Contemporary Mathematics
Volume **724**, 2019
https://doi.org/10.1090/conm/724/14593

An explicit descent of real algebraic varieties

Rubén A. Hidalgo

Abstract. Let X be an smooth complex affine algebraic variety admitting a symmetry L, that is, an antiholomorphic automorphism of order two. If both, X and L are defined over $\overline{\mathbb{Q}}$, then Koeck, Lau and Singerman showed the existence of a complex smooth algebraic variety Z admitting a symmetry T, both defined over $\mathbb{R} \cap \overline{\mathbb{Q}}$, and of an isomorphism $R : X \to Z$ so that $R \circ L \circ R^{-1} = T$. The provided proof is existential and, if explicit equations for X and L are given over $\overline{\mathbb{Q}}$, then it is not described how to get the explicit equations for Z and T over $\mathbb{R} \cap \overline{\mathbb{Q}}$. In this paper we provide an explicit rational map R defined over $\overline{\mathbb{Q}}$ so that $Z = R(X)$ is defined over $\mathbb{R} \cap \overline{\mathbb{Q}}$, $R : X \to Z$ is an isomorphisms and $T = R \circ L \circ R^{-1}$ being the usual conjugation map.

1. Introduction

Let $X \subset \mathbb{C}^n$ be an smooth complex affine algebraic variety, say defined by the polynomials $P_1, \ldots, P_m \in \mathbb{C}[x_1, \ldots, x_n]$. If $J_r(x_1, \ldots, x_r) = (\overline{x_1}, \ldots, \overline{x_r})$, the usual conjugation map on $\mathbb{C}^r$, then $\overline{X} = J_n(X)$ is defined by the polynomials $\overline{P_1}, \ldots, \overline{P_m} \in \mathbb{C}[x_1, \ldots, x_n]$, where $\overline{P_j} = J_1 \circ P_j \circ J_n$. By a *symmetry* of X we mean an antiholomorphic automorphism $L : X \to X$ of order two with $J_n \circ L : X \to \overline{X}$ being a biregular isomorphism; in this case, we say that X is *symmetric* and that the pair (X, L) is a *real algebraic variety*. Note that $J_n \circ L$ is a rational map defined over every point of X and its inverse is a rational map defined over every point of $\overline{X}$.

A symmetric algebraic variety may have different symmetries, even different conjugacy classes of them (inside its group of biholomorphic automorphisms). In complex dimension one (i.e., Riemann surfaces) the number of (conjugacy classes of) symmetries is well known (see, for instance, [**2**, **3**]).

Two real algebraic varieties (X, L) and (Y, T) are *isomorphic* if there is a biholomorphism $R : X \to Y$, being also a biregular isomorphism between algebraic varieties, with $T = R \circ L \circ R^{-1}$.

Let $\mathcal{Q}$ be a subfield of $\mathbb{C}$ and (X, L) a real algebraic variety. We say that (X, L) is (i) *defined* over $\mathcal{Q}$ if both, X and L, are defined over $\mathcal{Q}$, and (ii) *definable* over $\mathcal{Q}$ if there is a real algebraic variety (Y, T) defined over $\mathcal{Q}$ and isomorphic to (X, L).

2010 *Mathematics Subject Classification.* Primary 14E05, 14A10, 14P05.

Key words and phrases. Real algebraic varieties, fields of definition.

The author was partially supported by Project Fondecyt 1150003 and Anillo ACT 1415 PIA-CONICYT.

As a consequence of Weil's descent theorem [**19**] (see also [**17**]), every real algebraic variety is definable over $\mathbb{R}$.

In [**10**, **11**] Koeck, Lau and Singerman showed that a real algebraic variety (X, L) which is definable over the field $\overline{\mathbb{Q}}$ of algebraic numbers is also definable over $\mathbb{R} \cap \overline{\mathbb{Q}}$. More generally, as a consequence of Weil's descent theorem [**19**], if (X, L) is defined over a subfield $\mathcal{Q}$ of $\mathbb{C}$ so that $J_1(\mathcal{Q}) = \mathcal{Q}$ (i.e., $\mathcal{Q}$ is *conjugate-invariant*), then it is also definable over $\mathbb{R} \cap \mathcal{Q}$ (Theorem 1). The proof of such fact is existential in the sense that if we are given the explicit equations for X and L over $\mathcal{Q}$, then there is no explained how to construct explicitly R. In this paper, we describe an explicit rational isomorphism map R, defined over $\mathcal{Q}$, so that $R : X \to Z = R(X)$ is an isomorphism, Z is defined over $\mathbb{R} \cap \mathcal{Q}$ and with $T = R \circ L \circ R^{-1}$ being the usual conjugation map (see Theorem2). We hope that this may be of use in the construction of explicit examples, in special, at the level of real dessins d'enfants; the original motivation of this paper.

2. Main results

In this section, we fix a conjugate-invariant subfield $\mathcal{Q}$ of $\mathbb{C}$ and a real algebraic variety (X, L) defined over $\mathcal{Q}$. We first proceed to observe that (X, L) is definable over $\mathcal{Q} \cap \mathbb{R}$, a mild generalization of the results in [**10**, **11**], and then we proceed to describe an explicit rational map R.

THEOREM 1. *The real algebraic variety (X, L) is definable over $\mathcal{Q} \cap \mathbb{R}$.*

A short proof of this fact is provided at the beginning of Section 3.

Remark 1. Assume that $\mathcal{K}$, $\mathcal{N}$ and $\mathcal{L}$ are subfields of $\mathbb{C}$ so that $\mathcal{L}$ contains $\mathcal{K}$ as an algebraically closed subfield (i.e., the only $\mathcal{K}$-algebraic numbers of $\mathcal{L}$ belongs to $\mathcal{K}$) and $\mathcal{N}$ is a finite Galois extension of $\mathcal{K}$. Let X be a complex smooth algebraic variety, which is definable over $\mathcal{L}$ and also over $\mathcal{N}$ (maybe by different models). In [**10**], as a consequence of Weil's descent theorem, it is shown the existence of an isomorphism $R : X \to Z$, where Z is defined over $\mathcal{K}$ (the given proof does not provide a method to obtain explicitly an isomorphism $R : X \to Z$). We should observe that this result does not imply Theorem 1; for instance take $\mathcal{Q} = \mathbb{Q}(i)$.

