Group actions on curves over arbitrary fields

by

Mario Garcia Armas

Lic., Universidad de La Habana, 2008
M.Sc., Universidad de La Habana, 2010

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in

The Faculty of Graduate and Postdoctoral Studies

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

March 2015

© Mario Garcia Armas 2015

Abstract

This thesis consists of three parts. The common theme is finite group actions on algebraic curves defined over an arbitrary field k.

In Part I we classify finite group actions on irreducible conic curves defined over k. Equivalently, we classify finite (constant) subgroups of $\mathrm{SO}(q)$ up to conjugacy, where q is a nondegenerate quadratic form of rank 3 defined over k. In the case where k is the field of complex numbers, these groups were classified by F. Klein at the end of the 19th century. In recent papers of A. Beauville and X. Faber, this classification is extended to the case where k is arbitrary, but q is split. We further extend their results by classifying finite subgroups of $\mathrm{SO}(q)$ for any base field k of characteristic $\neq 2$ and any nondegenerate ternary quadratic form q.

In Part II we address the Hyperelliptic Lifting Problem (or HLP): Given a faithful G-action on $\mathbb{P}^1$ defined over k and an exact sequence $1 \to \mu_2 \to G' \to G \to 1$, determine the conditions for the existence of a hyperelliptic curve C/k endowed with a faithful G'-action that lifts the prescribed G-action on the projective line. Alternatively, this problem may be regarded as the Galois embedding problem given by the surjection $G' \twoheadrightarrow G$ and the G-Galois extension $k(\mathbb{P}^1)/k(\mathbb{P}^1)^G$. In this thesis, we find a complete solution to the HLP in characteristic 0 for every faithful group action on $\mathbb{P}^1$ and every exact sequence as above.

In Part III we determine whether, given a finite group G and a base field k of characteristic 0, there exists a strongly incompressible G-curve defined over k. Recall that a G-curve is an algebraic curve endowed with the action of a finite group G. A faithful G-curve C is called strongly incompressible if every dominant G-equivariant rational map of C onto a faithful G-variety is birational. We prove that strongly incompressible G-curves exist if G cannot act faithfully on the projective line over k. On the other hand, if G does embed into PGL_2 over k, we show that the existence of strongly incompressible G-curves depends on finer arithmetic properties of k.

Preface

The material in this thesis is the result of my own work under the supervision of Zinovy Reichstein, and it has been published or submitted for publication.

- Most of Chapter 3 appears in:

  Mario Garcia-Armas. Finite group actions on curves of genus zero. *J. Algebra*, 394:173–181, 2013.

- The material in Chapter 4 appears in:

  Mario Garcia-Armas. Finite group actions on hyperelliptic curves. Submitted for publication.

- The results in Chapter 5 appears in:

  Mario Garcia-Armas. Strongly incompressible curves. Accepted in *Canad. J. Math.*

Table of Contents

Acknowledgements

I would like to thank my advisor Zinovy Reichstein for introducing me to many fascinating mathematical problems and ideas. I really appreciate his extraordinary guidance and support during my time at UBC.

I also want to thank my professors in the math department, especially Julia Gordon, Kalle Karu and Lior Silberman, for everything I learnt from them. Last but not least, thanks to Shane Cernele, Alex Duncan, Jerome Lefebvre and Athena Nguyen for useful mathematical conversations.

Chapter 1

Introduction

1.1 Finite subgroups of $\mathrm{PGL}_1(A)$

The finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ have been known for over a century: these are cyclic, dihedral and the polyhedral groups A_4, S_4 and A_5 (see, e.g., [15]). Any two isomorphic finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ are conjugate. A finite group is said to be p-regular (resp. p-irregular) if its order is prime to (resp. divides) $\mathrm{char}(k)$, where k is a base field. If k is algebraically closed, the classification of finite p-regular subgroups of $\mathrm{PGL}_2(k)$ and their conjugacy classes is identical to the complex case (see [28, §2.5]). Using this result as a starting point, A. Beauville [2] classified, up to conjugacy, the finite p-regular subgroups of $\mathrm{PGL}_2(k)$ over an arbitrary field k. X. Faber [11] completed this picture by classifying the p-irregular subgroups of $\mathrm{PGL}_2(k)$, and describing their conjugacy classes.

We describe the finite (constant) subgroups of (possibly non-split) adjoint absolutely simple algebraic groups of type A_1 over a field k, as well as their conjugacy classes. To do so, we restrict our attention to arbitrary fields k of characteristic different from 2.

It is well known that an adjoint absolutely simple algebraic group of type A_1 over k is of the form $\mathrm{PGL}_1(A)$ for some quaternion algebra $A = (a, b)_2$, where $a, b \in k^\times$ (see, e.g., [16, §26.A and 26.B]). Alternatively, we may regard $\mathrm{PGL}_1(A)$ as the automorphism group of the conic associated to the quadratic form $q = \langle -a, -b, ab \rangle$, which implies the existence of an isomorphism $\mathrm{PGL}_1(A) \cong \mathrm{SO}(q)$ (see, e.g., [8, Cor. 69.6]). Any smooth projective curve of genus 0 is isomorphic to one such conic, so we completely classify faithful actions of finite groups on curves of genus 0, up to equivalence.

We will thus be interested in finite constant subgroups of $\mathrm{SO}(q)$ for any ternary nondegenerate quadratic form q. Replacing q by a scalar multiple of itself does not alter its isometry group, so we may assume throughout that q has discriminant 1.

We first deal with the p-irregular subgroups of $\mathrm{SO}(q)$. Interestingly, we show that this case reduces entirely to the classification in [11].

Theorem 1.1. *Let k be a field of characteristic $p > 2$ and suppose that $\mathrm{SO}(q)$ contains a p-irregular subgroup. Then q is isotropic, i.e., there exists an isomorphism $\mathrm{SO}(q) \cong \mathrm{PGL}_2$.*

It remains to classify the p-regular subgroups G of $\mathrm{SO}(q)$, so we may assume henceforth that $\mathrm{char}(k)$ is prime to $|G|$. Over an algebraic closure $\overline{k}$ of k, we have that $\mathrm{SO}(q)(\overline{k}) \cong \mathrm{PGL}_2(\overline{k})$. Thus any finite subgroup G of $\mathrm{SO}(q)$ embeds into $\mathrm{PGL}_2(\overline{k})$, so it must be isomorphic to $\mathbb{Z}/n\mathbb{Z}$, D_{2n} (the dihedral group of $2n$ elements), A_4, S_4 or A_5. Theorem 1.2 below classifies these subgroups up to isomorphism and Theorem 1.3 up to conjugacy. Taking $q \simeq \langle -1, -1, 1\rangle$ in these theorems, we recover the results in [2].

We will prove Theorem 1.2 in Section 3.1. Note that the classification of polyhedral groups in parts (b) and (c) is hinted at in [29]; here we make it explicit for completeness. In the next two theorems, we let ω_n denote a primitive n-th root of 1.

Theorem 1.2. *Let q be a nondegenerate quadratic form of discriminant 1.*

(a) *The group $D_4 \cong (\mathbb{Z}/2\mathbb{Z})^2$ is always contained in $\mathrm{SO}(q)$. For $n \geq 3$, the following are equivalent:*

  (i) *The group $\mathrm{SO}(q)$ contains $\mathbb{Z}/n\mathbb{Z}$.*

  (ii) *The group $\mathrm{SO}(q)$ contains D_{2n}.*

  (iii) *$\omega_n + \omega_n^{-1} \in k$, and q represents $4 - (\omega_n + \omega_n^{-1})^2$.*

(b) *The group $\mathrm{SO}(q)$ contains A_4 if and only if it contains S_4, which happens if and only if $q \simeq \langle 1, 1, 1\rangle$.*

(c) *The group $\mathrm{SO}(q)$ contains A_5 if and only if $\sqrt{5} \in k$ and $q \simeq \langle 1, 1, 1\rangle$.*

We will prove Theorem 1.3 in Section 3.2. Our argument relies on Galois cohomology techniques, building on the approach taken in [Beau10].

Theorem 1.3. *Let $q = \langle -a, -b, ab\rangle$ be a nondegenerate quadratic form.*

(a) *The conjugacy classes of $\mathbb{Z}/2\mathbb{Z}$ inside $\mathrm{SO}(q)$ are in natural bijective correspondence with the set $D(q) \subset k^\times/k^{\times 2}$ consisting of nonzero square classes represented by q.*

(b) *Let $Q_{a,b} = \{(\overline{x}, \overline{y}) \in (k^\times/k^{\times 2})^2 \,|\, (ax, by)_2 \cong (a, b)_2\}$. The symmetric group $S_3 = \{s, t | s^3 = t^2 = (st)^2 = 1\}$ acts on $Q_{a,b}$ by setting $s \cdot (\overline{x}, \overline{y}) = (\overline{-bxy}, \overline{abx})$ and $t \cdot (\overline{x}, \overline{y}) = (\overline{x}, \overline{-axy})$ for all $(\overline{x}, \overline{y}) \in Q_{a,b}$. Then the conjugacy classes of $(\mathbb{Z}/2\mathbb{Z})^2$ inside $\mathrm{SO}(q)$ are in natural bijective correspondence with $Q_{a,b}/S_3$.*

(c) *There is at most one conjugacy class of subgroups isomorphic to* $\mathbb{Z}/n\mathbb{Z}$ *(*$n \geq 3$*) inside* $\mathrm{SO}(q)$.

(d) *Suppose that* D_{2n} *is contained in* $\mathrm{SO}(q)$ *(*$n \geq 3$*). We write* $\beta_n = (\omega_n + \omega_n^{-1})^2 - 4$ *and let* $D(\langle 1, -\beta_n \rangle)$ *consist of the nonzero square classes represented by* $\langle 1, -\beta_n \rangle$*, which forms a subgroup of* $k^\times/k^{\times 2}$*. The square class* $\overline{\omega_n + \omega_n^{-1} + 2}$ *is contained in* $D(\langle 1, -\beta_n \rangle)$*; let* C *be the* 2*-element subgroup generated by this class. Then the conjugacy classes of* D_{2n} *inside* $\mathrm{SO}(q)$ *are in natural bijective correspondence with* $D(\langle 1, -\beta_n \rangle)/C$.

(e) *There is at most one conjugacy class of subgroups isomorphic to* A_4*,* S_4 *or* A_5 *inside* $\mathrm{SO}(q)$.

1.2 Finite group actions on hyperelliptic curves

Let k be an arbitrary base field. A *hyperelliptic curve* C/k is a smooth projective geometrically irreducible curve of genus at least 2 endowed with a finite k-morphism $C \to \mathbb{P}^1$ of degree 2. Equivalently, the function field $k(C)$ is a regular quadratic field extension of the rational function field $k(x)$ of genus at least 2.

Problem 1.4 (Hyperelliptic Lifting Problem or HLP)**.** Let G be a finite group and consider a faithful G-action on $\mathbb{P}^1$ via some embedding $G \hookrightarrow \mathrm{PGL}_2$ defined over k. Suppose that we have a central exact sequence

$$1 \to \mu_2 \to G' \to G \to 1.$$

Determine the conditions for the existence of a hyperelliptic curve C/k endowed with a faithful G'-action defined over k such that $C/\mu_2 \cong \mathbb{P}^1$ as G-varieties.

Over the complex numbers, finite group actions on hyperelliptic curves have been studied extensively (see, e.g., [5, 33]). In that case, Problem 1.4 is always solvable. Indeed, if G is a finite subgroup of PGL_2, the corresponding G-action on $\mathbb{P}^1$ over $\mathbb{C}$ is unique up to G-equivariant isomorphism and the results in [5] imply that any double cover of G acts on some hyperelliptic curve in the desired way. Over a non-algebraically closed field, several complications may arise in the study of Problem 1.4. First, the embeddings of a finite group G into PGL_2 are not necessarily conjugate, giving rise to non-equivalent actions on $\mathbb{P}^1$ (cf. Theorem 1.3). On the other hand, there are usually arithmetic constraints on the base field for the existence of a hyperelliptic curve with the required group action.

In Chapter 4, we find a complete solution to the HLP in characteristic 0. More explicitly, for every faithful action on $\mathbb{P}^1$ by a finite group G defined over a field k of characteristic 0 and every exact sequence $1 \to \mu_2 \to G' \to G \to 1$, we determine necessary and sufficient conditions on k for the solvability of the HLP in Sections 4.2 to 4.4, and we describe the corresponding families of solutions in Section 4.5.

1.3 Strongly incompressible curves

Let G be an algebraic group. A *G-compression* of a generically free G-variety X is a dominant G-equivariant rational map $X \dashrightarrow Y$, where Y is also generically free. We say that X is *strongly incompressible* if every G-compression of X is birational. This concept was introduced by Z. Reichstein in [24, §2], where the author asks for a classification of strongly incompressible G-varieties (see also [25, §7.1]).

A related problem arises when we only consider self rational maps. More precisely, given a generically free G-variety X, is every dominant G-equivariant rational map $X \dashrightarrow X$ a birational isomorphism? Even when G is trivial, this appears to be an interesting problem in many contexts. In [6], X. Chen proves that every dominant self rational map of a very general projective $K3$ surface of genus $g \geq 2$ is birational (see [7] for generalizations).

If a finite group G does not act faithfully on any curve of genus ≤ 1, then there exist strongly incompressible complex G-curves (see [24, Example 6]). N. Fakhruddin and R. Pardini have independently found examples of strongly incompressible complex G-surfaces for certain finite groups G. To our best knowledge, no examples of strongly incompressible varieties are known in higher dimensions.

If the base field k has characteristic $p > 0$, there exist no strongly incompressible G-varieties for any finite group G. We sketch a proof of this fact. Let X be a faithful G-variety and let $F_{X/\mathrm{Spec}(k)} \colon X \to X^{(p)}$ be the relative Frobenius morphism associated to X (see [21, §3.2.4] for details). By functoriality, we may endow $X^{(p)}$ with an action of the group $G^{(p)}$, which is canonically isomorphic to G (recall that G is a finite constant group). This action makes $F_{X/\mathrm{Spec}(k)}$ into a dominant G-equivariant morphism, which has degree $p^{\dim(X)}$ by [21, Cor. 2.27]. To complete the proof, we must show that the G-action on $X^{(p)}$ is faithful. If N is the kernel of such action, we must have $k(X^{(p)}) \subset k(X)^N \subset k(X)$, where the inclusion $k(X^{(p)}) \subset k(X)$ is a purely inseparable extension induced by $F_{X/\mathrm{Spec}(k)}$. Thus $k(X)/k(X)^N$ is both Galois and purely inseparable, which implies that N is trivial.

In Chapter 5, we study the question of existence of strongly incompressible G-curves for every finite group G. We may assume that the base field k has characteristic 0. We settle the classification problem for G-curves raised in [24], by considering finite groups G that can act on a curve of genus ≤ 1. In Section 5.2, we show that strongly incompressible G-curves do exist if G does not act faithfully on any curve of genus 0.

Theorem 1.5 (see Theorem 5.4)**.** *Suppose that G cannot act faithfully on a curve of genus 0 via k-morphisms. Then there exists a strongly incompressible G-curve defined over k.*

For finite groups G that can act faithfully on a curve of genus 0 over k (recall that these are always cyclic, dihedral, or polyhedral groups), the situation is more delicate. In particular, it is important to decide whether a faithful G-curve X can be G-compressed to $\mathbb{P}^1$, provided that there exists a faithful G-action on the projective line. To this end, we make a small detour in Section 5.3 and, given a projective representation $G \to \mathrm{PGL}(V)$, we construct a cohomological invariant associated to any faithful G-variety X, which allows us to determine whether X can be mapped G-equivariantly to $\mathbb{P}(V)$. In Section 5.4, we compute the invariant for certain group actions on the projective line.

We study the existence of strongly incompressible curves for groups that can act faithfully on a curve of genus 0 in Sections 5.5 to 5.8. Our results are summarized in the following theorem. For a definition of cohomological 2-dimension of a field k, denoted by $\mathrm{cd}_2(k)$, we refer the reader to [31, I.§3]. We remark that k has cohomological 2-dimension 0 if and only if every algebraic extension of k is quadratically closed (see [9, Lemma 2]).

Theorem 1.6. *Let ω_n be a primitive n-th root of 1 ($n \geq 2$).*

(a) *(Thm. 5.4, Prop. 5.14) Let G be either $\mathbb{Z}/n\mathbb{Z}$ or D_{2n}, where n is odd. Then there exist strongly incompressible G-curves if and only if $\omega_n + \omega_n^{-1} \notin k$.*

(b) *(Thm. 5.4, Prop. 5.13 and 5.16) Suppose that n is even. Then there exist strongly incompressible $\mathbb{Z}/n\mathbb{Z}$-curves if and only if $\omega_n \notin k$.*

(c) *(Prop. 5.17) There exist strongly incompressible $(\mathbb{Z}/2\mathbb{Z})^2$-curves if and only if $\mathrm{cd}_2(k) > 0$.*

(d) *(Thm. 5.4, Prop. 5.23) Suppose that $n \geq 4$ is even. Then there exist strongly incompressible D_{2n}-curves if and only if either $\omega_n + \omega_n^{-1} \notin k$, or $\mathrm{cd}_2(k) > 0$.*

(e) *(Prop. 5.29) Let G be a polyhedral group, i.e., $G = A_4$, S_4, or A_5. Then there exist strongly incompressible G-curves if and only if* $\mathrm{cd}_2(k) > 0$.

In particular, we note the following corollary of the above results, which answers the strong incompressibility problem for curves over an algebraically closed field, as posed in [24].

Corollary 1.7. *Let G be a finite group and let the base field k be algebraically closed. Then there exists a strongly incompressible G-curve if and only if G does not act faithfully on $\mathbb{P}^1$, i.e., G is not cyclic, dihedral, A_4, S_4 or A_5.*

Chapter 2

Notation and preliminaries

In this thesis, we let k denote a base field and we write k_s (resp. $\overline{k}$) for its separable (resp. algebraic) closure. A *k-variety* X is a geometrically reduced scheme of finite type over k (not necessarily irreducible). A *point* of a variety means a geometric point, unless stated otherwise. The word "curve" is reserved for a geometrically irreducible smooth projective 1-dimensional variety. A curve C/k is said to be *hyperelliptic* if its genus is at least 2 and there exists a finite k-morphism $C \to \mathbb{P}^1$ of degree 2.

2.1 Quaternion algebras

Given a central simple algebra A, we will denote its Brauer class by $[A]$. As usual, the symbol $(a, b)_2$ denotes the quaternion algebra with basis $1, i, j, ij$, subject to the relations $i^2 = a, j^2 = b$ and $ij + ji = 0$. The following simple observation will be used repeatedly in the sequel.

Lemma 2.1. *Let $k(x)$ be a rational function field over k, and suppose that the quaternion algebra $(f(x), g(x))_2$ is split over $k(x)$, where $f, g \in k[x]$ are separable. Then $f(\alpha)$ is a square in $k(\alpha)$ for any root $\alpha \in \overline{k}$ of g.*

Proof. Since the quaternion algebra $(f(x), g(x))_2$ is split, there exist coprime polynomials $p, q, r \in k[x]$ such that the polynomial identity

$$f(x)p(x)^2 + g(x)q(x)^2 = r(x)^2$$

holds. Substituting α in the above identity implies that $f(\alpha)p(\alpha)^2 = r(\alpha)^2$. Note that $p(\alpha) = 0$ implies $r(\alpha) = 0$. Conversely, suppose that $r(\alpha) = 0$. Then α is a root of $f(x)p(x)^2$ of multiplicity at least 2, which implies that $p(\alpha) = 0$ since f is separable. It follows that $r(\alpha) = 0$ if and only if $p(\alpha) = 0$.

Assume for the sake of contradiction that $p(\alpha) = r(\alpha) = 0$. Then it follows that α is a root of $g(x)q(x)^2$ of multiplicity at least 2. Since g is separable, we obtain that $q(\alpha) = 0$. Hence α is a common root of p, q, r, which is impossible since they are relatively prime. This contradiction shows that $p(\alpha)r(\alpha) \neq 0$ and therefore $f(\alpha) = r(\alpha)^2 p(\alpha)^{-2} \in k(\alpha)^{\times 2}$. □

2.2 Roots of unity

For each positive integer n, let ω_n denote a primitive n-th root of unity. We may select the system $\{\omega_n\}$ satisfying the following compatibility condition: if m/n is a power of 2, then $\omega_n = \omega_m^{m/n}$. For convenience, we also set $\alpha_n = (\omega_n + \omega_n^{-1})/2$ and $\beta_n = \alpha_n^2 - 1$.

The following lemma provides some useful computations.

Lemma 2.2. *Suppose that k contains α_n.*

(a) *We must have $\omega_n^r + \omega_n^{-r} \in k$ for every natural number r. In particular, the condition $k \ni \alpha_n$ is independent of the choice of ω_n.*

(b) *If n is odd, then $\alpha_{2n} \in k$.*

(c) *If n is even, then $(1+\omega_n^{-1})^n = (1+\omega_n)^n = -(2\alpha_n+2)^{n/2} = -(2\alpha_{2n})^n$.*

(d) *Suppose that $n \equiv 0$ (4) and $-1 \in k^{\times 2}$. Then it follows that $\omega_n \in k$.*

Proof. (a) This follows from the well known fact that $(x^r + x^{-r})/2$ is a polynomial in $(x + x^{-1})/2$ with integer coefficients.

(b) Note that $\zeta_{2n} = \omega_{2n}^{n+2} = -\omega_n$ is a *primitive* $2n$-th root of unity, which satisfies $(\zeta_{2n} + \zeta_{2n}^{-1})/2 = -\alpha_n \in k$. By part (a), we conclude that $\alpha_{2n} \in k$.

(c) The first and last equalities are straightforward. To prove the middle equality, note that

$$(1+\omega_n)^n = (1 + 2\omega_n + \omega_n^2)^{n/2} = \omega_n^{n/2}(2\alpha_n+2)^{n/2} = -(2\alpha_n+2)^{n/2}.$$

(d) Note that $\omega_4\omega_n$ is an n-th root of unity, so $\omega_4\omega_n = \omega_n^r$ for some natural number r. Thus, $\omega_n = 2\alpha_n + (\omega_n - \omega_n^{-1}) = 2\alpha_n + \omega_4^{-1}(\omega_n^r + \omega_n^{-r}) \in k$. □

Chapter 3

Finite group actions on curves of genus zero

3.1 Existence of finite subgroups

Let k denote a base field of characteristic different from 2.

Lemma 3.1. *Let q be a nondegenerate ternary quadratic form over k and let M be an element of $\mathrm{SO}(q)(k)$. Then the following results hold.*

(a) *Suppose that M is diagonalizable over $\overline{k}$. Then its eigenvalues are 1, λ, and λ^{-1} for some $\lambda \in \overline{k}^{\times}$. If $\lambda \neq \pm 1$, then q becomes isotropic over $k(\lambda)$, which is an extension of k of order dividing 2.*

(b) *Suppose that M is a nontrivial unipotent matrix. Then q must be isotropic.*

Proof. Let Q be the matrix associated to q. Note that $M^{-1} = Q^{-1}\,{}^{T}M\,Q$, whence the characteristic polynomial P of M satisfies $P(x) = -x^3 P(1/x)$. It follows easily that the eigenvalues of M must be $1, \lambda, \lambda^{-1}$ for some $\lambda \in \overline{k}$.

Suppose first that M is diagonalizable. Taking the trace of M, we obtain that $\lambda + \lambda^{-1} \in k$, whence $[k(\lambda) : k]$ is 1 or 2. We show that q becomes isotropic over $k(\lambda)$, provided that $\lambda \neq \pm 1$. Indeed, over this field we can select an eigenvector v of M associated to the eigenvalue λ. Then, we compute $q(v) = q(Mv) = \lambda^2 q(v)$, whence $q(v) = 0$. This completes the proof of part (a).

Suppose now that M is a nontrivial unipotent matrix. Then we can find nonzero vectors v_1, v_2 such that $Mv_1 = v_1$ and $Mv_2 = v_1 + v_2$ (this follows easily after conjugating M into Jordan canonical form). Let b_q be the symmetric bilinear form associated to q. Note that $b_q(v_1, v_2) = b_q(Mv_1, Mv_2) = q(v_1) + b_q(v_1, v_2)$, whence $q(v_1) = 0$. This finishes the proof. □

Proof of Theorem 1.1. Let G be a p-irregular subgroup inside $\mathrm{SO}(q)$ and let $M \in G$ be any element of order p. Note that $0 = M^p - I = (M-I)^p$, whence

M is a unipotent matrix. By Lemma 3.1(b), it follows that q is isotropic, so we obtain that $\mathrm{SO}(q) \cong \mathrm{PGL}_2$. □

Proof of Theorem 1.2. (a) The first statement is trivial: the diagonal subgroup $D_0 \subset \mathrm{SO}(q)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. Assume henceforth that $n \geq 3$. It suffices to prove that $\mathbb{Z}/n\mathbb{Z} \subset \mathrm{SO}(q) \Rightarrow \alpha_n \in k$ and q represents $-\beta_n \Rightarrow D_{2n} \subset \mathrm{SO}(q)$.

To prove the first implication, let M be an element of order n in $\mathrm{SO}(q)(k)$. By Lemma 3.1(a), we may assume that the eigenvalues of M are 1, ω_n and ω_n^{-1}, after replacing M by a power of itself if necessary. Using Lemma 3.1(a) again, we see that $\alpha_n \in k$ and q becomes isotropic over $k(\omega_n) = k(\sqrt{\beta_n})$. It suffices to prove that q is isotropic over $k(\sqrt{\beta_n})$ if and only if q represents $-\beta_n$. If q is isotropic over k, then q is universal, so there is nothing to prove. Suppose that q is anisotropic over k. It follows from [8, Prop. 34.8] that $q \simeq q_0 \otimes \mathrm{N}_{k(\sqrt{\beta_n})/k} \perp q_1$ for some nondegenerate quadratic forms q_0, q_1, where q_1 is anisotropic over $k(\sqrt{\beta_n})$. If q is isotropic over $k(\sqrt{\beta_n})$, we conclude that $q \neq q_1$ and thus $\dim(q_0) = \dim(q_1) = 1$ (since $\mathrm{N}_{k(\sqrt{\beta_n})/k} \simeq \langle 1, -\beta_n \rangle$). It follows that $q_1 \cong \langle -\beta_n \rangle$ by taking discriminants, whence q represents $-\beta_n$. Conversely, suppose that the latter holds. Then $q \simeq \langle -\beta_n, -\gamma, \beta_n\gamma \rangle$ for some $\gamma \in k^\times$, so it follows that q is isotropic over $k(\sqrt{\beta_n})$.

Suppose next that $\alpha_n \in k$ and q represents $-\beta_n$. We may thus assume that $q = \langle -\beta_n, -\gamma, \beta_n\gamma \rangle$ for some $\gamma \in k^\times$. The matrices

$$s = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha_n & \beta_n \\ 0 & 1 & \alpha_n \end{pmatrix}, \; t = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

are contained in $\mathrm{SO}(q)(k)$ and satisfy $s^n = t^2 = (st)^2 = 1$, whence they generate a subgroup isomorphic to D_{2n}. The proof of this part is complete.

