}(x)$  induced by  $\psi$  is the maximal extension of  $\mathbb{C}(x)$  unramified in  $Y_0$ .

Let  $F = \mathbb{C}(X) = \mathbb{C}(Y)$ . We identify  $G(F/\mathbb{C}(x))$  with  $G$  via  $h_0$ , and  $G(F/\mathbb{R}(x))$  with  $H$  via  $h_1$  (see (2.16) and (2.17)). Then,  $h: \text{Aut}(X/\mathbb{P}^1) \rightarrow G$  is the canonical isomorphism  $\text{Aut}(X/\mathbb{P}^1) \rightarrow G(F/\mathbb{C}(x))$  sending  $\alpha \in \text{Aut}(X/\mathbb{P}^1)$  to the element  $f \mapsto f \circ \alpha^{-1}$  of  $G(F/\mathbb{C}(x))$ . Similarly, let  $\hat{G} = G(\hat{F}/\mathbb{C}(x))$ , and let  $\hat{h}: \text{Aut}(\hat{Y}_0/Y_0) \rightarrow \hat{G}$  be the canonical map sending  $\hat{\alpha}$  to the element  $\hat{f} \mapsto \hat{f} \circ \hat{\alpha}^{-1}$ .

Let  $\iota: \Pi_1(\mathbb{P}^1 \setminus \mathbf{a}, 0) \rightarrow \text{Aut}(X/\mathbb{P}^1)$  be the epimorphism associated to the point  $y \in \chi^{-1}(0)$  (see (2.2)). Similarly define  $\hat{\iota}: \Pi_1(Y_0, 0) \rightarrow \text{Aut}(\hat{Y}_0/Y_0)$ , associated to the point  $\hat{y} \in \psi^{-1}(0)$ . Then there is a commutative diagram

$$\begin{array}{ccccc} \Pi_1(Y_0, 0) & \xrightarrow{\hat{\iota}} & \text{Aut}(\hat{Y}_0/Y_0) & \xrightarrow{\hat{h}} & \hat{G} \\ \downarrow \lambda_* & & \downarrow \varphi_* & & \downarrow \text{res}_F \\ \Pi_1(\mathbb{P}^1 \setminus \mathbf{a}, 0) & \xrightarrow{\iota} & \text{Aut}(X/\mathbb{P}^1) & \xrightarrow{h} & G \end{array}$$

where  $\lambda_*$  is induced from the inclusion  $\lambda: Y_0 \rightarrow \mathbb{P}^1 \setminus \mathbf{a}$ .

Put  $\hat{\sigma}_j = \hat{h} \circ \hat{\iota}(\gamma_j)$ , for  $j = 1, \dots, r$ . Then

$$(9) \quad \text{res}_F \hat{\sigma}_j = h \circ \iota \circ \lambda_*(\gamma_j) = f(\gamma_j) = \sigma_j, \quad \text{for } j = 1, \dots, r.$$

Let  $n = (r + e)/2 = e + m$ . By Remark 4.2(c) we may assume  $a_1 < \dots < a_e$  are real, and  $a_{e+(2m+1-j)}$  is the complex conjugate of  $a_{e+j}$ , for  $j = 1, \dots, m$ .

Observe that  $\hat{F}$  is the maximal extension of  $\mathbb{R}(x)$  unramified outside the primes of  $\mathbb{R}(x)$  induced by  $a_1, \dots, a_r, \infty$ . In this situation the proof of [KN, Satz 2] shows that there is  $\hat{\epsilon} \in \hat{H} = G(\hat{F}/\mathbb{R}(x))$  such that  $\hat{\epsilon}, \hat{\sigma}_1, \dots, \hat{\sigma}_n$  form a system of generators for  $\hat{H}$  with the defining relations

$$(10) \quad \hat{\epsilon}^2 = 1 \quad \text{and} \quad \hat{\sigma}_j^{\hat{\epsilon}} = \hat{\sigma}_1^{-1} \cdots \hat{\sigma}_{j-1}^{-1} \hat{\sigma}_j^{-1} \hat{\sigma}_{j-1} \cdots \hat{\sigma}_1, \quad \text{for } 1 \leq j \leq e.$$

Further,  $\hat{\sigma}_{e+j}^{\hat{\epsilon}} = \hat{\sigma}_{e+(2m+1-j)}^{-1}$  for  $j = 1, \dots, 2m$ . By (3) and (4) this implies that  $\text{res}_F \hat{\epsilon}$  and  $\epsilon$  act on  $G$  in the same way. Since  $H$  is a subgroup of  $\text{Aut}(G)$ , this implies that  $\text{res}_F \hat{\epsilon} = \epsilon$ .

Each involution of  $\hat{H}$  is conjugate to one of  $\hat{\epsilon}, \hat{\sigma}_1 \hat{\epsilon}, \hat{\sigma}_2 \hat{\sigma}_1 \hat{\epsilon}, \dots, \hat{\sigma}_e \cdots \hat{\sigma}_2 \hat{\sigma}_1 \hat{\epsilon}$ . Indeed, by [HJ2, Lemma 4.2 (Part E)],  $\hat{H}$  is the free profinite product of the free profinite group  $\langle \hat{\sigma}_{e+1}, \dots, \hat{\sigma}_n \rangle$  of rank  $n - e = m$  with  $e + 1$  groups

$$\langle \hat{\epsilon} \rangle, \langle \hat{\sigma}_1 \hat{\epsilon} \rangle, \langle \hat{\sigma}_2 \hat{\sigma}_1 \hat{\epsilon} \rangle, \dots, \langle \hat{\sigma}_e \cdots \hat{\sigma}_2 \hat{\sigma}_1 \hat{\epsilon} \rangle$$

that are of order two. Thus by [HR, Theorem A'] the elements of finite order in  $\hat{H}$  are the conjugates of the elements of these  $e + 1$  subgroups.

By Lemma 4.5 below, all involutions of  $\hat{H}$  are real. Using (9) and (5) conclude

$$\begin{aligned} I(F/\mathbb{R}(x)) &= \text{res}_F I(\hat{F}/\mathbb{R}(x)) = \text{res}_F \text{Con}_{\hat{H}}(\{\hat{\epsilon}, \hat{\sigma}_1 \hat{\epsilon}, \dots, \hat{\sigma}_e \cdots \hat{\sigma}_1 \hat{\epsilon}\}) = \\ &= \text{Con}_H(\{\epsilon, \sigma_1 \epsilon, \dots, \sigma_e \cdots \sigma_1 \epsilon\}) = \text{Con}_H(I). \quad \square \end{aligned}$$

LEMMA 4.5. *Let  $S$  be a finite set of finite prime divisors of the field  $\mathbb{R}(x)$ . Let  $\mathbb{R}(x)^S$  be the maximal extension of  $\mathbb{R}(x)$  unramified outside  $S \cup \{\infty\}$ , and set  $G^S = G(\mathbb{R}(x)^S/\mathbb{R}(x))$ . Then all involutions of  $G^S$  are real.*

PROOF. By [KN, Satz 3] the absolute Galois group  $\mathcal{G}$  of  $\mathbb{R}(x)$  has generators  $\{\delta, \tau_p \mid p \text{ a finite prime of } \mathbb{R}(x)/\mathbb{R}\}$  with the defining profinite relations

$$\delta^2 = 1 \quad \text{and} \quad \tau_p^\delta = \left( \prod_{p' < p} \tau_{p'}^{-1} \right) \tau_p^{-1} \left( \prod_{p' < p} \tau_{p'}^{-1} \right)^{-1} \quad \text{for all real } p.$$

Here  $\prod_{p' < p} \tau_{p'}^{-1}$  is the unique accumulation point of the products  $\tau_{p_1}^{-1} \cdots \tau_{p_r}^{-1} \in \mathcal{G}$  for real primes  $p_1, \dots, p_r$  with  $p_1 < \cdots < p_r < p$ . Furthermore, [KN] constructs this system of generators in such a way that for every finite set  $S$  of finite primes and every finite prime  $p \notin S$  the natural restriction map  $\mathcal{G} \rightarrow G^S$  maps  $\tau_p$  onto 1 [KN, p. 207].

Let  $p_1 < \cdots < p_e$  be the real, and  $p_{e+1}, \dots, p_n$  the complex primes of  $S$ . Let  $\hat{\sigma}_j$  be the image of  $\tau_{p_j}$ , for  $j = 1, \dots, n$ , and let  $\hat{\epsilon}$  be the image of  $\delta$  in  $G^S$ . Then  $\hat{\epsilon}, \hat{\sigma}_1, \dots, \hat{\sigma}_n$  generate  $G^S$  and satisfy (10). These are in fact defining relations for  $G^S$  by [KN, Satz 2]. As in the last part of the proof of Proposition 4.4, each involution of  $G^S$  is conjugate to some  $\hat{\sigma}_j \cdots \hat{\sigma}_1 \hat{\epsilon}$ , where  $0 \leq j \leq e$ . Thus it suffices to show that each  $\hat{\sigma}_j \cdots \hat{\sigma}_1 \hat{\epsilon}$  lifts to an involution of  $\mathcal{G}$ . To this end put

$$\delta_0 = \delta \quad \text{and} \quad \delta_j = \left( \prod_{p' \leq p_j} \tau_{p'}^{-1} \right)^{-1} \delta = \tau_{p_j} \left( \prod_{p' < p_j} \tau_{p'}^{-1} \right)^{-1} \delta$$

for  $1 \leq j \leq e$ . Then  $\delta_j$  maps onto the involution  $\hat{\sigma}_j \cdots \hat{\sigma}_1 \hat{\epsilon}$  in  $G^S$ . In fact, given another finite set  $S'$  of finite primes of  $\mathbb{R}(x)$  that contains  $S$ , the same argument shows that  $\delta_j$  restricts to an involution in  $G^{S'}$ . As  $\mathcal{G} = \varprojlim_{S'} G^{S'}$ , we get that  $\delta_j$  is an involution in  $\mathcal{G}$ .  $\square$

## 5. The regular real embedding problem over a PRC field

Let  $K$  be a PRC field of characteristic 0, and let  $\nu > 0$  be a rational number. We proceed as with PAC fields [FV2, Section 1] with some extra care.

Let  $X_1, \dots, X_m$  be a partition of  $X(K)$  into disjoint clopen subsets. Fix a closed system  $\mathcal{X}$  of representatives of the conjugacy classes of involutions in  $G(K)$ ; then  $\{\tilde{K}(\iota) \mid \iota \in \mathcal{X}\}$  is a closed subset of real closures of  $K$ , one for each ordering of  $K$  (see Section 1). Put  $\mathcal{X}_j = \mathcal{X} \cap I_{X_j}(\tilde{K}/K)$ . Then  $\mathcal{X}_1, \dots, \mathcal{X}_m$  is a partition of  $\mathcal{X}$  into disjoint clopen subsets.