If the conjugate-invariant subfield $\mathcal{Q}$ is also algebraically closed (for instance, $\mathcal{Q} = \overline{\mathbb{Q}}$, then Theorem 1 can be written as follows.

COROLLARY 1. *Let $\mathcal{Q}$ be an algebraically closed conjugate-invariant subfield of $\mathbb{C}$ and let X be a symmetric variety definable over $\mathcal{Q}$. If the group of birational automorphisms of X is finite, then X is definable over $\mathcal{Q} \cap \mathbb{R}$.*

PROOF. Let $L : X \to X$ be a symmetry of X. We claim that L is defined over $\mathcal{Q}$. In fact, if $\eta \in \mathrm{Gal}(\mathbb{C}/\mathcal{Q})$, then we have the symmetry $L^\eta : X \to X$. So, there is a birational automorphism t of X so that $L^\eta = L \circ t$. Set $K = \{\eta \in \mathrm{Gal}(\mathbb{C}/\mathcal{Q}) : L = L^\eta\}$ and let $\mathcal{U}$ be the fixed field of K. Assume $L = (L_1, \ldots, L_n)$, where L_j is a rational map of the form r_j/s_j, where r_j and s_j are relatively prime polynomials. We may assume the leading coefficient of s_j to be equal to 1. The equality $r_j^\eta/s_j^\eta = r_j/s_j$, for $\eta \in K$, implies that the set of zeroes of r_j (and the set of zeroes of s_j) is invariant under K. In particular, $r_j^\eta = a_\eta r_j$ and $s_j^\eta = b_\eta s_j$, for suitable $a_\eta, b_\eta \neq 0$. Since $r_j^\eta/s_j^\eta = r_j/s_j$, we also have that $b_\eta = a_\eta$. As the leading coefficient of s_j is equal to 1, we must have $b_\eta = 1$; so r_j and s_j are

polynomials defined over $\mathcal{U}$. We conclude that L is defined over $\mathcal{U}$. Now, as the group of birational automorphisms of X is finite, it follows that K is a subgroup of finite index of $\mathrm{Gal}(\mathbb{C}/\mathcal{Q})$; so $\mathcal{U}$ is a finite extension of $\mathcal{Q}$. As $\mathcal{Q}$ is assumed to be algebraically closed, it follows that $\mathcal{U} = \mathcal{Q}$ and we obtain the desired result for L. Now, we may apply Theorem 1. □

2.1. An explicit construction. Let $\mathcal{Q}$ be a conjugate-invariant subfield of $\mathbb{C}$ and let (X, L) be a real algebraic variety defined over $\mathcal{Q}$. Theorem 1 asserts the existence of a real algebraic variety (Z, T), defined over $\mathcal{Q} \cap \mathbb{R}$, and of an isomorphism $R : X \to Z$ so that $T = R \circ L \circ R^{-1}$. Of course, if $\mathcal{Q}$ is a subfield of $\mathbb{R}$, then it suffices to choose R as the identity. So, from now on, we assume that $\mathcal{Q}$ is not a subfield of $\mathbb{R}$ and that (X, L) is not already defined over $\mathcal{Q} \cap \mathbb{R}$. Under these assumptions, we proceed to the construction of a rational map R defined over $\mathcal{Q}$ so that: $R : X \to Z = R(X)$ is an isomorphism, Z is defined over $\mathcal{Q} \cap \mathbb{R}$ and $R \circ T \circ R^{-1}$ is the complex conjugation.

Assume $X \subset \mathbb{C}^n$ is defined by the polynomials $P_1(x_1, \ldots, x_n), \ldots, P_s(x_1, \ldots, x_n) \in \mathcal{Q}[x_1, \ldots, x_n]$.

2.1.1. **Step 1: Can assume $X \cap \overline{X} = \emptyset$.** In fact, if $X \cap \overline{X} \neq \emptyset$, then we may change (X, L) by an isomorphic real algebraic variety (X_0, L_0) so that $X_0 \cap \overline{X_0} = \emptyset$ as follows. Choose a point $\alpha \in \mathcal{Q} - \mathbb{R}$ and consider the algebraic variety $X_0 \subset \mathbb{C}^{n+1}$ (by adding the extra coordinate x_{n+1}) defined by the polynomials defining X and the extra polynomial $P_{s+1}(x_1, \ldots, x_{n+1}) = x_{n+1} - \alpha$ (that is, $X_0 = X \times \{\alpha\}$). The map $H(x_1, \ldots, x_n) = (x_1, \ldots, x_n, \alpha)$ induces a biregular isomorphism between X and X_0 (the projection $(x_1, \ldots, x_{n+1}) \mapsto (x_1, \ldots, x_n)$ induces its inverse). It is now clear that $X_0 \cap \overline{X_0} = \emptyset$. In this new model X_0 the symmetry is given as

$$L_0 = H \circ L \circ H^{-1} : X_0 \to X_0 : (x_1, \ldots, x_n, \alpha) \mapsto (L(x_1, \ldots, x_n), \alpha).$$

2.1.2. **Step 2: Construction of R.** By Step 1, we may assume $X \cap \overline{X} = \emptyset$. Consider the following polynomials in $\mathbb{Z}[x_1, \ldots, x_n, z_1, \ldots, z_n]$:

(1)
$$\left\{ \begin{array}{lcll} t_{1,j} & = & x_j + z_j; & j = 1, \ldots, n, \\ t_{2,j} & = & x_j z_j; & j = 1, \ldots, n, \\ t_{k,j} & = & x_{k-2}x_{k-2+j} + z_{k-2}z_{k-2+j}; & k = 3, \ldots, n,\ j = 1, \ldots, n+2-k, \\ t_{n+1,1} & = & x_{n-1}x_n + z_{n-1}z_n. & \end{array} \right\}$$

The reason of using these polynomials $t_{i,j}$ is clarified in the forthcoming Lemma 4.