(b) Let $q_0 = \langle 1, 1, 1 \rangle$. It clearly suffices to prove that $A_4 \subset \mathrm{SO}(q) \Rightarrow q \simeq q_0 \Rightarrow S_4 \subset \mathrm{SO}(q)$. We first prove the rightmost implication. Note that S_4 acts linearly on k^3 by rotations on the cube with vertices $(\pm 1, \pm 1, \pm 1)$ and the corresponding linear representation has determinant 1. The form q_0 is invariant under this action and therefore S_4 embeds into $\mathrm{SO}(q_0)$. If $q \simeq q_0$, then $\mathrm{SO}(q) \cong \mathrm{SO}(q_0)$ and the result follows.

We now prove that $A_4 \subset \mathrm{SO}(q) \Rightarrow q \simeq q_0$. Recall that A_4 acts linearly on k^3 by rotations on the tetrahedron with vertices $(\epsilon_1, \epsilon_2, \epsilon_1\epsilon_2)$, where $\epsilon_i = \pm 1$. This representation is absolutely irreducible and leaves q_0 invariant, i.e., we have a linear representation $\rho\colon A_4 \hookrightarrow \mathrm{SO}(q_0)$ defined over k. We claim that any absolutely irreducible representation of a finite group admits at most one nontrivial invariant quadratic form, up to a scalar. Modulo this claim, it

is easy to finish the proof. Indeed, it follows that $q \simeq c \cdot q_0$ for some $c \in k^\times$; taking discriminants, we conclude that $c = 1$.

It remains to give a proof of the claim. Let G be a finite group, let V be an absolutely irreducible G-module, and let q_1, q_2 be a nontrivial G-invariant quadratic form. Since $\mathrm{Ker}(q_i)$ $(i = 1, 2)$ is G-invariant, it must be trivial. It follows that q_1, q_2 must be nondegenerate, so we may view them as G-equivariant isomorphisms $V \to V^*$. Hence $(q_2)^{-1} \circ q_1$ is a G-equivariant automorphism of V. Passing to the algebraic closure and using Schur's lemma, we conclude that $(q_2)^{-1} \circ q_1$ must be a scalar.

(c) Note that $A_5 \subset \mathrm{SO}(q) \Rightarrow A_4 \subset \mathrm{SO}(q) \Rightarrow q \simeq q_0$ by part (b). Since A_5 contains elements of order 5, it is necessary that $\omega_5 + \omega_5^{-1} \in k$, which happens if and only if $\sqrt{5} \in k$.

Conversely, if $\sqrt{5} \in k$, the group A_5 acts linearly on k^3 by rotations on the icosahedron with vertices $(\pm\phi, \pm 1, 0), (0, \pm\phi, \pm 1), (\pm 1, 0, \pm\phi)$, where $\phi = (1 + \sqrt{5})/2$, and this action preserves q_0. The result readily follows. □

Example 3.2. Let $k = \mathbb{Q}$. A primitive n-th root of 1 is given by $\omega_n = \exp(2\pi i/n)$. Recall that $\omega_n + \omega_n^{-1} \in \mathbb{Q}$ if and only if $n = 1, 2, 3, 4$ or 6. The group $\mathrm{SO}(q)$ contains $\mathbb{Z}/4\mathbb{Z}$ and D_8 if and only if q represents 1. Moreover, $\mathrm{SO}(q)$ contains $\mathbb{Z}/3\mathbb{Z}$ and D_6 if and only if it contains $\mathbb{Z}/6\mathbb{Z}$ and D_{12} if and only if q represents 3.

3.2 Conjugacy classes of subgroups

The purpose of this section is to prove Theorem 1.3. We recall the following construction for convenience.

Construction 3.3. ([2, §2]) Let G be an algebraic group defined over k and let $H \subset G(k)$ be a subgroup. Fix a separable closure k_s of k and set $\Gamma = \mathrm{Gal}(k_s/k)$. Define the pointed set $\mathrm{Emb}_i(H, G(k))$ as the set of embeddings $H \hookrightarrow G(k)$ which are conjugate by an element of $G(k_s)$ to the natural inclusion $i\colon H \hookrightarrow G(k)$, modulo conjugacy by an element of $G(k)$. Also, define the pointed set $\mathrm{Conj}(H, G(k))$ consisting of subgroups of $G(k)$ which are conjugate to H over $G(k_s)$, modulo conjugacy over $G(k)$.

The centralizer of H in G, denoted by Z, will be a closed subgroup of G defined over k (cf. [4, Ch. 1, §1.7]). The kernel $H^1(k, Z)_0$ of the natural map $H^1(k, Z) \to H^1(k, G)$ is isomorphic to $\mathrm{Emb}_i(H, G(k))$ as pointed sets. The normalizer N of H in $G(k_s)$ acts on 1-cocycles $\Gamma \to Z(k_s)$ in the following way: an element $n \in N$ sends $\sigma \mapsto a_\sigma$ to $\sigma \mapsto n^{-1} a_\sigma \sigma(n)$. This (right)

action descends to $H^1(k,Z)$ and preserves $H^1(k,Z)_0$. Then there is an isomorphism of pointed sets between $H^1(k,Z)_0/N$ and $\mathrm{Conj}(H,G(k))$.

Now recall that any two isomorphic finite subgroups (of order prime to $\mathrm{char}(k)$) of $\mathrm{SO}(q)(k_s) \cong \mathrm{PGL}_2(k_s)$ are conjugate. Therefore, the conjugacy classes of finite subgroups of $\mathrm{SO}(q)$ of the same isomorphism type as some particular subgroup $H \subset \mathrm{SO}(q)$ are in natural bijective correspondence with $\mathrm{Conj}(H, \mathrm{SO}(q)(k))$, independently of the choice of H.

We now state some basic facts about the structure of $\mathrm{SO}(q)$. The proofs are easy and are left to the reader. In the sequel, we write $\mathrm{diag}(a_1,\ldots,a_n)$ for the diagonal matrix with entries $a_1,\ldots,a_n$ along the diagonal.

Lemma 3.4. *Let $q = \langle -a,-b,ab\rangle$ be a nondegenerate quadratic form. If H is a finite subgroup of $\mathrm{SO}(q)$, let Z be the centralizer of H in $\mathrm{SO}(q)$ and let N be the normalizer of H in $\mathrm{SO}(q)(k_s)$.*

(a) *Let $H \cong \mathbb{Z}/2\mathbb{Z}$ be generated by the diagonal matrix $\mathrm{diag}(1,-1,-1)$. Then we have that*

$$Z = \left\{ \begin{pmatrix} (\det M)^{-1} & 0 \\ 0 & M \end{pmatrix} : \ M \in \mathrm{O}(\langle -b,ab\rangle) \right\} \cong \mathrm{O}(\langle -b,ab\rangle)$$

and $N = Z(k_s)$.

(b) *Let $H \cong (\mathbb{Z}/2\mathbb{Z})^2$ be the diagonal subgroup inside $\mathrm{SO}(q)$. Then we have that $Z = H$ and N is isomorphic to S_4. Explicitly, if we set $u = \sqrt{-a}$ and $v = \sqrt{-b}$, the matrices*

$$\begin{pmatrix} 0 & vu^{-1} & 0 \\ 0 & 0 & u \\ v^{-1} & 0 & 0 \end{pmatrix}, \ \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -u \\ 0 & -u^{-1} & 0 \end{pmatrix},$$

generate a subgroup $N' \subset \mathrm{SO}(q)(k_s)$ isomorphic to S_3 and $N = H \rtimes N'$.

(c) *Let $n \geq 3$ and suppose that $H \cong \mathbb{Z}/n\mathbb{Z}$ is contained in $\mathrm{SO}(q)$. Using the same notation from Theorem 1.2, we may assume that $q = \langle -\beta_n, -\gamma, \beta_n\gamma\rangle$ and H is generated by the matrix*

$$s = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha_n & \beta_n \\ 0 & 1 & \alpha_n \end{pmatrix}.$$

Then we have that

$$Z = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & M \end{pmatrix} : \ M \in \mathrm{SO}(\langle -\gamma, \beta_n\gamma\rangle) \right\} \cong \mathrm{SO}(\langle -\gamma, \beta_n\gamma\rangle).$$

(d) *Let $n \geq 3$ and suppose that $H \cong D_{2n}$ is contained in $\mathrm{SO}(q)$. As before, assume that $q = \langle -\beta_n, -\gamma, \beta_n\gamma\rangle$ and H is generated by the matrices*

$$s = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha_n & \beta_n \\ 0 & 1 & \alpha_n \end{pmatrix}, \; t = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Then we have that $Z \cong \mathbb{Z}/2\mathbb{Z}$ is generated by $\mathrm{diag}(1,-1,-1)$ and the matrices

$$s' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha_{2n} & 2\alpha_{2n}\beta_{2n} \\ 0 & (2\alpha_{2n})^{-1} & \alpha_{2n} \end{pmatrix}, \; t = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

generate $N \cong D_{4n}$ inside $\mathrm{SO}(q)(k_s)$.

(e) *Let $H = A_4$, S_4 or A_5 and suppose that H is contained in $\mathrm{SO}(q)$. Then the centralizer Z is trivial.*

□

Remark 3.5. Since any two finite isomorphic subgroups H_1 and H_2 of $\mathrm{SO}(q)$ are conjugate over k_s, their centralizers will also be conjugate over k_s (in particular, they must be isomorphic). However, they are not necessarily isomorphic over k. For a concrete example, take $k = \mathbb{R}$, $q = \langle -1, -1, 1\rangle$, H_1 generated by $\mathrm{diag}(1,-1,-1)$ and H_2 generated by $\mathrm{diag}(-1,-1,1)$. A simple computation shows that $Z(H_1) \cong \mathrm{O}(\langle -1, 1\rangle)$ and $Z(H_2) \cong \mathrm{O}(\langle -1, -1\rangle)$. These groups are not isomorphic; the identity component $Z(H_1)^\circ$ is isomorphic to $\mathbb{G}_m$ while $Z(H_2)^\circ \cong \mathrm{SO}_2$, which is a non-split torus over $\mathbb{R}$.

Remark 3.6. Suppose we are in the situation of Lemma 3.4(c) with $\gamma = 1$. Then, $q = \langle -\beta_n, -1, \beta_n\rangle \simeq \langle -1, -1, 1\rangle$ and $\mathrm{SO}(q) \cong \mathrm{PGL}_2$, so we are dealing with the case studied in [2]. Any two cyclic subgroups of order n inside $\mathrm{SO}(q)$ are conjugate over k (see Theorem 1.3), so the centralizer of such a subgroup is unique up to conjugacy. By Lemma 3.4(c), it must be isomorphic to $\mathrm{SO}(\langle -1, \beta_n\rangle)$, which is a split torus if and only if $\beta_n = \frac{1}{4}(\omega_n - \omega_n^{-1})^2 \in k^{\times 2}$ if and only if $\omega_n \in k$ (since $\omega_n + \omega_n^{-1} \in k$). So in general the centralizer is not isomorphic to the split torus $\mathbb{G}_m$, contrary to an assertion made in the proof of [2, Thm. 4.2] and it might have nontrivial cohomology. However, the final result in [2] is unaffected since the map $H^1(k, Z) \to H^1(k, G)$ still has trivial kernel (see Theorem 1.3).

We now recall some facts about the Galois cohomology of orthogonal groups of quadratic spaces (see [16, §29.E] for details). Let q be any nondegenerate quadratic form of dimension n defined over k. The cohomology set $H^1(k, \mathrm{O}(q))$ classifies isometry classes of n-dimensional nondegenerate quadratic forms over k, while $H^1(k, \mathrm{SO}(q))$ classifies isometry classes of n-dimensional quadratic forms q' over k such that $\mathrm{disc}(q') = \mathrm{disc}(q)$. The natural map $H^1(k, \mathrm{SO}(q)) \to H^1(k, \mathrm{O}(q))$ is injective. Let $D_0 \cong (\mathbb{Z}/2\mathbb{Z})^{n-1}$ and $D \cong (\mathbb{Z}/2\mathbb{Z})^n$ be the subgroups of diagonal matrices inside $\mathrm{SO}(q)$ and $\mathrm{O}(q)$, respectively. We have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & D_0 & \hookrightarrow & D & \xrightarrow{\det} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle j} & & & & \\ & & \mathrm{SO}(q) & \hookrightarrow & \mathrm{O}(q) & & & & \end{array}$$

where the top row is exact. This induces a diagram on cohomology

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H^1(k, D_0) & \longrightarrow & (k^\times/k^{\times 2})^n & \xrightarrow{p} & k^\times/k^{\times 2} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle i_*} & & \downarrow{\scriptstyle j_*} & & & & \\ & & H^1(k, \mathrm{SO}(q)) & \longrightarrow & H^1(k, \mathrm{O}(q)) & & & & \end{array}$$

where $p\colon (\overline{c_1}, \ldots, \overline{c_n}) \mapsto \overline{c_1} \ldots \overline{c_n}$ is the product map. We have thus identified $H^1(k, D_0)$ with the elements $(\overline{c_1}, \ldots, \overline{c_n}) \in (k^\times/k^{\times 2})^n$ such that $\overline{c_1} \ldots \overline{c_n} = \overline{1}$.

In what follows, we will abuse notation and refer to quadratic forms as elements of the cohomology sets $H^1(k, \mathrm{SO}(q))$ and $H^1(k, \mathrm{O}(q))$. The reader should bear in mind that we are tacitly referring to their isometry classes.

Lemma 3.7. *Suppose that $q \simeq \langle b_1, \ldots, b_n \rangle$ is a nondegenerate quadratic form.*

(a) *The map j_* takes $(\overline{c_1}, \ldots, \overline{c_n})$ to $\langle c_1 b_1, \ldots, c_n b_n \rangle$ and consequently, i_* takes $(\overline{c_1}, \ldots, \overline{c_n})$ with $\overline{c_1} \ldots \overline{c_n} = \overline{1}$, to $\langle c_1 b_1, \ldots, c_n b_n \rangle$.*

(b) *Let $q' \simeq \langle d \rangle \perp q$ and define $f\colon \mathrm{SO}(q) \to \mathrm{SO}(q')$ by sending*

$$M \mapsto \begin{pmatrix} 1 & 0 \\ 0 & M \end{pmatrix}.$$

The induced map $f_*\colon H^1(k, \mathrm{SO}(q)) \to H^1(k, \mathrm{SO}(q'))$ sends

$$q'' \mapsto \langle d \rangle \perp q''.$$

(c) *Let* $q' \simeq \langle d \rangle \perp q$ *and define* $f\colon \mathrm{O}(q) \to \mathrm{SO}(q')$ *by sending*

$$M \mapsto \begin{pmatrix} (\det M)^{-1} & 0 \\ 0 & M \end{pmatrix}.$$

The induced map $f_*\colon H^1(k, \mathrm{O}(q)) \to H^1(k, \mathrm{SO}(q'))$ *sends*

$$q'' \mapsto \langle \mathrm{disc}(q'')\mathrm{disc}(q') \rangle \perp q''.$$

Proof. (a) This is well known; see, e.g., the proof of [26, Lemma 4.3].

(b) Let $i_q\colon D_{0,q} \hookrightarrow \mathrm{SO}(q)$ and $i_{q'}\colon D_{0,q'} \hookrightarrow \mathrm{SO}(q')$ be the embeddings corresponding to the subgroups of diagonal matrices. It is easy to see that the restriction $f|_{D_{0,q}}\colon D_{0,q} \to D_{0,q'}$ induces a map $F\colon H^1(k, D_{0,q}) \to H^1(k, D_{0,q'})$ sending $(\overline{c_1}, \ldots, \overline{c_n})$ to $(\overline{1}, \overline{c_1}, \ldots, \overline{c_n})$. Hence, if $q'' = \langle x_1, \ldots, x_n \rangle$ is any quadratic form such that $\mathrm{disc}(q'') = \mathrm{disc}(q)$, it follows that

$$f_*(q'') = f_*(i_{q*}(\overline{x_1/b_1}, \ldots, \overline{x_n/b_n})) = i_{q'*}(F(\overline{x_1/b_1}, \ldots, \overline{x_n/b_n})) = \langle d \rangle \perp q''.$$

(c) Let $j_q\colon D_q \hookrightarrow \mathrm{O}(q)$ and $i_{q'}\colon D_{0,q'} \hookrightarrow \mathrm{SO}(q')$ be as before. Note that the restriction $f|_{D_q}\colon D_q \to D_{0,q'}$ induces a map $F\colon H^1(k, D_q) \to H^1(k, D_{0,q'})$ sending $(\overline{c_1}, \ldots, \overline{c_n})$ to $(\overline{c_1} \ldots \overline{c_n}, \overline{c_1}, \ldots, \overline{c_n})$. The result follows using a similar argument to the one in part (b). □

We are ready to prove the main result of this section.

Theorem 3.8. *Let* $q = \langle -a, -b, ab \rangle$ *be a nondegenerate quadratic form.*

(a) *The conjugacy classes of embeddings* $\mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{SO}(q)$ *are in natural bijective correspondence with the set* $D(q) \subset k^\times/k^{\times 2}$ *consisting of nonzero square classes represented by* q*.*

(b) *The conjugacy classes of embeddings* $(\mathbb{Z}/2\mathbb{Z})^2 \hookrightarrow \mathrm{SO}(q)$ *are in natural bijective correspondence with* $Q_{a,b}$*, as defined in Theorem 1.3(b).*

(c) *There is at most one conjugacy class of embeddings* $\mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathrm{SO}(q)$ *(*$n \geq 3$*).*

(d) *Suppose that* D_{2n} *is contained in* $\mathrm{SO}(q)$ *(*$n \geq 3$*). Then the conjugacy classes of embeddings* $D_{2n} \hookrightarrow \mathrm{SO}(q)$ *are in natural bijective correspondence with* $D(\langle 1, -\beta_n \rangle)$*.*

(e) *There is at most one conjugacy class of embeddings of* A_4*,* S_4 *or* A_5 *into* $\mathrm{SO}(q)$*.*

Proof. (a) Let $H \cong \mathbb{Z}/2\mathbb{Z}$ be generated by $\mathrm{diag}(1,-1,-1)$ inside $\mathrm{SO}(q)$. By Lemma 3.4(a), its centralizer Z is isomorphic to $\mathrm{O}(\langle -b, ab\rangle)$. By Lemma 3.7(c), the inclusion $Z \hookrightarrow \mathrm{SO}(q)$ induces a map $H^1(k,Z) \to H^1(k,\mathrm{SO}(q))$ sending a binary quadratic form q' to $\langle \mathrm{disc}(q')\rangle \perp q'$. Hence, the kernel $H^1(k,Z)_0$ consists of the binary quadratic forms q' such that $\langle \mathrm{disc}(q')\rangle \perp q' \simeq q$ (in particular, $\overline{\mathrm{disc}(q')} \in D(q)$). Define a map $\Psi\colon H^1(k,Z)_0 \to D(q)$ sending $q' \mapsto \overline{\mathrm{disc}(q')}$. If $q', q'' \in H^1(k,Z)_0$ satisfy $\Psi(q') = \Psi(q'')$, then $\langle \Psi(q')\rangle \perp q' \simeq \langle \Psi(q'')\rangle \perp q'' \simeq q$ implies $q' \simeq q''$ by Witt's Cancellation Theorem, so Ψ is injective. To prove that Ψ is surjective, let $\overline{d} \in D(q)$ be arbitrary. Then $q = \langle d\rangle \perp q'$ for some quadratic form q'. Taking discriminants yields $\overline{\mathrm{disc}(q')} = \overline{d}$. This implies that $q' \in H^1(k,Z)_0$ and $\Psi(q') = \overline{d}$. This proves that $H^1(k,Z)_0$ is in natural bijection with $D(q)$.

(b) Let $H \cong (\mathbb{Z}/2\mathbb{Z})^2$ be the subgroup D_0 of diagonal matrices inside $\mathrm{SO}(q)$. By Lemma 3.4(b), we have that $Z = H$ and the map $H^1(k,Z) \to H^1(k,\mathrm{SO}(q))$ sends $(\overline{x},\overline{y},\overline{z})$, with $\overline{xyz} = \overline{1}$, to $\langle -ax, -by, abz\rangle$. Therefore, $(\overline{x},\overline{y},\overline{z}) \in H^1(k,Z)_0$ if and only if $\langle -ax,-by,abz\rangle \simeq \langle -a,-b,ab\rangle$, which is equivalent to $(ax,by)_2 \cong (a,b)_2$. It follows easily that $H^1(k,Z)_0 \cong Q_{a,b}$.

(c) We may assume that we are in the situation of Lemma 3.4(c), i.e., $q = \langle -\beta_n, -\gamma, \beta_n\gamma\rangle$ and the centralizer Z is isomorphic to $\mathrm{SO}(\langle -\gamma, \beta_n\gamma\rangle)$. By Lemma 3.7(b), the natural map $H^1(k,Z) \to H^1(k,\mathrm{SO}(q))$ sends a binary quadratic form q' (with $\mathrm{disc}(q') = -\beta_n$) to $\langle -\beta_n\rangle \perp q'$. By Witt's Cancellation Theorem, the kernel $H^1(k,Z)_0$ is trivial and the claim follows.

(d) We may assume that $q = \langle -\beta_n, -\gamma, \beta_n\gamma\rangle$ and $H \cong D_{2n}$ is as in Lemma 3.4(d). The centralizer $Z \cong \mathbb{Z}/2\mathbb{Z}$ is generated by $\mathrm{diag}(1,-1,-1)$. Let $D_0 \subset \mathrm{SO}(q)$ be the subgroup of diagonal matrices; the natural inclusion $Z \hookrightarrow D_0$ induces a map $H^1(k,Z) \cong k^\times/k^{\times 2} \to H^1(k,D_0)$ sending $\overline{c} \in k^\times/k^{\times 2}$ to $(\overline{1},\overline{c},\overline{c})$. Therefore the natural map $H^1(k,Z) \to H^1(k,\mathrm{SO}(q))$ sends $\overline{c} \in k^\times/k^{\times 2}$ to $\langle -\beta_n, -c\gamma, c\beta_n\gamma\rangle$. By Witt's Cancellation Theorem, the kernel $H^1(k,Z)_0$ is given by those square classes $\overline{c}$ such that $\langle -c\gamma, c\beta_n\gamma\rangle \simeq \langle -\gamma,\beta_n\gamma\rangle$. It follows easily that $\overline{c} \in H^1(k,Z)_0$ if and only if $\langle 1, -\beta_n\rangle$ represents $\overline{c}$, i.e., $H^1(k,Z)_0 \cong D(\langle 1,-\beta_n\rangle)$.

(e) This is immediate from Lemma 3.4(e). □

Proof of Theorem 1.3. In view of Theorem 3.8, it suffices to analyze the different actions of the normalizers N described in Lemma 3.4 on $H^1(k,Z)_0$. Parts (c) and (e) are immediate because $H^1(k,Z)_0$ itself is trivial, so we may focus our attention on parts (a), (b) and (d).

(a) Note that $N = Z(k_s)$, whence the action of N on $H^1(k,Z)$ (and *a fortiori* $H^1(k,Z)_0$) is trivial. This finishes the proof.

(b) Recall that $N = H \rtimes N'$, where $N' \cong S_3$. Since H acts trivially on

$H^1(k,Z)$, we only need to determine how N' acts on $H^1(k,Z)_0$. As we saw before, the subgroup N' is generated by the matrices

$$s = \begin{pmatrix} 0 & vu^{-1} & 0 \\ 0 & 0 & u \\ v^{-1} & 0 & 0 \end{pmatrix},\ t = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -u \\ 0 & -u^{-1} & 0 \end{pmatrix},$$

where $u = \sqrt{-a}$ and $v = \sqrt{-b}$. Note that a 1-cocycle $l\colon \mathrm{Gal}(k_s/k) \to Z(k_s)$ representing $(\overline{x},\overline{y}) \in Q_{a,b}$ is given by

$$\sigma \mapsto l_\sigma = \mathrm{diag}(x_1^{-1}\sigma(x_1), y_1^{-1}\sigma(y_1), x_1^{-1}\sigma(x_1)y_1^{-1}\sigma(y_1)),$$

where $x_1^2 = x$ and $y_1^2 = y$. We compute

$$s^{-1}l_\sigma\sigma(s) = \mathrm{diag}((vx_1y_1)^{-1}\sigma(vx_1y_1), (uvx_1)^{-1}\sigma(uvx_1), (uy_1)^{-1}\sigma(uy_1)),$$

and

$$t^{-1}l_\sigma\sigma(t) = \mathrm{diag}(x_1^{-1}\sigma(x_1), (ux_1y_1)^{-1}\sigma(ux_1y_1), (uy_1)^{-1}\sigma(uy_1)).$$

Thus, the 1-cocycles $\sigma \mapsto s^{-1}l_\sigma\sigma(s)$ and $\sigma \mapsto t^{-1}l_\sigma\sigma(t)$ correspond to the elements $(\overline{-bxy}, \overline{abx})$ and $(\overline{x}, \overline{-axy})$ in $Q_{a,b}$, respectively. Hence $N' \cong S_3$ acts on $Q_{a,b}$ as claimed and the result follows easily.

(d) Recall that $N \cong D_{4n}$ is generated by

$$s' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha_{2n} & 2\alpha_{2n}\beta_{2n} \\ 0 & (2\alpha_{2n})^{-1} & \alpha_{2n} \end{pmatrix},\ t = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Note that H is the subgroup of N generated by $s = (s')^2$ and t. Clearly the action of H on $H^1(k,Z)_0$ is trivial, so we only need to compute the action of s' on $H^1(k,Z)_0$. Unraveling the identification $H^1(k,Z)_0 \cong D(\langle 1, -\beta_n\rangle)$, we see that a 1-cocycle $l\colon \mathrm{Gal}(k_s/k) \to Z(k_s)$ representing $\overline{c} \in H^1(k,Z)_0$ is given by $\sigma \to l_\sigma = \mathrm{diag}(1, c_1^{-1}\sigma(c_1), c_1^{-1}\sigma(c_1))$, where $c_1 \in k_s^\times$ satisfies $c_1^2 = c$. Then we compute the 1-cocycle

$$\sigma \mapsto (s')^{-1}l_\sigma\sigma(s') = \mathrm{diag}(1, (\alpha_{2n}c_1)^{-1}\sigma(\alpha_{2n}c_1), (\alpha_{2n}c_1)^{-1}\sigma(\alpha_{2n}c_1)).$$

It corresponds to the square class of $(\alpha_{2n}c_1)^2$, which is precisely $\overline{2(\alpha_n+1)c}$. This completes the proof. □

Remark 3.9. Suppose we are in the situation of Theorem 1.3(d) and n is odd. Then note that $2(\alpha_n+1) = (2\alpha_{2n})^2 \in k^{\times 2}$ by Lemma 2.2(b). Therefore, the conjugacy classes of D_{2n} are in natural bijective correspondence with $D(\langle 1, -\beta_n\rangle)$ for n odd. This is not necessarily true for even n.

We now make the correspondences in parts (a), (b) and (d) of Theorem 3.8 more explicit, by exhibiting representatives for each conjugacy class.

- Let $q = \langle -a, -b, ab\rangle$, let $d \in D(q)$ and let $q' = \langle d, x, y\rangle$ be a quadratic form isometric to q. Select $P \in \mathrm{GL}_3(k)$ such that $q = q' \circ P$. Then the element $d \in D(q)$ corresponds to the conjugacy class of the embedding $\mathbb{Z}/2\mathbb{Z} \cong P^{-1}HP \hookrightarrow \mathrm{SO}(q)$, where H is generated by $\mathrm{diag}(1, -1, -1)$.