LEMMA 5.1. *Let  $\Lambda: \mathcal{H} \rightarrow \bar{\mathcal{H}}$  be an unramified Galois cover of absolutely irreducible, non-singular varieties defined over  $K$ . Assume that all the automorphisms of  $\mathcal{H}/\bar{\mathcal{H}}$  are defined over  $K$ . Let  $\beta: G(K) \rightarrow \text{Aut}(\mathcal{H}/\bar{\mathcal{H}})$  be a homomorphism, and let  $L$  be the fixed field of  $\ker(\beta)$ . Assume that  $L$  is not formally real. Let  $\mathbf{q}_1, \dots, \mathbf{q}_m \in \mathcal{H}(\tilde{K})$  satisfy the following.*

$$(1) \quad \iota \mathbf{q}_j = \beta(\iota)(\mathbf{q}_j), \text{ for each } \iota \in \mathcal{X}_j, \text{ for } j = 1, \dots, m.$$

Then there exists  $\mathbf{p} \in \mathcal{H}(\tilde{K})$  such that

- (2)  $\sigma \mathbf{p} = \beta(\sigma)(\mathbf{p})$  for each  $\sigma \in G(K)$ ;
- (3)  $\|\mathbf{p} - \mathbf{q}_j\|_\iota^2 \leq \nu^2$  in  $\tilde{K}(\iota)$ , for each  $\iota \in \mathcal{X}_j$ , for  $j = 1, \dots, m$ ;
- (4) the point  $\Lambda(\mathbf{p})$  of  $\bar{\mathcal{H}}$  is  $K$ -rational and  $K(\mathbf{p}) = L$ .

PROOF. First notice that (4) follows from (2). Indeed, an automorphism of the unramified cover  $\mathcal{H} \rightarrow \bar{\mathcal{H}}$  has no fixed points. If (2) holds, then for each  $\sigma \in G(K)$  we have  $\sigma(\Lambda(\mathbf{p})) = \Lambda(\sigma(\mathbf{p})) = \Lambda(\beta(\sigma)(\mathbf{p})) = \Lambda(\mathbf{p})$  and

$$\sigma(\mathbf{p}) = \mathbf{p} \iff \beta(\sigma)(\mathbf{p}) = \mathbf{p} \iff \beta(\sigma) = 1 \iff \sigma \in G(L).$$

The rest is a straightforward modification of the proof of [FV2, Lemma 1]. Apply Weil's descent [W, Theorem 3] to the maps  $f_{\tau, \rho} = \beta(\tau) \circ \beta(\rho)^{-1}$  to get a variety  $\mathcal{H}'$  defined over  $K$ , and a linear isomorphism  $f: \mathcal{H}' \rightarrow \mathcal{H}$  defined over  $L$  with these properties. The map  $\Lambda \circ f: \mathcal{H}' \rightarrow \bar{\mathcal{H}}$  is defined over  $K$  and  $\sigma f = \beta(\sigma) \circ f$ , for each  $\sigma \in G(K)$ . In particular, suppose that  $\mathbf{q}' \in \mathcal{H}'(\tilde{K})$  and  $\mathbf{q} = f(\mathbf{q}') \in \mathcal{H}(\tilde{K})$ . Then, for every  $\sigma \in G(K)$

$$\beta(\sigma)(\mathbf{q}) = (\beta(\sigma) \circ f)(\mathbf{q}') = (\sigma f)(\mathbf{q}') = \sigma(f(\sigma^{-1} \mathbf{q}')).$$

Conclude that

$$(5) \quad \sigma \mathbf{q} = \beta(\sigma)(\mathbf{q}) \iff \mathbf{q}' = \sigma \mathbf{q}' \iff \mathbf{q}' \in \mathcal{H}'(\tilde{K}(\sigma)).$$

Use (5) and equation (3) of Section 1 to translate (1)–(3) via  $f$  from  $\mathcal{H}$  to  $\mathcal{H}'$ . Let  $\mathbf{q}'_j = f^{-1}(\mathbf{q}_j) \in \mathcal{H}'(\tilde{K})$ , for  $j = 1, \dots, m$ . Then,

$$(1') \quad \mathbf{q}'_j \in \mathcal{H}'(\tilde{K}(\iota)), \text{ for each } \iota \in \mathcal{X}_j, \text{ for } j = 1, \dots, m.$$

We must find  $\mathbf{p}' \in \mathcal{H}'(\tilde{K})$  such that

$$(2') \quad \mathbf{p}' \in \mathcal{H}'(\tilde{K}(\sigma)) \text{ for each } \sigma \in G(K), \text{ that is, } \mathbf{p}' \in \mathcal{H}'(K);$$

$$(3') \quad \|\mathbf{p}' - \mathbf{q}'_j\|_\iota^2 \leq \nu^2 / \|f\|_\iota^2 \text{ in } \tilde{K}(\iota), \text{ for each } \iota \in \mathcal{X}_j, \text{ for } j = 1, \dots, m.$$

Suppose  $\iota \in \mathcal{X}_j$  for some  $1 \leq j \leq m$ . As  $\|f\|_\iota^2$  is algebraic over  $K$ , there is  $a_j \in K$  with  $a_j^2 > \|f\|_\iota^2$  in  $\tilde{K}(\iota)$ . Replace  $\mathcal{X}_1, \dots, \mathcal{X}_m$  by a finer partition to assume this is true for each  $\iota \in \mathcal{X}_j$ . Thus (3') follows from a stronger statement:

$$(3'') \quad \|\mathbf{p}' - \mathbf{q}'_j\|_\iota^2 \leq \nu^2 / a_j^2 \text{ in } \tilde{K}(\iota), \text{ for each } \iota \in \mathcal{X}_j, \text{ for } j = 1, \dots, m.$$

By Proposition 1.2 there is  $\mathbf{p}' \in \mathcal{H}'(K)$  such that (3'') holds.  $\square$

**THEOREM 5.2.** *Let  $L/K$  be a finite Galois extension with  $L$  not formally real and let  $\pi: H \rightarrow G(L/K)$  be an epimorphism of finite groups. For each  $1 \leq j \leq m$  let  $I_j \subseteq H$  be a conjugacy domain of involutions such that  $\pi(I_j) = I_{X_j}(L/K)$ . Then there exists a regular extension  $F$  of  $L$ , Galois over  $K(x)$ , and an isomorphism  $h_1: G(F/K(x)) \rightarrow H$  that maps  $I_{X_j}(F/K(x))$  onto  $I_j$ . In addition, the following diagram commutes.*

$$\begin{array}{ccc} G(F/K(x)) & \xrightarrow{h_1} & H \\ \text{res}_L \searrow & & \swarrow \pi \\ & G(L/K) & \end{array}$$

In particular,  $h_1$  maps  $I(F/K(x))$  onto  $\bigcup_j I_j$ .

**PROOF.** By Skolem-Löwenheim Principle [FJ, Proposition 6.4] we may assume that  $K \subseteq \mathbb{C}$ . We divide the proof into five parts.

**Part 1. Weakening of commutativity.** Let  $G = \text{Ker}(\pi)$ . Instead of commutativity of the diagram it suffices to show that  $h_1$  maps  $G(F/L(x))$  onto  $G$ . Indeed, apply Lemma 3.3. This gives an epimorphism of finite groups  $\rho: \tilde{H} \rightarrow H$  and conjugacy domains of involutions  $\tilde{I}_1, \dots, \tilde{I}_m \subseteq \tilde{H}$  with  $\rho(\tilde{I}_j) = I_j$ . In addition, every automorphism of  $G(L/K)$  that preserves the  $I_{X_j}(L/K)$  lifts (under  $\rho \circ \pi$ ) to an automorphism of  $\tilde{H}$  that preserves the  $\tilde{I}_j$ . Let  $\tilde{G} = \text{Ker}(\rho \circ \pi)$ .

Assume that we can find a regular extension  $\hat{F}$  of  $L$ , Galois over  $K(x)$ , and an isomorphism  $\hat{h}_1: G(\hat{F}/K(x)) \rightarrow \hat{H}$  that maps  $G(\hat{F}/L(x))$  onto  $\hat{G}$  and the  $I_{X_j}(\hat{F}/K(x))$  onto the  $\hat{I}_j$ . In particular,  $\text{Ker}(\pi \circ \rho \circ \hat{h}_1) = G(\hat{F}/L(x)) = \text{Ker}(\text{res}_L)$ . Hence there exists an automorphism  $\alpha$  of  $G(L/K)$  such that  $\alpha \circ \pi \circ \rho \circ \hat{h}_1 = \text{res}_L$  and  $\alpha$  preserves the  $I_{X_j}(L/K)$ . We can lift  $\alpha$  to an automorphism  $\hat{\alpha}$  of  $\hat{H}$  that preserves the  $\hat{I}_j$ . Thus, by composing  $h_1$  with  $\hat{\alpha}$  we may assume that  $(\pi \circ \rho) \circ \hat{h}_1 = \text{res}_L$ .

Now let  $F$  be the fixed field of  $\text{Ker}(\rho)$  in  $\hat{F}$ . Then  $h_1$  induces an isomorphism  $h_1: G(F/K(x)) \rightarrow H$  with the required properties.

**Part 2.** *Reduce to commutators generate*  $M(G)$ ,  $H \subseteq \text{Aut}(G)$ , and  $|I_j| \geq 2$ . As  $L$  is not formally real,  $1 \notin I_{X_j}(L/K) = \pi(I_j)$ , for each  $1 \leq j \leq m$ . Thus  $I_j \subseteq H \setminus G$ . Let  $\tilde{H}$  and  $\tilde{G}$  be as in Lemma 3.2, and let  $\tilde{I}_j$  be the inverse image of  $I_j$  in the set of involutions of  $\tilde{H}$ . Suppose there is  $\hat{F}$  regular over  $L$ , with  $\hat{F}/K(x)$  is Galois, and an isomorphism  $\tilde{h}: G(\hat{F}/K(x)) \rightarrow \tilde{H}$  that maps  $G(\hat{F}/L(x))$  onto  $\tilde{G}$  and  $I_{X_j}(\hat{F}/K(x))$  onto  $\tilde{I}_j$ . As in Part 1, the subfield of  $\hat{F}$  corresponding to the kernel of the map  $\tilde{H} \rightarrow H$  (sending  $\tilde{G}$  to  $G$ ) is the desired  $F$ .