For $x = (x_1, \ldots, x_n) \in X$, set $z = (z_1, \ldots, z_n) = J_n(L(x)) \in \overline{X}$ and consider the rational map

$$R : X \to \mathbb{C}^{(n^2+3n)/2} : x \mapsto t = (t_{1,1}, \ldots, t_{n+1,1}).$$

Observe that R is defined over $\mathcal{Q}$. Next result states that R as constructed above is the one we are searching.

THEOREM 2. *Under the above assumptions, the following hold.*

1. *$Z = R(X)$ is defined over $\mathcal{Q} \cap \mathbb{R}$.*
2. *$R : X \to Z$ is a birational isomorphism (biregular if $J \circ L$ is a polynomial), defined over $\mathcal{Q}$.*
3. *$R \circ L \circ R^{-1} = J_{(n^2+3n)/2}$.*

3. Proof of Theorems 1 and 2

We only need to take care of the case when the conjugate-invariant subfield $\mathcal{Q}$ is not already a subfield of $\mathbb{R}$. So $\mathcal{Q}$ is a Galois extension of degree two of $\mathcal{K} = \mathcal{Q} \cap \mathbb{R}$. Let $\Gamma := \mathrm{Gal}(\mathcal{Q}/\mathcal{K}) = \langle \sigma(z) = \overline{z} \rangle \cong \mathbb{Z}_2$.

Let $P_1, \ldots, P_s \in \mathcal{Q}[x_1, \ldots, x_n]$ be a set of generators of the ideal of $X \subset \mathbb{C}^n$ and $L = (L_1, \ldots, L_n)$, where $J_1 \circ L_j \in \mathcal{Q}(x_1, \ldots, x_n)$. Observe that $\overline{X} = J_n(X) = X^\sigma$. If $\sigma_2 = \sigma$ and $\sigma_1 = e$ is the identity, then we set $f_2 = f_{\sigma_2} = J_n \circ L : X \to \overline{X}$, which is an isomorphism defined over $\mathcal{Q}$ (since L is defined over $\mathcal{Q}$), and $f_1 = f_{\sigma_1} = I$ is the identity.

3.1. Proof of Theorem 1. As the collection $\{f_1, f_2\}$ satisfies Weil's co-cycle conditions $f_{\sigma_i \sigma_j} = f_{\sigma_j}^{\sigma_i} \circ f_{\sigma_i}$, for $i, j \in \{1, 2\}$, it follows from Weil's descent theorem [**19**] the existence of a complex algebraic variety Z, defined over $\mathcal{K}$, and an isomorphism $R : X \to Z$, defined over $\mathcal{Q}$, so that $R = R^{\sigma_j} \circ f_{\sigma_j}$, for $j = 1, 2$. Now, if $T = R \circ L \circ R^{-1}$, then

$$\begin{aligned} T^\sigma &= R^\sigma \circ L^\sigma \circ (R^{-1})^\sigma = R^\sigma \circ L^\sigma \circ (R^\sigma)^{-1} = R^\sigma \circ L^\sigma \circ (f_2 \circ R^{-1}) \\ &= R^\sigma \circ L^\sigma \circ (J_n \circ L \circ R^{-1}) = R^\sigma \circ (J_n \circ L \circ J_n) \circ J_n \circ L \circ R^{-1} \\ &= R^\sigma \circ (J_n \circ L) \circ L \circ R^{-1} = (R^\sigma \circ f_2) \circ L \circ R^{-1} = R \circ L \circ R^{-1} \\ &= T, \end{aligned}$$

that is, T is defined over $\mathcal{K}$.

3.2. Proof of Theorem 2. As above, we fix the notation $\mathcal{K} := \mathbb{Q} \cap \mathbb{R}$, since it is constantly employed.

Now we are assuming that $\overline{X} \cap X = \emptyset$. Let us consider the explicit rational map, defined over $\mathcal{Q}$,

$$\Phi : X \subset \mathbb{C}^n \to \mathbb{C}^n \times \mathbb{C}^n = \mathbb{C}^{2n} : \quad x \mapsto (f_1(x), f_2(x)) = (x, z)\,.$$

As each f_j is an isomorphism, $\Phi : X \to \Phi(X)$ is a birational isomorphism whose inverse is given by the restriction to $\Phi(X)$ of the projection map $\pi : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}^n : (x, z) \mapsto x$.

Remark 2. If f_2 is polynomial (i.e. when L is polynomial), the map $\Phi : X \to \Phi(X)$ is a biregular isomorphism and $\Phi(X)$ is described by the equations

$$\left\{ \begin{array}{c} z = f_2(x), \\ P_1(x) = 0, \ldots, P_s(x) = 0. \end{array} \right\}.$$

If

$$f_2(x) = \left(\frac{r_1(x)}{s_1(x)}, \ldots, \frac{r_n(x)}{s_n(x)} \right),$$

where $r_j, s_j \in \mathcal{Q}[x_1, \ldots, x_n]$ are relatively prime, then $\Phi(X)$ is defined by the equations

$$\left\{ \begin{array}{c} z_1 s_1(x) = r_1(x), \ldots, z_n s_n(x) = r_n(x), \\ P_1(x) = 0, \ldots, P_s(x) = 0, \\ P_1^{\sigma_2}(z) = 0, \ldots, P_s^{\sigma_2}(z) = 0, \end{array} \right\}.$$

In any of the above situations, $\Phi(X)$ still defined over $\mathcal{Q}$.