- Let $q = \langle -a, -b, ab\rangle$, let $(x, y) \in Q_{a,b}$ and let $q' = \langle -ax, -by, abxy\rangle$. Select $P \in \mathrm{GL}_3(k)$ such that $q = q' \circ P$. The element (x, y) corresponds to the conjugacy class of the embedding $(\mathbb{Z}/2\mathbb{Z})^2 \cong P^{-1}D_0P \hookrightarrow \mathrm{SO}(q)$, where D_0 is the subgroup of diagonal matrices in $\mathrm{SO}(q)$.

- Let k contain α_n, let $q = \langle -\beta_n, -\gamma, \beta_n\gamma\rangle$ and let $c \in D(\langle 1, -\beta_n\rangle)$. Then the quadratic form $q' = \langle -\beta_n, -c\gamma, c\beta_n\gamma\rangle$ is isometric to q, so we may select $P \in \mathrm{GL}_3(k)$ such that $q = q' \circ P$. The element c corresponds to the conjugacy class of the embedding $D_{2n} \cong P^{-1}HP \hookrightarrow \mathrm{SO}(q)$, where $H \cong D_{2n}$ is as in Lemma 3.4(d).

Recall that if q is isotropic, then $\mathrm{SO}(q) \cong \mathrm{PGL}_2$, so we recover the case studied in [2]. Using the above correspondences, we can fully describe the embeddings of finite groups into PGL_2, up to conjugacy. We collect their descriptions here for convenience, as these results will be needed in the remainder of the thesis. The details of the proof are left to the reader.

Proposition 3.10. (a) *The embeddings $\mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{PGL}_2$ are parametrized by $k^\times/k^{\times 2}$, up to conjugacy, and for every $a \in k^\times$, the embedding*

$$\rho_a : -1 \mapsto \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} \tag{3.1}$$

corresponds to $\overline{a} \in k^\times/k^{\times 2}$.

(b) *The conjugacy classes of embeddings $(\mathbb{Z}/2\mathbb{Z})^2 \hookrightarrow \mathrm{PGL}_2$ are parametrized by the pairs $(\overline{a}, \overline{b}) \in (k^\times/k^{\times 2})^2$ such that the quaternion algebra $(a, b)_2$ is split. Denote the corresponding embedding by $\rho_{(a,b)}$ and fix generators e_1, e_2 of $(\mathbb{Z}/2\mathbb{Z})^2$. We have the following three cases:*

- *If both a and b are non-squares, we have*

$$\rho_{(a,b)} \colon e_1 \mapsto \begin{pmatrix} \lambda & -a \\ 1 & -\lambda \end{pmatrix}, \quad e_2 \mapsto \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}, \tag{3.2}$$

where $\overline{\lambda^2 - a} = \overline{b}$ (we can find such $\lambda \in k$ because $(a, b)_2$ is split).

- *If $a \in k^{\times 2}$, we have*

$$\rho_{(a,b)} \colon e_1 \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}, \quad e_2 \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{3.3}$$

- *If $b \in k^{\times 2}$, we have*

$$\rho_{(a,b)} \colon e_1 \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad e_2 \mapsto \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}. \tag{3.4}$$

(If both a and b are squares, the last two embeddings are conjugate, and we will assume $\rho_{(a,b)}$ is given by (3.4).)

(c) *Let k contain α_n, where $n \geq 3$. Then there exists a unique conjugacy class of embeddings $\mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathrm{PGL}_2$, which is represented by*

$$\rho \colon \sigma \mapsto \begin{pmatrix} \alpha_n + 1 & \beta_n \\ 1 & \alpha_n + 1 \end{pmatrix}, \tag{3.5}$$

where σ is a generator of $\mathbb{Z}/n\mathbb{Z}$.

(d) *Let k contain α_n, where $n \geq 3$. The conjugacy classes of embeddings $D_{2n} \hookrightarrow \mathrm{PGL}_2(k)$ are parametrized by the set $D(\langle 1, -\beta_n \rangle)$ of nonzero square classes represented by the binary quadratic form $x^2 - \beta_n y^2$. The correspondence is as follows: to the class $\overline{a}$ of the element $a = x^2 - \beta_n y^2$ $(x, y \in k)$, we assign*

$$\rho_a \colon \sigma \mapsto \begin{pmatrix} \alpha_n + 1 & \beta_n \\ 1 & \alpha_n + 1 \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} x & -y\beta_n \\ y & -x \end{pmatrix}, \tag{3.6}$$

where $\sigma, \tau \in D_{2n}$ satisfy $\sigma^n = \tau^2 = (\sigma\tau)^2 = 1$.

(e) *Let k contain elements a, b such that $a^2 + b^2 = -1$. Then the embeddings of A_4 and S_4 into PGL_2 are all conjugate. The matrices*

$$R := \begin{pmatrix} a - b - 1 & a + b + 1 \\ a + b - 1 & b - a - 1 \end{pmatrix}, \quad S := \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \tag{3.7}$$

satisfy $R^3 = S^4 = (R^{-1}S)^2 = 1$ in PGL_2, and thus generate a subgroup isomorphic to S_4. Moreover, R and $S' := S^2$ satisfy $R^3 = S'^2 = (R^{-1}S')^3 = 1$ in PGL_2 and generate a subgroup isomorphic to A_4.

(f) *Let k contain elements a, b such that $a^2 + b^2 = -1$ and suppose that $5 \in k^{\times 2}$. Then the group A_5 embeds into PGL_2 in a unique way, up to conjugacy. Write $\phi = (1+\sqrt{5})/2$ and consider the matrix*

$$U := \begin{pmatrix} \phi a + \phi^{-1} & \phi b - 1 \\ \phi b + 1 & -\phi a + \phi^{-1} \end{pmatrix}. \tag{3.8}$$

Then $R^3 = U^5 = (R^{-1}U)^2 = 1$ in PGL_2, where R is as in (3.7), and these two matrices generate a subgroup isomorphic to A_5.

□

Chapter 4

Finite group actions on hyperelliptic curves

4.1 Equivalent characterizations of the HLP

Let k denote a base field of characteristic 0 and suppose that we have a central exact sequence $1 \to \mu_2 \to G' \to G \to 1$ of finite groups. A projective representation $\rho\colon G \hookrightarrow \mathrm{PGL}_2$ defined over k induces a G-variety structure on the projective line, which we denote by ${}_\rho\mathbb{P}^1$. We set $k(x) = k({}_\rho\mathbb{P}^1)$ and $k(t) = k({}_\rho\mathbb{P}^1)^G$, where $k(x)/k(t)$ is G-Galois.

Proposition 4.1. *The following are equivalent.*

(a) *There exists a hyperelliptic curve C/k endowed with a faithful G'-action such that $C/\mu_2 \cong {}_\rho\mathbb{P}^1$ as G-varieties.*

(b) *Let $c \in H^1(k(t), G)$ be the class corresponding to the G-Galois field extension $k(x)/k(t)$ and let $\delta\colon H^1(k(t), G) \to H^2(k(t), \mu_2)$ be the connecting homomorphism induced by $1 \to \mu_2 \to G' \to G \to 1$. Then $\delta(c)$ is trivial.*

Proof. Suppose first that (a) holds. It follows that the function field extension $k(C)/k(t)$ is G'-Galois and the natural morphism $H^1(k(t), G') \to H^1(k(t), G)$ maps its class to c. The long exact sequence in cohomology

$$H^1(k(t), \mu_2) \to H^1(k(t), G') \to H^1(k(t), G) \to H^2(k(t), \mu_2)$$

then implies that $\delta(c)$ is trivial.

Suppose next that (b) holds. From the long exact sequence in cohomology, it follows that c is the image of a class $c' \in H^1(k(t), G')$, which is represented by some G'-Galois algebra $M/k(t)$ such that $M^{\mu_2} = k(x)$. We claim that we may assume that M is the function field $k(C)$ of a hyperelliptic curve C. We may complete the proof modulo this statement, as the G'-Galois action on $k(C)$ induces a faithful G'-variety structure on C, satisfying the conditions required in (a).

It remains to verify the claim. We prove a stronger statement; namely that we may assume that M is the function field of a hyperelliptic curve of arbitrarily large genus. We may write $M = k(x)[Y]/(Y^2 - \omega(x))$, where $\omega(x)$ is a separable polynomial. Recall that $H^1(k(t), \mu_2) \cong k(t)^\times / k(t)^{\times 2}$ acts on the fiber above c in the following way: the element $r \cdot k(t)^{\times 2}$ sends M to the G'-Galois algebra $k(x)[Y]/(Y^2 - r\omega(x))$. Write t as a rational function $t = p(x)/q(x)$, where p, q are coprime polynomials in $k[x]$. Then we can select $\alpha_1, \ldots, \alpha_l \in k$ ($l \geq 6$) such that $\omega(\alpha_i)q(\alpha_i) \neq 0$ for all i, $p(\alpha_i)/q(\alpha_i) \neq p(\alpha_j)/q(\alpha_j)$ for all $i \neq j$, and α_i is a simple root of $q(\alpha_i)p(x) - p(\alpha_i)q(x)$ for all i. If we set $r = \prod_i (t - p(\alpha_i)/q(\alpha_i))$, the Galois algebra $k(x)(\sqrt{r\omega(x)})$ is then the function field of the hyperelliptic curve

$$y^2 = \omega(x) \prod_i \left(\frac{p(x)}{q(x)} - \frac{p(\alpha_i)}{q(\alpha_i)} \right),$$

which ramifies over $\alpha_1, \ldots, \alpha_l$ by construction. The genus of such curve is at least $l/2 - 1$, which can be made arbitrarily large. □

Corollary 4.2. *If $G' = \mu_2 \times G$, then the HLP is solvable.*

Proof. Left to the reader. □

The main result of this section relates the solvability of the HLP to the existence of certain linear representations of G' that are nontrivial on μ_2.

Proposition 4.3. *The HLP in Problem 1.4 is solvable if and only if at least one of the following conditions holds:*

(a) *There exists a homomorphism $G' \to \mu(k)$ that is nontrivial on μ_2, where $\mu(k)$ is the group of roots of unity in k.*

(b) *There exists an embedding $G' \hookrightarrow \mathrm{GL}_2$ lifting $G \hookrightarrow \mathrm{PGL}_2$.*

Proof. By [1, Lemma 6.12], the solvability of the HLP implies that either (a) or (b) must hold. It remains to prove the converse.

In the notation of Proposition 4.1(b), it is enough to prove that $\delta(c)$ is trivial in each case. Via the natural map $H^1(k(t), \mu_2) \hookrightarrow H^1(k(t), \mathbb{G}_m)$, we may regard $\delta(c)$ as a Brauer class in $\mathrm{Br}(k(t))$.

Suppose first that (a) holds. By a theorem of Karpenko and Merkurjev [14, Thm. 4.4, Rem. 4.5], the index of $\delta(c)$ divides $\dim(V)$, for any linear representation V of G' that is nontrivial on μ_2. By assumption, there exists such linear representation of dimension 1, whence $\delta(c)$ must be trivial.

Suppose next that (b) holds. Consider the following commutative diagram whose rows are central exact sequences

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathrm{GL}_2 & \longrightarrow & \mathrm{PGL}_2 & \longrightarrow & 1 \\
 & & \| & & \uparrow{\scriptstyle \overline{\rho}} & & \uparrow{\scriptstyle \rho} & & \\
1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & G'' & \longrightarrow & G & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \| & & \\
1 & \longrightarrow & \mu_2 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & 1
\end{array}$$

where G'' is the full preimage of G in GL_2. We obtain the corresponding diagram in cohomology

$$\begin{array}{ccccc}
 & & H^1(k(t),\mathrm{PGL}_2) & \longrightarrow & H^2(k(t),\mathbb{G}_m) \\
 & & \uparrow{\scriptstyle \rho_*} & & \| \\
H^1(k(t),G'') & \longrightarrow & H^1(k(t),G) & \longrightarrow & H^2(k(t),\mathbb{G}_m) \\
\uparrow & & \| & & \uparrow \\
H^1(k(t),G') & \longrightarrow & H^1(k(t),G) & \xrightarrow{\delta} & H^2(k(t),\mu_2)
\end{array}$$

We may endow $\mathbb{A}^2$ with a generically free G''-action via $\overline{\rho}$. Then, note that the class $c \in H^1(k(t),G)$ of the G-torsor $k(x)/k(t)$ comes from the class of a G''-torsor in $H^1(k(t),G'')$, namely $k(\mathbb{A}^2)/k(\mathbb{A}^2)^{G''}$. The commutativity of the above diagram then implies that $\delta(c)$ is trivial. □

Remark 4.4. The condition in Proposition 4.3(a) above is independent of the choice of the embedding $G \hookrightarrow \mathrm{PGL}_2$. In other words, the existence of such homomorphism implies the solvability of the HLP, regardless of the faithful G-action on $\mathbb{P}^1$. On the other hand, the condition in part (b) depends heavily on the particular embedding $G \hookrightarrow \mathrm{PGL}_2$.

Remark 4.5. In [1, Lemma 6.12], it is proven that if the G-action on $\mathbb{P}^1$ can be lifted to a G'-action on a hyperelliptic curve of odd (resp. even) genus, then the condition in Proposition 4.3(a) (resp. (b)) holds. However, the converse of this statement is not true. In particular, in the following example there exists a homomorphism $G' \to \mu(k)$ which is nontrivial on μ_2 but the G-action on $\mathbb{P}^1$ cannot be lifted to a G'-action on any hyperelliptic curve of odd genus. Consider a field k that contains a primitive 8-th root of 1, and consider the HLP given by the exact sequence $1 \to \mu_2 \to \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to 1$

and the $\mathbb{Z}/4\mathbb{Z}$-action on $\mathbb{P}^1$ defined by $z \mapsto \omega_8^2 z$. The mapping $\sigma \mapsto \omega_8$, where σ is a generator of $\mathbb{Z}/8\mathbb{Z}$, defines a homomorphism $\mathbb{Z}/8\mathbb{Z} \to \mu(k)$ that is nontrivial on μ_2. However, note that $k(t) = k(x^4)$ and $k(\sqrt{x})/k(x^4)$ is an element in the fiber above $k(x)/k(x^4)$ under the natural morphism $H^1(k(x^4), \mathbb{Z}/8\mathbb{Z}) \to H^1(k(x^4), \mathbb{Z}/4\mathbb{Z})$. Hence, any element in such fiber is of the form $L = k(x)(\sqrt{xQ(x^4)})$, where we may assume that Q is a separable polynomial. Then, observe that L is the function field of the hyperelliptic curve $Y^2 = xQ(x^4)$, which has even genus $2\deg(Q)$. Of course, the existence of such solution to the HLP implies the existence of an embedding $G' \hookrightarrow \mathrm{GL}_2$ lifting $G \hookrightarrow \mathrm{PGL}_2$, which is given by

$$\sigma \mapsto \begin{pmatrix} \omega_8 & 0 \\ 0 & \omega_8^{-1} \end{pmatrix}.$$

Our goal for the remainder of the chapter is to solve the HLP for every possible embedding $G \hookrightarrow \mathrm{PGL}_2$ and every non-split extension of G by μ_2.

4.2 HLP for cyclic groups

Throughout this section, we assume that $G = \mathbb{Z}/n\mathbb{Z}$. If n is odd, there are no non-split extensions of $\mathbb{Z}/n\mathbb{Z}$ by μ_2. On the other hand, if n is even, there exists a unique non-split extension given by

$$1 \to \mu_2 \to \mathbb{Z}/2n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 1. \tag{4.1}$$

In what follows, we assume that n is even and write $n = 2^h q$, where $h \geq 1$ and q is odd.

Proposition 4.6. *There exists a homomorphism $\mathbb{Z}/2n\mathbb{Z} \to \mu(k)$ that is nontrivial on μ_2 if and only if $\omega_{2^{h+1}} \in k$.*

Proof. Note that $\mathbb{Z}/2^{h+1}\mathbb{Z}$ is a direct factor of $\mathbb{Z}/2n\mathbb{Z}$, so we may assume without loss of generality that $q = 1$. Any homomorphism $\mathbb{Z}/2^{h+1}\mathbb{Z} \to \mu(k)$ that is nontrivial on μ_2 must be faithful, which implies the existence of a primitive 2^{h+1}-root of unity in k. The converse is left to the reader. □

We now deal with the case $G = \mathbb{Z}/2\mathbb{Z}$ and we assume that ρ_a is as in (3.1) for some $a \in k^{\times 2}$.

Proposition 4.7. *The HLP given by ρ_a and $1 \to \mu_2 \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 1$ is solvable if and only if either $-1 \in k^{\times 2}$ or $-a \in k^{\times 2}$.*

Proof. In view of Propositions 4.3 and 4.6, it suffices to prove that we can lift ρ_a to $\mathbb{Z}/4\mathbb{Z} \hookrightarrow \mathrm{GL}_2$ if and only if $-a \in k^{\times 2}$. Indeed, such a lift is equivalent to the existence of $\lambda \in k$ such that

$$\begin{pmatrix} 0 & \lambda a \\ \lambda & 0 \end{pmatrix}^2 = -I,$$

which can be found if and only if $-a$ is a square in k. □

For the remainder of the section, we assume that $n \geq 4$ and $\alpha_n \in k$, and we define $\rho\colon \mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathrm{PGL}_2$ as in (3.5).

Proposition 4.8. *Suppose that k contains α_n, where n is even. Then, ρ lifts to an embedding $\mathbb{Z}/2n\mathbb{Z} \hookrightarrow \mathrm{GL}_2$ if and only if one of the following conditions holds:*

(a) $\alpha_{2n} \in k$.

(b) $\omega_4\alpha_{2n} \in k$ *and* $n \equiv 0\ (4)$.

Proof. There exists such a lift if and only if we can find $\lambda \in k$ such that

$$\widetilde{\sigma} = \lambda \begin{pmatrix} \alpha_n + 1 & \beta_n \\ 1 & \alpha_n + 1 \end{pmatrix}$$

satisfies $\widetilde{\sigma}^n = -I$. Note that the eigenvalues of $\widetilde{\sigma}$ are $\lambda(1+\omega_n^{\pm 1})$, so it follows from Lemma 2.2(c) that $\widetilde{\sigma}^n = -(2\lambda\alpha_{2n})^n I$, whence we can lift ρ if and only if $(2\lambda\alpha_{2n})^n = 1$ for some $\lambda \in k$.

If (a) (resp. (b)) holds, we choose $\lambda = (2\alpha_{2n})^{-1}$ (resp. $\lambda = (2\omega_4\alpha_{2n})^{-1}$) to satisfy the above relation. Conversely, suppose that $(2\lambda\alpha_{2n})^n = 1$ for some $\lambda \in k$. Then we can write $2\lambda\alpha_{2n} = \zeta_n$ for some n-th root of unity ζ_n, not necessarily primitive. If ζ_n is a primitive 4-th root of unity (which is only possible if 4 divides n), then we obtain condition (b). Assume henceforth that this is not the case (in particular, $\zeta_n + \zeta_n^{-1} \neq 0$). Then, we compute $\zeta_n + \zeta_n^{-1} = (4\lambda^2\alpha_{2n}^2 + 1)/(2\lambda\alpha_{2n})$ and therefore, we have

$$\alpha_{2n} = \frac{4\lambda^2\alpha_{2n}^2 + 1}{2\lambda(\zeta_n + \zeta_n^{-1})} = \frac{\lambda^2(2\alpha_n + 2) + 1}{2\lambda(\zeta_n + \zeta_n^{-1})}.$$

By Lemma 2.2(a), we have $\zeta_n + \zeta_n^{-1} \in k$, whence $\alpha_{2n} \in k$ as desired. □

Proposition 4.9. *Suppose that k contains α_n, where $n \equiv 2\ (4)$ and $n \geq 6$. Then the HLP given by ρ and $1 \to \mu_2 \to \mathbb{Z}/2n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 1$ is solvable if and only if either $\alpha_{2n} \in k$ or $-1 \in k^{\times 2}$.*

Proof. This follows immediately from Propositions 4.3, 4.6 and 4.8. □

Proposition 4.10. *Suppose that k contains α_n, where $n \equiv 0\ (4)$. Then the HLP given by ρ and $1 \to \mu_2 \to \mathbb{Z}/2n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 1$ is solvable if and only if either $\alpha_{2n} \in k$ or $\omega_4\alpha_{2n} \in k$.*

Proof. In view of Propositions 4.3, 4.6 and 4.8, it suffices to show that $\omega_{2^{h+1}} \in k$ implies that $\alpha_{2n} \in k$. We actually prove a stronger statement, namely that $\omega_{2^{h+1}} \in k \Rightarrow \omega_{2n} \in k$. By Lemma 2.2(d), the conditions $\alpha_n \in k$ and $\omega_{2^{h+1}} \in k$ together imply that $\omega_n \in k$. Finally, note that $\omega_{2^{h+1}}\omega_n$ is a primitive $2n$-th root of unity contained in k, which implies the result. □

4.3 HLP for dihedral groups

In this section, we assume throughout that $G = D_{2n}$, with the usual presentation $D_{2n} = \langle \sigma,\ \tau \,|\, \sigma^n = 1,\ \tau^2 = 1,\ (\sigma\tau)^2 = 1\rangle$. Let G' be any double cover of D_{2n}. We denote the nontrivial element of μ_2 by -1, which is central in G', and let s, t by lifts of σ, τ to G', respectively. We refer the reader to [5, Lemma 4.1] for the cohomology calculations needed below.

If n is odd, we have the equality $H^2(G, \mu_2) = \mu_2$. The unique non-split extension (up to equivalence) of G by μ_2 is given by

$$1 \to \mu_2 \to Dic_{4n} \to D_{2n} \to 1, \tag{4.2}$$

where Dic_{4n} is the dicyclic group

$$\langle s,\ t \,|\, s^n = -1,\ t^2 = -1,\ (st)^2 = -1\rangle.$$

The element t generates a Sylow 2-subgroup of Dic_{4n}, which is isomorphic to $\mathbb{Z}/4\mathbb{Z}$. The corresponding exact sequence of Sylow 2-subgroups is the unique non-split extension of $\mathbb{Z}/2\mathbb{Z}$ by μ_2.

If n is even, it is well known that $H^2(G, \mu_2) = \mu_2^3$ and the extensions are given by groups of the form $G' = \langle s,\ t \,|\, s^n = \epsilon_1,\ t^2 = \epsilon_2,\ (st)^2 = \epsilon_3\rangle$, where $(\epsilon_1, \epsilon_2, \epsilon_3) \in \mu_2^3$. We introduce some notation for the non-split group extensions of G by μ_2 (cf. [19, §3.7]). For simplicity, we will label the resulting exact sequences by their corresponding element in $H^2(G, \mu_2)$.

Element of μ_2^3	Notation for G'
$(-1, 1, 1)$	D_{4n}
$(1, \mp 1, \pm 1)$	V_{4n}
$(1, -1, -1)$	$\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$
$(-1, \mp 1, \pm 1)$	SD_{4n}
$(-1, -1, -1)$	Dic_{4n}

Remark 4.11. (a) The exact sequence $(1,-1,1)$ (resp. $(-1,-1,1)$) is not equivalent to $(1,1,-1)$ (resp. $(-1,1,-1)$), as they represent different elements in $H^2(D_{2n},\mu_2)$.

(b) In the case $G'=\mathbb{Z}/n\mathbb{Z}\rtimes\mathbb{Z}/4\mathbb{Z}$, a generator of $\mathbb{Z}/4\mathbb{Z}$ acts on $\mathbb{Z}/n\mathbb{Z}$ by inversion.

(c) The groups SD_{4n} and Dic_{4n} are sometimes called *semidihedral group* and *generalized quaternion group* respectively, especially when n is a power of 2.

(d) If $n\equiv 0\ (4)$, it is not hard to prove that V_{4n} is isomorphic to the pull-back $D_{2n}\curlywedge\mathbb{Z}/4\mathbb{Z}=D_{2n}\times_{(f,g)}\mathbb{Z}/4\mathbb{Z}$, where $f\colon D_{2n}\to\mathbb{Z}/2\mathbb{Z}$ and $g\colon\mathbb{Z}/4\mathbb{Z}\to\mathbb{Z}/2\mathbb{Z}$ have kernels $\langle\sigma^2,\tau\rangle$ and $\mathbb{Z}/2\mathbb{Z}$ respectively.

(e) $SD_8\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, $V_8\cong D_8$, and $Dic_8\cong Q_8$. In this case, $(-1,1,1)$, $(1,-1,1)$ and $(1,1,-1)$ are three inequivalent extensions yielding the same group, and so are $(1,-1,-1)$, $(-1,-1,1)$ and $(-1,1,-1)$.

Suppose that $n=2^hq$, with $h\geq 1$ and q odd. A Sylow 2-subgroup G'_2 of G' is generated by s^q and t, and it fits into an exact sequence $1\to\mu_2\to G'_2\to D_{2^{h+1}}\to 1$, having the same label as $1\to\mu_2\to G'\to D_{2n}\to 1$.

Proposition 4.12. *Let $1\to\mu_2\to G'\to G\to 1$ be either (4.2) if n is odd or the exact sequence $(\epsilon_1,\epsilon_2,\epsilon_3)$ if n is even, where $\epsilon_i=\pm1$, not all equal to 1. Then there exists a homomorphism $G'\to\mu(k)$ nontrivial on μ_2 if and only if $-1\in k^{\times 2}$ and one of the following conditions holds:*

(a) *n is odd.*

(b) *n is even and $\epsilon_1=(\epsilon_2\epsilon_3)^{n/2}$.*

Proof. Write $n=2^hq$, where $h\geq 0$ and q is odd, and let G'_2 be a Sylow 2-subgroup of G'. If n is even (resp. odd), we may assume that G'_2 is generated by the elements $s'=s^q$ and t satisfying $s'^{2^h}=\epsilon_1$, $t^2=\epsilon_2$, $(s't)^2=\epsilon_3$ (resp. $G'_2\cong\mathbb{Z}/4\mathbb{Z}$ is generated by t). In either case, there exists a surjection $G'\to G'_2$ sending $-1\mapsto -1$, $s\mapsto s'=s^q$ and $t\mapsto t$, with kernel $\mathbb{Z}/q\mathbb{Z}$. It is then clear that the existence of the desired homomorphism $G'\to\mu(k)$ is equivalent to the existence of such homomorphism for G'_2, so we may assume henceforth that $q=1$ (and therefore $G'=G'_2$). If n is odd, the result follows immediately from Proposition 4.6 after this reduction, so we only need to deal with the case where n is even.

Suppose that there exists a homomorphism $G' \to \mu(k)$ nontrivial on μ_2. Then, since $s^{2^{h+1}} = t^4 = 1$, the homomorphism sends $s \to \zeta_{2^{h+1}}$ and $t \to \zeta_4$, where ζ_l is a (not necessarily primitive) l-th root of unity in k. As the homomorphism is nontrivial on μ_2, we must have $\zeta_{2^{h+1}}^{2^h} = \epsilon_1$, $\zeta_4^2 = \epsilon_2$ and $(\zeta_{2^{h+1}}\zeta_4)^2 = \epsilon_3$. Since at least one ϵ_i is equal to -1, it follows that at least one of $\zeta_{2^{h+1}}^{2^{h-1}}$, ζ_4 or $\zeta_{2^{h+1}}\zeta_4$ must be a *primitive* 4-th root of unity, whence $-1 \in k^{\times 2}$. We also compute the condition

$$\epsilon_1 = (\zeta_{2^{h+1}}^2)^{2^{h-1}} = (\zeta_{2^{h+1}}^2\zeta_4^2)^{2^{h-1}}(\zeta_4^{-2})^{2^{h-1}} = (\epsilon_2\epsilon_3)^{2^{h-1}},$$

which is equivalent to (b).