Thus, assume that commutators generate  $M(G)$ ,  $C_H(G) = 1$ , and  $|I_j| \geq 2$  for each  $j$ . In particular, the conjugation action of  $H$  on  $G$  induces a monomorphism  $H \rightarrow \text{Aut}(G)$ . Identify  $H$  with its image in  $\text{Aut}(G)$  (and  $G$  with  $\text{Inn}(G)$ ). Then  $G(L/K)$  is a subgroup of  $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$ , and  $\pi: H \rightarrow G(L/K)$  is the restriction of the quotient map  $\pi: \text{Aut}(G) \rightarrow \text{Out}(G)$  to  $H$ .

**Part 3. Construction.** Let  $\Lambda: \mathcal{H} \rightarrow \bar{\mathcal{H}}$  be the cover of Hurwitz spaces, associated with  $G$ , defined in Section 4. Let  $\beta: G(K) \rightarrow \text{Aut}(\mathcal{H}/\bar{\mathcal{H}})$  be the composition of the restriction  $G(K) \rightarrow G(L/K) \leq \text{Out}(G)$  with the isomorphism  $\delta: \text{Out}(G) \rightarrow \text{Aut}(\mathcal{H}/\bar{\mathcal{H}})$  (2.14). Furthermore, let  $\nu$  be as in Remark 4.2(d).

Let  $M$  be the field generated over  $\mathbb{Q}$  by  $\sqrt{-1}$  and the conjugates of basic points associated with  $G$ ,  $\epsilon$ , and  $I$  as in Definition 4.1, for all possible  $\epsilon$  and  $I$ . This is a finite extension of  $\mathbb{Q}$  (Remark 4.2(b)). Refine the partition  $X_1, \dots, X_m$  of  $X(K)$ , and hence also the corresponding partition  $\mathcal{X}_1, \dots, \mathcal{X}_m$  of  $\mathcal{X}$ , so that for each  $1 \leq j \leq m$  there are unique  $\bar{\epsilon}_j \in G(L/K)$  and  $\bar{\iota}_j \in G(M/\mathbb{Q})$  such that  $\text{res}_L \mathcal{X}_j = \{\bar{\epsilon}_j\}$  and  $\text{res}_M \mathcal{X}_j = \{\bar{\iota}_j\}$ .

Fix  $1 \leq j \leq m$ . Put  $I'_j = \{\epsilon \in I_j \mid \pi(\epsilon) = \bar{\epsilon}_j\}$  and choose  $\epsilon_j \in I'_j$ . Then  $I'_j \subseteq G \times \langle \epsilon_j \rangle$ . Let  $\mathbf{q}$  be the basic point associated with  $G$ ,  $\epsilon_j$ , and  $I'_j$ . Then  $\mathbb{Q}(\mathbf{q}) \subseteq M$ . As the real involutions in  $G(M/\mathbb{Q})$  are conjugate, there is  $\lambda_j \in G(M/\mathbb{Q})$  with  $\lambda_j^{-1} \bar{\iota}_j \lambda_j = \text{res}_M c$ :  $c$  is complex conjugation. Set  $\mathbf{q}_j = \lambda_j(\mathbf{q})$ . By Lemma 4.3,  $\delta_\epsilon(\mathbf{q}) = c(\mathbf{q})$ . Therefore,  $\delta_\epsilon(\mathbf{q}_j) = \delta_\epsilon \lambda_j(\mathbf{q}) \lambda_j \delta_\epsilon(\mathbf{q}) = (\lambda_j c \lambda_j^{-1})(\mathbf{q}_j) = \bar{\iota}_j(\mathbf{q}_j)$ .

Let  $\iota \in \mathcal{X}_j$ . Then  $\delta_{\epsilon_j} = \delta(\pi(\epsilon_j)) = \delta(\bar{\epsilon}_j) = (\delta \circ \text{res}_L)(\iota) = \beta(\iota)$ . So  $\iota(\mathbf{q}_j) = \bar{\iota}_j(\mathbf{q}_j) = \delta_{\epsilon_j}(\mathbf{q}_j) = \beta(\iota)(\mathbf{q}_j)$ . Thus  $\mathbf{q}_1, \dots, \mathbf{q}_m$  satisfy (1). Therefore there exists  $\mathbf{p} \in \mathcal{H}(\tilde{K})$  that satisfies (2)-(4). Let  $F/K(x)$  be the Galois extension and  $h_1: G(F/K(x)) \rightarrow \text{Aut}(G)$  the embedding associated with  $\mathbf{p}$  over  $K$  (2.17).

**Part 4.** *The image of*  $h_1$ . Let  $\tau \in H$ . There is  $\sigma \in G(K)$  such that  $\text{res}_L \sigma = \pi(\tau)$ . By (2),  $\sigma(\mathbf{p}) = \delta(\text{res}_L \sigma)(\mathbf{p}) = \delta_\tau(\mathbf{p})$ . Hence by the criterion of (2.17),  $\tau$  is in the image of  $h_1$ . Thus  $H \leq \text{im}(h_1)$ . But

$$|H| = |G| \cdot |G(L/K)| = [F : L(x)] \cdot [L : K] = [F : K(x)] = |\text{im}(h_1)|,$$

and hence  $H = \text{im}(h_1)$ .

**Part 5.**  $h_1(I_{X_j}(F/K(x))) = I_j$ . Let  $1 \leq j \leq m$  and  $P \in X_j$ . By Prop. 4.4(d),  $h_1(I_P(F/K(x))) = \text{Con}_H(I'_j)$ . As  $\text{Con}_{G(K)}(\mathcal{X}_j) = I_{X_j}(\tilde{K}/K)$ ,  $\text{Con}_{G(L/K)}(\bar{\epsilon}_j) = I_{X_j}(L/K)$ . Conclude:  $\text{Con}_H(I'_j) = I_j$ . Thus  $h_1(I_P(F/K(x))) = I_j$ .  $\square$

Theorem 5.2 tells about the structure of the absolute Galois group of  $K(x)$ . For instance, every finite group is realizable over  $K(x)$ . This isn't new [DF2, Theorem 5.7]. Still, the precise information about real involutions gives more.

**THEOREM 5.3.** *Let  $K$  be a formally real PRC field. Let  $G$  be a finite group, and let  $G_0$  be a normal subgroup of  $G$  generated by involutions. There is a Galois extension  $N/K(x)$  with Galois group  $G$  such that the fixed field of  $G_0$  in  $N$  is the maximal totally real extension of  $K(x)$  in  $N$ .*

**PROOF.** Let  $\langle \epsilon \rangle$  be a group of order 2. Put  $H = G \times \langle \epsilon \rangle$  and  $H_0 = G_0 \times \langle \epsilon \rangle$ , and let  $\pi: H \rightarrow G(K(\sqrt{-1})/K)$  be the epimorphism with kernel  $G$ . The set  $I_0$  of involutions in  $G_0$  generates  $G_0$ . Therefore  $I_1 = (I_0 \cup \{1\}) \times \{\epsilon\}$  generates  $H_0$ . It is a conjugacy domain in  $H$ . Theorem 5.2 (with  $m = 1$ ) gives a Galois extension  $F$  of  $E = K(x)$  that contains  $\sqrt{-1}$  such that  $G(F/E) = H$ ,  $G(F/E(\sqrt{-1})) = G$ , and  $I_1$  is the set of real involutions in  $G(F/E)$ . Let  $N$  be the fixed field of  $\epsilon$  and  $N'$  the fixed field of  $H_0 = \langle I_1 \rangle$ . The last condition means that  $N'$  is the maximal totally real extension of  $E$  in  $F$ , and, therefore, also in  $N$ . Clearly  $G(N/E) \cong G$  and  $N'$  is the fixed field of  $G_0$  in  $N$ .  $\square$

## 6. Totally real Hilbertian fields

As in the preceding sections, all fields are of characteristic 0. Let  $S/R$  be a Galois cover of rings [FJ, Definition 5.4] with  $F/E$  the corresponding Galois extension of quotient fields. Thus  $R$  is an integrally closed domain and there is  $z \in S$  integral over  $R$  such that  $S = R[z]$  and the discriminant  $d_E(z)$  of  $z$  over  $E$  is a unit of  $R$ . We call such  $z$  a **primitive element** for  $S/R$ . Assume  $S/R$  is **real** [HL, Definition 4.2]:  $R$  is a regular ring and  $F$  is not formally real.

**LEMMA 6.1.** *The integral closure  $S'$  of  $R$  in each intermediate extension  $F'$  of  $F/E$  is also a regular ring.*

**PROOF.** Observe that  $S/S'$  is also a Galois cover. By [R, p. 75] it suffices to show that  $S'/R$  is étale. i.e., flat and unramified. We have  $S = \bigoplus_{i=0}^{d-1} Rz^i$ , where  $d = [F : E]$ , and so  $S/R$  is faithfully flat. Similarly  $S/S'$  is faithfully flat. By the descent property [Ma, (4.B)],  $S'/R$  is (faithfully) flat.

To show that  $S'/R$  is unramified, let  $q$  be a prime of  $S$ , and let  $p = q \cap S'$  and  $m = q \cap R$ . Replace  $R$ ,  $S'$ , and  $S$  by their localizations at these primes to assume that they are local rings. Then  $S/S'$  and  $S'/R$  are still faithfully flat. As  $S/S'$  is unramified, the field extension  $(S/q)/(R/m)$  is separable and finite. Hence so is its subextension  $(S'/p)/(R/m)$ . As  $S/R$  and  $S/S'$  are unramified,  $mS = q$  and  $pS = q$ . Thus  $(mS')S \cap S' = pS \cap S'$ . But  $S/S'$  is faithfully flat, hence [Ma, (4.C)],  $mS' = p$ .  $\square$

Let  $M$  be a field. Every homomorphism  $\varphi: R \rightarrow M$  extends to a homomorphism  $\psi: S \rightarrow \widetilde{M}$ , and  $\psi$  induces a group homomorphism  $\psi^*: G(M) \rightarrow G(F/E)$ :

$$(1) \quad \psi(\psi^*(\sigma)(x)) = \sigma(x) \quad \text{for } x \in S.$$

[FJ, Lemma 5.5]. If  $\psi'$  is another extension of  $\varphi$ , then  $\psi'^*$  and  $\psi^*$  differ by an inner automorphism of  $G(F/E)$  [L, Corollary 1 on p. 247]. In particular, for  $\sigma \in G(M)$  and a conjugacy domain  $I \subseteq G(F/E)$  we have  $\psi'^*(\sigma) \in I$  if and only if  $\psi^*(\sigma) \in I$ . This allows us to abuse the notation and write  $\varphi^*(\sigma) \in I$  instead of  $\psi^*(\sigma) \in I$ . (Cf. also [HL, Remark 4.1].)