LEMMA 1. *The symmetry that induces L, by Φ, on $\Phi(X)$ is given by*

$$L_\Phi(x, z) = (\overline{z}, \overline{x}).$$

PROOF.

$$L_\Phi(x,z) = \Phi \circ L \circ \Phi^{-1}(x,z) = \Phi(L(x)) = (L(x), J_n \circ L(L(x))) = (\overline{z}, \overline{x}).$$

□

Each $\sigma_i \in \Gamma$ produces a permutation $\theta(\sigma_i) \in \mathfrak{S}_2$ by the rule $\sigma_i\sigma_j = \sigma_{\theta(\sigma_i)(j)}$. In fact, $\theta(\sigma_1) = (1)(2) = e$ is the identity and $\theta(\sigma_2) = (1,2)$. We consider the natural isomomorphism (Cayley representation)

$$\theta : \Gamma \to \mathfrak{S}_2 : \sigma \mapsto \theta(\sigma).$$

The symmetric group $\mathfrak{S}_2$ produces a natural permutation action $\eta(\mathfrak{S}_2)$ on $\mathbb{C}^n \times \mathbb{C}^n$ defined as follows. If $x, z \in \mathbb{C}^n$, then

$$\eta(e)(x,z) = (x,z), \quad \eta(1,2)(x,z) = (z,x).$$

In this way, the composition $\widehat{\theta} = \eta \circ \theta$ determines a representation of Γ as a subgroup of linear holomorphic automorphisms of $\mathbb{C}^n \times \mathbb{C}^n$ given by

$$\widehat{\theta}(\sigma_1)(x,z) = \tau_1(x,z) = (x,z), \quad \widehat{\theta}(\sigma_2)(x,z) = \tau_2(x,z) = (z,x)$$

where $x, z \in \mathbb{C}^n$. In the following, if $\eta \in \Gamma$, then $\widehat{\eta}$ is an extension of it to a field automorphism of $\mathbb{C}$.

LEMMA 2. *If $j = 1, 2$, then*

(*) $\widehat{\sigma}_j(\Phi(x)) = \tau_j \circ \Phi \circ f_{\sigma_j}^{-1}(\widehat{\sigma}_j(x))$.

(**) *If $y \in \Phi(X)$, then $\widehat{\sigma}_j(y) \in \tau_j(\Phi(X))$.*

PROOF. Let us recall that, for $\tau, \eta \in \Gamma$ we have the co-cycle relation $f_{\tau\eta} = f_\eta^\tau \circ f_\tau$. This co-cycle condition permits to see that, for $\eta \in \Gamma$, we have the following sequence of equalities

$$\begin{cases} \widehat{\eta}\left(f_j(x)\right) = f_j^\eta\left(\widehat{\eta}(x)\right) = f_{\sigma_j}^\eta\left(\widehat{\eta}(x)\right) = f_{\eta\sigma_j}\left(f_\eta^{-1}\left(\widehat{\eta}(x)\right)\right) = \\ = f_{\sigma_{\theta(\eta)(j)}}\left(f_\eta^{-1}\left(\widehat{\eta}(x)\right)\right) = f_{\theta(\eta)(j)}\left(f_\eta^{-1}\left(\widehat{\eta}(x)\right)\right). \end{cases}$$

□

As a consequence of Lemma 2 we have the following commutative diagram (the top part is just the definition of Φ^σ and the bottom part is a consequence of the previous lemma)

$$\begin{array}{lcl} X & \stackrel{\Phi}{\to} & \Phi(X) \\ \downarrow\widehat{\sigma}_j & & \downarrow\widehat{\sigma}_j \\ X^{\sigma_j} & \stackrel{\Phi^{\sigma_j}}{\to} & \Phi^{\sigma_j}\left(X^{\sigma_j}\right) = \Phi(X)^{\sigma_j} = \widehat{\sigma}_j\left(\Phi(X)\right) = \tau_j\left(\Phi(X)\right) \\ \downarrow f_{\sigma_j}^{-1} & & \downarrow\tau_j^{-1} \\ X & \stackrel{\Phi}{\to} & \Phi(X) \end{array}$$

LEMMA 3. $\tau_2\left(\Phi(X)\right) \cap \Phi(X) = \emptyset$.

PROOF. Let us assume we have a point $(x,z) \in \tau_2\left(\Phi(X)\right) \cap \Phi(X)$. By the definition, $(x,z) \in \Phi(X)$ implies that $x \in X$ and $z = f_2(x) \in X^{\sigma_2} = \overline{X}$. Since $(x,z) \in \tau_2\left(\Phi(X)\right)$, we also have that $(z,x) \in \Phi(X)$, that is, $z \in X$. This, in particular, ensures that $X \cap X^{\sigma_2} = X \cap \overline{X} \neq \emptyset$, a contradiction. □

Next ingredient in the computational method concerns with the algebra of invariants of a finite group of linear transformations. Let us briefly recall the general facts. Let $\mathcal{V}$ be a finite dimensional vector space over a field $\mathcal{R}$, say of dimension $n \geq 1$. Let $v_1, \ldots, v_n$ be a basis of $\mathcal{V}^*$. The symmetric algebra $S(\mathcal{V}^*)$ over $\mathcal{R}$ can be identified with the algebra $\mathcal{R}[v_1, \ldots, v_n]$. If G is a group acting linearly over $\mathcal{V}$, then it also acts linearly on $\mathcal{V}^*$. This provides a linear action on $\mathcal{R}[v_1, \ldots, v_n]$. A theorem due to Hilbert-Noether [**13**, **14**] (Chap. 14 in [**15**]) states that, if G is a finite group, then the algebra of G-invariants $\mathcal{R}[\mathcal{V}]^G$ is finitely generated.

In our situation, $G = \Gamma$ is a cyclic group of order 2. Noether's bound theorem (see [**16**] for a proof) states that a set of invariant generators can be chosen on the set of polynomials of degree at most 2. More precisely, the following provides explicit generators.

LEMMA 4. *The algebra of $\widehat{\theta}(\Gamma)$-invariant polynomials is generated by the $(n^2 + 3n)/2$ ones provided in* (1) *in Section* 2.

PROOF. A polynomial $Q(x_1, \ldots, x_n, z_1, \ldots, z_n)$ is $\widehat{\theta}(\Gamma)$-invariant if and only if it is symmetric with respect to permutations of the variables x_i with z_i, for all $i = 1, \ldots, n$. By Noether's bound theorem a set of invariant generators can be chosen on the set of polynomials of degree at most 2. Now, let us assume we have a polynomial P, of degree at most 2, which is invariant under $\widehat{\theta}(\Gamma)$ and let us consider a monomial of P. It will be of the form x_i or z_j or $x_i x_j$ or $z_i z_j$ or $x_i z_j$. The invariance ensures that its symmetric monomial must also belong to P; that is, z_i or x_j or $z_i z_j$ or $x_i x_j$ or $z_i x_j$, respectively. As $x_i z_j + x_j z_i = (x_i + z_i)(x_j + z_j) - (x_i x_j + z_i z_j)$ and $x_i^2 + z_i^2 = (x_i + z_i)^2 - 2x_i z_i$, it follows that P can be generated by polynomials of the form $x_i + z_i$, $x_i z_i$ and, for $i \neq j$, $x_i x_j + z_i z_j$. □

Let us consider the polynomial map

$$\Psi : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}^{(n^2+3n)/2}; \quad \Psi(x, z) = (t_{1,1}, \ldots, t_{n+1,1}),$$

and, as before, $\tau_1(x, z) = (x, z)$ and $\tau_2(x, z) = (z, x)$, where $x, z \in \mathbb{C}^n$.