Conversely, suppose that $\omega_4 \in k$ and (b) holds. The existence of the desired homomorphism is equivalent to the solvability of the system of equations

$$\gamma_1^{2^h} = \epsilon_1, \quad \gamma_2^2 = \epsilon_2, \quad \gamma_1^2\gamma_2^2 = \epsilon_3$$

for some $\gamma_1, \gamma_2 \in k$. Note that the last equation is equivalent to $\gamma_1^2 = \epsilon_2\epsilon_3$. Then the first equation becomes superfluous, since $(\epsilon_2\epsilon_3)^{2^{h-1}} = \epsilon_1$ by condition (b). Finally, we can always find γ_1, γ_2 satisfying $\gamma_2^2 = \epsilon_2$ and $\gamma_1^2 = \epsilon_2\epsilon_3$ because $\omega_4 \in k$ by assumption. The proof is complete. □

We now concentrate on the case $n = 2$, i.e., $G \cong (\mathbb{Z}/2\mathbb{Z})^2$, and we define $\rho_{(a,b)}$ as in Proposition 3.10.

Proposition 4.13. *Let $1 \to \mu_2 \to G' \to G \to 1$ be the exact sequence $(\epsilon_1, \epsilon_2, \epsilon_3)$, where $\epsilon_i = \pm 1$, not all equal to 1 (cf. Remark 4.11(e)). The embedding $\rho_{(a,b)}$ lifts to an embedding $G' \hookrightarrow \mathrm{GL}_2$ if and only if $\epsilon_1\epsilon_2\epsilon_3 = -1$, $\epsilon_1 b \in k^{\times 2}$, and $\epsilon_2 a \in k^{\times 2}$.*

Proof. Let $\widetilde{e_1}$, $\widetilde{e_2}$ be lifts of $\rho_{(a,b)}(e_1)$, $\rho_{(a,b)}(e_2)$ to GL_2, respectively. In any of the three cases (3.2), (3.3) and (3.4), a computation shows that $\widetilde{e_1}^2 = \mu_1^2 bI$, $\widetilde{e_2}^2 = \mu_2^2 aI$ and $(\widetilde{e_1}\widetilde{e_2})^2 = -\mu_1^2\mu_2^2 abI$, where $\mu_1, \mu_2 \in k$. Therefore, these elements define an embedding $G' \hookrightarrow \mathrm{GL}_2$ lifting $\rho_{(a,b)}$ if and only if the system of equations

$$\mu_1^2 b = \epsilon_1, \quad \mu_2^2 a = \epsilon_2, \quad -\mu_1^2\mu_2^2 ab = \epsilon_3$$

is solvable for some $\mu_1, \mu_2 \in k$. It is then easy to see this is the case if and only if $\epsilon_1\epsilon_2\epsilon_3 = -1$, $\epsilon_1 b \in k^{\times 2}$, and $\epsilon_2 a \in k^{\times 2}$. □

We can now solve the HLP for actions of $(\mathbb{Z}/2\mathbb{Z})^2$ on the projective line.

Proposition 4.14. *The HLP given by $\rho_{(a,b)}$ and the extension $(\epsilon_1, \epsilon_2, \epsilon_3)$ is solvable if and only if one of the following conditions holds:*

(a) $\epsilon_1\epsilon_2\epsilon_3 = -1$ *and* $\epsilon_1 b, \epsilon_2 a \in k^{\times 2}$. *(Cases: $G' \cong D_8, Q_8$.)*

(b) $\epsilon_1\epsilon_2\epsilon_3 = 1$ *and* $-1 \in k^{\times 2}$. *(Case: $G' \cong \mathbb{Z}/2 \times \mathbb{Z}/4\mathbb{Z}$.)*

Proof. This follows easily from Propositions 4.3, 4.12 and 4.13. □

For the remainder of the section, we assume that $n \geq 3$ and $\alpha_n \in k$, and we define $\rho_a \colon D_{2n} \hookrightarrow \mathrm{PGL}_2$ as in (3.6) for some $\overline{a} \in D(\langle 1, -\beta_n \rangle)$.

Proposition 4.15. *Let k contain α_n and let $1 \to \mu_2 \to G' \to G \to 1$ be either (4.2) if n is odd or the exact sequence $(\epsilon_1, \epsilon_2, \epsilon_3)$ if n is even, where $\epsilon_i = \pm 1$, not all equal to 1. The embedding ρ_a lifts to an embedding $G' \hookrightarrow \mathrm{GL}_2$ if and only if one of the following conditions holds:*

(a) *n is odd and $-a \in k^{\times 2}$.*

(b) *n is even, $\epsilon_1 = -(\epsilon_2\epsilon_3)^{n/2}$, $\epsilon_2 a \in k^{\times 2}$, and $(\epsilon_2\epsilon_3)^{1/2}\alpha_{2n} \in k$.*

Proof. Consider respective lifts

$$\widetilde{\sigma} = \lambda \begin{pmatrix} \alpha_n + 1 & \beta_n \\ 1 & \alpha_n + 1 \end{pmatrix}, \quad \widetilde{\tau} = \mu \begin{pmatrix} u & -\beta_n v \\ v & -u \end{pmatrix}$$

of $\rho_a(\sigma), \rho_a(\tau)$ to GL_2. We then compute $\widetilde{\sigma}^n = -(2\lambda\alpha_{2n})^n I$ (see the proof of Proposition 4.8), $\widetilde{\tau}^2 = \mu^2 a I$, and $(\widetilde{\sigma}\widetilde{\tau})^2 = 4\lambda^2\mu^2\alpha_{2n}^2 a I$.

If n is odd, note that we can have $\widetilde{\tau}^2 = -I$ if and only if $-a \in k^{\times 2}$, so this is a necessary condition for the existence of the lift $G' \hookrightarrow \mathrm{GL}_2$. Conversely, we prove that the condition $-a \in k^{\times 2}$ is also sufficient. Indeed, note that $\alpha_{2n} \in k$ by Lemma 2.2 (b), so we can take $\lambda = (2\alpha_{2n})^{-1}$ and $\mu = (-a)^{-1/2}$ to produce the desired lift.

Assume henceforth that n is even ($n \geq 4$). By the computation we carried out at the beginning of the proof, we see that a lift $G' \hookrightarrow \mathrm{GL}_2$ is possible if and only if we can find $\lambda, \mu \in k$ such that

$$-(2\lambda\alpha_{2n})^n = \epsilon_1, \quad \mu^2 a = \epsilon_2, \quad 4\lambda^2\mu^2\alpha_{2n}^2 a = \epsilon_3.$$

The last equation is equivalent to $(2\lambda\alpha_{2n})^2 = \epsilon_2\epsilon_3$, which is possible if and only if $(\epsilon_2\epsilon_3)^{1/2}\alpha_{2n} \in k$. On the other hand, the second relation above is possible if and only if $\epsilon_2 a \in k^{\times 2}$, and the first relation holds if and only if

$$\epsilon_1 = -(2\lambda\alpha_{2n})^n = -((2\lambda\alpha_{2n})^2)^{n/2} = -(\epsilon_2\epsilon_3)^{n/2}.$$

This completes the proof of the proposition. □

We can now solve the HLP for dihedral actions on the projective line. We separate the odd and even cases for the sake of clarity.

Proposition 4.16. *Suppose that n is odd and k contains α_n. The HLP given by ρ_a and the exact sequence* (4.2) *is solvable if and only if either $-1 \in k^{\times 2}$ or $-a \in k^{\times 2}$.*

Proof. The proof follows from Propositions 4.3, 4.12 and 4.15. □

Proposition 4.17. *Suppose that n is even and k contains α_n. The HLP given by ρ_a and the exact sequence $(\epsilon_1, \epsilon_2, \epsilon_3)$ is solvable if and only if one of the following conditions holds:*

(a) $\epsilon_1 = (\epsilon_2\epsilon_3)^{n/2}$ *and* $-1 \in k^{\times 2}$.

(b) $\epsilon_1 = -(\epsilon_2\epsilon_3)^{n/2}$, $\epsilon_2 a \in k^{\times 2}$, *and* $(\epsilon_2\epsilon_3)^{1/2}\alpha_{2n} \in k$.

Proof. Again, the proof follows from Propositions 4.3, 4.12 and 4.15. □

4.4 HLP for polyhedral groups

Recall that a polyhedral group G ($= A_4$, S_4, or A_5) embeds into PGL_2 if and only if -1 is a sum of two squares over k, with the additional condition that $\sqrt{5} \in k$ if $G = A_5$. Under these conditions, the embeddings into PGL_2 are all conjugate, so the solvability of HLP's for polyhedral groups are independent of the chosen embedding. For any such group G, we fix the embedding $G \hookrightarrow \mathrm{PGL}_2$ to be the one described in Proposition (3.10).

4.4.1 Alternating groups

In this subsection, let $G = A_n$ for $n = 4, 5$. Recall that $H^2(G, \mu_2) = \mu_2$, whence G has a unique non-split central extension

$$1 \to \mu_2 \to \widetilde{G} \to G \to 1. \tag{4.3}$$

Actually, it is well known that $\widetilde{A_4} \cong \mathrm{SL}_2(\mathbb{F}_3)$ and $\widetilde{A_5} \cong \mathrm{SL}_2(\mathbb{F}_5)$ (see, e.g., [32, §9.1.3, Ex. 1]). Since G is generated by squares, it follows that $\widetilde{G}$ embeds into GL_2 as a lift of $G \hookrightarrow \mathrm{PGL}_2$. Alternatively, the lifts $\frac{1}{2}R$ and $\frac{1}{2}S'$ generate $\widetilde{A_4}$ inside GL_2, while $\frac{1}{2}R$ and $\frac{1}{2}U$ generate $\widetilde{A_5}$ inside GL_2. (Here, R, S' and U are as defined in 3.10.) This fact implies the following result.

Proposition 4.18. *Suppose that $-1 = a^2 + b^2$ for $a, b \in k$, and $\sqrt{5} \in k$ if $G = A_5$. Then the HLP given by $G \hookrightarrow \mathrm{PGL}_2$ and* (4.3) *is solvable.*

Proof. The proof follows immediately from Proposition 4.3. □

Remark 4.19. It is not hard to see that any homomorphism $\widetilde{A_n} \to \mu(k)$ $(n = 4, 5)$ must be trivial on μ_2. Indeed, this follows from the well known fact that μ_2 is contained in the commutator subgroup $[\widetilde{A_n}, \widetilde{A_n}]$.

4.4.2 Symmetric group on 4 letters

In this subsection, we assume that $G = S_4$. Recall that $H^2(S_4, \mu_2) = \mu_2^2$ (see [5, Lemma 4.1]), which gives rise to three non-split central extensions of S_4 by μ_2. As we did in the case of even dihedral groups, we label the exact sequences by their corresponding element of $H^2(S_4, \mu_2)$. Select generators r, s of S_4 satisfying $r^3 = s^4 = (r^{-1}s)^2 = 1$, and pick respective lifts r', s' of r, s to G' (changing r' by $-r'$ if necessary, we assume without loss of generality that $r'^3 = 1$). Then, the extensions are parametrized by the nontrivial pairs $(\epsilon_1, \epsilon_2) \in \mu_2^2$ via the relations $s'^4 = \epsilon_1$, $(r'^{-1}s')^2 = \epsilon_2$. The different cases are outlined below.

(i) The pair $(1, -1)$ corresponds to the group $\overline{S_4}$, which is the only nontrivial extension of S_4 by μ_2 that restricts to the trivial extension of A_4 by μ_2. (This group is denoted by S_4' in [32, §9.1.3].) The transpositions (resp. products of disjoint transpositions) lift to elements of order 4 (resp. 2) in $\overline{S_4}$. It is isomorphic to the pull-back $S_4 \curlywedge \mathbb{Z}/4\mathbb{Z} = S_4 \times_{(\chi, g)} \mathbb{Z}/4\mathbb{Z}$, where $\chi\colon S_4 \to \mathbb{Z}/2\mathbb{Z}$ is the sign character and $g\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ has kernel $\mathbb{Z}/2\mathbb{Z}$. Its Sylow 2-subgroups are thus isomorphic to V_{16}.

(ii) The pair $(-1, 1)$ case corresponds to the group $\widetilde{S_4}$, which is isomorphic to $\mathrm{GL}_2(\mathbb{F}_3)$ (see [32, §9.1.3, Ex. 2(a)]). The transpositions (resp. products of disjoint transpositions) lift to elements of order 2 (resp. 4) in $\widetilde{S_4}$. Its Sylow 2-subgroups are isomorphic to SD_{16}.

(iii) The pair $(-1, -1)$ corresponds to the group $\widehat{S_4}$, which is also known as the binary octahedral group. Both transpositions and the products of disjoint transpositions lift to elements of order 4 in $\widehat{S_4}$. Its Sylow 2-subgroups are isomorphic to Dic_{16}.

Proposition 4.20. *Let $1 \to \mu_2 \to G' \to G \to 1$ be the exact sequence (ϵ_1, ϵ_2), $\epsilon_i = \pm 1$, $(\epsilon_1, \epsilon_2) \neq (1, 1)$. Then there exists a homomorphism $G' \to \mu(k)$ nontrivial on μ_2 if and only if $(\epsilon_1, \epsilon_2) = (1, -1)$ and $-1 \in k^{\times 2}$.*

Proof. We claim that if $(\epsilon_1, \epsilon_2) = (-1, \pm 1)$, such a homomorphism does not exist. Indeed, in that case G' contains $\widetilde{A_4}$ as a subgroup of index 2, so the claim follows by Remark 4.19.

If $(\epsilon_1, \epsilon_2) = (1, -1)$, G' is generated by r', s' such that $r'^3 = 1$, $s'^4 = 1$ and $(r'^{-1}s')^2 = -1$. The latter relation implies that $-1 \in k^{\times 2}$ is a necessary condition for the desired homomorphism to exist. Conversely, $r' \mapsto 1, s' \mapsto \omega_4$ satisfies the required properties if $-1 \in k^{\times 2}$. □

Proposition 4.21. *Let $1 \to \mu_2 \to G' \to G \to 1$ be the exact sequence (ϵ_1, ϵ_2), $\epsilon_i = \pm 1$, $(\epsilon_1, \epsilon_2) \neq (1, 1)$. Then there exists $G' \hookrightarrow \mathrm{GL}_2$ lifting the prescribed embedding $G \hookrightarrow \mathrm{PGL}_2$ if and only if $\epsilon_1 = -1$ and $-2\epsilon_2 \in k^{\times 2}$.*

Proof. Let

$$\widetilde{R} = \lambda \begin{pmatrix} a-b-1 & a+b+1 \\ a+b-1 & b-a-1 \end{pmatrix}, \quad \widetilde{S} = \mu \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

be lifts of R and S to GL_2, respectively. A computation shows that $\widetilde{R}^3 = 8\lambda^3 I$, $\widetilde{S}^4 = -4\mu^4 I$ and $(\widetilde{R}^{-1}\widetilde{S})^2 = -(2\lambda^2)^{-1}\mu^2 I$. Hence, a lift $G' \hookrightarrow \mathrm{GL}_2$ is possible if and only if we can find $\lambda, \mu \in k$ such that

$$8\lambda^3 = 1, \quad -4\mu^4 = \epsilon_1, \quad -(2\lambda^2)^{-1}\mu^2 = \epsilon_2.$$

Assume first that λ and μ exist. From the first equation, $\lambda = \zeta_3/2$ for some third root of unity ζ_3. Squaring the last equation, we obtain $1 = \epsilon_2^2 = (\zeta_3/4)^{-1}\mu^4 = (\zeta_3/4)^{-1}(-\epsilon_1/4) = -\epsilon_1/\zeta_3$. It follows easily that $\epsilon_1 = -1$ and $\zeta_3 = 1$. The last equation then becomes $\mu^2 = -\epsilon_2/2$, which implies that $-2\epsilon_2 \in k^{\times 2}$.

Conversely, if we assume $\epsilon_1 = -1$ and $-2\epsilon_2 \in k^{\times 2}$, it suffices to take $\lambda = 1/2$ and $\mu = (-2\epsilon_2)^{1/2}/2$. The proof is complete. □

Proposition 4.22. *Suppose that $-1 = a^2 + b^2$ for $a, b \in k$. Then the HLP given by $G \hookrightarrow \mathrm{PGL}_2$ and the exact sequence (ϵ_1, ϵ_2) is solvable if and only if one of the following conditions holds:*

(a) $(\epsilon_1, \epsilon_2) = (1, -1)$ *and* $-1 \in k^{\times 2}$.

(b) $(\epsilon_1, \epsilon_2) = (-1, \pm 1)$ *and* $-2\epsilon_2 \in k^{\times 2}$.

Proof. This follows immediately from Propositions 4.3, 4.20 and 4.21. □

4.5 Explicit solutions to the HLP

Suppose that the HLP given by an embedding $G \hookrightarrow \mathrm{PGL}_2$ and a non-split extension $1 \to \mu_2 \to G' \to G \to 1$ is solvable. Recall that the complete family of solutions to this HLP is the set of hyperelliptic curves with function field of the form $k(x)(\sqrt{r\omega(x)})$, for some fixed separable polynomial $\omega(x) \in k[x]$ and $r \in k(t)^\times$ arbitrary (see the proof of Proposition 4.3).

In this section, we compile the solutions to the HLP's that we studied earlier. Note that it suffices to indicate $\omega(x)$, so that is exactly what we will do.

With the aid of the following lemma, we can compute the group actions on the explicit solutions to the HLP's.

Lemma 4.23. *Let σ be an element of order $n \geq 2$ in $\mathrm{PGL}_2(k)$, fix a lift $\widetilde{\sigma} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$ of σ, and let $\mu_1, \mu_2 \in \overline{k}$ be its eigenvalues. Consider the polynomial $Q(x,y) = \prod_{i=0}^{n-1} (y_i x - x_i y) \in k(x_0, y_0)[x,y]$, where x_0, y_0 are indeterminates and $(x_i : y_i) = \sigma^i(x_0 : y_0)$ for $i = 0, \ldots, n-1$. Then we have*

$$Q(ax+by, cx+dy) = \mu_1^n Q(x,y) = \mu_2^n Q(x,y).$$

Proof. Note first that $\mu_1^n = \mu_2^n$, since σ has order n in $\mathrm{PGL}_2(k)$. This proves the second equality.

The homogeneous forms $Q(ax+by, cx+dy)$ and $Q(x,y)$ have the same roots, namely $(x_i : y_i)$ for $0 \leq i \leq n-1$. Hence they differ by a constant factor, which *a priori* could depend on x_0, y_0. Let $(u,v)^T$ be an eigenvector of $\widetilde{\sigma}$, say corresponding to the eigenvalue μ_1. Then $Q(au+bv, cu+dv) = Q(\mu_1 u, \mu_1 v) = \mu_1^n Q(u,v)$. It follows that the constant factor equals $\mu_1^n = \mu_2^n$, independently of x_0, y_0. □

Definition 4.24. Given $z \in \mathbb{P}^1(\overline{k})$, we denote its orbit under G by $\mathcal{O}_z$. Then we define the *orbit polynomial* $P_z \in \overline{k}[x]$ as follows:

$$P_z(x) = \prod_{z' \in \mathcal{O}_z - \{\infty\}} (x - z'),$$

and we write $Q_z = P_z^{|G|/|\mathcal{O}_z|}$. (Note that $\deg Q_z = |G|(1 - 1/|\mathcal{O}_\infty|)$ if $\mathcal{O}_z = \mathcal{O}_\infty$, and $\deg Q_z = |G|$ otherwise.) If P_z (or equivalently Q_z) has coefficients in k, we say that $\mathcal{O}_z$ is a k-rational orbit. This is the case if and only if $\mathrm{Gal}(\overline{k}/k)\mathcal{O}_z = \mathcal{O}_z$.

Proposition 4.25. *Let $\sigma \in G$ be an element of order $n \geq 2$ and select a lift $\widetilde{\sigma} \in \mathrm{GL}_2(k)$ as in Lemma 4.23. Define $U = \{l \in \mathcal{O}_z : \sigma l = l\}$. If $l \in U$, we denote the eigenvalue of $\widetilde{\sigma}$ corresponding to any lift of l by μ_l, and we denote the other eigenvalue by μ_l'. Then we have the equality*

$$P_z(\sigma(x)) = \prod_{l \in U} \mu_l' \frac{\mu_1^{|\mathcal{O}_z|-|U|}}{(cx+d)^{|\mathcal{O}_z|}} P_z(x).$$

Proof. Let S be the stabilizer of z in G and for every $gS \in G/S$, write $gz = (x_g : y_g) \in \mathbb{P}^1(\overline{k})$. We may assume that $y_g = 1$ if $gz \neq \infty$ and $x_g = -1, y_g = 0$ when $gz = \infty$. Define the following homogenization of P_z:

$$\overline{P_z}(x,y) = \prod_{gS \in G/S} (y_g x - x_g y) \in \overline{k}[x,y].$$

Note that we can recover $P_z(x) = \overline{P_z}(x,1)$.

Let g be any element of G. We claim that either $\sigma gz = gz$, or $\sigma^i gz \neq \sigma^j gz$ for every $0 \leq i < j < n$. Assume to the contrary that $\sigma gz \neq gz$, but $\sigma^{i_0} gz = \sigma^{j_0} gz$ for some $0 \leq i_0 < j_0 < n$. If we write $m = j_0 - i_0$, it follows that $\sigma^m gz = gz$, where $0 < m < n$. However, note that σ has exactly two distinct fixed points in $\mathbb{P}^1(\overline{k})$ (corresponding to eigenvectors of $\widetilde{\sigma}$), which are therefore fixed points of σ^m as well. Since σ^m has at most two fixed points, we conclude that $\sigma gz = gz$, in contradiction with our assumption.

Let $F \subset G$ be a set of representatives of classes $gS \in G/S$ such that $gz \in U$ $(0 \leq |F| \leq 2)$. By the claim above, we can express

$$G/S = \coprod_{g \in F} gS \ \sqcup \coprod_{i=1}^{s} \coprod_{j=0}^{n-1} \sigma^j g_i S,$$

for some $g_1, \ldots, g_s$ in G. A convenient way to think about these elements is by noting that $F \sqcup \{g_1, \ldots, g_s\}$ is a set of representatives for $\langle\sigma\rangle \backslash G/S$. If we define $Q_j(x,y) = \prod_{i=0}^{n-1} (y_{\sigma^i g_j} x - x_{\sigma^i g_j} y)$, we can then write

$$\overline{P_z}(x,y) = \prod_{g \in F} (y_g x - x_g y) \prod_{j=1}^{s} Q_j(x,y).$$

By Lemma 4.23, we have that $Q_j(ax+by, cx+dy) = \mu_1^n Q_j(x,y)$. On the other hand, if $g \in F$, then $gz = (x_g : y_g)$ is fixed by σ by assumption and the lift $(x_g, y_g)^T$ of gz is an eigenvector of $\widetilde{\sigma}$ with eigenvalue μ_{gz}. It follows

that $ax_g + by_g = \mu_{gz} x_g$ and $cx_g + dy_g = \mu_{gz} y_g$. We now compute

$$\begin{aligned} y_g(ax+by) - x_g(cx+dy) &= (ay_g - cx_g)x - (dx_g - by_g)y \\ &= (a + d - \mu_{gz})(y_g x - x_g y) \\ &= \mu'_{gz}(y_g x - x_g y). \end{aligned}$$

We thus obtain the equality

$$\overline{P_z}(ax+by, cx+dy) = \prod_{g \in F} \mu'_{gz}\, \mu_1^{ns}\, \overline{P_z}(x,y) = \prod_{l \in U} \mu'_l\, \mu_1^{|\mathcal{O}_z|-|U|}\, \overline{P_z}(x,y).$$

It follows that

$$\begin{aligned} P_z(\sigma(x)) &= \frac{1}{(cx+d)^{|\mathcal{O}_z|}} \overline{P_z}(ax+b, cx+d) \\ &= \prod_{l \in U} \mu'_l\, \frac{\mu_1^{|\mathcal{O}_z|-|U|}}{(cx+d)^{|\mathcal{O}_z|}} \overline{P_z}(x,1) \\ &= \prod_{l \in U} \mu'_l\, \frac{\mu_1^{|\mathcal{O}_z|-|U|}}{(cx+d)^{|\mathcal{O}_z|}} P_z(x). \end{aligned}$$

□

Corollary 4.26. *Let $\sigma \in G$ and select a lift $\widetilde{\sigma} \in \mathrm{GL}_2(k)$ as in Lemma 4.23. Then*

$$Q_z(\sigma x) = \frac{\mu_1^{|G|}}{(cx+d)^{|G|}} Q_z(x).$$

Proof. The result is obvious if σ is the identity in G, so we may assume henceforth that σ has order $n \geq 2$. Using the notation from Proposition 4.25, we compute

$$Q_z(\sigma x) = \prod_{l \in U} {\mu'_l}^{\frac{|G|}{|\mathcal{O}_z|}}\, \frac{\mu_1^{|G|-|U|\frac{|G|}{|\mathcal{O}_z|}}}{(cx+d)^{|G|}} Q_z(x).$$

Hence it suffices to prove that

$$\prod_{l \in U} {\mu'_l}^{\frac{|G|}{|\mathcal{O}_z|}} = \mu_1^{|U|\frac{|G|}{|\mathcal{O}_z|}}.$$

If $|U| = 0$, there is nothing to prove. If $|U| = 1$ or 2, it means that $\mathcal{O}_z$ contains an element l fixed by σ. Consequently, $\langle \sigma \rangle$ is a subgroup of $\mathrm{Stab}(l)$ and therefore, n divides $|\mathrm{Stab}(x)| = |G|/|\mathcal{O}_z|$. Thus $\mu_1^{\frac{|G|}{|\mathcal{O}_z|}} = \mu_2^{\frac{|G|}{|\mathcal{O}_z|}}$ and the result follows. □

Corollary 4.27. *The fixed field $k(x)^G$ is equal to the rational field $k(t)$, where $t = Q_z(x)/Q_\infty(x)$ for any k-rational orbit $\mathcal{O}_z \neq \mathcal{O}_\infty$.*

Proof. Since x is a root of the polynomial $Q_z(x) - tQ_\infty(x)$, which is a monic polynomial of degree $|G|$, it follows that $[k(x) : k(t)] \leq |G|$. Since $[k(x) : k(x)^G] = |G|$, it suffices to prove that $k(t) \subset k(x)^G$. To see this, consider an arbitrary element σ in G. By Corollary 4.26, it follows that

$$\sigma t = Q_z(\sigma x)/Q_\infty(\sigma x) = Q_z(x)/Q_\infty(x) = t.$$

Since σ is arbitrary, this completes the proof of the corollary. □

We use the notation we have introduced in this section to produce explicit solutions to the HLP's we already studied. In every case, we describe the action of G' on $k(x)[y]/(y^2 - \omega(x))$.

4.5.1 Extensions of cyclic groups

In this subsection, we exhibit the solutions for the HLP given by an extension of cyclic groups.

Extension (4.1)**:** $1 \to \mu_2 \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 1$.