REMARK 6.2. Let  $S_0/R_0$  be another real Galois cover of rings, with  $L/K$  the corresponding extension of the quotient fields. Assume that  $R$  is finitely generated over  $R_0$ , the field  $K$  is algebraically closed in  $E$ , and  $L$  is the algebraic closure of  $K$  in  $F$ . Furthermore,  $R_0 \subseteq M$  and  $\varphi: R \rightarrow M$  is an  $R_0$ -homomorphism.

We may choose the extension  $\psi$  of  $\varphi$  to be an  $S_0$ -homomorphism. From (1):

- (a) Composition of  $\psi^*$  with  $\text{res}_L: G(F/E) \rightarrow G(L/K)$  is the restriction map  $\text{res}_L: G(M) \rightarrow G(L/K)$ .
- (b) For each  $P \in X(K)$ ,  $\varphi^*(I_P(M)) \subseteq I_P(F/E)$ . Thus,  $\varphi^*(I(M)) \subseteq I(F/E)$ .

Indeed, let  $\epsilon \in I_P(M)$ , and let  $\psi: S \rightarrow \widetilde{M}$  be an extension of  $\varphi$ . It follows from (1) that  $\psi$  maps the integral closure  $S'$  of  $R$  in  $F(\psi^*(\epsilon))$  into  $\widetilde{M}(\epsilon)$ . The latter field is real closed. Thus, by Knebusch's Theorem [HL, Proposition 1.2],  $P$  extends to an ordering on  $F(\psi^*(\epsilon))$ .

Through this section and for an ambient field  $K$  consider the following setup:  $x$  is transcendental over  $K$ ,  $E = K(x)$  and  $R = K[x, h(x)^{-1}]$ . Also,  $S$  is a real Galois cover of  $R$  with  $F/E$  the corresponding extension of quotient fields.

- (2) Let  $X_1, \dots, X_m$  be a partition of  $X(K)$  into disjoint clopen subsets. For each  $1 \leq j \leq m$ , let  $Q_j \in X(E)$  so that  $\text{res}_K Q_j \in X_j$ .

Therefore,  $a \in K$  with  $h(a) \neq 0$  defines  $\varphi_a: R \rightarrow K$  by  $x \mapsto a$ .

LEMMA 6.3. *In (2) let  $Q$  be an ordering on  $E$  with  $P$  its restriction to  $K$ . Denote the real closure of  $(K, P)$  by  $\overline{K}$ . There exist branch points  $x_1 < x_2$  in  $\overline{K}$  of the extension  $F/E$  with no other  $\overline{K}$  branch points between them. They have this property. For each  $a \in K$  in the interval  $(x_1, x_2)$ ,  $\varphi_a^*(I_P(K)) \subseteq I_Q(F/E)$ .*

PROOF. Let  $\epsilon \in I_Q(F/E)$ . Choose a primitive element  $y$  for  $F(\epsilon)/E$ , integral over  $K[x]$ . Let  $f_\epsilon = \text{irr}(y, E) \in K[x, Y]$  and  $S'$  the integral closure of  $R$  in  $F(\epsilon)$ . The sentence  $(\exists X, Y)[f_\epsilon(X, Y) = 0 \wedge \frac{\partial f}{\partial Y}(X, Y) \neq 0]$  holds in  $F(\epsilon)$ , and therefore also in the real closure of  $(E, Q)$ . By Tarski's principle it is valid in  $\overline{K}$ . Thus there is  $\bar{a} \in \overline{K}$  such that  $f_\epsilon(\bar{a}, Y)$  has a simple root in  $\overline{K}$ . This certainly remains true if  $\bar{a}$  is replaced by  $a$  in the neighborhood  $\overline{U}$  of  $\bar{a}$  in  $\overline{K}$  determined by nearest branch points of  $F/E$  in  $\overline{K}$ .

Let  $\iota$  be the generator of  $G(\overline{K})$ , and let  $S'$  be the integral closure of  $R$  in  $F(\epsilon)$ . Let  $a \in \overline{U} \cap K$ . Then  $\varphi_a: R \rightarrow K \subseteq \overline{K}$  extends to a homomorphism  $\psi: S' \rightarrow \overline{K}$ . It follows that its extension  $\psi: S \rightarrow \widetilde{K}$  satisfies  $\psi^*(\iota) = \epsilon$ . As  $I_P(K)$  and  $I_Q(F/E)$  are the conjugacy classes of  $\iota$  and  $\epsilon$  in the respective groups, we have  $\varphi_a^*(I_P(K)) \subseteq I_Q(F/E)$ .  $\square$

DEFINITION 6.4. A formally real field  $K$  is **totally real Hilbertian**, if in each setup (2) the following holds. When  $G(F/E) = \langle \bigcup_{j=1}^m I_{Q_j}(F/E) \rangle$ , then there exists a  $K$ -homomorphism  $\varphi: R \rightarrow K$  with  $\varphi^*(G(K)) = G(F/E)$  and  $\varphi^*(I_{X_j}(K)) = I_{Q_j}(F/E)$ , for each  $1 \leq j \leq m$ . Thus,  $\varphi^*(I(K)) = I(F/E)$ .

COROLLARY 6.5. *If  $K$  is a number field, then  $K$  is totally real Hilbertian.*

PROOF. Consider (2). For each  $j$  put  $P_j = \text{res}_K Q_j$ . Since  $|X(K)| < \infty$ , we may refine  $X_1, \dots, X_m$  to assume  $X_j = \{P_j\}$ . As  $K$  is dense in each of its real closures, Lemma 6.3 gives a nonempty open subset  $U_j$  of  $K$  (with respect to  $P_j$ ) so that  $\varphi_a^*(I_{P_j}(K)) \subseteq I_{Q_j}(F/E)$  for each  $a \in U_j$ . Consider the Hilbert set

$$H_K = \{a \in K \mid h(a) \neq 0 \text{ and } \varphi_a^*(G(K)) = G(F/E)\}$$

[FJ, Lemma 12.12]. By [G, Lemma 3.4],  $H_K$  is dense in  $K$  in the product topology induced by  $P_1, \dots, P_n$ , that is, there is  $a \in H_K \cap U_1 \cap \dots \cap U_m$ . Observe that  $I_{Q_j}(F/E)$  is a conjugacy class in  $G(F/E)$ . The surjectivity of  $\varphi_a^*$  implies that  $\varphi_a^*(I_{P_j}(K)) = I_{Q_j}(F/E)$ .  $\square$

PROPOSITION 6.6. *Let  $K = \mathbb{Q}^{\text{tr}}$ . Then  $K$  is totally real Hilbertian.*

PROOF. Assume (2). Let  $z$  be a primitive element for the cover  $S/R$ . Let  $K' \subseteq K$  be a number field such that  $h(x) \in K'[x]$ . Put  $R' = K'[x, h(x)^{-1}]$  and  $S' = R'[z]$ , and let  $E'$  and  $F'$  be their quotient fields. For each  $j$  let  $Q'_j$  be the restriction of  $Q_j$  to  $E'$ , and let  $X'_j$  be the restriction of  $X_j$  to  $K'$ . Take  $K'$  sufficiently large to assume the following.

- (i)  $S'/R'$  is a real Galois cover.
- (ii)  $[F' : E'] = [F : E]$ , and therefore  $K$  and  $F'$  are linearly disjoint over  $K'$ .
- (iii) The sets  $X'_1, \dots, X'_m$  are distinct.

Then  $X'_1, \dots, X'_m$  is a partition of  $X(K')$  and  $G(F'/E') \cong G(F/E)$ .

By Corollary 6.4 there exists  $a \in K'$  such that an extension  $\psi': S' \rightarrow \tilde{K}$  of  $\varphi_a: R' \rightarrow K'$  satisfies  $\psi'^*(I_{X'_j}(K')) = I_{Q'_j}(F'/E')$ . Extend  $\varphi_a$  to the  $K$ -homomorphism  $\varphi_a: R \rightarrow K$ . As  $K$  and  $S'$  are linearly disjoint over  $K'$ , it is possible to extend this  $\varphi_a$  and  $\psi'$  to the same  $K$ -homomorphism  $\psi: S \rightarrow \tilde{K}$ . By (1), the following diagram commutes.

$$\begin{array}{ccccc} G(F/E) & \xleftarrow{\psi^*} & G(K) & \xleftarrow{\quad} & I(K) \\ \downarrow \text{res}_{F'} & & \downarrow & & \downarrow \\ G(F'/E') & \xleftarrow{\psi'^*} & G(K') & \xleftarrow{\quad} & I(K') \end{array}$$

From (ii), the left vertical map is an isomorphism. As  $K = \mathbb{Q}^{\text{tr}}$ ,  $I(K) = I(\mathbb{Q}) = I(K')$ . Thus, the right vertical inclusion is surjective and maps  $I_{X_j}(K)$  onto  $I_{X'_j}(K')$ . Diagram chasing yields  $\psi^*(I_{X_j}(K)) = I_{Q_j}(F/E)$ . But  $G(F/E) = \langle \bigcup_{j=1}^m I_{Q_j}(F/E) \rangle$ , and hence  $\psi^*(G(K)) = G(F/E)$ .  $\square$



## 7. Absolute Galois group of the totally real algebraic numbers

In this section we consider the following category. An **involutory structure** is a pair  $(G, I_G) = \mathbf{G}$  for short, where  $G$  is a profinite group and  $I_G$  is a closed set of involutions in  $G$ . A **morphism** of involutory structures  $\varphi: \mathbf{G} \rightarrow \mathbf{H}$  is a continuous homomorphism of groups  $\varphi: G \rightarrow H$  such that  $\varphi(I_G) \subseteq I_H$ . We say that  $\varphi: \mathbf{G} \rightarrow \mathbf{H}$  is an **epimorphism** if  $\varphi(G) = H$  and  $\varphi(I_G) = I_H$ .

EXAMPLE 7.1(A). Let  $L/K$  be a Galois extension with  $L$  not formally real. Then  $\mathbf{G}(L/K) = (G(L/K), I(L/K))$  is an involutory structure. Let  $E$  be an extension of  $K$ , and let  $F/E$  be a Galois extension such that  $L \subseteq F$ . Then the restriction  $\text{res}_L: \mathbf{G}(F/E) \rightarrow \mathbf{G}(L/K)$  is a morphism. Moreover, suppose that  $E/K$  is regular and totally real: every ordering on  $K$  extends to  $E$ . Then  $\text{res}_L$  is an epimorphism (cf. [HJ1, Lemma 3.5]).

EXAMPLE 7.1(B). Let  $S/R$  be a real Galois cover with  $F/E$  the corresponding Galois extension of fields. Let  $M$  be a field and let  $\varphi: R \rightarrow M$  be a homomorphism. Extend  $\varphi$  to a homomorphism  $\psi: S \rightarrow \widetilde{M}$ . Then the group homomorphism  $\psi^*: G(M) \rightarrow G(F/E)$  is a morphism of involutory structures  $\psi^*: \mathbf{G}(M) \rightarrow \mathbf{G}(F/E)$  (Remark 6.2(b)).