LEMMA 5. *Keeping all the previous notations, the map Ψ satisfies the following properties:*

(1) $\Psi^{\sigma_j} = \Psi$, *for every* $j = 1, 2$;
(2) $\Psi \circ \tau_j = \Psi$, *for every* $j = 1, 2$; *and*
(3) $\Psi(w_1) = \Psi(w_2)$ *if and only if there is some* $j \in \{1, 2\}$ *so that* $w_2 = \tau_j(w_1)$.

PROOF. Properties (1) and (2) are trivial to see from the construction of Ψ. Now, if $\Psi(x, z) = \Psi(u, v)$, then, for $j = 1, \ldots, n$, it holds that

$$x_j + z_j = u_j + v_j, \quad x_j z_j = u_j v_j.$$

The first equality asserts that $v_j = x_j + z_j - u_j$ and now the second one states that

$$u_j^2 - u_j(x_j + z_j) + x_j z_j = 0.$$

As the roots of the above are x_j and z_j, we are done. □

Set $V = \Psi(\mathbb{C}^n \times \mathbb{C}^n) \subset \mathbb{C}^{(n^2+3n)/2}$. Lemma 5, together classical invariant theory (see, for instance, [**7**, **12**]), asserts that V is a (singular) algebraic variety of dimension $2n$ whose singular part is $\Psi(\Delta)$, where $\Delta = \{(x, z) \in \mathbb{C}^{2n} : x = z\}$.

Remark 3. If $N = (n^2 + 3n)/2$, then the algebra of regular functions on $V \subset \mathbb{C}^N$ (obtained above) is known to be isomorphic to the algebra $\mathbb{C}[x,z]^{\widehat{\theta}(\Gamma)}$ [**6**], where $\widehat{\theta}$ was defined just before Lemma 2. In fact, by taking as above the generators $t_1, \ldots, t_N$ the generators of the algebra of invariant polynomials $\mathbb{C}[x,z]^{\widehat{\theta}(\Gamma)}$, then $\xi : \mathbb{C}[V] \to \mathbb{C}[x,z]^{\widehat{\theta}(\Gamma)}$, defined by $\xi(p) = p(t_1, ..., t_N)$, defines an isomomorphism.

The map $\Psi : \mathbb{C}^n \times \mathbb{C}^n \to V$ is a degree two branched regular holomorphic covering with $\widehat{\theta}(\Gamma)$ as its deck group (see [**18**] for the general concept of a topological branched cover). The branch locus of Ψ is $\Psi(\Delta)$. In particular, $\Psi : \mathbb{C}^n \times \mathbb{C}^n - \Delta \to V - \Psi(\Delta)$ is a regular holomorphic cover map with $\widehat{\theta}(\Gamma)$ as its deck group.

LEMMA 6. *The map $\Psi : \Phi(X) \to Z = \Psi(\Phi(X))$ defines a biregular isomorphism. In particular, $R = \Psi \circ \Phi : X \to Z$ is defined over $\mathcal{Q}$ and it is a birational isomorphism, which is biregular if f_2 is polynomial.*

PROOF. Set $\Phi(X) = W$. Since $\tau_2(W) \cap W = \emptyset$, we have that the polynomial map $\Psi : W \to Z$ is bijective. Now, set $\widehat{W} = W \cup \tau_2(W)$, which is a reducible affine variety whose irreducible components are W and $\tau_2(W)$. Since these irreducible components are pairwise disjoint, we may see that the algebra of regular functions on $\widehat{W}$, say $\mathcal{C}[\widehat{W}]$, is the product of the algebras of regular functions of the components, that is,

$$\mathcal{C}[\widehat{W}] = \mathcal{C}[W] \times \mathcal{C}[\tau_2(W)].$$

The above isomorphism is just given by the restriction of each regular function of $\widehat{W}$ to each of its irreducible components. There is also natural isomorphism $\rho : \mathcal{C}[W] \to \mathcal{C}[\widehat{W}]^{\widehat{\theta}(\Gamma)}$, where $\mathcal{C}[\widehat{W}]^{\widehat{\theta}(\Gamma)}$ denotes the sub-algebra of $\widehat{\theta}(\Gamma)$-invariant regular functions on $\widehat{W}$. This isomorphism is given as follows. If $p \in \mathcal{C}[W]$, then $\rho(p) = (p, p \circ \tau_2^{-1})$ defines an injective homomorphism. It is clear that every $\widehat{\theta}(\Gamma)$-invariant regular function of $\widehat{W}$ is obtained in that way (so ρ is surjective). On the other hand, $\mathcal{C}[Z]$ is isomorphic to $\mathcal{C}[\widehat{W}]^{\widehat{\theta}(\Gamma)}$. To see this, one may consider the injective homomorphism $\chi : \mathcal{C}[Z] \to \mathcal{C}[\widehat{W}]^{\widehat{\theta}(\Gamma)}$ defined by $\chi(p) = p \circ \Psi$. Now, to see that χ is onto, we only need to note that $\rho^{-1}(\chi(\mathcal{C}[Z]))$ is a sub-algebra of $\mathcal{C}[W]$, that W is irreducible and that Z has the same dimension as W. In this way, $\chi^{-1} \circ \rho$ produces an isomorphism between $\mathcal{C}[W]$ and $\mathcal{C}[Z]$, that is, $\Psi : \Phi(X) \to Z$ is a biregular isomorphism and, in particular, $R = \Psi \circ \Phi : X \to Z$ is a birational isomorphism. As $\Psi : W \to Z$ is biregular isomorphism and $\Phi : X \to W$ is biregular if f_2 is polynomial, then $R : X \to Z$ turns out to be biregular if f_2 is polynomial. □

In order to finish the proof, we only need to show that Z is defined over $\mathcal{K}$ since by Lemma 1 and the definition of Ψ we have that $R \circ L \circ R^{-1}$ is just the conjugation map.