Embedding: $\rho_a \colon \mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{PGL}_2$, where $a \in k^\times$ (see (3.1)).

Conditions for solvability of the HLP: Either $-a \in k^{\times 2}$ or $-1 \in k^{\times 2}$ (see Proposition 4.7).

Solutions:

Condition	ω	Generator of $\mathbb{Z}/4\mathbb{Z}$
$-a \in k^{\times 2}$	$x^2 - a$	$(x, y) \mapsto \left(\frac{a}{x}, \frac{\sqrt{-a}}{x} y\right)$
$-1 \in k^{\times 2}$	$x(x^2 - a)$	$(x, y) \mapsto \left(\frac{a}{x}, \frac{\omega_4 a}{x^2} y\right)$

Example 4.28. We illustrate here how to compute different solutions to the HLP above. Assume we are dealing with the case where $-1 \in k^{\times 2}$. Note that the equation $y^2 = x(x^2 - a)$ defines a curve of genus 1, which is therefore not a solution to the HLP. However, we are free to modify the right hand side by an element $r \in k(t)^\times$. Using Corollary 4.27, we may take $t = (x^2 + a)/x$. Choosing, say, $r = t(t + 1)$, we obtain a hyperelliptic curve with equation

$$y^2 = x(x^4 - a^2)(x^2 + x + a),$$

which is a solution to the above HLP. The $\mathbb{Z}/4\mathbb{Z}$-action is given by

$$\sigma' \colon (x, y) \mapsto \left(\frac{a}{x}, \frac{\omega_4 a^2}{x^4} y\right).$$

We now switch our attention to the case $n \geq 4$ (n even) and let k contain α_n. Assume that $\rho\colon \mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathrm{PGL}_2$ is defined as in (3.5). The orbits of the elements $\pm\sqrt{\beta_n}$ are singletons and hence $P_{\pm\sqrt{\beta_n}}(x) = x \mp \sqrt{\beta_n}$. On the other hand, $|\mathcal{O}_\infty| = n$. By Proposition 4.25, we may compute

$$P_{\sqrt{\beta_n}}(\sigma(x))P_{-\sqrt{\beta_n}}(\sigma(x)) = \frac{2\alpha_n + 2}{(x+\alpha_n+1)^2} P_{\sqrt{\beta_n}}(x)P_{-\sqrt{\beta_n}}(x)$$

and

$$P_\infty(\sigma(x)) = -\frac{(2\alpha_n+2)^{\frac{n}{2}}}{(x+\alpha_n+1)^n} P_\infty(x).$$

Extension (4.1)**:** $1 \to \mu_2 \to \mathbb{Z}/2n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 1$.
Conditions for solvability of the HLP: See Propositions 4.9 and 4.10.
Solutions:

Condition	ω	Generator of $\mathbb{Z}/2n\mathbb{Z}$
$\alpha_{2n} \in k$	$x^2 - \beta_n$	$(x,y) \mapsto \left(\sigma(x), \frac{2\alpha_{2n}}{x+\alpha_n+1} y\right)$
$\omega_4\alpha_{2n} \in k$	$(x^2-\beta_n)P_\infty(x)$	$(x,y) \mapsto \left(\sigma(x), \frac{2\omega_4\alpha_{2n}(2\alpha_n+2)^{\frac{n}{4}}}{(x+\alpha_n+1)^{\frac{n+2}{2}}} y\right)$
$-1 \in k^{\times 2}$	$(x^2-\beta_n)P_\infty(x)$	$(x,y) \mapsto \left(\sigma(x), \frac{\omega_4(2\alpha_n+2)^{\frac{n+2}{4}}}{(x+\alpha_n+1)^{\frac{n+2}{2}}} y\right)$

In the second (resp. third) row above, we assume that $n \equiv 0$ (4) (resp. $n \equiv 2$ (4)). In each case, note that the $\mathbb{Z}/2n\mathbb{Z}$-action is defined over k.

4.5.2 Extensions of the Klein group

We turn our attention to the HLP for extensions of $(\mathbb{Z}/2\mathbb{Z})^2$ by μ_2. In this subsection, we always consider one of the embeddings $\rho_{(a,b)}\colon (\mathbb{Z}/2\mathbb{Z})^2 \hookrightarrow \mathrm{PGL}_2$ that we specified in (3.2), (3.3) and (3.4). In every case, it is not hard to see that we can choose respective lifts

$$\widetilde{e_1} = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \quad \widetilde{e_2} = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

of $\rho_{(a,b)}(e_1)$, $\rho_{(a,b)}(e_2)$, such that $\widetilde{e_1}$ has eigenvalues $\pm\sqrt{b}$, $\widetilde{e_2}$ has eigenvalues $\pm\sqrt{a}$, and $\widetilde{e_1}\widetilde{e_2}$ has eigenvalues $\pm\sqrt{-ab}$.

Let P_1 (resp. P_2, resp. P_3) be the orbit polynomial of the solutions of $e_1 z = z$ (resp. $e_2 z = z$, resp. $e_1 e_2 z = z$), which lie in the same orbit. For example, if both a and b are non-squares (cf. (3.2)), we have $P_1(x) =$

$x^2 - 2\lambda x + a$, $P_2(x) = x^2 - a$, and $P_3(x) = x^2 - 2\frac{a}{\lambda}x + a$ if $\lambda \neq 0$ (resp. $P_3(x) = x$ if $\lambda = 0$). By Proposition 4.25, we can compute

$$\begin{aligned} P_1(e_1(x)) &= \frac{-bP_1(x)}{(c_1x+d_1)^2}, \quad P_1(e_2(x)) = \frac{aP_1(x)}{(c_2x+d_2)^2}, \\ P_2(e_1(x)) &= \frac{bP_2(x)}{(c_1x+d_1)^2}, \quad P_2(e_2(x)) = \frac{-aP_2(x)}{(c_2x+d_2)^2}, \\ P_3(e_1(x)) &= \frac{bP_3(x)}{(c_1x+d_1)^2}, \quad P_3(e_2(x)) = \frac{aP_3(x)}{(c_2x+d_2)^2}. \end{aligned}$$

Extension $(\epsilon_1, \epsilon_2, \epsilon_3)$**:** $1 \to \mu_2 \to G' \to (\mathbb{Z}/2\mathbb{Z})^2 \to 1$.

Conditions for solvability of the HLP: Either $\epsilon_1\epsilon_2\epsilon_3 = 1$ and $-1 \in k^{\times 2}$, or $\epsilon_1\epsilon_2\epsilon_3 = -1$ and $\epsilon_1 b, \epsilon_2 a \in k^{\times 2}$ (see Proposition 4.14).

Solution: Let $\eta_i = \frac{1-\epsilon_i}{2}$ for $i = 1, 2, 3$; i.e., $\eta_i = 1$ if $\epsilon_i = -1$, and $\eta_i = 0$ if $\epsilon_i = 1$. Then we can take

$$\omega(x) = P_1(x)^{\eta_1} P_2(x)^{\eta_2} P_3(x)^{\eta_3}.$$

The G'-action on $k(x)[y]/(y^2 - \omega(x))$ is generated by

$$\sigma' \colon (x, y) \mapsto \left(e_1(x), \frac{(-1)^{\frac{\eta_1}{2}} b^{\frac{\eta_1+\eta_2+\eta_3}{2}}}{(c_1x+d_1)^{\eta_1+\eta_2+\eta_3}} y \right)$$

and

$$\tau' \colon (x, y) \mapsto \left(e_2(x), \frac{(-1)^{\frac{\eta_2}{2}} a^{\frac{\eta_1+\eta_2+\eta_3}{2}}}{(c_2x+d_2)^{\eta_1+\eta_2+\eta_3}} y \right).$$

An easy computation shows that $\sigma'^2 = \epsilon_1$, $\tau'^2 = \epsilon_2$ and $(\sigma'\tau')^2 = \epsilon_3$. To prove that σ' and τ' are defined over k, it suffices to prove that the numerators of the coefficients of y in each map belong to k. We consider both sets of conditions for solvability separately:

Case $\epsilon_1\epsilon_2\epsilon_3 = 1$ and $-1 \in k^{\times 2}$: In this case, we have $\frac{\eta_1+\eta_2+\eta_3}{2} = 1$. Thus, the numerators are $(-1)^{\frac{\eta_1}{2}} b$ and $(-1)^{\frac{\eta_2}{2}} a$, which belong to k.

Case $\epsilon_1\epsilon_2\epsilon_3 = -1$ and $\epsilon_1 b, \epsilon_2 a \in k^{\times 2}$: In this situation, a computation shows that $(-1)^{\frac{\eta_1}{2}} b^{\frac{\eta_1+\eta_2+\eta_3}{2}} = (\epsilon_1 b)^{\frac{1}{2}} b^{\eta_2\eta_3}$ and $(-1)^{\frac{\eta_2}{2}} a^{\frac{\eta_1+\eta_2+\eta_3}{2}} = (\epsilon_2 a)^{\frac{1}{2}} a^{\eta_1\eta_3}$.

4.5.3 Extensions of dihedral groups

In this subsection, we let k be a base field containing α_n, where $n \geq 3$, and define $\rho_a \colon D_{2n} \hookrightarrow \mathrm{PGL}_2$ as in (3.6).

The solutions $\pm\sqrt{\beta_n}$ to $\sigma z = z$ form a two element orbit $\mathcal{O}_1$ permuted by τ, with orbit polynomial $P_1(x) = x^2 - \beta_n$. If n is odd, the orbits of the solutions of $\tau z = z$ are disjoint and each one contains a solution of $\sigma\tau z = z$; we denote them by $\mathcal{O}_2$ and $\mathcal{O}_3$. (Note that these orbits are not necessarily k-rational, but $\mathcal{O}_2 \cup \mathcal{O}_3$ is $\mathrm{Gal}(\overline{k}/k)$-stable.) If n is even, both solutions of $\tau z = z$ (resp. $\sigma\tau z = z$) lie in the same orbit, which we denote by $\mathcal{O}_2$ (resp. $\mathcal{O}_3$). (In particular, this implies that $\mathcal{O}_2$ and $\mathcal{O}_3$ are k-rational for n even.) We denote the corresponding orbit polynomials by P_2 and P_3. For convenience, we define P_4 to be the orbit polynomial of any fixed k-rational orbit of cardinality $|G|$. (Note that $\mathcal{O}_\infty$ may not satisfy this condition). Using Proposition 4.25, we compute

$$\begin{aligned}
P_1(\sigma(x)) &= \frac{(2\alpha_n+2)P_1(x)}{(x+\alpha_n+1)^2}, \quad P_1(\tau(x)) = \frac{aP_1(x)}{(vx-u)^2},\\
P_2(\sigma(x)) &= \frac{-(2\alpha_n+2)^{\frac{n}{2}}P_2(x)}{(x+\alpha_n+1)^n}, \quad P_2(\tau(x)) = \frac{-a^{\frac{n}{2}}P_2(x)}{(vx-u)^n},\\
P_3(\sigma(x)) &= \frac{-(2\alpha_n+2)^{\frac{n}{2}}P_3(x)}{(x+\alpha_n+1)^n}, \quad P_3(\tau(x)) = \frac{a^{\frac{n}{2}}P_3(x)}{(vx-u)^n},\\
P_4(\sigma(x)) &= \frac{(2\alpha_n+2)^n P_4(x)}{(x+\alpha_n+1)^{2n}}, \quad P_4(\tau(x)) = \frac{a^n P_4(x)}{(vx-u)^{2n}}.
\end{aligned}$$

We first deal with the unique nontrivial extension of odd dihedral groups.

Extension (4.2)**:** $1 \to \mu_2 \to Dic_{4n} \to D_{2n} \to 1$, where n is odd.

Conditions for solvability of the HLP: Either $-1 \in k^{\times 2}$, or $-a \in k^{\times 2}$ (see Proposition 4.16).

Solutions:

Condition	ω	Generators of Dic_{4n}
$-1 \in k^{\times 2}$	$\prod_{i=1}^{3} P_i(x)$	$\sigma'\colon (x,y) \mapsto \left(\sigma(x), \frac{(2\alpha_{2n})^{n+1}}{(x+\alpha_n+1)^{n+1}}y\right)$ $\tau'\colon (x,y) \mapsto \left(\tau(x), \frac{\omega_4 a^{\frac{n+1}{2}}}{(vx-u)^{n+1}}y\right)$
$-a \in k^{\times 2}$	$\prod_{i=1}^{4} P_i(x)$	$\sigma'\colon (x,y) \mapsto \left(\sigma(x), \frac{(2\alpha_{2n})^{2n+1}}{(x+\alpha_n+1)^{2n+1}}y\right)$ $\tau'\colon (x,y) \mapsto \left(\tau(x), \frac{(\sqrt{-a})^{2n+1}}{(vx-u)^{2n+1}}y\right)$

Recall that if n is odd, then $\alpha_n \in k$ implies that $\alpha_{2n} \in k$ by Lemma 2.2 (b), so σ' and τ' are defined over k. On the other hand, a simple computation shows that $\sigma'^n = \tau'^2 = (\sigma'\tau')^2 = -1$.

Extension $(\epsilon_1, \epsilon_2, \epsilon_3)$**:** $1 \to \mu_2 \to G' \to D_{2n} \to 1$, where n is even.

Conditions for solvability of the HLP: Either $\epsilon_1 = (\epsilon_2\epsilon_3)^{n/2}$ and $-1 \in k^{\times 2}$, or $\epsilon_1 = -(\epsilon_2\epsilon_3)^{n/2}$, $\epsilon_2 a \in k^{\times 2}$, and $(\epsilon_2\epsilon_3)^{1/2}\alpha_{2n} \in k$. (see Proposition 4.17).

Solution: As before, define $\eta_i = \frac{1-\epsilon_i}{2}$ for $i = 1, 2, 3$, and choose

$$\omega(x) = P_1(x)^{\eta_1} P_2(x)^{\eta_2} P_3(x)^{\eta_3}.$$

The G'-action on $k(x)[y]/(y^2 - \omega(x))$ is then generated by

$$\sigma' \colon (x, y) \mapsto \left(\sigma(x), \frac{(-1)^{\frac{\eta_2+\eta_3}{2}} (2\alpha_n + 2)^{\frac{\eta_1}{2} + \frac{n(\eta_2+\eta_3)}{4}}}{(x + \alpha_n + 1)^{\eta_1 + \frac{n(\eta_2+\eta_3)}{2}}} y \right)$$

and

$$\tau' \colon (x, y) \mapsto \left(\tau(x), \frac{(-1)^{\frac{\eta_2}{2}} a^{\frac{\eta_1}{2} + \frac{n(\eta_2+\eta_3)}{4}}}{(vx - u)^{\eta_1 + \frac{n(\eta_2+\eta_3)}{2}}} y \right).$$

A computation shows that $\sigma'^n = \epsilon_1$, $\tau'^2 = \epsilon_2$ and $(\sigma'\tau')^2 = \epsilon_3$. We need to show that σ' and τ' are defined over k. Again, we separate the proof into two cases:

Case $\epsilon_1 = (\epsilon_2\epsilon_3)^{n/2}$ and $-1 \in k^{\times 2}$: In this case, it is not hard to see that $N = \frac{\eta_1}{2} + \frac{n(\eta_2+\eta_3)}{4}$ is an integer. Therefore, the numerators $(-1)^{\frac{\eta_2+\eta_3}{2}}(2\alpha_n + 2)^N$ and $(-1)^{\frac{\eta_2}{2}} a^N$ belong to k by our assumption $-1 \in k^{\times 2}$.

Case $\epsilon_1 = -(\epsilon_2\epsilon_3)^{n/2}$, $\epsilon_2 a \in k^{\times 2}$, and $(\epsilon_2\epsilon_3)^{1/2}\alpha_{2n} \in k$: In this situation, it is not hard to verify that we can write

$$(-1)^{\frac{\eta_2+\eta_3}{2}} (2\alpha_n + 2)^{\frac{\eta_1}{2} + \frac{n(\eta_2+\eta_3)}{4}} = 2(-1)^{\eta_2\eta_3} (\epsilon_2\epsilon_3)^{\frac{1}{2}} \alpha_{2n} (2\alpha_n + 2)^{\frac{\eta_1 - 1}{2} + \frac{n(\eta_2+\eta_3)}{4}}$$

and

$$(-1)^{\frac{\eta_2}{2}} a^{\frac{\eta_1}{2} + \frac{n(\eta_2+\eta_3)}{4}} = (\epsilon_2 a)^{\frac{1}{2}} a^{\frac{\eta_1 - 1}{2} + \frac{n(\eta_2+\eta_3)}{4}}.$$

Moreover, note that $\epsilon_1 = -(\epsilon_2\epsilon_3)^{n/2}$ implies that $\frac{\eta_1 - 1}{2} + \frac{n(\eta_2+\eta_3)}{4}$ is an integer.

4.5.4 Extensions of polyhedral groups

Recall that polyhedral groups have three orbits $\mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3$ of order $< |G|$, which correspond to the vertices, faces and edges of the corresponding Platonic solids. The sizes of the orbits are detailed below.

G	$\lvert\mathcal{O}_1\rvert$	$\lvert\mathcal{O}_2\rvert$	$\lvert\mathcal{O}_3\rvert$
A_4	4	4	6
S_4	6	8	12
A_5	12	20	30

We denote the corresponding orbit polynomials by P_1, P_2, P_3. Applying $\mathrm{Gal}(\overline{k}/k)$ to an orbit yields another orbit of the same size, so it follows that the above orbits are all k-rational, except possibly for $\mathcal{O}_1$ and $\mathcal{O}_2$ if $G = A_4$. The computations of $P_i(\sigma(x))/P_i(x)$, where σ is a generator of G, can be carried out with the help of Proposition 4.25 as usual; we omit the details for the sake of brevity, but still describe the group actions derived from these computations.

In what follows, we will use the notation for the embeddings of polyhedral groups introduced in Proposition 3.10.

Extension (4.3)**:** $1 \to \mu_2 \to \widetilde{A_4} \to A_4 \to 1$.

Conditions for solvability of the HLP: Always solvable (see Proposition 4.18).

Solution:

ω	Generators of $\widetilde{A_4}$
$P_3(x)$	$r\colon (x,y) \mapsto \left(R(x), \frac{8}{((a+b-1)x+b-a-1)^3}y\right)$ $s'\colon (x,y) \mapsto \left(-\frac{1}{x}, \frac{y}{x^3}\right)$

Extension (4.3)**:** $1 \to \mu_2 \to \widetilde{A_5} \to A_5 \to 1$.

Conditions for solvability of the HLP: Always solvable (see Proposition 4.18).

Solution:

ω	Generators of $\widetilde{A_5}$
$P_3(x)$	$r'\colon (x,y) \mapsto \left(R(x), \frac{32768}{((a+b-1)x+b-a-1)^{15}}y\right)$ $u\colon (x,y) \mapsto \left(U(x), \frac{32768}{((\phi b+1)x-\phi a+\phi^{-1})^{15}}y\right)$

Remark 4.29. If $G = A_4$, note that $P_3(x) = (x^2+1)(x^2+2\frac{b}{a}x-1)(x^2-2\frac{a}{b}x-1)$ if $a, b \neq 0$, while $P_3(x) = x(x^4-1)$ if $ab = 0$ (i.e., if $-1 \in k^{\times 2}$). The general expression of P_3 for the group A_5 is very cumbersome, so we decided to omit it.

Extension $(1,-1)$**:** $1 \to \mu_2 \to \overline{S_4} \to S_4 \to 1$.

Conditions for solvability of the HLP: $-1 \in k^{\times 2}$ (see Proposition 4.22).

Solution:

ω	Generators of $\overline{S_4}$
$P_3(x)$	$r'\colon (x,y) \mapsto \left(R(x), \frac{64}{((a+b-1)x+b-a-1)^6}y\right)$ $s'\colon (x,y) \mapsto \left(S(x), \frac{8\omega_4}{(-x+1)^6}y\right)$

Extension $(-1,1)$**:** $1 \to \mu_2 \to \widetilde{S_4} \to S_4 \to 1$.
Conditions for solvability of the HLP: $-2 \in k^{\times 2}$ (see Proposition 4.22).
Solution:

ω	Generators of $\widetilde{S_4}$
$P_1(x)$	$r'\colon (x,y) \mapsto \left(R(x), \frac{8}{((a+b-1)x+b-a-1)^3}y\right)$ $s'\colon (x,y) \mapsto \left(S(x), \frac{2\sqrt{-2}}{(-x+1)^3}y\right)$

Extension $(-1,-1)$**:** $1 \to \mu_2 \to \widehat{S_4} \to S_4 \to 1$.
Conditions for solvability of the HLP: $2 \in k^{\times 2}$ (see Proposition 4.22).
Solution:

ω	Generators of $\widehat{S_4}$
$P_1(x)P_3(x)$	$r'\colon (x,y) \mapsto \left(R(x), \frac{512}{((a+b-1)x+b-a-1)^9}y\right)$ $s'\colon (x,y) \mapsto \left(S(x), \frac{16\sqrt{2}}{(-x+1)^9}y\right)$

Remark 4.30. Note that $P_1(x) = (x^2+1)(x^2+2\frac{b}{a}x-1)(x^2-2\frac{a}{b}x-1)$ if $ab \neq 0$, while $P_1(x) = x(x^4-1)$ if $ab = 0$. We can also compute

$$P_3(x) = \left(x^4 + \frac{4ab}{a^2-1}x^3 + \frac{6b^2}{a^2-1}x^2 - \frac{4ab}{a^2-1}x + 1\right) \times \left(x^4 - \frac{4ab}{b^2-1}x^3 + \frac{6a^2}{b^2-1}x^2 + \frac{4ab}{b^2-1}x + 1\right) \times \left(x^4 + \frac{8ab}{a^2-b^2}x^3 - 6x^2 - \frac{8ab}{a^2-b^2}x + 1\right),$$

if $(a^2-1)(b^2-1)(a^2-b^2) \neq 0$. Note that the latter product can only vanish if $-2 \in k^{\times 2}$; in this case, we can take $a = b = 1/\sqrt{-2}$, which implies

$$P_3(x) = x\left(x^{10} + \frac{11}{9}x^8 + \frac{22}{3}x^6 - \frac{22}{3}x^4 - \frac{11}{9}x^2 - 1\right).$$

Chapter 5

Strongly incompressible curves

5.1 Rational quotients

As usual, a rational map $X \dashrightarrow Y$ of k-varieties is an equivalence class of k-morphisms $U \to Y$, where U is a dense open subset of X. We denote the algebra of rational functions of X by $k(X)$. In general, $k(X)$ is the direct sum of the function fields of the irreducible components of X.

An *algebraic group G over k* is a smooth affine group scheme of finite type over k. We say that X is a *G-variety* if G acts morphically on X. The inclusion $k(X)^G \hookrightarrow k(X)$ induces a *rational quotient map* $\pi_X \colon X \dashrightarrow W$, where $k(W) = k(X)^G$ (see [23, §2.3]). The variety W is denoted by X/G and is unique up to birational isomorphism. If N is a normal subgroup of G, there exists a model of X/N with a regular action of G/N (see [23, Remark 2.6]). It is uniquely defined up to G/N-equivariant birational isomorphism. A rational map $X \dashrightarrow Y$ of G-varieties gives rise to a G/N-equivariant rational map $\overline{f} \colon X/N \dashrightarrow Y/N$ such that $\overline{f} \circ \pi'_X = \pi'_Y \circ f$, where $\pi'_X \colon X \dashrightarrow X/N$ and $\pi'_Y \colon Y \dashrightarrow Y/N$ are the rational quotient maps.

A G-action on X is said to be *generically free* if there exists a dense G-invariant open subset of X with trivial scheme-theoretic stabilizers. (In particular, a faithful action of a finite group is generically free.) A *G-compression* is a G-equivariant dominant rational map $X \dashrightarrow Y$, where X and Y are generically free G-varieties. A generically free G-variety X contains a dense G-invariant open subset U which is the total space of a G-torsor $\pi_U \colon U \to U/G$ (see [3, Thm. 4.7]). We say that X is *primitive* if G transitively permutes the irreducible components of X (equivalently, if X/G is irreducible). Under this condition, the fiber at the generic point of U/G is a G-torsor $T \to \operatorname{Spec}(K)$, where $K \cong k(X)^G$. The class of this torsor in $H^1(K, G)$ will be denoted by $[X]$. Conversely, given a finitely generated field extension K of k, any class in $H^1(K, G)$ determines a generically free primitive G-variety X endowed with a k-isomorphism $k(X)^G \cong K$, uniquely

up to G-equivariant birational isomorphism. In what follows, we assume all G-varieties to be primitive, unless stated otherwise.

5.2 Strong incompressibility of curves

In the sequel, the word "curve" will be reserved for smooth projective geometrically irreducible varieties of dimension 1, unless stated otherwise.

Let G be a finite group. Recall that a faithful G-variety X is said to be strongly incompressible if any G-compression $X \dashrightarrow Y$ onto a faithful G-variety Y is birational. We are interested in the study of strong incompressibility of G-curves. We remark that the existence of strongly incompressible G-curves depends not only on the group G, but also on the base field k.

Note also that G-compressions of curves extend naturally to surjective finite G-equivariant morphisms, so we will regard G-compressions of curves as morphisms in the sequel. The following simple lemma is extremely useful in our analysis.

Lemma 5.1 (cf. [24, Example 6])**.** *Suppose that there exists a faithful G-curve X that cannot be G-compressed to any G-curve of genus ≤ 1. Then there exists a strongly incompressible G-curve.*

Proof. Consider the set S consisting of faithful G-curves Y such that there exists a G-compression $X \to Y$. By assumption, the genus $g(Y) \geq 2$ for all $Y \in S$. Select a curve $Y_0 \in S$ having minimal genus. We claim that Y_0 is strongly incompressible. Indeed, suppose that we have a G-compression $f\colon Y_0 \to Y'$, which implies that $Y' \in S$. In particular, we must have $g(Y') \geq g(Y_0) \geq 2$. However, by Hurwitz Formula (see [21, Thm 7.4.16]) it also follows that $g(Y_0) \geq g(Y')$, whence equality must hold. This implies that f is birational. □

The following result will be instrumental in the sequel. It is a special case of [27, Prop. 8.6] (see also [27, Rem. 9.9]), whose proof depends on resolution of singularities. We include an alternative proof because it works over any base field of characteristic 0, it is more elementary and, in particular, does not rely on resolution of singularities.

Theorem 5.2. *There exists a faithful G-curve X defined over k such that every element of G fixes some geometric point of X.*

Proof. See Appendix A. □

We now recall some facts about the automorphism group of an elliptic curve.

Lemma 5.3. *Let E be an elliptic curve defined over a field k.*

(a) *There exists a split exact sequence*

$$1 \longrightarrow E \xrightarrow{i} \mathrm{Aut}(E) \xrightarrow{\pi} \mathrm{Aut}_0(E) \longrightarrow 1\ , \tag{5.1}$$

where E acts on itself by translations and $\mathrm{Aut}_0(E)$ denotes the group of automorphisms of E that preserve the origin.