A **finite image** of  $\mathbf{G}$  is a finite involutory structure  $\mathbf{H}$  for which there exists an epimorphism  $\varphi: \mathbf{G} \rightarrow \mathbf{H}$ . Clearly, up to an isomorphism, it is of the form  $(G/N, \{\epsilon N/N \mid \epsilon \in I_G\})$ , where  $N$  is an open normal subgroup of  $G$  not meeting  $I_G$ . Let  $\text{Im}\mathbf{G}$  be the class of all finite images of  $\mathbf{G}$ .

A **finite embedding problem** for  $\mathbf{G}$  consists of an epimorphism  $\pi: \mathbf{H} \rightarrow \mathbf{A}$  of finite involutory structures, together with an epimorphism  $\varphi: \mathbf{G} \rightarrow \mathbf{A}$ . A **solution** is an epimorphism  $\psi: \mathbf{G} \rightarrow \mathbf{H}$  such that  $\pi \circ \psi = \varphi$ . We say that  $\mathbf{G}$  has the **embedding property** if every finite embedding problem  $(\pi: \mathbf{H} \rightarrow \mathbf{A}, \varphi: \mathbf{G} \rightarrow \mathbf{A})$  for  $\mathbf{G}$ , in which  $H$  is a finite image of  $\mathbf{G}$ , has a solution.

EXAMPLE 7.2. Let  $D$  be the free profinite product  $\prod_{x \in X_\omega} \langle \epsilon_x \rangle$  of groups of order 2 over  $X_\omega$  (Remark 1.5), and let  $I_D^0 = \{\epsilon_x \mid x \in X_\omega\}$ . A finite involutory structure  $(A, I_A)$  is a finite image of  $(D, I_D^0)$  if and only if  $A$  is generated by  $I_A$ . Furthermore,  $(D, I_D^0)$  has the embedding property.

With  $D$  and  $I_D^0$  as above, put  $\mathbf{D} = (D, I_D)$ , where  $I_D$  is the conjugacy domain  $\text{Con}_D(I_D^0)$  of  $D$  generated by  $I_D^0$ .

LEMMA 7.3. (a)  $I_D$  is all involutions in  $D$ , and  $D$  is of rank  $\aleph_0$ .

(b) A finite involutory structure  $\mathbf{A}$  is in  $\text{Im}\mathbf{D}$  if and only if  $I_A \neq \emptyset$  is a conjugacy domain in  $A$  and  $A = \langle I_A \rangle$ .

(c)  $\mathbf{D}$  has the embedding property.

PROOF OF (a). See [HJ2, Corollary 3.2 and Lemma 2.2]

PROOF OF (b). Immediate from Example 7.2.

PROOF OF (c). Let  $\pi: \mathbf{H} \rightarrow \mathbf{A}$ ,  $\varphi: \mathbf{D} \rightarrow \mathbf{A}$  be a finite embedding problem for  $\mathbf{D}$ . Then  $I_A \subseteq A$  and  $I_H \subseteq H$  are conjugacy domains. Let  $I_A^0 = \varphi(I_D^0)$  and let  $I_H^0 = \{\epsilon \in I_H \mid \pi(\epsilon) \in I_A^0\}$ . As  $\text{Con}_D(I_D^0) = I_D$ , we have  $\text{Con}_A(I_A^0) = I_A$ ; it follows that  $\text{Con}_H(I_H^0) = I_H$ .

By Example 7.2,  $I_A^0$  generates  $A$ . But  $\mathbf{H} \in \text{Im} \mathbf{D}$  implies that  $I_H$  generates  $H$ . We have  $\pi(I_H^0) = I_A^0$  and  $\text{Con}_H(I_H^0) = I_H$ . By an analogue of Gaschütz' lemma [**HL**, Lemma 3.3 with  $n = 0$ ],  $I_H^0$  generates  $H$ .

By Example 7.2 there is an epimorphism  $\psi: D \rightarrow H$  such that  $\pi \circ \psi = \varphi$  and  $\psi(I_D^0) = I_H^0$ . Clearly  $\psi(I_D) = I_H$ .  $\square$

**THEOREM 7.4.** *Let  $K$  be a totally real Hilbertian PRC field. Assume that  $K$  has no proper totally real algebraic extensions and  $X(K)$  has no isolated points. Put  $\mathbf{G} = (G, I_G)$ , where  $G$  is the absolute Galois group of  $K$  and  $I_G$  is the conjugacy domain of all involutions in  $G$ . Then*

- (a) *A finite embedding problem  $(\pi: \mathbf{H} \rightarrow \mathbf{A}, \varphi: \mathbf{G} \rightarrow \mathbf{A})$  for  $\mathbf{G}$  has a solution, if (\*)  $I_H \neq \emptyset$  is a conjugacy domain in  $H$  and  $H = \langle I_H \rangle$ .*
- (b) *A finite involutory structure  $\mathbf{H}$  is in  $\text{Im} \mathbf{G}$  if and only if (\*) holds.*
- (c)  *$\mathbf{G}$  has the embedding property.*

PROOF. The fixed field of  $I_G$  in  $G$  is totally real over  $K$ . Thus  $G = \langle I_G \rangle$ .

PROOF OF (a). As  $1 \notin I_A = \varphi(I_G)$ ,  $\text{Ker}(\varphi) \cap I_G = \emptyset$ . Therefore the fixed field  $L$  of  $\text{Ker}(\varphi)$  is not formally real. Without loss of generality  $\mathbf{A} = \mathbf{G}(L/K)$  and  $\varphi$  is the restriction map.

Theorem 5.2 (with  $m = 1$ ,  $X_1 = X(K)$ , and  $I_1 = I_H$ ) identifies  $\pi: \mathbf{H} \rightarrow \mathbf{A}$  with the restriction map  $\text{res}_L: \mathbf{G}(F/E) \rightarrow \mathbf{G}(L/K)$ , where  $E$  is a simple transcendental extension of  $K$ , and  $F$  is a Galois extension of  $E$  that contains  $L$  and is regular over  $L$ .

Therefore,  $G(F/E) = \langle I(F/E) \rangle$ . Choose  $Q_1, \dots, Q_m \in X(E)$  with

$$I(F/E) = \bigcup_{j=1}^m I_{Q_j}(F/E).$$

We may assume their restrictions  $P_1, \dots, P_m \in X(K)$  to  $K$  are distinct. Indeed, each  $P_j$  is not isolated in  $X(K)$ , and hence there is  $P \in X(K)$  distinct from  $P_1, \dots, P_m$  and arbitrarily close to  $P_j$ . By Remark 1.8(b) we may assume that  $I_P(F/E) = I_{P_j}(F/E)$ . As  $I_P(F/E) = \bigcap_{\substack{Q \in X(E) \\ Q \supseteq P}} I_Q(F/E)$ , there is  $Q \in X(E)$  above  $P$  such that  $I_Q(F/E) = I_{P_j}(F/E)$ . We replace  $Q_j$  by  $Q$ .

Let  $X_1, \dots, X_m$  be a partition of  $X(K)$  into disjoint clopen sets such that  $P_j \in X_j$ . This gives the setup (2) of Section 6. As  $K$  is totally real Hilbertian, there is  $a \in K$  and an epimorphism  $\varphi_a^*: \mathbf{G}(K) \rightarrow \mathbf{G}(F/E)$ . By Remark 6.2(a),  $\varphi_a^*$  is a solution to our embedding problem.

PROOF OF (b). Condition (\*) is necessary, since  $I_G \neq \emptyset$  is a conjugacy domain in  $G$  and  $G = \langle I_G \rangle$ . Conversely, assume (\*). Let  $A = \langle a \rangle = G(K(\sqrt{-1})/K)$  and  $\mathbf{A} = (A, \{a\})$ , where  $a$  is the generator of  $A$ , and let  $\varphi: \mathbf{G} \rightarrow \mathbf{A}$  be the

restriction map. We construct below a finite involutory structure  $\hat{\mathbf{H}}$  that satisfies (\*), with epimorphisms  $\hat{\mathbf{H}} \rightarrow \mathbf{H}$  and  $\pi: \hat{\mathbf{H}} \rightarrow \mathbf{A}$ . By (a) there is an epimorphism  $\psi: \mathbf{G} \rightarrow \hat{\mathbf{H}}$ , and hence  $\mathbf{H} \in \text{Im}\mathbf{G}$ .

If there is an epimorphism  $\pi: \mathbf{H} \rightarrow \mathbf{A}$ , let  $\hat{\mathbf{H}} = \mathbf{H}$ . If not, let  $\hat{\mathbf{H}} = (H \times A, I_H \times \{a\})$ . Both  $\mathbf{A}$  and  $\mathbf{H}$  are quotients of  $\hat{\mathbf{H}}$ . Observe that (\*) holds for  $\hat{\mathbf{H}}$ . Otherwise  $I_H \times \{a\}$  generates a proper subgroup  $\Gamma$  of  $H \times A$  such that the projection  $H \times A \rightarrow H$  maps  $\Gamma$  onto  $H = \langle I_H \rangle$ . Thus  $\Gamma = \{(h, \pi(h)) \mid h \in H\}$ , where  $\pi: H \rightarrow A$  is an epimorphism. As  $I_H \times \{a\} \subseteq \Gamma$ , we have  $\pi(I_H) = a$ . Thus  $\pi$  induces an epimorphism  $\mathbf{H} \rightarrow \mathbf{A}$ , a contradiction.

PROOF OF (c). Clear from (a) and (b).  $\square$

If, in addition to the assumptions of the theorem,  $K$  is countable, then  $G$  is of rank at most  $\aleph_0$ . Thus the involutory structures  $\mathbf{G}$  and  $\mathbf{D}$  are very similar, by Lemma 7.3 and Theorem 7.4. In fact, we have the following straightforward modification of [FJ, Lemma 24.1].