PROPOSITION 1. *Z is defined over $\mathcal{K}$.*

PROOF. If $\eta \in \mathrm{Aut}(\mathbb{C}/\mathcal{Q})$, then, as $X^\eta = X$, $\Phi^\eta = \Phi$ (since L and X are defined over $\mathcal{Q}$) and $\Psi^\eta = \Psi$ (since Ψ is defined over the basic field $\mathbb{Q}$), one has that $R^\eta = R$; in particular, $Z^\eta = R(X)^\eta = R^\eta(X^\eta) = R(X) = Z$. So, Z is defined over $\mathcal{Q}$. We have that $\mathcal{Q}$ is a degree two extension of $\mathcal{K}$ and $\mathrm{Gal}(\mathcal{Q}/\mathcal{K})$ is generated by σ_2. It follows, from $(**)$ in Lemma 2 and (3) in Lemma 4, that $\widehat{\sigma_2} : Z \to Z$ is a bijection, that is, $Z^{\sigma_2} = Z$; so Z is defined over $\mathcal{K}$ as desired. □

3.3. Some final computational remarks.

3.3.1. *Equations for V.* It is not difficult to check, for $1 \leq i < j \leq n$ (so $n(n-1)/2$ cases), the following equality

$$t_{1,i}^2 t_{2,j} - t_{1,i} t_{1,j} t_{i+2,j-i} + t_{1,j}^2 t_{2,i} - 4 t_{2,i} t_{2,j} + t_{i+2,j-i}^2 = 0. \tag{2}$$

It follows that, on V, we have that $t_{i+2,j-i}$ is rationally determined by the variables $t_{1,i}$, $t_{2,i}$, $t_{1,j}$ and $t_{2,j}$. In particular, the algebraic variety V is a subvariety of the algebraic variety $\widehat{V}$ defined by the above $n(n-1)/2$ polynomial equations in (2). In worked examples we have seen that $V = \widehat{V}$. We believe that, in the general case, $V = \widehat{V}$.

3.3.2. *Finding the inverse of R.* In order to find explicitly an inverse of $R : X \to Z$, we need to search for rational expressions for the variables x_i's in the variables t_j's. In fact, we will see that we only need the variables $t_{1,i}$, $t_{2,i}$ and $t_{3,i}$ (see Section 3.3.1). We first note that

$$z_j = t_{1,j} - x_j, \quad j = 1, \ldots, n.$$

If $j = 2, \ldots, n$, then

$$t_{3,j-1} + t_{1,j} x_1 - t_{1,j} t_{1,1} = x_1 x_j + z_1 z_j + (x_j + z_j) x_1 - (x_j + z_j)(x_1 + z_1) =$$

$$= x_1 x_j - x_j z_1 = (x_1 - z_1) x_j = (x_1 - (t_{1,1} - x_1)) x_j = (2x_1 - t_{1,1}) x_j,$$

that is,

$$x_j = \frac{t_{3,j-1} + t_{1,j}(x_1 - t_{1,1})}{2x_1 - t_{1,1}}, \quad j = 2, \ldots, n.$$

All the above states that each of the variables $x_2, \ldots, x_n$ can be expressed rationally in terms of the variables $t_{1,1}, \ldots, t_{3,n-1}$ and x_1. Since $t_{1,1} x_1 - t_{2,1} = (x_1 + z_1) x_1 - x_1 z_1 = x_1^2$, we also have

$$x_1^2 = t_{1,1} x_1 - t_{2,1}. \tag{3}$$

Using the polynomial equations of X and/or the first coordinate polynomial equation of f_2 (which provides z_1 in terms of $x_1, \ldots, x_n$) and equality (3) (which permits to pass high powers of x_1 to a degree 1 power of it) we may obtain a linear equation on x_1 whose coefficients are rational forms of $t_{1,1}, \ldots, t_{3,n-1}$. In this way, each of the variables $x_1, \ldots, x_n$ is now rationally expressed in the variables $t_{1,1}, \ldots, t_{3,n-1}$ and the inverse map $R^{-1} : Z \to X$ is then obtained.

3.3.3. *Elimination of variables for Z.* Observe (see Section 3.3.1) that, when we are restricted to X, the coordinates $t_{2+i,j}$ (where $i < j$) are determined by the coordinates $t_{1,1}$, $t_{1,2}$, ..., $t_{1,n}$, $t_{2,n}$; so Z can be described using only these $2n$ coordinates.

4. An example

Let us consider the real algebraic curve (X, L), defined over $\mathbb{Q}(i)$, where

$$X : \left\{ \begin{array}{rcrcrcl} 1 & + & x_1^2 & + & x_2^2 & = & 0 \\ -1 & + & x_1^2 & + & x_3^2 & = & 0 \\ i & + & x_1^2 & + & x_4^2 & = & 0 \end{array} \right\} \subset \mathbb{C}^4,$$

and

$$L : \mathbb{C}^4 \to \mathbb{C}^4 : (x_1, x_2, x_3, x_4) \mapsto (-i\,\overline{x_1}, -i\,\overline{x_3}, -i\,\overline{x_2}, -i\,\overline{x_4}).$$

In this example,

$$f_2 = J_4 \circ L : \mathbb{C}^4 \to \mathbb{C}^4 : (x_1, x_2, x_3, x_4) \mapsto (ix_1, ix_3, ix_2, ix_4),$$

$$\tau_2 : \mathbb{C}^4 \times \mathbb{C}^4 \to \mathbb{C}^4 \times \mathbb{C}^4 : (x_1, x_2, x_3, x_4, z_1, z_2, z_3, z_4) \mapsto (z_1, z_2, z_3, z_4, x_1, x_2, x_3, x_4),$$