(b) *There exists a natural isomorphism $\mathrm{Aut}_0(E) \cong \mu_n$, where*

$$n = \begin{cases} 2, & \text{if } j(E) \neq 0, 1728; \\ 4, & \text{if } j(E) = 1728; \\ 6, & \text{if } j(E) = 0. \end{cases}$$

(c) *If $j(E) = 1728$ (resp. 0), we have $\mathrm{Aut}_0(E)(k) = \mathbb{Z}/4\mathbb{Z}$ (resp. $\mathbb{Z}/6\mathbb{Z}$) if and only if $\omega_4 \in k$ (resp. $\omega_3 \in k$).*

(d) *The translation by $P_0 \in E$ and the automorphism $\alpha \in \mathrm{Aut}_0(E)$ commute if and only if $\alpha(P_0) = P_0$.*

Proof. (a) See, e.g., [34, §X.5]. Note that in [34], $\mathrm{Aut}(E)$ and $\mathrm{Aut}_0(E)$ are denoted by $\mathrm{Isom}(E)$ and $\mathrm{Aut}(E)$, respectively.

(b) See [34, Cor. III.10.2].

(c) This follows directly from part (c).

(d) Let τ_{P_0} denote the translation by P_0. Then note that τ_{P_0} and α commute if and only if $\alpha(P) + \alpha(P_0) = \alpha \circ \tau_{P_0}(P) = \tau_{P_0} \circ \alpha(P) = \alpha(P) + P_0$ for all $P \in E$, which implies the desired result. □

Theorem 5.4. *Suppose that G cannot act faithfully on a curve of genus 0 via k-morphisms. Then there exists a strongly incompressible G-curve.*

Proof. By Lemma 5.1, it suffices to prove that there exists a faithful G-curve X that cannot be G-compressed to any curve of genus 1.

Note that G is not isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for $n = 1, 2, 3, 4, 6$, because these groups act faithfully on $\mathbb{P}^1$ over k (see, e.g., [2]). By Theorem 5.2, there exists a faithful G-curve X such that every $g \in G$ fixes a geometric point of X. For the sake of contradiction, suppose that there exists a G-compression $X \to E$, where E is a curve of genus 1 endowed with a faithful G-action. In the algebraic closure, we obtain a G-compression $X_{\overline{k}} \to E_{\overline{k}}$. Regard G

as a subgroup of $\mathrm{Aut}(E_{\overline{k}})$. By the exact sequence (5.1) and the fact that $G \ncong \mathbb{Z}/n\mathbb{Z}$ for $n = 1, 2, 3, 4, 6$; we conclude that $G \cap i(E_{\overline{k}}) \neq \emptyset$. Since $i(E_{\overline{k}})$ acts on $E_{\overline{k}}$ by translations, $G \cap i(E_{\overline{k}})$ acts freely on $E_{\overline{k}}$. However, every $g \in G$ must fix a point on $E_{\overline{k}}$ by our assumption on $X_{\overline{k}}$. This contradiction shows that X cannot be G-compressed to any G-curve of genus 1. □

In view of the above theorem, it remains to study the existence of strongly incompressible G-curves when G can act faithfully on a curve of genus 0. We will devote Section 5.3 to the study of equivariant rational maps to projective spaces, and we will use these results to understand compressions onto curves of genus 0.

5.3 Equivariant maps to projective spaces

Let G be an algebraic group defined over a field k. A projective representation $\rho\colon G \hookrightarrow \mathrm{PGL}(V)$ gives rise to a G-action on $\mathbb{P}(V)$. We will denote the resulting G-variety by ${}_{\rho}\mathbb{P}(V)$. If ρ and σ are projective G-representations, it is clear that ${}_{\rho}\mathbb{P}(V)$ and ${}_{\sigma}\mathbb{P}(V)$ are G-equivariantly isomorphic if and only if ρ and σ are conjugate. In what follows, we always assume that the G-action on ${}_{\rho}\mathbb{P}(V)$ is generically free.

Consider the commutative diagram whose rows are central exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathrm{GL}(V) & \longrightarrow & \mathrm{PGL}(V) & \longrightarrow & 1 \\ & & \| & & \uparrow{\scriptstyle \overline{\rho}} & & \uparrow{\scriptstyle \rho} & & \\ 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & 1 \end{array} \tag{5.2}$$

where G' is the full preimage of G in $\mathrm{GL}(V)$. Given a field extension K/k, we obtain the corresponding diagram in cohomology

$$\begin{array}{ccccccc} & & 1 & \longrightarrow & H^1(K, \mathrm{PGL}(V)) & \longrightarrow & H^2(K, \mathbb{G}_m) \\ & & \uparrow{\scriptstyle \overline{\rho}_*} & & \uparrow{\scriptstyle \rho_*} & & \| \\ 1 & \longrightarrow & H^1(K, G') & \xrightarrow{\varphi} & H^1(K, G) & \xrightarrow{\Delta_\rho} & H^2(K, \mathbb{G}_m) \end{array} \tag{5.3}$$

(Note that $H^1(K, \mathbb{G}_m)$ and $H^1(K, \mathrm{GL}(V))$ are trivial by Hilbert's Theorem 90.) This construction defines a cohomological invariant $\Delta_\rho\colon H^1(K, G) \to H^2(K, \mathbb{G}_m) = \mathrm{Br}(K)$. If X is a generically free primitive G-variety and $L = k(X)^G$, we denote the Brauer class associated to $[X] \in H^1(L, G)$ by $\Delta_\rho(X)$. Note that $\Delta_\rho(X)$ is trivial if and only if $[X]$ lifts to a G'-torsor $[X'] \in H^1(L, G')$.

Construction 5.5. Let Y be a primitive closed G-subvariety of ${}_\rho\mathbb{P}(V)$. Endow V with a linear G'-action via $\overline{\rho}$ and define $\widetilde{Y} \subset V$ to be the affine cone over Y *with the origin removed*. It is not hard to see that $\widetilde{Y}$ is a primitive G'-variety. Moreover, it is well known that $\widetilde{Y}$ is a $\mathbb{G}_m$-torsor and Y is isomorphic to the *geometric* quotient $\widetilde{Y}/\mathbb{G}_m$. Note also that the group $G'/\mathbb{G}_m \cong G$ acts naturally on $\widetilde{Y}/\mathbb{G}_m$, in such a way that the above isomorphism is G-equivariant.

Lemma 5.6. *Let Y be a generically free primitive closed G-subvariety of ${}_\rho\mathbb{P}(V)$. Then $\Delta_\rho(Y)$ is trivial.*

Proof. We need to show that $[Y]$ is in the image of the map $\varphi\colon H^1(K, G') \to H^1(K, G)$, where $K = k(Y)^G$. Let $\widetilde{Y}$ be as in Construction 5.5. If $x \in Y$ has trivial stabilizer in G, then any lift $\widetilde{x} \in \widetilde{Y}$ of x has trivial stabilizer in G'. It follows that $\widetilde{Y}$ is a generically free primitive G'-variety and clearly $\varphi([\widetilde{Y}]) = [\widetilde{Y}/\mathbb{G}_m] = [Y]$. □

Proposition 5.7. *Let G be a finite group, let $\rho\colon G \hookrightarrow \mathrm{PGL}(V)$ be a projective representation and let X be a faithful primitive G-variety.*

(a) *Suppose that there exists a G-equivariant rational map $f\colon X \dashrightarrow {}_\rho\mathbb{P}(V)$. Then $\Delta_\rho(X)$ is trivial.*

(b) *Conversely, suppose that $\Delta_\rho(X)$ is trivial. Then, given any G-invariant open subset $U \subset {}_\rho\mathbb{P}(V)$, there exists a G-equivariant rational map $X \dashrightarrow U$.*

Proof. (a) We write $Y = \overline{f(X)}$, $K = k(Y)^G$ and $L = k(X)^G$. We separate the proof into two cases.

Case 1: Suppose that Y is a faithful G-variety. This case follows from the fact that Δ_ρ is a cohomological invariant. The G-compression $f\colon X \dashrightarrow Y$ naturally induces a k-field homomorphism $i\colon K \hookrightarrow L$ and we have a commutative diagram

$$\begin{array}{ccc} H^1(K, G) & \xrightarrow{\Delta_\rho^K} & H^2(K, \mathbb{G}_m) \\ {\scriptstyle i_*}\downarrow & & \downarrow \\ H^1(L, G) & \xrightarrow{\Delta_\rho^L} & H^2(L, \mathbb{G}_m) \end{array} \tag{5.4}$$

It is well known that in the above situation, we must have $i_*([Y]) = [X]$. By Lemma 5.6, we have $\Delta_\rho^K(Y) = 1$. The commutativity of the above diagram then implies that $\Delta_\rho^L(X) = 1$.

Case 2: Suppose that the G-action on Y has a kernel H. Let $\widetilde{Y}$ be as in Construction 5.5, and let H' be the kernel of the G'-action on $\widetilde{Y}$. We claim that $\pi^{-1}(H)$ splits as $\mathbb{G}_m \times H'$, where $\pi\colon G' \to G$ is the natural projection. Since G/H is finite and acts faithfully on Y, it also acts generically freely. Hence, we can select a geometric point $y \in Y$ such that $\mathrm{Stab}_G(y) = H$. Fix any lift $\widetilde{y} \in \widetilde{Y}$ of y; by construction, it follows that $\mathrm{Stab}_{G'}(\widetilde{y}) = H'$.

Let $h \in H$ and let $h^* \in \pi^{-1}(h)$ be any lift. Since h acts trivially on y, there exists $\lambda_{h^*} \in \mathbb{G}_m$ such that $h^* \cdot \widetilde{y} = \lambda_{h^*}\widetilde{y}$. It follows that $\lambda_{h^*}^{-1}h^*$ stabilizes $\widetilde{y}$, whence it must be contained in H'. Since $\widetilde{Y}$ is a $\mathbb{G}_m$-torsor, it is easy to see that $\lambda_{h^*}^{-1}h^*$ is the unique element in $\pi^{-1}(h)$ contained in H'; in particular, it is independent of the lift h^*. It follows that the section $s\colon H \to \pi^{-1}(H)$ given by $h \to \lambda_{h^*}^{-1}h^*$ is a well-defined homomorphism satisfying $s(H) = H'$. Hence the exact sequence $1 \to \mathbb{G}_m \to \pi^{-1}(H) \to H \to 1$ splits in the desired way. This finishes the proof of the claim.

We thus have a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & G' & \xrightarrow{\pi} & G & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & G'/H' & \longrightarrow & G/H & \longrightarrow & 1
\end{array}$$

Since H acts trivially on Y, the dominant G-equivariant rational map $X \dashrightarrow Y$ induces a G/H-compression $X/H \dashrightarrow Y$, which gives rise to a k-field homomorphism $i\colon K \hookrightarrow L$. Using the bottom sequence above, we obtain a commutative diagram in cohomology

$$\begin{array}{ccccc}
H^1(K, G'/H') & \longrightarrow & H^1(K, G/H) & \longrightarrow & H^2(K, \mathbb{G}_m) \\
\downarrow & & \downarrow{\scriptstyle i_*} & & \downarrow \\
H^1(L, G'/H') & \longrightarrow & H^1(L, G/H) & \longrightarrow & H^2(L, \mathbb{G}_m)
\end{array}$$

The G/H-variety Y represents a class $[Y] \in H^1(K, G/H)$, which maps to $[X/H] \in H^1(L, G/H)$ under i_*. It is easy to see that the G'/H'-action on $\widetilde{Y}$ is generically free, so it follows that $[Y]$ comes from a class in $H^1(K, G'/H')$ and therefore its image in $H^2(K, \mathbb{G}_m)$ is trivial. By the commutativity of the above diagram, the image of $[X/H]$ in $H^2(L, \mathbb{G}_m)$ is also trivial.

To complete the proof of Case 2, note that we have a commutative

diagram

$$\begin{array}{ccccc} H^1(L,G') & \longrightarrow & H^1(L,G) & \xrightarrow{\Delta_\rho} & H^2(L,\mathbb{G}_m) \\ \downarrow & & \downarrow & & \| \\ H^1(L,G'/H') & \longrightarrow & H^1(L,G/H) & \longrightarrow & H^2(L,\mathbb{G}_m) \end{array}$$

The image of $[X] \in H^1(L,G)$ under the middle vertical map is precisely $[X/H]$. It thus follows that $\Delta_\rho(X)$ is trivial.

(b) By assumption, $[X]$ can be lifted to a class in $H^1(L,G')$, i.e., there exists a generically free primitive G'-variety X' such that $X'/\mathbb{G}_m$ is birationally isomorphic to X as a G-variety. Without loss of generality, we may identify $X'/\mathbb{G}_m$ with X.

We may view V as a generically free linear G'-variety and the natural projection $\pi_V \colon V \dashrightarrow {}_\rho\mathbb{P}(V)$ as a rational quotient map. Let $U' = \pi_V^{-1}(U)$, which is clearly a G'-invariant open subset of V. Note that V is a versal G'-variety (see, e.g., [13, Example 5.4]), whence there exists a G'-equivariant rational map $X' \dashrightarrow U'$. Taking quotients by $\mathbb{G}_m$, we obtain a G-equivariant rational map $X = X'/\mathbb{G}_m \dashrightarrow U'/\mathbb{G}_m = U$. □

We record the following corollary for future reference.

Corollary 5.8. *Let $\rho \colon G \hookrightarrow \mathrm{PGL}_2$ be a projective representation of a nontrivial finite group G and let X be a faithful irreducible G-variety. Then there exists a G-compression $X \dashrightarrow {}_\rho\mathbb{P}^1$ if and only if $\Delta_\rho(X) = 1$.*

Proof. The "only if" part follows directly from Proposition 5.7(a). On the other hand, suppose that $\Delta_\rho(X) = 1$. Since G is nontrivial, ${}_\rho\mathbb{P}^1$ has a finite number of G-fixed points. Therefore, we can find a G-invariant open $U \subset {}_\rho\mathbb{P}^1$ not containing any G-fixed points. By Proposition 5.7(b), there exists a G-equivariant rational map $f \colon X \dashrightarrow {}_\rho\mathbb{P}^1$ such that $f(X) \subset U$. The closure $\overline{f(X)}$ is a G-invariant closed irreducible subset of ${}_\rho\mathbb{P}^1$. By construction, it cannot be a fixed point, so it coincides with ${}_\rho\mathbb{P}^1$ itself. This proves that f is dominant. □

5.4 Some explicit computations

In this section, we explicitly compute the invariant introduced in Section 5.3 for certain actions on the projective line. We will use these results later to study the strong incompressibility of G-curves in the case where G acts faithfully on $\mathbb{P}^1$.

Recall that the conjugacy classes of embeddings of $(\mathbb{Z}/2\mathbb{Z})^2 \hookrightarrow \mathrm{PGL}_2(k)$ are parametrized by the pairs $(\overline{a}, \overline{b}) \in (k^\times/k^{\times 2})^2$ such that the quaternion algebra $(a, b)_2$ is split. The corresponding embedding is denoted by $\rho_{(a,b)}$, which is defined in Proposition 3.10. For simplicity, denote the $(\mathbb{Z}/2\mathbb{Z})^2$-variety ${}_{\rho_{(a,b)}}\mathbb{P}^1$ by ${}_{(a,b)}\mathbb{P}^1$. Clearly, ${}_{(a,b)}\mathbb{P}^1$ and ${}_{(a',b')}\mathbb{P}^1$ are isomorphic as $(\mathbb{Z}/2\mathbb{Z})^2$-varieties if and only if $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$.

Lemma 5.9. *Let $\rho_{(a,b)}$ be as above, let K/k be a field extension and identify $H^1(K, (\mathbb{Z}/2\mathbb{Z})^2)$ with $(K^\times/K^{\times 2})^2$. Then $\Delta_{\rho_{(a,b)}}(\overline{c}, \overline{d}) = [(ac, bd)_2]$ for all $c, d \in K^\times$.*

Proof. It suffices to prove that $\rho_{(a,b)*}\colon (K^\times/K^{\times 2})^2 \to H^1(K, \mathrm{PGL}_2)$ maps $(\overline{c}, \overline{d})$ to $(ac, bd)_2$. Let $U, V \in \mathrm{GL}_2$ be lifts of $\rho_{(a,b)}(e_1)$, $\rho_{(a,b)}(e_2)$, respectively. Note that $U^2 = b'I$, $V^2 = a'I$ and $UV + VU = 0$, where $\overline{a'} = \overline{a}$ and $\overline{b'} = \overline{b}$. Rescaling the lifts if necessary, we may assume that $a' = a$ and $b' = b$. Let $\mathcal{A}$ be the split quaternion algebra $(b, a)_2$. Note that there is a k-algebra isomorphism $\mathcal{A} \cong \mathrm{M}_2$ given by $i \mapsto U$, $j \mapsto V$, which induces isomorphisms $\mathrm{GL}_1(\mathcal{A}) \cong \mathrm{GL}_2$ and $\mathrm{PGL}_1(\mathcal{A}) \cong \mathrm{PGL}_2$. By construction, $\rho_{(a,b)}$ factors as

$$(\mathbb{Z}/2\mathbb{Z})^2 \xhookrightarrow{\varphi} \mathrm{PGL}_1(\mathcal{A}) \xrightarrow{\cong} \mathrm{PGL}_2,$$

where the embedding φ is given by $e_1 \mapsto [i]$, $e_2 \mapsto [j]$. We have therefore reduced the problem to showing that $\varphi_*\colon (K^\times/K^{\times 2})^2 \to H^1(K, \mathrm{PGL}_1(\mathcal{A}))$ sends $(\overline{c}, \overline{d})$ to $(ac, bd)_2$ for all $c, d \in K^\times$.

We give a proof of this fact by Galois descent. Let $L = K(\sqrt{c}, \sqrt{d})$; then we may view $\varphi_*(\overline{c}, \overline{d})$ as an element of $H^1(\mathrm{Gal}(L/K), \mathrm{PGL}_1(\mathcal{A})(L))$. For simplicity, assume that c, d and cd are non-squares; the remaining cases are easier and left to the reader. Define generators $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/K)$ such that σ_1 fixes $\sqrt{d}$ and sends $\sqrt{c}$ to $-\sqrt{c}$, while σ_2 fixes $\sqrt{c}$ and sends $\sqrt{d}$ to $-\sqrt{d}$. Note that the 1-cocycle $v\colon \mathrm{Gal}(L/K) \to \mathrm{PGL}_1(\mathcal{A})(L)$ representing $\varphi_*(\overline{c}, \overline{d})$ is given by $\sigma_1 \mapsto [i]$, $\sigma_2 \mapsto [j]$. Then we twist the Galois action on $\gamma = x + yi + zj + tij \in \mathcal{A} \otimes_K L$ by setting

$$\sigma_1 * \gamma = v_{\sigma_1}(\sigma_1(\gamma)) = i^{-1}\sigma_1(\gamma)i = \sigma_1(x) + \sigma_1(y)i - \sigma_1(z)j - \sigma_1(t)ij;$$
$$\sigma_2 * \gamma = v_{\sigma_2}(\sigma_2(\gamma)) = j^{-1}\sigma(\gamma)j = \sigma_2(x) - \sigma_2(y)i + \sigma_2(z)j - \sigma_2(t)ij.$$

It follows that γ is invariant under the twisted Galois action if and only if $\gamma = x + y_1\sqrt{d}\,i + z_1\sqrt{c}\,j + t_1\sqrt{cd}\,ij$ for $x, y_1, z_1, t_1 \in K$. This implies that $\varphi_*(\overline{c}, \overline{d})$ is generated as a K-algebra by $i' = \sqrt{d}\,i$ and $j' = \sqrt{c}\,j$, which satisfy $i'^2 = bd$, $j'^2 = ac$ and $i'j' + j'i' = 0$. Consequently, we obtain that $\varphi_*(\overline{c}, \overline{d}) = (bd, ac)_2 \cong (ac, bd)_2$. □

Let $\rho_a\colon \mathbb{Z}/2\mathbb{Z} \hookrightarrow \mathrm{PGL}_2$ be as in (3.1) and denote ${}_{\rho_a}\mathbb{P}^1$ simply by ${}_a\mathbb{P}^1$. Note that ${}_a\mathbb{P}^1$ and ${}_{a'}\mathbb{P}^1$ are isomorphic as $\mathbb{Z}/2\mathbb{Z}$-varieties if and only if $\overline{a} = \overline{a'}$. By [20, Example 6], it follows that ${}_a\mathbb{P}^1$ is versal if and only if $a \in k^{\times 2}$.

Corollary 5.10. *Let ρ_a be as above, let K/k be a field extension and identify $H^1(K, \mathbb{Z}/2\mathbb{Z})$ with $K^\times/K^{\times 2}$. Then $\Delta_{\rho_a}(\overline{c}) = [(c,a)_2]$ for all $c \in K^\times$.*

Proof. We need to show that $\rho_{a*}\colon K^\times/K^{\times 2} \to H^1(K, \mathrm{PGL}_2)$ maps $\overline{c}$ to $(c,a)_2$ for all $c \in K^\times$. Note that we may write $\rho_a = \rho_{(1,a)} \circ \phi$, where $\phi\colon \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/2\mathbb{Z})^2$ sends $-1 \mapsto e_1$. Therefore we must have

$$\rho_{a*}(\overline{c}) = \rho_{(1,a)*} \circ \phi_*(\overline{c}) = \rho_{(1,a)*}(\overline{c}, \overline{1}) = (c,a)_2,$$

where the last equality follows from Lemma 5.9. □

5.5 Cyclic and dihedral groups: Compressibility of $\mathbb{P}^1$

Recall that the groups $\mathbb{Z}/n\mathbb{Z}$ and D_{2n} act faithfully on some curve of genus 0 if and only if they act faithfully on $\mathbb{P}^1$, which happens if and only if $\alpha_n \in k$ (see Theorem 1.2). If the latter condition does not hold, the existence of strongly incompressible curves for $\mathbb{Z}/n\mathbb{Z}$ and D_{2n} follows from Theorem 5.4.

Lemma 5.11. *Let $n \geq 3$ be any integer, let k be a field containing α_n, and define the embedding $\rho_1\colon D_{2n} \hookrightarrow \mathrm{PGL}_2$ by sending*

$$\sigma \mapsto \begin{pmatrix} \alpha_n + 1 & \beta_n \\ 1 & \alpha_n + 1 \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{5.5}$$

where σ, τ are the usual generators of D_{2n}. (This results from choosing $a = x = 1, y = 0$ in (3.6).) Then ${}_{\rho_1}\mathbb{P}^1$ is not strongly incompressible.

Proof. We need to exhibit a G-equivariant map ${}_{\rho_1}\mathbb{P}^1 \to {}_{\rho_1}\mathbb{P}^1$ that is not injective. Select a square root of β_n (possibly in a quadratic extension of k) and define

$$Q = \begin{pmatrix} 1 & 1 \\ -\beta_n^{-1/2} & \beta_n^{-1/2} \end{pmatrix},$$

in such a way that

$$Q^{-1}\rho_1(\sigma)Q = \begin{pmatrix} 1 + \omega_n & 0 \\ 0 & 1 + \omega_n^{-1} \end{pmatrix}, \quad Q^{-1}\rho_1(\tau)Q = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Let $F\colon \mathbb{P}^1 \to \mathbb{P}^1$ be given by $F(x:y) = (x^{n+1} : y^{n+1})$. A calculation shows that

$$F \circ (Q^{-1}\rho_1(\sigma)Q) = (Q^{-1}\rho_1(\sigma)Q) \circ F$$

and

$$F \circ (Q^{-1}\rho_1(\tau)Q) = (Q^{-1}\rho_1(\tau)Q) \circ F.$$

It follows that $Q \circ F \circ Q^{-1}$ is a G-equivariant map ${}_{\rho_1}\mathbb{P}^1 \to {}_{\rho_1}\mathbb{P}^1$ defined over $k(\beta_n^{1/2})$. Explicitly, note that $Q \circ F \circ Q^{-1}$ sends $(x:y)$ to $(u:v)$, where

$$\begin{aligned} u &= (x + \beta_n^{1/2}y)^{n+1} + (x - \beta_n^{1/2}y)^{n+1}; \\ v &= \beta_n^{-1/2}\left((x + \beta_n^{1/2}y)^{n+1} - (x - \beta_n^{1/2}y)^{n+1}\right). \end{aligned}$$

In particular, it follows that $Q \circ F \circ Q^{-1}$ is actually defined over k. Since it has degree $n+1$, it is not injective and we are done. □

Remark 5.12. Restricting the embedding (5.5) to $\mathbb{Z}/n\mathbb{Z}$, the above lemma proves *a fortiori* that the projective line is not strongly incompressible as a $\mathbb{Z}/n\mathbb{Z}$-variety.

Proposition 5.13. *Let $n \geq 2$ be any integer and let k be a field containing ω_n. Then there are no strongly incompressible $\mathbb{Z}/n\mathbb{Z}$-varieties.*

Proof. This is proved in [24, Example 5]; we supply a short alternative proof. Recall that the embedding $\rho\colon \mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathrm{PGL}_2$ sending a generator of $\mathbb{Z}/n\mathbb{Z}$ to the diagonal matrix $\mathrm{diag}(\omega_n, 1)$, is generic, i.e., ${}_{\rho}\mathbb{P}^1$ is versal. Any faithful $\mathbb{Z}/n\mathbb{Z}$-variety can thus be $\mathbb{Z}/n\mathbb{Z}$-compressed to ${}_{\rho}\mathbb{P}^1$. Moreover, ${}_{\rho}\mathbb{P}^1$ is not strongly incompressible, as shown by the nontrivial $\mathbb{Z}/n\mathbb{Z}$-compression $(x:y) \mapsto (x^{n+1} : y^{n+1})$. □

The techniques introduced above can be used to show that there are no strongly incompressible varieties for odd cyclic and odd dihedral groups if they act faithfully on the projective line.

Proposition 5.14. *Let $n \geq 3$ be an odd integer, let k be a field containing α_n, and let G be either $\mathbb{Z}/n\mathbb{Z}$ or D_{2n}. Then there are no strongly incompressible G-varieties.*

Proof. We focus on the case $G = D_{2n}$; the cyclic case follows along the same lines. Note that the embedding ρ_1 defined in (5.5) is generic for odd n, i.e., the G-variety ${}_{\rho_1}\mathbb{P}^1$ is versal (see [20, Thm. 8]). It follows that any faithful G-variety can be G-compressed to ${}_{\rho_1}\mathbb{P}^1$. It thus suffices to prove that ${}_{\rho_1}\mathbb{P}^1$ is not strongly incompressible, which follows directly from Lemma 5.11. □

5.6 Strongly incompressible curves for even cyclic groups

Let $G = \mathbb{Z}/n\mathbb{Z}$, where $n \geq 4$ is even, and let k be a field containing α_n. Define $\rho\colon G \hookrightarrow \mathrm{PGL}_2$ as in (3.5), which is unique up to conjugacy. By the results in Proposition 5.13, it remains to analyze the case where $\omega_n \notin k$. (In this situation, ${}_\rho\mathbb{P}^1$ is not versal.) Interestingly, we will prove that there exist strongly incompressible G-curves under this assumption. With this goal in mind, we first prove the following technical lemma.

Lemma 5.15. *Let k be a field such that $\alpha_n \in k$. Then there exists $s \in k[x]$ square-free satisfying the following properties:*

(a) *$s(a) = 0$ for some $a \in k$.*

(b) *The hyperelliptic curve C with equation $y^2 = s(x)$ can be endowed with a faithful G-action, in such a way that the unique element of order 2 in G acts as the hyperelliptic involution on C.*

Proof. Suppose first that $n = 4$. In that case, we can take $s(x) = x^5 - x$ and $a = 0$. The $\mathbb{Z}/4\mathbb{Z}$-action on the hyperelliptic curve $y^2 = s(x)$ is given by $\sigma \cdot (x, y) \mapsto (-1/x, y/x^3)$, where σ is a generator of $\mathbb{Z}/4\mathbb{Z}$.