LEMMA 7.5. *Let  $\mathbf{G}$  and  $\mathbf{H}$  be involutory structures with embedding property, such that  $G$  and  $H$  are of rank at most  $\aleph_0$ . If  $\text{Im}\mathbf{G} = \text{Im}\mathbf{H}$ , then  $\mathbf{G} \equiv \mathbf{H}$ .*

THEOREM 7.6. *Let  $K$  be a countable totally real Hilbertian PRC field. Assume that  $K$  has no proper totally real algebraic extensions and  $X(K)$  has no isolated points. Then  $\mathbf{G}(K) \equiv \mathbf{D}$ , and hence  $G(K) \equiv D$ .*

The field  $\mathbb{Q}^{\text{tr}}$  of totally real algebraic numbers is PRC by [P]. (We remark that although Pop [P] states this result, he only gives the proof for an analog. Therefore in all our results about  $\mathbb{Q}^{\text{tr}}$  the reference [P] should be replaced by a subsequent version, where this omission will be remedied.) It is clearly countable. By Proposition 6.6 it is totally real Hilbertian, and by Remark 1.5,  $X(\mathbb{Q}^{\text{tr}})$  has no isolated points. Therefore:

COROLLARY 7.7. *The absolute Galois group of the field  $\mathbb{Q}^{\text{tr}}$  of totally real algebraic numbers is the free profinite product  $D$  of groups of order 2 over the universal Boolean space  $X_\omega = \{0, 1\}^{\aleph_0}$  of weight  $\aleph_0$ .*

## 8. Real Frobenius fields

Let  $S/R$  be a real Galois ring cover, and let  $F/E$  be the corresponding field extension. Let  $K$  be a subfield of  $R$  and  $L$  the algebraic closure of  $K$  in  $F$ .

The following definitions are valuable [HL, Definition 4.2].

- (a)  $S/R$  is **regular over**  $K$ , if the extension  $E/K$  is regular. In that case  $L/K$  is a finite Galois extension.
- (b)  $S/R$  is **finitely generated** over  $K$ , if  $R$  and  $S$  are finitely generated rings over  $K$ .
- (c)  $F/E$  is **amply real** over  $K$  if  $E/K$  is a regular extension, the algebraic closure  $L$  of  $K$  in  $F$  is not formally real, and the extension  $F(\epsilon)/L(\epsilon)$  is totally real for every real involution  $\epsilon \in G(F/E)$ .

DEFINITION 8.1. A field  $M$  is said to be **real Frobenius** if it satisfies the following condition: Let  $S/R$  be a real Galois ring cover, finitely generated and regular over  $M$ , with  $F/E$  the corresponding field extension amply real over  $M$ . Let  $N$  be the algebraic closure of  $M$  in  $F$ . Let  $\mathbf{H} \leq \mathbf{G}(F/E)$  such that  $\mathbf{H} \in \text{Im}\mathbf{G}(M)$  and  $\text{res}_N \mathbf{H} = \mathbf{G}(N/M)$ . Then there exists an  $M$ -homomorphism  $\psi: S \rightarrow \widetilde{M}$  such that  $\psi(R) = M$  and  $\psi^*(\mathbf{G}(M)) = \mathbf{H}$ .

PROPOSITION 8.2. *Let  $M$  be a PRC field. If  $\mathbf{G}(M)$  has the embedding property, then  $M$  is real Frobenius.*

PROOF. (Cf. [HL, Proposition 5.6].) Let  $S/R$ ,  $F/E$ ,  $N$ , and  $\mathbf{H}$  be as in Definition 8.1. The embedding property gives an epimorphism of involutory structures  $h: \mathbf{G}(M) \rightarrow \mathbf{H}$  with  $\text{res}_N \circ h = \text{res}_N$ . Put  $L = \widetilde{M}F$ . Then

$$G(L/E) = G(\widetilde{M}E/E) \times_{G(NE/E)} G(F/E) = G(M) \times_{G(N/M)} G(F/E).$$

Let  $D$  be the fixed field of  $\Delta = \{(\delta, h(\delta)) \mid \delta \in G(M)\}$  in  $L$ . Then  $D/M$  is regular,  $DF = D\widetilde{M} = L$ , and  $D \cap F = E$  [FJ, p. 354]. We show that  $D/M$  is totally real. Let  $P$  be an ordering on  $M$ . There is  $\epsilon \in I(M)$  such that  $P$  is the restriction of  $P_\epsilon$  from  $\widetilde{M}(\epsilon)$ . Then  $h(\epsilon) \in I_H \subseteq I(F/E)$ . Observe that  $\widetilde{M}(\epsilon)$  and  $F(h(\epsilon))$  are linearly disjoint over  $N(\epsilon)$  and  $L(\epsilon, h(\epsilon)) = D(\epsilon)F(h(\epsilon))$  contains  $D$ . By assumption there is an ordering  $Q$  of  $F(h(\epsilon))$  such that  $\text{res}_{N(\epsilon)} Q = \text{res}_{N(\epsilon)} P_\epsilon$ . Therefore  $P_\epsilon$  and  $Q$  extend to an ordering of  $L(\epsilon, h(\epsilon))$  [J, p. 241]. The restriction of this ordering to  $D$  extends  $P$ .

The integral closure  $U$  of  $R$  in  $D$  is finitely generated over  $M$  [FJ, p. 354] and hence  $U$  is the coordinate ring of an absolutely irreducible variety  $V$  defined over  $M$ . Since  $M$  is PRC, there exists an  $M$ -homomorphism  $\psi_0: U \rightarrow M$ . Extend  $\psi_0$  to an  $\widetilde{M}$ -epimorphism  $\widetilde{M}U \rightarrow \widetilde{M}$ , and let  $\psi: S \rightarrow \widetilde{M}$  be its restriction to  $S$ . Then  $\psi(R) = M$ , and, by [FJ, Remark on p. 9], we may arrange it so that  $\psi^*: G(M) \rightarrow G(F/E)$  coincides with  $h$ . Therefore  $\psi^*(\mathbf{G}(M)) = \mathbf{H}$ .  $\square$

By Corollary 7.7 and Lemma 7.3(c),  $\mathbf{G}(\mathbb{Q}^{\text{tr}})$  has the embedding property. By [P],  $\mathbb{Q}^{\text{tr}}$  is PRC. Therefore:

COROLLARY 8.3.  *$\mathbb{Q}^{\text{tr}}$  is real Frobenius.*

## 9. Real Galois Stratification

This section gives a quantifier elimination procedure for the theory of real Frobenius fields in the language below. The procedure is similar to [FJ, Chapter 25] and almost the same as in [HL]. So we only comment on the differences.

A **Galois ring/set cover**  $C/A$  over a field  $K$  [FJ, p. 403] is **real** if  $A$  is nonsingular,  $\text{char}(K) = 0$ , and  $K(C)$  is not formally real. Put  $\mathbf{G}(C/A) = \mathbf{G}(K(C)/K(A))$  (Example 7.1(a)) and let  $\text{Sub}[C/A]$  be the involutory substructures of  $\mathbf{G}(C/A)$ .

Let  $K \subseteq M$  be a field. Each  $\mathbf{a} \in A(M)$  determines a  $K$ -homomorphism  $\varphi: K[A] \rightarrow M$ , and therefore (see Section 6) a homomorphism  $\varphi^*: G(M) \rightarrow$

$G(C/A)$  (unique up to an inner automorphism of  $G(C/A)$ ). Example 7.1(b) says that  $\varphi^*(\mathbf{G}(M) \leq \mathbf{G}(C/A))$ . Omitting the reference to  $C$  and  $M$ , define the **Artin symbol**  $\mathbf{Ar}(A, \mathbf{a})$  as the set  $\{\varphi^*(\mathbf{G}(M)^\sigma \mid \sigma \in G(C/A))\}$ . This is a conjugacy class in  $\text{Sub}[C/A]$ . For properties of the Artin symbol see [FJ, Section 5.3].

For  $n \geq 0$  let  $\pi: \mathbb{A}^{n+1} \rightarrow \mathbb{A}^n$  be the projection on the first  $n$  coordinates. Let  $A \subseteq \mathbb{A}^{n+1}$  and  $B \subseteq \mathbb{A}^n$  be two non-singular basic sets [FJ, p. 244] such that  $\pi(A) = B$ . Then  $K[B] \subseteq K[A]$ . Let  $\mathbf{x}$  and  $(\mathbf{x}, y)$  be generic points of  $B$  and  $A$ , respectively. Then  $K(A) = K(B)(y)$ . Furthermore, let  $C/A$  and  $D/B$  be real Galois covers such that  $K(D)$  contains the algebraic closure of  $K(B)$  in  $K(C)$ .

**DEFINITION 9.1** [HL, Definition 7.1]. Let  $M$  be a field extension of  $K$ . An  **$M$ -specialization** of the pair  $(C/A, D/B)$  is a  $K$ -homomorphism  $\varphi$  from  $C$  into an overfield of  $M$  with these properties:  $\varphi(K[B]) \subseteq M$ ; and if  $y$  is transcendental over  $K(B)$ , then  $\varphi(y)$  is transcendental over  $M$ .

For such a specialization put  $y' = \varphi(y)$ ,  $N = M[\varphi(D)]$ ,  $R = M[\varphi(K[A])]$ ,  $E = M(y')$  (the quotient field of  $R$ ),  $S = M[\varphi(C)]$ , and  $F = E[\varphi(C)]$  (the quotient field of  $S$ ). Then  $\varphi$  induces an embedding  $\varphi^*: G(F/E) \rightarrow G(C/A)$ .

Assume that  $\dim A = \dim B + 1$ . The pair  $(C/A, D/B)$  is **specialization compatible** if the following properties hold for every  $M$  and each  $M$ -specialization  $\varphi$  as above.

- (i)  $K(D)$  is the algebraic closure of  $K(B)$  in  $K(C)$ . and for every  $M$  and each  $M$ -specialization  $\varphi$  as above  $[K(C) : K(D)(y)] = [F : N(y')]$ .
- (ii) The cover  $K(C)/K(A)$  is amply real over  $K(B)$ .
- (iii) For each involution  $\epsilon \in G(F/E)$  with  $\varphi^*(\epsilon)$  real the extension  $F(\epsilon)/N(\epsilon)$  is totally real.

Assume that  $\dim A = \dim B$ . The pair  $(C/A, D/B)$  is said to be **specialization compatible** if  $K[A]$  is integral over  $K[B]$  and  $C = D$ .