By Theorem 1, (X, L) is definable over $\mathbb{Q} = \mathbb{Q}(i) \cap \mathbb{R}$. Theorem 2 states that the map

$$R : X \to Z$$
$$R(x_1, x_2, x_3, x_4) = (t_1 = t_{1,1}, \ldots, t_{14} = t_{5,1}), \text{where}$$

$$t_1 = (1+i)x_1,\ t_2 = x_2 + ix_3,\ t_3 = x_3 + ix_2,\ t_4 = (1+i)x_4,$$
$$t_5 = ix_1^2,\ t_6 = x_2 + ix_3,\ t_7 = ix_2x_3,\ t_8 = ix_4^2,$$
$$t_9 = x_1x_2 - x_1x_3,\ t_{10} = x_1x_3 - x_1x_2,\ t_{11} = 0,\ t_{12} = 0,$$
$$t_{13} = x_2x_4 - x_3x_4,\ t_{14} = x_3x_4 - x_2x_4,$$

provides an isomorphism between the real algebraic curves (X, L) and (Z, J_{14}) with Z defined over $\mathbb{Q}$. It is not difficult to check that

$$R^{-1} : Z \to X : (t_1, \ldots, t_{14}) \mapsto (x_1, x_2, x_3, x_4) = \left(\frac{t_1}{1+i}, \frac{t_2 - it_3}{2}, \frac{t_3 - it_2}{2}, \frac{t_4}{1+i} \right).$$

The curve Z is defined by the following equations

$$t_{14} = -t_{13} = t_4(t_3 - t_2)/2,\ t_{12} = t_{11} = 0,\ t_{10} = -t_9 = -t_1(t_2 - t_3)/2,$$
$$t_8 = t_4^2/2,\ t_7 = (t_2^2 + t_3^2)/4,\ t_6 = t_2,\ t_5 = t_1^2/2,$$
$$4 + t_2^2 - t_3^2 = 0,\ t_1^2 + t_2t_3 = 0,\ t_1^2 + t_4^2 - 2 = 0.$$

Remark 4. (1) The above also asserts that X is isomorphic to

$$Y = \left\{ \begin{array}{c} 4 + w_2^2 - w_3^2 = 0 \\ w_1^2 + w_2w_3 = 0 \\ w_1^2 + w_4^2 - 2 = 0 \end{array} \right\} \subset \mathbb{C}^4,$$

the isomorphism given by

$$\widehat{R} : X \to Y : (x_1, x_2, x_3, x_4) \mapsto (t_1, t_2, t_3, t_4) = (w_1, w_2, w_3, w_4).$$

(2) The curve X admits the group $H = \langle A_1, A_2, A_3, A_4 \rangle \cong \mathbb{Z}_2^4$ as subgroup of conformal automorphisms, where

$$A_1(x_1, x_2, x_3, x_4) = (-x_1, x_2, x_3, x_4),\ A_2(x_1, x_2, x_3, x_4) = (-x_1, -x_2, x_3, x_4),$$
$$A_3(x_1, x_2, x_3, x_4) = (x_1, x_2, -x_3, x_4),\ A_4(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, -x_4).$$

In the model Y, these correspond to

$$A_1(w_1, w_2, w_3, w_4) = (-w_1, w_2, w_3, w_4),\ A_2(w_1, w_2, w_3, w_4) = (w_1, iw_3, -iw_2, w_4),$$
$$A_3(w_1, w_2, w_3, w_4) = (w_1, -iw_3, iw_2, w_4),\ A_4(w_1, w_2, w_3, w_4) = (w_1, w_2, w_3, -w_4),$$

which are defined over $\mathbb{Q}(i)$. Observe that the minimal field of definition of the pair (X, H) is $\mathbb{Q}(i)$.

5. MAGMA implementation

A simple pseudo-routine in MAGMA [**4**] to make the computations as in Theorem 2, under the mild assumption that L is polynomial, is the following. Let us assume $\mathcal{Q} = \mathbb{Q}(\alpha) < \overline{\mathbb{Q}}$ and that $q(t) \in \mathbb{Q}[t]$ is the irreducible polynomial associated to α. We have each $z_j = z_j(x_1, \ldots, x_n) \in \mathcal{Q}[x_1, \ldots, x_n]$.

First we state the ambient spaces.

```
> Q:=Rationals( );
> P < t >:=PolynomialRing(Q);
> q := q(t);
> K < r >:=SplittingField(q);
> A < x_1, ..., x_n >:=AffineSpace(K,n);
> B < t_{1,1}, ..., t_{n+1,1} >:=AffineSpace(K, (n^2 + 3n)/2);
```

We introduce the algebraic variety $X \subset \mathbb{C}^n$

```
> X:=Scheme(A,[P_1(x_1, ..., x_n), ..., P_s(x_1, ..., x_n)]);
```

We introduce the rational map $R : X \to Z$

```
> R:=map< A- > B|[x_1 + z_1, ..., x_{n-1} * x_n + z_{n-1} * z_n] >;
```

We now ask for equations of the image $Z = R(X)$.

```
> Image(R);
> R(X);
```

Remark 5.

(1) Note that in the above one should replace the "..." by the corresponding data; for instance, if $n = 3$, then the line
"$A < x_1, \ldots, x_n >$:=AffineSpace(K,n);"
should be replaced by the line
"$A < x_1, x_2, x_3 >$:=AffineSpace(K,3);".

(2) Usually MAGMA will provide the defining polynomials over $\mathcal{Q} \cap \mathbb{R}$, but in case that some of these polynomials, say $M \in \mathcal{Q}[t_{1,1}, \ldots, t_{n+1,1}]$, is not defined over the desired field, then we may replace it by the two new trace polynomials $\mathrm{Tr}(M) = M + \overline{M}, \mathrm{Tr}(aM) = aM + \overline{a}\overline{M} \in \mathcal{Q} \cap \mathbb{R}[t_{1,1}, \ldots, t_{n+1,1}]$, where $\{1, a\}$ is a basis of $\mathcal{Q}$ as a $\mathcal{Q} \cap \mathbb{R}$-vector space and $\overline{M}$ is obtained from M after conjugating its coefficients. Since $M = \lambda_1 \mathrm{Tr}(M) + \lambda_2 \mathrm{Tr}(aM)$, where $\lambda_1 = \overline{a}/(\overline{a} - a)$ and $\lambda_2 = 1/(a - \overline{a})$, the new set of polynomials, all of them defined over $\mathcal{Q} \cap \mathbb{R}$, will generate the ideal of Z.