Assume henceforth that $n \geq 6$, and consider the exact sequence $1 \to \mathbb{Z}/2\mathbb{Z} \to G \to \mathbb{Z}/m\mathbb{Z} \to 1$, where $m = n/2$. Using Proposition 4.9 (resp. 4.10) if m is odd (resp. even) and the fact that $\alpha_{2m} \in k$, it follows that there exists a hyperelliptic curve C/k with a faithful G-action satisfying (b). We claim that we can select C such that (a) holds as well.

Let $L = k(x)$ and $K = k(t)$ be rational function fields such that $L = k(C)^{\mathbb{Z}/2\mathbb{Z}}$ and $K = L^{\mathbb{Z}/m\mathbb{Z}}$. By the results from Section 4.5, it follows that $k(C) = L\left(\sqrt{(x^2 - \beta_m)r}\right)$, where we are free to choose $r \in k(t)^\times$. Recall that t is a rational function of x, say $t = p(x)/q(x)$. Choose $a \in k$, which is not a zero of q or $qp' - pq'$, and let $r = q(a)t - p(a)$. A hyperelliptic equation for C is then given by $y^2 = s(x)$, where $s(x)$ is the square-free part of

$$(x^2 - \beta_m)(q(a)p(x) - p(a)q(x))q(x).$$

By construction, $s(a) = 0$, which finishes the proof. □

Proposition 5.16. *Let k be a field such that $\alpha_n \in k$ and $\omega_n \notin k$. Then there exists a strongly incompressible G-curve.*

Proof. Let C be the hyperelliptic curve constructed in Lemma 5.15. It suffices to prove that C cannot be G-compressed to any curve of genus ≤ 1, as the result then follows from Lemma 5.1.

We claim that C cannot be G-compressed to any curve of genus 0. First of all, such a curve would be forced to be ${}_{\rho}\mathbb{P}^1$ since C has k-rational points. For the sake of contradiction, suppose that there exists a G-compression $C \to {}_{\rho}\mathbb{P}^1$. Regard this map as a $\mathbb{Z}/2\mathbb{Z}$-compression. Note that

$$\rho(\sigma^m) = \begin{pmatrix} 0 & \beta_n \\ 1 & 0 \end{pmatrix}$$

and therefore ${}_{\rho}\mathbb{P}^1$ is isomorphic to ${}_{\beta_n}\mathbb{P}^1$ as a $\mathbb{Z}/2\mathbb{Z}$-variety. On the other hand, if we regard C as a $\mathbb{Z}/2\mathbb{Z}$-variety, its class $[C] \in H^1(L, \mathbb{Z}/2\mathbb{Z}) = L^{\times}/L^{\times 2}$ is given by $\overline{s(x)}$. (Here, we have $L = k(C)^{\mathbb{Z}/2\mathbb{Z}} = k(x)$ as in the proof of Lemma 5.15.) If we denote the restriction of ρ to $\mathbb{Z}/2\mathbb{Z}$ by ρ', we conclude using Corollary 5.10 that $\Delta_{\rho'}(C) = [(s(x), \beta_n)_2]$. This class must be trivial over $L = k(x)$ by Corollary 5.8. If we apply Lemma 2.1 to the root a of s, we obtain that $\beta_n \in k^{\times 2}$, i.e., $\omega_n - \omega_n^{-1} \in k$. However, this contradicts the fact that $\omega_n \notin k$.

It remains to show that C cannot be G-compressed to any G-curve of genus 1. Since C has k-rational points, it suffices to prove that there is no G-compression $C \to E$, where E is an elliptic curve endowed with a faithful G-action. Suppose there is such a G-compression and regard G as a subgroup of $\mathrm{Aut}(E)$. By Lemma 5.3(a), we can write $G \cong G_0 \times \pi(G)$, where $G_0 = G \cap E$ and $\pi(G) \subset \mathrm{Aut}_0(E)$. Since G is cyclic, we conclude that G_0 and $\pi(G)$ are cyclic groups of relatively prime order. We claim that σ^m (the unique element of order 2 inside G) belongs to G_0, or equivalently that G_0 has even order. Suppose on the contrary that the order of $\pi(G)$ is even, i.e., $\pi(G) \cong \mathbb{Z}/d\mathbb{Z}$ for $d = 2$, 4, or 6. By Lemma 5.3(d), the translation by $P_0 \in E$ and the automorphism $\alpha \in \mathrm{Aut}_0(E)$ commute if and only if $\alpha(P_0) = P_0$. Since $\pi(G)$ has even order, it contains the inversion map $P \mapsto -P$. Therefore any point of E fixed by $\pi(G)$ has order dividing 2. Since we are assuming that G_0 is a cyclic group of odd order that commutes with $\pi(G)$, it must be trivial. It follows that $G = \pi(G) \cong \mathrm{Aut}_0(E) \cong \mathbb{Z}/n\mathbb{Z}$ for $n = 4$ or 6. By Lemma 5.3(c), this contradicts the assumption that k does not contain the appropriate roots of unity. We have proved that $\sigma^m \in G_0$, and hence acts as a translation on E. On the other hand, note that σ^m fixes a k-rational point in C, namely $(a, 0)$. Hence, it must also fix a point in E. This contradiction completes the proof. □

5.7 Strongly incompressible curves for even dihedral groups

5.7.1 The Klein 4-group

Throughout this subsection, let G denote the Klein 4-group with generators e_1, e_2. Recall that G acts faithfully on $\mathbb{P}^1$ over any field k, but such an action is never versal. Our goal is to prove the following proposition.

Proposition 5.17. *The following are equivalent:*

(i) *There are no strongly incompressible G-curves over k.*

(ii) $\mathrm{cd}_2(k) = 0$.

Proof of (ii) $\Rightarrow$ (i). Assume that k has cohomological 2-dimension 0 and let X be any faithful G-curve. The field $K = k(X)^G$ is a transcendence degree 1 extension of k, so $\mathrm{cd}_2(K) \leq 1$ by [31, Prop. II.4.2.11]. Then, by [31, Prop. II.2.3.4], it follows that $\mathrm{Br}_2(K)$ is trivial. Let $\rho\colon (\mathbb{Z}/2\mathbb{Z})^2 \hookrightarrow \mathrm{PGL}_2$ be any embedding. We claim that X can be G-compressed to ${}_\rho\mathbb{P}^1$. Indeed, note that $\Delta_\rho(X)$ is the class of a quaternion algebra defined over K and therefore trivial. The result then follows from Corollary 5.8. To conclude the proof of the sufficiency, we need to prove that ${}_\rho\mathbb{P}^1$ is not strongly incompressible. We are free to select ρ conveniently, so we may assume that ρ is as in (3.4) with $a = 1$, i.e., $\rho = \rho_{(1,1)}$. Then, it is obvious that $(x : y) \mapsto (x^3 : y^3)$ is a G-compression of ${}_\rho\mathbb{P}^1$ to itself that is not birational. □

It remains to prove that (i) $\Rightarrow$ (ii). To achieve this, we need the following result.

Proposition 5.18. *Let $P, Q \in k[x]$ be separable polynomials of degree ≥ 1 satisfying the following conditions.*

(i) *P and Q have no common roots.*

(ii) *$P(0) \neq 0$, $Q(0) \neq 0$.*

(iii) *There exists a root $x_1 \in k$ of P (resp. $x_2 \in k$ of Q) such that $x_1 Q(x_1) \in k^{\times 2}$ (resp. $x_2 P(x_2) \in k^{\times 2}$).*

Then the curve X with function field $L = K(\sqrt{xP(x)}, \sqrt{xQ(x)})$, where $K = k(x)$ is rational, can be endowed with a faithful G-action such that every element of G fixes at least one geometric point of X.

Proof. Let $\mathbb{A}^3$ be the affine 3-space over k and let $Y \subset \mathbb{A}^3$ be the affine variety cut out by the ideal $I = \langle y^2 - xP(x), z^2 - xQ(x)\rangle$. Note that Y is an irreducible affine curve having a unique singularity at $(0,0,0)$ and its function field is precisely L. We can endow Y with a faithful G-action by setting $e_1 \cdot (x,y,z) = (x,-y,z)$ and $e_2 \cdot (x,y,z) = (x,y,-z)$. This action can be lifted to the unique nonsingular projective curve X which is birational to Y, in such a way that the natural birational isomorphism $X \dashrightarrow Y$ is G-equivariant. Note also that X can be seen as a Galois G-cover of $\mathbb{P}^1$ induced by the inclusion $K \hookrightarrow L$.

We claim that every element of G fixes at least one geometric point of X. We first prove the assertion for $e_1 \in G$ to illustrate the procedure. Note that $A = (x_1, 0, \sqrt{x_1 Q(x_1)})$ is a nonsingular k-rational point of Y fixed by e_1. Therefore, the natural G-equivariant rational map $Y \dashrightarrow X$ must be defined at the point A and its image in X is fixed by e_1 as desired. Analogously, we see that $B = (x_2, \sqrt{x_2 P(x_2)}, 0)$ is a nonsingular k-rational point of Y fixed by e_2 and the result follows along the same lines.

It remains to prove that e_1e_2 fixes a point in X. Unfortunately, the only fixed point of e_1e_2 in Y is $O = (0,0,0)$, which is not smooth. To overcome this difficulty, we consider the blowup of $\mathbb{A}^3$ at the origin O with exceptional divisor E and consider the strict transform Y' of Y. The G-action lifts naturally to Y', in such a way that the birational morphism $Y' \to Y$ is G-equivariant. We claim that Y' has a smooth point fixed by e_1e_2, which has to be contained in $Y' \cap E$. Recall that

$$\mathrm{Bl}_O\mathbb{A}^3 = \{((x,y,z),(t_0:t_1:t_2)) \in \mathbb{A}^3 \times \mathbb{P}^2 \mid xt_1 = yt_0, xt_2 = zt_0, yt_2 = zt_1\}$$

is covered by three affine charts $U_i = \{t_i \neq 0\}$ isomorphic to $\mathbb{A}^3$. We pick coordinates $y, u = t_0/t_1, v = t_2/t_1$ in U_1 (so that $x = yu$ and $z = yv$) and compute Y' in this coordinates. Any point in $Y' \cap U_1$ must satisfy the equations $y - uP(yu) = 0$ and $yv^2 - uQ(yu) = 0$. Moreover, note that the polynomial $Q(0)(y - uP(yu)) - P(0)(yv^2 - uQ(yu))$ is divisible by y and consequently we obtain that

$$Q(0) - P(0)v^2 - u^2Q(0)P_1(yu) + u^2P(0)Q_1(yu) = 0,$$

for all points $(y,u,v) \in Y' \cap U_1$, where $P_1(x) = (P(x) - P(0))/x$ and $Q_1(x) = (Q(x) - Q(0))/x$. Then it is easy to see that the above three equations define $Y' \cap U_1$ and that $Y' \cap U_1 \cap E = \{(0,0,\pm\sqrt{Q(0)/P(0)})\}$. (Actually one can see by looking at the other two charts that $Y' \cap E$ consists only of these two points.) We now look at the G-action on $Y' \cap U_1$. Note that $e_1e_2 \cdot (y,u,v) = (-y,-u,v)$, since $e_1e_2 \cdot (x,y,z) = (x,-y,-z)$ in Y. Therefore, the points

$(0, 0, \pm\sqrt{P(0)/Q(0)})$ are fixed by e_1e_2. Moreover, by applying the Jacobian criterion to the three polynomials defining $Y' \cap U_1$, one can show that both points are smooth; the details are left to the reader. Since the G-equivariant rational map $Y' \to Y \dashrightarrow X$ is defined at all smooth points, it follows that e_1e_2 has a fixed point in X. □

Lemma 5.19. *Let X be any (smooth projective) G-curve obtained from Proposition 5.18. Then X cannot be G-compressed to any curve of genus* 1.

Proof. Suppose that such a G-compression $X \to E$ exists. We may assume that E is an elliptic curve since X has k-rational points. By parts (a) and (b) of Lemma 5.3, some element of G must act freely on E. This contradicts the fact that every element of G fixes a point in X. □

We are ready to prove that (i) ⇒ (ii) in Proposition 5.17. Suppose that k does not have cohomological 2-dimension 0. We will produce a faithful G-curve that cannot be G-compressed to any G-curve of genus ≤ 1 by using Proposition 5.18. The following well known lemma provides more manageable conditions on k.

Lemma 5.20. *Let k be a field. The following are equivalent:*

(i) $\mathrm{cd}_2(k) = 0$.

(ii) *k is hereditarily quadratically closed, i.e., every algebraic extension of k is quadratically closed.*

(iii) *ξ is a square in $k(\xi)$ for every $\xi \in \overline{k}$.*

(iv) $\mathrm{Br}_2(k(x)) = 0$.

Proof. The equivalence (ii) ⇔ (iii) is straightforward and left to the reader, while (i) ⇔ (ii) follows directly from [9, Lemma 2]. We now prove that (i) ⇒ (iv). If $\mathrm{cd}_2(k) = 0$, it follows from [31, Prop. II.4.1.11] that $\mathrm{cd}_2(k(x)) \leq 1$. Then we conclude that $\mathrm{Br}_2(k(x)) = 0$ by [31, Prop. II.2.3.4]. To complete the proof, it suffices to show that (iv) ⇒ (iii). Suppose that (iv) holds, but there exists $\xi \in \overline{k}$, which is not a square in $k(\xi)$. Let $h \in k[x]$ be the minimal polynomial of ξ over k. The quaternion algebra $(x, h(x))_2$ must be split over $k(x)$, which implies that ξ is a square over $k(\xi)$ by Lemma 2.1. This contradiction completes the proof. □

Construction 5.21. In view of Lemma 5.20, given that $\mathrm{cd}_2(k) \neq 0$, we can choose an element ξ algebraic over k, which is not a square in $k(\xi)$. Let $h \in k[x]$ be the minimal polynomial of ξ over k and define polynomials

$$\begin{aligned} P(x) &= (x-\alpha)\left(\frac{(x-\alpha-1)h(x-\alpha)+(\alpha+1)h(-\alpha)}{(\alpha+1)h(-\alpha)x}\right), \\ Q(x) &= \alpha(\alpha+1-x)h(0)h(x-\alpha), \end{aligned}$$

where $\alpha \in k$ is taken such that P has no multiple roots, $P(0) \neq 0$ and $Q(0) \neq 0$. (It is not hard to see that such a selection of α is always possible.) We conclude that P and Q satisfy the conditions of Proposition 5.18; in what follows, let X denote the corresponding curve.

Lemma 5.22. *Let X be the curve obtained in Construction 5.21. Then there is no G-compression $X \to Y$, where Y is a curve of genus 0.*

Proof. Note that X has k-rational points. Hence, such a G-compression could only be possible if $Y \cong {}_{(a,b)}\mathbb{P}^1$ for some embedding $\rho_{(a,b)} \colon G \hookrightarrow \mathrm{PGL}_2$. From Proposition 5.18, we observe that $\overline{k(X)}^G = K = k(x)$ and the class $[X] \in H^1(K,G)$ corresponds to $(\overline{xP(x)}, \overline{xQ(x)}) \in (K^\times/K^{\times 2})^2$. By Lemma 5.9, we obtain that $\Delta_{\rho_{(a,b)}}(X) = [(axP(x), bxQ(x))_2] \in \mathrm{Br}(K)$.

Suppose that there exists a G-compression $X \to {}_{\rho}\mathbb{P}^1$. Then, by Corollary 5.8, the quaternion algebra $(axP(x), bxQ(x))_2$ must be split over K. Applying Lemma 2.1 to the roots $\alpha+1$ and $\alpha+\xi$ of $bxQ(x)$, we obtain that $a \in k^{\times 2}$ and $a\xi \in k(\xi)^{\times 2}$, respectively. This contradicts the assumption that ξ is not a square in $k(\xi)$. □

To finish the proof of Proposition 5.17, we use Lemmas 5.19 and 5.22 to conclude that X cannot be G-compressed to any curve of genus ≤ 1. Thus, it follows from Lemma 5.1 that there exist strongly incompressible G-curves if $\mathrm{cd}_2(k) > 0$. The proof is now complete.

5.7.2 Even dihedral groups of order ≥ 8

In this subsection, G will always denote the dihedral group D_{2n}, where $n \geq 4$ is an even integer. A result similar to Proposition 5.17 holds in this case.

Proposition 5.23. *Let k be a field such that $\alpha_n \in k$. Then there exist no strongly incompressible G-curves defined over k if and only if $\mathrm{cd}_2(k) = 0$.*

Proof. Suppose first that $\mathrm{cd}_2(k) = 0$. Similarly to the proof of Proposition 5.17, it follows that any faithful G-curve X can be G-compressed to ${}_{\rho}\mathbb{P}^1$,

where the embedding $\rho\colon G \hookrightarrow \mathrm{PGL}_2$ is as in (5.5). Moreover, it follows from Lemma 5.11 that ${}_\rho\mathbb{P}^1$ is not strongly incompressible.

To prove the converse, assume that $\mathrm{cd}_2(k) > 0$. We must show that there exists a strongly incompressible G-curve under this assumption. We first study the special case where $\omega_n \notin k$, i.e., β_n is not a square in k. We only sketch the argument, as it is very similar to the proof of Proposition 5.16. Using the results from Section 4.5, one can construct a hyperelliptic G-curve C such that the central element $\sigma^{n/2} \in G$ acts as the hyperelliptic involution of C, and there exists a k-rational point of C fixed by $\sigma^{n/2}$. Suppose that C can be G-compressed to ${}_\eta\mathbb{P}^1$, where η is any embedding $G \hookrightarrow \mathrm{PGL}_2$. Regard the G-compression as a $\mathbb{Z}/2\mathbb{Z}$-compression *with respect to the center of* G. As a $\mathbb{Z}/2\mathbb{Z}$-variety, ${}_\eta\mathbb{P}^1$ is isomorphic to ${}_{\beta_n}\mathbb{P}^1$. As in the proof of Proposition 5.16, we must have $\beta_n \in k^{\times 2}$, contradicting our assumption. Similarly, it follows that C cannot be G-compressed to any curve of genus 1. By Lemma 5.1, there exists a strongly incompressible G-curve in this case.

In what follows, assume that $\omega_n \in k$. By Lemma 5.20, there exists $\xi \in \overline{k}$ such that ξ is not a square in $k(\xi)$. Using this information, we construct a hyperelliptic G-curve C that cannot be G-compressed to any curve of genus ≤ 1. Let $m = n/2$, and define C to be the hyperelliptic curve with equation

$$y^2 = xf\left(\frac{x^m + x^{-m}}{2}\right),$$

where $f \in k[t]$ will be determined later. This curve can be endowed with a faithful G-action given by $\sigma\colon (x, y) \mapsto (\omega_n^2 x, \omega_n y)$, $\tau\colon (x, y) \mapsto (x^{-1}, yx^{-1})$. Note that we can regard C as a $(\mathbb{Z}/2\mathbb{Z})^2$-variety under the action of the subgroup $\langle \sigma^m, \tau \rangle$. We can write the function field of C in the form

$$k(C) = k(x, y)/\left(y^2 - xf\left(\frac{x^m + x^{-m}}{2}\right)\right).$$

It is not hard to see that

$$\begin{aligned} k(C)^{\langle \sigma^m \rangle} &= k(x), \\ k(C)^{\langle \tau \rangle} &= k\left(\frac{x + x^{-1}}{2}, y(1 + x^{-1})\right) / \left(y^2 - xf\left(\frac{x^m + x^{-m}}{2}\right)\right), \\ k(C)^{\langle \sigma^m, \tau \rangle} &= k\left(\frac{x + x^{-1}}{2}\right). \end{aligned}$$

Recall that there exists a polynomial T_m such that $T_m((x + x^{-1})/2) = (x^m + x^{-m})/2$. For simplicity, write $s = (x + x^{-1})/2$. Note that

$$y^2(1 + x^{-1})^2 = xf\left(\frac{x^m + x^{-m}}{2}\right)(1 + 2x^{-1} + x^{-2}) = (2s + 2)f(T_m(s)),$$

whence $k(C)^{\langle\tau\rangle}$ is obtained from $k(s)$ by adjoining $\sqrt{(2s+2)f(T_m(s))}$. On the other hand, note that $k(C)^{\langle\sigma^m\rangle}$ is obtained from $k(s)$ by adjoining $\sqrt{s^2-1}$. It follows that the class $[C] \in H^1(k(s),(\mathbb{Z}/2\mathbb{Z})^2)$ is equal to $(\overline{2(s+1)f(T_m(s))},\overline{s^2-1})$.

Suppose that C can be G-compressed to a curve of genus 0. Since C has k-rational points, such genus 0 curve must be G-equivariantly isomorphic to ${}_{\rho_a}\mathbb{P}^1$, where ρ_a is the embedding (3.6) for some class $\overline{a}$. Note that we are assuming that β_n is a square in k, so the binary form $\langle 1,-\beta_n\rangle$ is universal and therefore, $\overline{a} \in k^\times/k^{\times 2}$ is arbitrary. Since $\omega_n \in k$, the embedding ρ_a can be conjugated to the embedding

$$\eta\colon \sigma \mapsto \begin{pmatrix} \omega_n & 0 \\ 0 & 1 \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix},$$

so it follows that ${}_{\eta}\mathbb{P}^1 \cong {}_{\rho_a}\mathbb{P}^1$ as G-varieties. It is then straightforward to see that ${}_{\eta}\mathbb{P}^1 \cong {}_{(a,1)}\mathbb{P}^1$ as $(\mathbb{Z}/2\mathbb{Z})^2$-varieties. Using Lemma 5.9, we compute $\Delta_{\rho_{(a,1)}}(C) = [(2a(s+1)f(T_m(s)), s^2-1)_2]$. If we regard the assumed G-compression $C \to {}_{\eta}\mathbb{P}^1$ as a $(\mathbb{Z}/2\mathbb{Z})^2$-compression, then it follows that $\Delta_{\rho_{(a,1)}}(C)$ is trivial in $\mathrm{Br}(k(s))$.

We will now select f to arrive to a contradiction. Let $\gamma,\delta \in \overline{k}$ be such that $\gamma^2 = 1+\xi$ and $\delta^2 = 1+\xi^{-1}$. Replacing ξ by another element in $\xi \cdot k^{\times 2}$ if necessary, we can choose f satisfying the following properties:

- $f(T_m(\gamma)) = f(T_m(\delta)) = 0$.
- The polynomial $(s+1)f(T_m(s))$ is separable.

Since $(2a(s+1)f(T_m(s)), s^2-1)_2$ is split over $k(s)$, we can apply Lemma 2.1 to γ and obtain that ξ is a square in $k(\gamma)$. It follows that $k(\gamma) = k(\sqrt{\xi})$, since $[k(\sqrt{\xi}) : k(\xi)] = 2$ by assumption. We can thus write $\gamma = l_1 + l_2\sqrt{\xi}$ for some $l_1, l_2 \in k(\xi)$. Squaring, we obtain that $\xi+1 = l_1^2 + l_2^2\xi + 2l_1l_2\sqrt{\xi}$, whence $l_1l_2 = 0$. If $l_2 = 0$, it follows that $\xi+1$ is a square in $k(\xi)$, contradicting the fact that $[k(\gamma) : k(\xi)] = 2$. Hence we must have $l_1 = 0$, which implies that $1+\xi^{-1}$ is a square in $k(\xi)$, i.e., $k(\delta) = k(\xi)$. However, applying Lemma 2.1 to δ implies that ξ^{-1} (and hence ξ) is a square in $k(\delta)$, which contradicts our assumption. This proves that a G-compression $C \to {}_{\rho_a}\mathbb{P}^1$ is not possible.

It remains to prove that C cannot be G-compressed to any curve of genus 1. Suppose there is such a G-compression $C \to E$. By construction, the hyperelliptic involution of C, namely σ^m, fixes a k-rational point of C. Hence, σ^m must fix some k-rational point of E, which we may assume to be an elliptic curve. We adopt the notation of Lemma 5.3(a), where

$\pi\colon \mathrm{Aut}(E) \to \mathrm{Aut}_0(E)$ denotes the natural projection. Since $\mathrm{Aut}_0(E)$ is abelian, the relation $(\sigma\tau)^2 = 1$ implies that $\pi(\sigma\tau)^2 = \pi(\sigma^2)\pi(\tau^2) = \pi(\sigma^2) = 1$. It follows that σ^2 acts as a translation on E. We claim that σ acts as a translation as well. For the sake of contradiction, assume the contrary. By Lemma 5.3(a), we may write $\sigma = \tau_{P_0} \circ \alpha$, where τ_{P_0} denotes the translation by $P_0 \in E$, and $\alpha \in \mathrm{Aut}_0(E)$ is nontrivial. Since σ^2 acts as a translation, it follows that $\sigma^2(P) - P = \alpha^2(P) - P + \alpha(P_0) + P_0$ must be constant for all $P \in E$. This implies that the isogeny $\alpha^2 - \mathrm{id}$ is constant, so it is the zero map. This proves that α has order 2 in $\mathrm{Aut}_0(E)$, whence α is the inversion map $P \mapsto -P$. It follows that $\sigma^2 = \mathrm{id}$ in $\mathrm{Aut}(E)$, which is a contradiction because σ has order $n \geq 4$. We have proved that σ acts as a translation on E, and therefore so does σ^m. Hence σ^m cannot fix any point of E. □

5.8 Polyhedral groups

It remains to study the incompressibility of curves endowed with a faithful action of a polyhedral group G, i.e., $G = A_4$, S_4, or A_5.

5.8.1 Serre's cohomological invariant

Let $\widehat{G}$ be the binary polyhedral group associated to G. If G is an alternating group, then $\widehat{G}$ coincides with the unique nontrivial central extension of G by $\mathbb{Z}/2\mathbb{Z}$. If $G = S_4$, then $\widehat{G}$ is the unique central extension of G by $\mathbb{Z}/2\mathbb{Z}$ in which transpositions and products of disjoints transpositions lift to elements of order 4. (This is not the double cover studied in [30], in which transpositions lift to involutions). We have a central exact sequence

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \widehat{G} \longrightarrow G \longrightarrow 1\ ,$$

which yields a corresponding sequence in cohomology

$$H^1(K, \widehat{G}) \longrightarrow H^1(K, G) \xrightarrow{\widehat{\Delta}} \mathrm{Br}_2(K),$$

for any field extension K/k. Note that $\widehat{\Delta}\colon H^1(K, G) \to H^2(K, \mathbb{Z}/2\mathbb{Z}) = \mathrm{Br}_2(K)$ defines a cohomological invariant. If X is a faithful primitive G-variety and $L = k(X)^G$, we denote the Brauer class associated to $[X] \in H^1(L, G)$ by $\widehat{\Delta}(X)$. Note that $\widehat{\Delta}(X)$ is trivial if and only if $[X]$ lifts to a $\widehat{G}$-torsor $[\widehat{X}] \in H^1(L, \widehat{G})$. The following result follows from the definition of cohomological invariant.