**LEMMA 9.2.** *Assume that  $\dim A = \dim B + 1$  and that  $(C/A, D/B)$  is specialization compatible. Let  $\text{Con}(A)$  be a conjugacy domain in  $\text{Sub}[C/A]$ , and let  $\mathcal{S}$  be a set of (isomorphism types of) involutory structures. Define*

$$\text{Con}(B) = \begin{cases} \text{res}_{K(D)}(\mathcal{S} \cap \text{Con}(A)) & \text{if } \dim A = \dim B + 1; \\ \{\mathbf{G}^\sigma \mid \mathbf{G} \in \text{Con}(A), \sigma \in G(C/B)\} & \text{if } \dim A = \dim B. \end{cases}$$

*Let  $M$  be a real Frobenius field that contains  $K$ , and let  $\mathbf{b} \in B(M)$ . Assume  $\text{Im}\mathbf{G}(M) \cap \text{Sub}[C/A] = \mathcal{S}$ . Then  $\mathbf{Ar}(B, \mathbf{b}) \subseteq \text{Con}(B)$  if and only if there is  $\mathbf{a} \in A(M)$  such that  $\pi(\mathbf{a}) = \mathbf{b}$  and  $\mathbf{Ar}(A, \mathbf{a}) \subseteq \text{Con}(A)$ .*

**PROOF.** See [HL, Lemma 7.2] in case  $\dim A = \dim B + 1$  and [HL, Lemma 7.3] in case  $\dim A = \dim B$ . (Replace everywhere the  $e$ -structures of [HL] by our involutory structures.)  $\square$

**LEMMA 9.3** [HL, Lemma 7.5]. *Let  $K_1$  be a finite extension of  $K(D)$ . There are Zariski open subsets  $A' \subseteq A$ ,  $B' \subseteq B$  and a specialization compatible pair of real Galois covers  $(C'/A', D'/B')$  such that  $K(C) \subseteq K(C')$  and  $K_1 \subseteq K(D')$ .*

From now on we can proceed exactly as in [FJ, Chapter 25]. Replace Galois covers with real Galois covers, and conjugacy classes of subgroups of  $G(C_i/A_i)$  with conjugacy classes of involutory substructures of  $\mathbf{G}(C_i/A_i)$  (cf. [HL, Sections 8 and 9]).

This includes the definition of Galois stratification and Galois formulas [FJ, p. 410]. Thus, a **real** Galois stratification

$$\mathcal{A} = \langle \mathbb{A}^n, C_i/A_i, \text{Con}(A_i) \mid i \in I \rangle,$$

is a partition of the affine space  $\mathbb{A}^n$  over  $K$  as a finite disjoint union  $\mathbb{A}^n = \bigcup_{i \in I} A_i$  of nonsingular  $K$ -basic sets, each of them equipped with a real Galois cover  $C_i/A_i$  and a conjugacy domain  $\text{Con}(A_i)$  in  $\text{Sub}[C_i/A_i, \mathbf{P}_0]$ . The corresponding **real** Galois formula is a formal expression  $\mathbf{Ar}(\mathcal{A}, \mathbf{X}) \subseteq \text{Con}(\mathcal{A})$  with the following interpretation. For be an extension  $M$  of  $K$  and  $\mathbf{a} \in M^n$  write  $M \models \mathbf{Ar}(\mathcal{A}, \mathbf{a}) \subseteq \text{Con}(\mathcal{A})$  if  $\mathbf{Ar}(A_i, \mathbf{a}) \subseteq \text{Con}(A_i)$  for the unique  $i$  such that  $\mathbf{a} \in A_i(M)$ .

If  $K$  is a presented field with elimination theory [FJ, Definition 17.9], we get an effective elimination of quantifiers for the theory of real Frobenius fields in this language. Moreover, every formula in the language  $\mathcal{L}(K)$  of rings with parameters from  $K$  is equivalent to a real Galois formula (cf. [FJ, Remark 25.8]). The corresponding real Galois stratification may satisfy  $C_i = K[A_i][\sqrt{-1}]$ , for each  $i \in I$ . Conclude the following.

**PROPOSITION 9.4** [HL, Theorem 9.2(a)]. *Let  $K$  be a presented field with elimination theory, and let  $\vartheta$  be a sentence in  $\mathcal{L}(K)$ . We can effectively find a finite Galois extension  $L$  of  $K$  with  $\sqrt{-1} \in L$ , a finite family  $\mathcal{H} \supseteq \text{Sub}[L/K]$  (isomorphism types of) finite involutory structures, and for each  $\mathcal{S} \subseteq \mathcal{H}$  a conjugacy domain  $\text{Con}(\mathcal{S})$  in  $\text{Sub}[L/K]$  contained in  $\mathcal{S}$  with the following property. For every real Frobenius field  $M$  that contains  $K$  and satisfies  $\text{Im}\mathbf{G}(M) \cap \mathcal{H} = \mathcal{S}$  we have  $M \models \vartheta$  if and only if  $\text{res}_L \mathbf{G}(M) \in \text{Con}(\mathcal{S})$ .*

In particular, Proposition 9.4 holds for  $K = \mathbb{Q}$ .

## 10. Model theoretic results.

Let  $K'$  be a given finite extension of  $\mathbb{Q}$ , say as  $K' = \mathbb{Q}[X]/(f)$ , where  $f \in \mathbb{Z}[X]$  is a given monic irreducible polynomial. Then  $K'$  is formally real (resp.  $K' \subseteq \mathbb{Q}^{\text{tr}}$ ) if and only if  $f$  has a root in  $\mathbb{R}$  (resp.  $f$  splits over  $\mathbb{R}$ ). We can effectively decide whether this condition holds [L, p. 276].

In particular, given a finite Galois extension  $L$  of  $\mathbb{Q}$ , we can effectively find the field  $L \cap \mathbb{Q}^{\text{tr}}$  and the involutory structure  $\mathbf{G}(L/L \cap \mathbb{Q}^{\text{tr}})$ .

Let  $\mathcal{L}(K)$  denote the elementary language of fields with parameters from  $K$ .

**THEOREM 10.1.** *The elementary theory of  $\mathbb{Q}^{\text{tr}}$  is effectively decidable.*

**PROOF.** Apply Proposition 9.4. The field  $\mathbb{Q}^{\text{tr}}$  is real Frobenius (Corollary 8.3) and  $\text{Im}\mathbf{G}(\mathbb{Q}^{\text{tr}}) = \text{Im}\mathbf{D}$  (Corollary 7.7) is the family of finite involutory structures  $\mathbf{H}$  in which  $I_H \neq \emptyset$  is a conjugacy domain in  $H$  and  $H = \langle I_H \rangle$

(Lemma 7.3(b)). Furthermore, if  $L/\mathbb{Q}$  is a finite Galois extension and  $K' = L \cap \mathbb{Q}^{\text{tr}}$ , then  $\mathbb{Q}^{\text{tr}}/K'$  is totally real, and hence  $\text{res}_{K'} X(\mathbb{Q}^{\text{tr}}) = X(K')$ . Therefore  $\text{res}_L \mathbf{G}(\mathbb{Q}^{\text{tr}}) = (G(L/K'), I(L/K')) = \mathbf{G}(L/K')$ .

Let  $\vartheta$  be a sentence in  $\mathcal{L}(\mathbb{Q})$ . Proposition 9.4 effectively gives a finite Galois extension  $L$  of  $\mathbb{Q}$  with  $\sqrt{-1} \in L$ , a finite family  $\mathcal{H}$  of (isomorphism types of) finite involutory structures, and, for

$$\mathcal{S} = \{\mathbf{H} \in \mathcal{H} \mid I_{\mathbf{H}} \neq \emptyset \text{ is a conjugacy domain in } H \text{ and } H = \langle I_{\mathbf{H}} \rangle\},$$

a conjugacy domain  $\text{Con} = \text{Con}(\mathcal{S})$  in  $\text{Sub}[L/\mathbb{Q}]$  contained in  $\mathcal{S}$ . For these,  $\mathbb{Q}^{\text{tr}} \models \vartheta$  if and only if  $\mathbf{G}(L/L \cap \mathbb{Q}^{\text{tr}}) \in \text{Con}$ . This condition is checkable, by the remarks preceding this corollary.  $\square$

LEMMA 10.2. *There is a formula  $\theta(X_1, \dots, X_n) \in \mathcal{L}(\mathbb{Q})$  with the following property. Let  $M$  be a PRC field, let  $\mathbf{a} = (a_1, \dots, a_n) \in M^n$ , and put  $f = Z^n + a_1 Z^{n-1} + \dots + a_n \in M[Z]$ . Then  $M \models \theta(\mathbf{a})$  if and only if*

(\*)  *$f$  has a root  $\alpha$  in  $\widetilde{M}$  such that  $M(\alpha)$  is formally real.*

PROOF. Condition (\*) is equivalent to this: There is an ordering  $P$  on  $M$  such that  $f$  has a root in the real closure of  $(M, P)$ . By Tarski's principle [HL, Proposition 1.4] this is equivalent to a finite disjunction of statements of this form: There is an ordering  $P$  on  $M$  with  $\bigwedge_{i=1}^r f_i(\mathbf{a}) = 0 \wedge \bigwedge_{j=1}^m g_j(\mathbf{a}) \in P$ , where  $f_1, \dots, f_r, g_1, \dots, g_m \in \mathbb{Z}[X_1, \dots, X_n]$  do not depend on  $M$  and  $\mathbf{a}$ .

Put  $g_0 = 1$ , and let  $\Delta$  be the set of finite sums of squares in  $M$ . By [P1, Corollary 1.6],  $\sum_{i,j=0}^m g_i(\mathbf{a})g_j(\mathbf{a})\Delta$  is the intersection of all orderings on  $M$  that contain  $g_1(\mathbf{a}), \dots, g_m(\mathbf{a})$ . Therefore the last statement is equivalent to:  $\bigwedge_{i=1}^r f_i(\mathbf{a}) = 0 \wedge -1 \notin \sum_{i,j=0}^m g_i(\mathbf{a})g_j(\mathbf{a})\Delta$ . As  $\Delta$  is the set of sums of two squares in the PRC field  $M$  [P2, Proposition 1.5], a formula in  $\mathcal{L}(\mathbb{Q})$  expresses this statement.  $\square$

PROPOSITION 10.3. *Every real Galois formula  $\theta$  over a field  $K$  is equivalent to a formula in  $\mathcal{L}(K)$ , modulo the theory of PRC fields  $M$  containing  $K$ .*

PROOF. It suffices to express in  $\mathcal{L}(K)$  the statement  $\mathbf{Ar}(A, \mathbf{X}) \in \text{Con}$ , with  $C/A$  a real Galois ring/set cover over  $K$  and  $\text{Con} = \{\mathbf{H}^\sigma \mid \sigma \in G(C/A)\}$ , where  $\mathbf{H} = (H, I_{\mathbf{H}})$  is a involutory substructure of  $\mathbf{G}(C/A)$ . Let  $E = K(A)$  and  $F = K(C)$  be the quotient fields. For each  $G \leq G(C/A) = G(F/E)$  let  $F(G)$  be the fixed field of  $G$  in  $F$ , and let  $z_G$  be a primitive element for  $F(G)/E$ . Replacing  $A$  by an open subset  $A'$  (that is, replacing the given Galois stratification by its refinement) we may assume that  $K[A][z_G]/K[A]$  is a ring cover [FJ, Definition 5.4] and  $z_G$  is a primitive element for it.