(3) In the example provided in Section 4, the MAGMA pseudo-routine described above with $q = t^2 + 1$ provides the following equations for Z (all of them already over $\mathbb{Q}$):

$$\left\{\begin{array}{c} t_{13} + t_{14} = 0,\ t_{12} = 0,\ t_{11} = 0,\ t_9 + t_{10} = 0, \\ t_1 + \frac{1}{4}t_3t_{10}^3 - \frac{3}{2}t_3t_{10} + \frac{1}{8}t_4t_{10}^3t_{14} + \frac{1}{8}t_4t_{10}t_{14}^3 + \frac{3}{4}t_4t_{10}t_{14} = 0, \\ t_7 - t_8 - \frac{1}{2}t_{10}^2 - \frac{1}{2}t_{14}^2 + 1 = 0, \\ t_8t_{14}^2 - t_8 + \frac{1}{4}t_{10}^2t_{14}^2 + \frac{1}{4}t_{14}^4 - t_{14}^2 = 0, \\ t_8t_{10}^2 + t_8 - \frac{1}{4}t_{10}^2t_{14}^2 - \frac{1}{4}t_{14}^4 = 0, \\ t_{10}^4 + 2t_{10}^2t_{14}^2 - 4t_{10}^2 + t_{14}^4 - 4 = 0, \\ t_6 - t_8 - \frac{1}{2}t_{10}^2 - \frac{1}{2}t_{14}^2 + 1 = 0, \\ t_5 + t_8 - 1 = 0,\ t_4^2 - 2t_8 = 0, \\ t_3t_{14} - \frac{1}{2}t_4t_{10}^2 - \frac{1}{2}t_4t_{14}^2 - t_4 = 0, \\ t_3t_8 - t_4t_8t_{14} - \frac{1}{4}t_4t_{10}^2t_{14} - \frac{1}{4}t_4t_{14}^3 + \frac{1}{2}t_4t_{14} = 0, \\ t_2 + \frac{1}{2}t_3t_{10}^2 - 2t_3 + \frac{1}{4}t_4t_{10}^2t_{14} + \frac{1}{4}t_4t_{14}^3 + \frac{3}{2}t_4t_{14} = 0, \\ t_3t_4 - 2t_8t_{14} - \frac{1}{2}t_{10}^2t_{14} - \frac{1}{2}t_{14}^3 + t_{14} = 0, \\ t_3^2 - 2t_8 - t_{10}^2 - t_{14}^2 = 0. \end{array}\right\}.$$

Acknowledgments

We are grateful to the referees for their several useful comments, corrections and their careful reading.

References

[1] A. Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, Cambridge, 1984. MR781734

[2] E. Bujalance, F. J. Cirre, J. M. Gamboa, and G. Gromadzki, *Symmetries of compact Riemann surfaces*, Lecture Notes in Mathematics, vol. 2007, Springer-Verlag, Berlin, 2010. MR2683160

[3] E. Bujalance, G. Gromadzki, and M. Izquierdo, *On real forms of a complex algebraic curve*, J. Aust. Math. Soc. **70** (2001), no. 1, 134–142, DOI 10.1017/S1446788700002329. MR1808396

[4] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[5] A. Carocca, V. González-Aguilera, R. A. Hidalgo, and R. E. Rodríguez, *Generalized Humbert curves*, Israel J. Math. **164** (2008), 165–192, DOI 10.1007/s11856-008-0025-2. MR2391145

[6] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, 3rd ed., Undergraduate Texts in Mathematics, Springer, New York, 2007. An introduction to computational algebraic geometry and commutative algebra. MR2290010

[7] D. Hilbert, *Ueber die Theorie der algebraischen Formen* (German), Math. Ann. **36** (1890), no. 4, 473–534, DOI 10.1007/BF01208503. MR1510634

[8] G. Humbert. Sur un complexe remarquable de coniques. *Jour. Ecole Polyth.* **64** (1894), 123–149.

[9] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original. MR600654

[10] B. Köck and E. Lau, *A note on Belyi's theorem for Klein surfaces*, Q. J. Math. **61** (2010), no. 1, 103–107, DOI 10.1093/qmath/han034. MR2592026

[11] B. Köck and D. Singerman, *Real Belyi theory*, Q. J. Math. **58** (2007), no. 4, 463–478, DOI 10.1093/qmath/ham017. MR2371466

[12] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, 3rd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)], vol. 34, Springer-Verlag, Berlin, 1994. MR1304906

[13] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen* (German), Math. Ann. **77** (1915), no. 1, 89–92, DOI 10.1007/BF01456821. MR1511848

[14] E. Noether. Der Endlichkeitssatz der Invarianten endlicher linear Gruppen der Characteristik p. *Nachr. Akad. Wiss. Göttingen* (1926), 28–35.

[15] C. Procesi. *Lie Groups: An approach through invariants and representations*. (Universitex) Springer-Verlag, 2006.
[16] B. J. Schmid. Finite groups and invariant theory. Séminaire d'Algèbre (P. Dubriel et M.-P. Malliavin, 1989–1990). *Lecture Notes in Math.*, vol. **1478**, Springer-Verlag, Heidelberg, Berlin, 1991.
[17] R. Silhol. Moduli problems in real algebraic geometry. *Real Algebraic Geometry* (1972), 110–119. Ed. M. Coste et al. (Springer-Verlag, Berlin).
[18] A. W. Tucker, *Branched and folded coverings*, Bull. Amer. Math. Soc. **42** (1936), no. 12, 859–862, DOI 10.1090/S0002-9904-1936-06446-3. MR1563453
[19] A. Weil, *The field of definition of a variety*, Amer. J. Math. **78** (1956), 509–524, DOI 10.2307/2372670. MR0082726

Departamento de Matemática y Estadística, Universidad de La Frontera. Temuco, Chile
Email address: ruben.hidalgo@ufrontera.cl