Write  $K[A]$  as  $K[\mathbf{x}, g(\mathbf{x})^{-1}]$ , where  $\mathbf{x}$  is a generic point of  $A$  over  $K$ . Let  $f_G$  be a polynomial over  $K$  such that  $f_G(\mathbf{x}, g(\mathbf{x})^{-1}, Z) = \text{irr}(z_G, E)$ . For every  $\epsilon \in H$  let  $h_\epsilon$  be a polynomial over  $K$  with  $h_\epsilon(\mathbf{x}, g(\mathbf{x})^{-1}, z_H, Z') = \text{irr}(z_{(\epsilon)}, F(H))$ .

Then  $M \models \mathbf{Ar}(A, \mathbf{a}) \in \text{Con}$  means the following conditions hold.

(a)  $\mathbf{a} \in A$ : there is a specialization  $\mathbf{x} \rightarrow \mathbf{a}$  such that  $g(\mathbf{a}) \neq 0$ .

- (b)  $\mathbf{x} \rightarrow \mathbf{a}$  extends to a homomorphism  $\psi: C \rightarrow \widetilde{M}$  such that  $\psi^*(G(M)) = H$ .
- (c)  $\psi^*(I(M)) = I_H$ : for every involution  $\epsilon \in H$ ,  $\epsilon \in I_H$  if and only if
- (c $_{\epsilon}$ )  $\epsilon \in \psi^*(I(M))$ .

Assume (a). Then (b) means the conjunction of the following two statements [FJ, Remark 25.14]:

- (b1)  $f_H(\mathbf{a}, g(\mathbf{a})^{-1}, Z)$  has a root  $c \in M$ ; and
- (b2) if  $G < H$ , then  $f_G(\mathbf{a}, g(\mathbf{a})^{-1}, Z)$  has no root in  $M$ .

Assume (a) and (b), and let  $\epsilon \in H$  be an involution. Condition (c $_{\epsilon}$ ) says

- (c' $_{\epsilon}$ )  $h_{\epsilon}(\mathbf{a}, g(\mathbf{a})^{-1}, c, Z')$  has a root  $\alpha \in \widetilde{M}$  such that  $M(\alpha)$  is formally real.

Therefore the assertion follows by Lemma 10.2.  $\square$

PROPOSITION 10.4. *The following collection of conditions on a field  $M$  is equivalent to a primitive recursive set of elementary sentences in  $\mathcal{L}(\mathbb{Q})$ .*

- (1)  $M$  is PRC.
- (2)  $M \cap \widetilde{\mathbb{Q}} = \mathbb{Q}^{\text{tr}}$ .
- (3)  $\text{Im}\mathbf{G}(M) = \{\mathbf{H} \mid H = \langle I_H \rangle\}$ .
- (4)  $\mathbf{G}(M)$  has the embedding property.
- (5)  $M/\mathbb{Q}^{\text{tr}}$  is totally real.

PROOF. For (1) see [P2, Theorem 4.1]. Condition (2) says each irreducible polynomial  $f \in \mathbb{Q}[X]$  has a root in  $M$  if and only if  $f$  has a root in  $\mathbb{Q}^{\text{tr}}$ . This is equivalent to  $f$  splits over the real closure of  $\mathbb{Q}$ . Express the latter in  $\mathcal{L}(\mathbb{Q})$  either by Tarski's principle [HL, Proposition 1.4] or by Sturm's Theorem [L, Chapter XI, §2]. Conditions (3) and (4) easily follow from Lemma 10.2.

Assume (1) and (2). By Remark 1.8(b), the image  $X$  of restriction  $X(M) \rightarrow X(\mathbb{Q}^{\text{tr}})$  is closed in  $X(\mathbb{Q}^{\text{tr}})$ . Thus, (5) is equivalent to  $X$  dense in  $X(\mathbb{Q}^{\text{tr}})$ . Now,  $X(\mathbb{Q}^{\text{tr}})$  has a basis from the sets  $\{P \in X(\mathbb{Q}^{\text{tr}}) \mid P \text{ extends to } \mathbb{Q}^{\text{tr}}(\alpha)\}$ , where  $\alpha$  runs through the elements of  $\widetilde{\mathbb{Q}}$ . Indeed, by Remark 1.8(b) these sets are clopen. By [P1, Corollary 9.2],  $\mathbb{Q}^{\text{tr}}$  is SAP. That is, the sets

$$H(c) = \{P \in X(\mathbb{Q}^{\text{tr}}) \mid c \in P\} = \{P \in X(\mathbb{Q}^{\text{tr}}) \mid P \text{ extends to } \mathbb{Q}^{\text{tr}}(\sqrt{c})\}$$

form a basis for the Harrison topology on  $X(\mathbb{Q}^{\text{tr}})$ , as  $c$  varies on  $\mathbb{Q}^{\text{tr}}$ .

It suffices to consider only  $\alpha \in \widetilde{\mathbb{Q}}$  with  $\mathbb{Q}(\alpha)$  formally real; otherwise the corresponding set of orderings is empty. Thus (5) is equivalent to this statement: If  $\mathbb{Q}(\alpha)$  is a finite formally real extension of  $\mathbb{Q}$ , then  $M(\alpha)$  is formally real. Now use Lemma 10.2.  $\square$

COROLLARY 10.5. *A field  $M$  is a model of  $\text{Th}(\mathbb{Q}^{\text{tr}})$  if and only if it satisfies conditions (1)–(5).*

PROOF. The conditions hold for  $M = \mathbb{Q}^{\text{tr}}$ . By Remark 10.4 they thus hold for each model  $M$  of  $\text{Th}(\mathbb{Q}^{\text{tr}})$ . Conversely, assume (1)–(5). Then  $M$  is a real Frobenius field (Proposition 8.3), and  $\text{Im}\mathbf{G}(M) = \text{Im}\mathbf{G}(\mathbb{Q}^{\text{tr}})$ , by (3). So, (2) and (5) imply  $\text{res}_{\widetilde{\mathbb{Q}}}\mathbf{G}(M) = \mathbf{G}(\mathbb{Q}^{\text{tr}})$ . By Proposition 9.4 (with  $K = \mathbb{Q}$ ) the fields  $M$  and  $\mathbb{Q}^{\text{tr}}$  satisfy the same sentences in  $\mathcal{L}(\mathbb{Q})$ .  $\square$



## REFERENCES

- [C] T.C. Craven, *The topological space of orderings of a rational function field*, Duke Math. J. **41** (1974), 339–347.
- [DF1] P. Debes and M.D. Fried, *Rigidity and real residue class fields*, Acta Arith. **56** (1990), 1–31.
- [DF2] P. Debes and M.D. Fried, *Nonrigid constructions in Galois theory*, Pac. Jour. **163** #1 (1994), 81–122.
- [ELW] R. Elman, T.Y. Lam and A.R. Wadsworth, *Orderings under field extensions*, J. Reine Angew. Math. **306** (1979), 7–27.
- [F] M.D. Fried, *Fields of definition of function fields and Hurwitz families – groups as Galois group*, Comm. Alg. **5** (1977), 17–82.
- [FHJ] M.D. Fried, D. Haran and M. Jarden, *Galois stratification over Frobenius fields*, Advances in Math. **51** (1984), 1–35.
- [FHV] M.D. Fried, D. Haran and H. Völklein, *Absolute Galois group of the totally real numbers*, C.R. Acad. Sci. Paris **317** (1993), 95–99.
- [FJ] M.D. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik III, vol. 11, Springer Verlag, Heidelberg, 1986.
- [FV1] M.D. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli space*, Math. Ann. **290** (1991), 771–800.
- [FV2] M.D. Fried and H. Völklein, *The embedding problem over a Hilbertian PAC-field*, Annals of Math. **135** (1992), 469–481.
- [FV3] M.D. Fried and H. Völklein, *The absolute Galois group of a Hilbertian PRC field*, Israel J. Math. **85** (1994), 85–101.
- [G] W.-D. Geyer, *Galois groups of intersections of local fields*, Israel J. Math. **30** (1978), 382–396.
- [HJ1] D. Haran and M. Jarden, *The absolute Galois group of a pseudo real closed field*, Annali della Scuola Normale Superiore — Pisa, Serie IV **12** (1985), 449–489.
- [HJ2] D. Haran and M. Jarden, *Real free groups and the absolute Galois group of  $\mathbb{R}(t)$* , J. of pure and applied algebra **37** (1985), 155–165.
- [HL] D. Haran and L. Lauwers, *Galois stratification over  $e$ -fold ordered Frobenius fields*, Israel J. Math. **85** (1994), 169–197.
- [H] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, Springer-Verlag, 1977.
- [HR] W. Herfort and L. Ribes, *Torsion elements and centralizers in free products of profinite groups*, J. für die reine und angewandte Mathematik **358** (1985), 155–161.
- [J] M. Jarden, *The elementary theory of large  $e$ -fold ordered fields*, Acta mathematica **149** (1982), 239–260.
- [KN] W. Krull and J. Neukirch, *Die Struktur der absoluten Galoisgruppe über dem Körper  $\mathbb{R}(t)$* , Math. Ann. **193** (1971), 197–209.
- [L] S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1970.
- [M] W.S. Massey, *Algebraic topology: An introduction*, Graduate Texts in Mathematics, Springer-Verlag, 1977.
- [Ma] H. Matsumura, *Commutative Algebra*, Benjamin/Cummings, Reading, Mass., 1980.
- [P] F. Pop, *Fields of totally  $\Sigma$ -adic numbers*, preprint (1992).
- [P1] A. Prestel, *Lectures on formally real fields*, IMPA Publications, vol. 1093, Springer Verlag, 1984.
- [P2] A. Prestel, *Pseudo real closed fields*, Set Theory and Model Theory, Lecture Notes in Mathematics, vol. 872, Springer Verlag, 1981, pp. 127–156.
- [P3] A. Prestel, *On the axiomatization of PRC-fields*, Methods of Mathematical Logic, Lecture Notes in Mathematics, vol. 1130, Springer Verlag, 1985, pp. 351–359.
- [R] M. Raynaud, *Lecture Notes in Mathematics*, vol. 169, Springer-Verlag, 1970.
- [R1] Julia Robinson, *The undecidability of algebraic rings and fields*, Proc. Amer. Math. Soc. **10** (1959), 950–957.
- [R2] Julia Robinson, *On the decision problem for algebraic rings*, Studies in math. analysis and related topics, Stanford Univ. Press, Stanford, Calif., 1962, pp. 297–304.

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

UC IRVINE, IRVINE, CA 92717, USA

EMAIL: mfried@math.uci.edu

RAYMOND AND BEVERLY SACKLER FACULTY OF EXACT SCIENCES,

TEL AVIV UNIVERSITY, TEL AVIV 69978, ISRAEL

EMAIL: haran@math.tau.ac.il

UNIVERSITY OF FLORIDA, GAINESVILLE, FL 32611, USA

EMAIL: helmut@math.ufl.edu