Proposition 5.24. *Let X, Y be faithful primitive G-varieties and suppose that there exists a G-compression $f\colon X \dashrightarrow Y$. Let $i\colon k(Y)^G \hookrightarrow k(X)^G$ be the natural inclusion induced by f and define $i_*\colon \mathrm{Br}_2(k(Y)^G) \to \mathrm{Br}_2(k(X)^G)$ as the corresponding functorial map. Then $i_*(\widehat{\Delta}(Y)) = \widehat{\Delta}(X)$.*

Proof. Left to the reader. □

J.-P. Serre has described an effective way to compute $\widehat{\Delta}$. An element of $H^1(K, G)$ can be viewed as (the isomorphism class of) an étale K-algebra E, which has trivial discriminant if G is alternating. Then we have the following result.

Proposition 5.25 (cf. [30, Th. 1])**.** *Let q_E is the trace form of E/K. Then*

$$\widehat{\Delta}(E) = w_2(q_E) + [(-2, d_E)_2],$$

where w_2 denotes the second Stiefel-Whitney class and d_E is the discriminant of E.

Proof. See [30, Th. 1] or [35, §2]. □

Remark 5.26. If the field k satisfies some additional conditions, we may view $\widehat{\Delta}$ as a particular case of the cohomological invariant defined in Section 5.3. Suppose that the following assumptions hold.

(i) There exists an embedding $\rho\colon G \hookrightarrow \mathrm{PGL}_2$. This is the case if and only if -1 is the sum of two squares over k, with the additional requirement that $\sqrt{5} \in k$ if $G = A_5$ (see [2]).

(ii) There exists an embedding $\overline{\rho}\colon \widehat{G} \hookrightarrow \mathrm{GL}_2$ that fits in a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathrm{GL}_2 & \longrightarrow & \mathrm{PGL}_2 & \longrightarrow & 1 \\ & & \uparrow & & \uparrow{\scriptstyle \overline{\rho}} & & \uparrow{\scriptstyle \rho} & & \\ 1 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \widehat{G} & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

This is automatic if G is alternating. In the case $G = S_4$, it is true if and only if $\sqrt{2} \in k$.

Passing to cohomology in the above diagram, we conclude that $\widehat{\Delta}$ coincides with Δ_ρ, if we regard both their images to lie in the Brauer group.

5.8.2 Computation of the invariant for curves of genus ≤ 1

We first compute the cohomological invariant $\widehat{\Delta}$ for polyhedral actions on curves of genus 0. Recall that, up to equivariant birational isomorphism, there is only one action of a polyhedral group G on a curve of genus 0. In what follows, let $q_0(x,y,z) = x^2+y^2+z^2$ and denote by $X_0 \subset \mathbb{P}^2$ the corresponding quadric. Then, G acts on X_0 via the standard embedding $\rho\colon G \hookrightarrow \mathrm{SO}(q_0)$ as a rotation group. If $G = A_4$ or S_4, the action is defined over any field k, while for $G = A_5$ the action is defined over k if and only if $\sqrt{5} \in k$. Recall also that $K := k(X_0)^G$ is isomorphic to a rational function field, i.e., $X_0/G \cong \mathbb{P}^1$.

Proposition 5.27. (a) *If G is alternating, then $\widehat{\Delta}(X_0) = [(-1,-1)_2]$ in $\mathrm{Br}_2(K)$.*

(b) *If $G = S_4$, then $\widehat{\Delta}(X_0) = [(-1,-1)_2] + [(2,t)_2]$ in $\mathrm{Br}_2(K)$, where t is some generator of K/k.*

Proof. (a) Let k'/k be a field extension, and suppose that q_0 is isotropic over k'. We claim that $\widehat{\Delta}(X_0')$ is trivial in $\mathrm{Br}_2(k'(X_0')^G)$, where $X_0' = X_0 \times_{\mathrm{Spec}(k)} \mathrm{Spec}(k')$. Indeed, note that $\mathrm{PGL}_2 \cong \mathrm{SO}(q_0)$ over k', whence there exists an embedding $\rho\colon G \hookrightarrow \mathrm{PGL}_2$ defined over k' and a G-equivariant isomorphism $X_0' \cong {}_\rho\mathbb{P}^1$. It follows from Remark 5.26 that $\widehat{\Delta}(X_0') = \Delta_\rho(X_0') = \Delta_\rho({}_\rho\mathbb{P}^1)$, which is trivial by Lemma 5.6. This completes the proof of the claim.

Let E be the étale algebra corresponding to $[X_0] \in H^1(K,G)$. Then $q_E \cong \langle 1,a,b,ab\rangle$ for some $a,b \in K$ if $G = A_4$ (resp. $q_E \cong \langle 1,a,b,c,abc\rangle$ for some $a,b,c \in K$ if $G = A_5$). It follows that $\widehat{\Delta}(X_0) = w_2(q_E) = [(-a,-b)_2] + [(-1,-1)_2]$ if $G = A_4$ (resp. $[(-ac,-bc)_2] + [(-1,-1)_2]$ if $G = A_5$). In any case, we can write $\widehat{\Delta}(X_0) = [(u,v)_2] + [(-1,-1)_2]$ for some $u,v \in K$, so it suffices to prove that $(u,v)_2$ is split over K. Since q_0 is isotropic over $k' := k(s,t)/(s^2+t^2+1)$ and $(-1,-1)_2$ splits over k', it follows from the previous paragraph that $(u,v)_2$ splits over $k'(X_0')^G \cong K(s,t)/(s^2+t^2+1)$. Equivalently, the Pfister form $\langle 1,-u,-v,uv\rangle$ is hyperbolic over $K(s,t)/(s^2+t^2+1)$, which is the function field of the quadratic form $\langle 1,1,1\rangle$ defined over K. By [17, Th. X.4.5], either $\langle 1,-u,-v,uv\rangle$ is isotropic (hence hyperbolic) over K, or $\langle 1,-u,-v,uv\rangle \cong \langle 1,1,1,1\rangle$ over K. Equivalently, either $(u,v)_2$ splits, or $(u,v)_2 \cong (-1,-1)_2$. The former case yields the desired result, while the latter implies that $\widehat{\Delta}(X_0)$ is trivial. Hence, it suffices to prove that $\widehat{\Delta}(X_0)$ is nontrivial whenever $(-1,-1)_2$ is not split over K (equivalently over k, since K is purely transcendental over k).

Assume for the sake of contradiction that $(-1,-1)_2$ is not split over k and $\widehat{\Delta}(X_0)$ is trivial. This implies that $[X_0]$ comes from a class in $H^1(K,\widehat{G})$,

i.e., there exists a faithful primitive $\widehat{G}$-variety $\widehat{X_0}$ such that $\widehat{X_0}/(\mathbb{Z}/2\mathbb{Z})$ is birationally isomorphic to X_0 as a G-variety. Note that $\widehat{X_0}$ must be geometrically irreducible since $1 \to \mathbb{Z}/2\mathbb{Z} \to \widehat{G} \to G \to 1$ is not split. Thus, we may assume without loss of generality that $\widehat{X_0}$ is a (smooth projective) $\widehat{G}$-curve, endowed with a 2-1 quotient morphism $\widehat{X_0} \to X_0$. It follows that $\widehat{X_0}$ is a hyperelliptic curve (in the sense that its canonical divisor is not very ample). Moreover, note that $\mathrm{Aut}(\widehat{X_0})(\overline{k})$ contains $\widehat{G}$, which equals $\mathrm{SL}_2(\mathbb{F}_3)$ if $G = A_4$ (resp. $\mathrm{SL}_2(\mathbb{F}_5)$ if $G = A_5$). By [33, Table 1], it follows that the genus of $\widehat{X_0}$ is even. However, it is well known that this implies that $\widehat{X_0}/(\mathbb{Z}/2\mathbb{Z}) = X_0$ has a k-rational point (see, e.g., [22, §2.1]), which is equivalent to the splitting of $(-1,-1)_2$ over the field k. This contradiction concludes the proof.

(b) Note that S_4 embeds into $\mathrm{SO}(q_0)$ as the matrices of the form DP, where D is diagonal with entries ± 1 and P is a permutation matrix. (There are 24 such matrices of determinant 1.) The étale K-algebra corresponding to $[X_0] \in H^1(K, S_4)$ is the field extension $k(X_0)^H/K$, where H is any copy of S_3 inside S_4. For convenience, we choose the subgroup H generated by

$$\sigma = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \tau = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}.$$

Note that $S_4 = V \rtimes H$, where V is the subgroup of diagonal matrices in S_4.

We write $k(X_0) = k(a,b)/(a^2+b^2+1)$, where $a = x/z$ and $b = y/z$ in the usual coordinates of X_0. Note that $\sigma(a) = b/a$ and $\sigma(b) = 1/a$, while $\tau(a) = 1/a$ and $\tau(b) = b/a$. An easy computation then shows that $k(X_0)^H = k(\alpha)$, where $\alpha = a + b/a + 1/b + 1/a + b + a/b$. By Galois Theory, the minimal polynomial of α over K is equal to

$$P(Y) = \prod_{g \in V} (Y - g(\alpha)) = Y^4 - 6Y^2 + 8Y + t + 24,$$

where

$$t = \frac{(a-1)^2(a+1)^2(2a^2+1)^2(a^2+2)^2}{a^4(a^2+1)^2}$$

is a generator of K/k, which proves that $k(X_0)^H = K[Y]/(p(Y))$. By a simple computation, the trace form of $K[Y]/(p(Y))$ over K is isomorphic to $\langle 1, 3, -(t+27), -3t(t+27)\rangle$. It follows that its Stiefel-Whitney class is equal to $[(-3t, t(t+27))_2] + [(-1,-t)_2]$. The first quaternion algebra is split over K because $(-3t)3^2 + t(t+27) = t^2$. It follows that $\widehat{\Delta}(X_0) = [(-1,-t)_2] + [(-2,t)_2] = [(-1,-1)_2] + [(2,t)_2]$. The proof is complete. □

We now focus our attention on polyhedral actions on curves of genus 1. In this case, we only need to consider A_4-actions, since S_4 and A_5 cannot act faithfully on curves of genus 1.

Proposition 5.28. *Let C be a curve of genus 1 endowed with a faithful A_4-action defined over a field k. Then the following properties hold.*

(a) *The Jacobian $E \cong \mathrm{Pic}^0(C)$ has j-invariant 0.*

(b) *The elliptic curve E can be endowed with a faithful A_4-action defined over k.*

(c) *The curve C is A_4-equivariantly isomorphic to E over some extension k'/k of odd degree.*

(d) *We have the equality $\widehat{\Delta}(C) = [(-1,-1)_2]$ in $\mathrm{Br}_2(k(C)^{A_4})$.*

Proof. We will extensively use the results and notation from [34, §X.3] (see also [18]). Recall that C is a principal homogeneous space under E. A k-automorphism $g\colon C \to C$ induces a group automorphism of $\mathrm{Pic}^0(C)$, hence also a k-automorphism $\hat{g}\colon E \to E$ fixing the origin. Explicitly, it is not hard to see that $\hat{g}(P) = g(p_0 + P) - g(p_0)$, where the definition is independent of $p_0 \in C(\overline{k})$. Note also that $\hat{g}$ is the identity if and only if g is a translation by an element of $E(k)$. This proves that we have an exact sequence

$$1 \longrightarrow E(k) \longrightarrow \mathrm{Aut}(C)(k) \xrightarrow{\pi} \mathrm{Aut}_0(E)(k).$$

Regard A_4 as a subgroup of $\mathrm{Aut}(C)(k)$. It follows that $E(k) \cap A_4 \cong (\mathbb{Z}/2\mathbb{Z})^2$ and $\pi(A_4) = \mathbb{Z}/3\mathbb{Z} \subset \mathrm{Aut}_0(E)(k)$. By Lemma 5.3(b), it follows that $j(E) = 0$.

We now proceed with the proof of part (b). Note that $E(k)$ contains a subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, whence the 2-torsion points of E are k-rational. Using Lemma 5.3(b), we conclude from part (a) that k contains a primitive third root of unity ω_3 and $\mathrm{Aut}_0(E)(k) = \mathbb{Z}/6\mathbb{Z}$. We now explicitly construct the A_4-action on E. Since E has j-invariant 0, it has a Weierstrass equation $y^2 = x^3 + b$ for some $b \in k^\times$. Let the normal subgroup $V = (\mathbb{Z}/2\mathbb{Z})^2 \subset A_4$ act on E via translation by 2-torsion points (as it does on C as well). Then we can write $A_4 = V \rtimes H$, and let $H \cong \mathbb{Z}/3\mathbb{Z}$ act on E by $\alpha \cdot (x, y) = (\omega_3 x, y)$, where α is a generator of H. For convenience, we fix the above notation for the remainder of the proof.

To prove part (c), we first show that C has a k'-rational point over some extension k'/k of odd degree. Fix an element $g \in A_4 \subset \mathrm{Aut}(C)(k)$ of order

3 and assume without loss of generality that $\hat{g} = \alpha$. Note that $g(q) = g(p) + \alpha(q-p)$ for any $p, q \in C(\overline{k})$. Taking $q = p^\sigma$ for any $\sigma \in \mathrm{Gal}(\overline{k}/k)$ and using the fact that g is defined over k, we obtain that $g(p)^\sigma - g(p) = \alpha(p^\sigma - p)$, i.e., $(1-\alpha)(p^\sigma - p) = P^\sigma - P$ for $P = p - g(p) \in E(\overline{k})$. By [34, Thm. X.3.6], it follows that the class $\{C/k\} \in H^1(k, E)$ belongs to the kernel of the map $(1-\alpha)_*\colon H^1(k,E) \to H^1(k,E)$ induced by $1 - \alpha \in \mathrm{End}(E)$. However, note that $(2+\alpha) \circ (1-\alpha) = 3$, which implies that the class $\{C/k\}$ is 3-torsion. It follows that there exists an extension k'/k such that $[k' : k]$ is a power of 3 and C has a k'-rational point (see [18, Prop. 5] and the remark that follows).

We claim that after possibly taking a cubic extension of k', we can find an A_4-equivariant isomorphism $C \to E$. Fix a point $p_0 \in C(k')$. We would like to find $P_0 \in E(\overline{k})$ such that $(1-\alpha)(P_0) = g(p_0) - p_0 \in E(k')$. It is not hard to see that such a point P_0 can be found over some cubic extension of k'. (For example, this can be done by noting that the coordinates of P_0 satisfy cubic polynomials with coefficients in k'.) Without loss of generality, assume that $P_0 \in E(k')$ and define $q_0 = p_0 + P_0 \in C(k')$. Note that $g(q_0) = g(p_0) + \alpha(P_0) = p_0 + P_0 = q_0$. We claim that the k'-isomorphism $\varphi\colon C \to E$ defined by $q \mapsto q - q_0$ is A_4-equivariant. Since it clearly commutes with translations, it suffices to show that $\varphi(g(q)) = \alpha(\varphi(q))$. We compute $\varphi(g(q)) = g(q) - q_0 = g(q) - g(q_0) = \alpha(\varphi(q))$, which completes the proof of the claim.

It remains to prove part (d). We reduce the problem to curves of genus 1 with k-rational points. Assume the result is true in this case. Then we must have $\widehat{\Delta}(E) = [(-1,-1)_2]$ in $\mathrm{Br}_2(k(E)^{A_4})$, where E is the Jacobian of C. By part (c), we can find an odd degree extension k'/k such that $E_{k'} \cong C_{k'}$ as A_4-varieties. Therefore, we must have $\widehat{\Delta}(C_{k'}) = [(-1,-1)_2]$ in $\mathrm{Br}_2(k'(C)^{A_4})$. The natural map $\mathrm{Br}_2(k(C)^{A_4}) \to \mathrm{Br}_2(k'(C)^{A_4})$ is injective since $[k'(C)^{A_4} : k(C)^{A_4}]$ is odd, so it follows that $\widehat{\Delta}(C) = [(-1,-1)_2]$ in $\mathrm{Br}_2(k(C)^{A_4})$. This implies that it suffices to prove the statement for E.

We explicitly compute $\widehat{\Delta}(E) \in \mathrm{Br}(k(E)^{A_4})$. It is easy to check that the rational map $E \dashrightarrow \mathbb{P}^1$ given by

$$(x,y) \mapsto t = \frac{(y^4 + 18by^2 - 27b^2)}{y^3}$$

is an A_4-invariant map of degree 12, so it coincides with the rational quotient map $E \dashrightarrow E/A_4$. We may view the element $[E] \in H^1(k(t), A_4)$ as the A_4-Galois field extension $k(E)/k(t)$. Therefore, its corresponding étale $k(t)$-algebra is (isomorphic to) the fixed field $k(E)^H = k(y)$ (recall that $A_4 =$

$V \rtimes H$). Note that y is a root of

$$p(Y) = Y^4 - tY^3 + 18bY^2 - 27b^2,$$

so it follows that $k(y) = k(t)[Y]/(p(Y))$. A computation shows that the trace form of this étale algebra is isomorphic to $\langle 1, A, B, AB\rangle$, where $A = 3t^2 - 144b$ and $B = (192b - 3t^2)(144b - 3t^2)$. It follows that its Stiefel-Whitney class is equal to $[(-A, -B)_2] + [(-1, -1)_2]$. By Proposition 5.25, it suffices to show that $(-A, -B)_2$ is split over $k(t)$. Note that we have an isomorphism

$$(-A, -B)_2 \cong (144b - 3t^2, 192b - 3t^2)_2.$$

Recall that -3 is a square in k because k contains a primitive third root of unity. Hence the identity

$$(144b - 3t^2)2^2 + (192b - 3t^2)(\sqrt{-3})^2 = (\sqrt{-3}\, t)^2$$

holds over $k(t)$, which proves that the above quaternion algebra is split. □

5.8.3 Strong incompressibility

Proposition 5.29. *Let G be a polyhedral group. The following are equivalent:*

(i) *There are no strongly incompressible G-curves defined over k.*

(ii) $\mathrm{cd}_2(k) = 0$.

Proof of (ii) ⇒ (i). Suppose that $\mathrm{cd}_2(k) = 0$. By Lemma 5.20, it follows that k satisfies the hypotheses of Lemma 5.30 below. In particular, there exists an embedding $\rho\colon G \hookrightarrow \mathrm{PGL}_2$ defined over k. We claim that any faithful G-curve X can be G-compressed to ${}_\rho\mathbb{P}^1$. Indeed, the field $K = k(X)^G$ satisfies $\mathrm{cd}_2(K) = 1$ and therefore, $\mathrm{Br}_2(K) = 1$. Hence $\Delta_\rho(X) = 1$ and the claim follows from Corollary 5.8. To finish the proof, we must show that ${}_\rho\mathbb{P}^1$ is not strongly incompressible. This is achieved in Lemma 5.30. □

Lemma 5.30. *Let G be a polyhedral group. Suppose that $\omega_4 \in k$ if $G = A_4$ or S_4 (resp. $\omega_5 \in k$ if $G = A_5$), and let $\rho\colon G \hookrightarrow \mathrm{PGL}_2$ be an embedding defined over k (it is unique up to conjugacy). Then the G-variety ${}_\rho\mathbb{P}^1$ is not strongly incompressible.*

Proof. As the group A_4 is contained in S_4, it suffices to find non-birational compressions for S_4 and A_5.

Case 1: Suppose that $G = S_4$. The matrices

$$\begin{pmatrix} \omega_4 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \omega_4 & \omega_4 \\ -1 & 1 \end{pmatrix},$$

generate a subgroup isomorphic to S_4 inside PGL_2, whence we may assume that $\rho(G)$ is this particular subgroup. Then a computation shows that

$$(x : y) \mapsto (7x^4y^3 + y^7 : -x^7 - 7x^3y^4)$$

is a G-compression ${}_\rho\mathbb{P}^1 \to {}_\rho\mathbb{P}^1$, which is clearly not birational.

Case 2: Suppose that $G = A_5$. Consider the matrices

$$\begin{pmatrix} \omega_5 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \omega_5 + \omega_5^{-1} & 1 \\ 1 & -\omega_5 - \omega_5^{-1} \end{pmatrix};$$

they generate a subgroup isomorphic to A_5 inside $\mathrm{PGL}_2(k)$. Again, assume that $\rho(G)$ coincides with this subgroup. Then the morphism

$$(x : y) \mapsto (x^{11} + 66x^6y^5 - 11xy^{10} : -11x^{10}y - 66x^5y^6 + y^{11})$$

is a non-birational G-compression ${}_\rho\mathbb{P}^1 \to {}_\rho\mathbb{P}^1$. □

It remains to prove (i) ⇒ (ii) in Proposition 5.29. The following lemma will be useful in the sequel.

Lemma 5.31. *Let k be a field, let $(a, b)_2$ be a quaternion algebra defined over k and let $n \geq 4$ be an integer. Then we have the following properties.*

(a) *There exists an n-dimensional étale k-algebra E_1 with trivial discriminant such that the Stiefel-Whitney class $w_2(q_{E_1}) = [(a, b)_2]+[(-1, -1)_2]$,*

(b) *If $(a, b)_2 \ncong (-1, -1)_2$, there exists an n-dimensional étale k-algebra E_2 with nontrivial discriminant d_{E_2} such that $w_2(q_{E_2}) = [(a, b)_2] + [(-1, -d_{E_2})_2]$.*

Proof. It suffices to prove the results for $n = 4$, as adding copies of the trivial étale algebra k to E does not change the discriminant of E, or $w_2(q_E)$. By [13, Lemma 31.19], the k-algebra $E[A, B] = k[X]/(X^4 - 2AX^2 + B)$ is étale when $AB(A^2 - B) \neq 0$, has discriminant $64B(A^2 - B)^2$, and its trace form is isomorphic to $\langle 1, A, A^2 - B, AB(A^2 - B)\rangle$. A computation shows that

$$w_2(q_{E[A,B]}) = [(-A, -B(A^2 - B))_2] + [(-1, -B)_2].$$

To prove part (a), select $c \in k^\times$ such that $b^2c^4 - 1 \neq 0$, and put $A = -a(bc^2-1)^2$ and $B = a^2(b^2c^4-1)^2$. It is easy to see that $-A \equiv a \mod k^{\times 2}$ and $-B(A^2-B) \equiv b \mod k^{\times 2}$, whence $E_1 = E[A,B]$ satisfies the required properties.

To prove part (b), we may assume without loss of generality that $-b \notin k^{\times 2}$ and $b \neq 1$, by changing the presentation of $(a,b)_2$ if necessary. Define $A = -a$ and $B = -4ba^2/(b-1)^2$; then we obtain that $A^2 - B \in k^{\times 2}$. The algebra $E_2 = E[A,B]$ has discriminant $-b \notin k^{\times 2}$ and satisfies $w_2(q_{E_2}) = [(a,b)_2] + [(-1,b)_2]$. □

Remark 5.32. The conclusion in part (b) of the above theorem might fail if $(a,b)_2 \cong (-1,-1)_2$. Indeed, suppose that $k = \mathbb{R}$. By [13, Thm. 31.18], we observe that the trace form of any 4-dimensional étale algebra E has the form $q_E = \langle 1, A, A^2 - B, AB(A^2-B)\rangle$, which has second Stiefel-Whitney invariant $w_2(q_E) = [(-A, -B(A^2-B))_2] + [(-1,-B)_2]$. Since we want the discriminant to be nontrivial, B must be negative, so $w_2(q_E) = [(-A, A^2-B)_2]$. This class is obviously trivial because $A^2 - B > 0$, so we cannot obtain $[(-1,-1)_2]$.

Proof of (i) ⇒ (ii) in Proposition 5.29. Suppose that $\mathrm{cd}_2(k) > 0$ and let $K = k(x)$. Note in particular that the field K is Hilbertian (see [12, Prop. 13.2.1]).

Case 1: Suppose that $G = A_n$, where $n = 4$ or 5. By Lemma 5.20, there exists a nonsplit quaternion algebra A defined over K. Using Lemma 5.31(a), we can construct an n-dimensional étale K-algebra E with trivial discriminant such that $w_2(q_E) = [A] + [(-1,-1)_2]$. By [10, Thm. 1], there exists a field extension L/K of degree n whose trace form is isometric to q_E; moreover, we may assume that its Galois closure $\widetilde{L}/K$ has Galois group G. Therefore, the class of L (viewed as an étale K-algebra) in $H^1(K,G)$ corresponds to a faithful G-curve X defined over k with function field $\widetilde{L}$. By Proposition 5.25, we must have $\widehat{\Delta}(X) = [A] + [(-1,-1)_2]$.

We claim that X cannot be G-compressed to any curve of genus ≤ 1. Any faithful G-curve of genus 0 is G-equivariantly isomorphic to X_0. Suppose that there exists a G-compression $X \to X_0$. By Proposition 5.24, the image of $\widehat{\Delta}(X_0)$ in $\mathrm{Br}_2(K)$ under the induced map is equal to $\widehat{\Delta}(X) = [A] + [(-1,-1)_2]$. By Proposition 5.27(a), it follows that $[A]$ is trivial, which is a contradiction.

If $G = A_5$, the claim follows because A_5 does not act on any curve of genus 1. On the other hand, suppose that there exists a A_4-compression $X \to C$, where C has genus 1. (A word of warning: Here we cannot assure

that C is an elliptic curve because it might not have k-rational points.) As before, it follows that $\widehat{\Delta}(C)$ maps to $\widehat{\Delta}(X) \in \mathrm{Br}_2(K)$ under the map induced by the compression. However, Lemma 5.28(d) contradicts the fact that A is not split. This completes the proof of the claim. By Lemma 5.1, there exist strongly incompressible G-curves.

Case 2: Suppose that $G = S_4$. We claim that there exists a quaternion algebra $A \ncong (-1,-1)_2$ over K which does not split over $k'(x)$, where $k' = k(\sqrt{2})$. If 2 is a square in k and $(-1,-1)_2$ is split over K, the result follows immediately from Lemma 5.20. If 2 is a square but $(-1,-1)_2$ is not split over K, we choose $A = (-1,x)_2$. Note that $A \cong (-1,-1)_2$ over K if and only if $(-1,-x)_2$ is split. By Lemma 2.1, if either A is split or $A \cong (-1,-1)_2$, it would follow that -1 is a square in k, which contradicts our assumption that $(-1,-1)_2$ is not split.

Finally, if 2 is not a square over k, we choose $A = (x, x^2-4x+2)_2$. Suppose for the sake of contradiction that A splits over $k'(x)$. By Lemma 2.1, $2+\sqrt{2}$ is a square over k', i.e., $2+\sqrt{2} = (l_1+l_2\sqrt{2})^2$ for some $l_1, l_2 \in k$. Taking norms with respect to k'/k yields $2 = (l_1^2 - 2l_2^2)^2$, which contradicts our assumption. We now prove that $A \ncong (-1,-1)_2$, where we may assume that $(-1,-1)_2$ is not split. Indeed, such an isomorphism would imply that the quadratic forms $\langle 1,1,1\rangle$ and $\langle -x, -(x^2-4x+2), x(x^2-4x+2)\rangle$ are isomorphic over K. It follows that $\langle 1,1,1\rangle$ represents $-x$, i.e., there exist coprime polynomials $p,q,r,s \in k[x]$ such that $p(x)^2+q(x)^2+r(x)^2 = -xs(x)^2$. Making $x = 0$ yields $p(0) = q(0) = r(0) = 0$ since we are assuming that $\langle 1,1,1\rangle$ is anisotropic over k. This implies that $p(x), q(x), r(x)$ are divisible by x, whence $s(x)$ is divisible by x as well. This contradicts the fact that p,q,r,s are coprime.

By Lemma 5.31(b), we can construct a 4-dimensional étale K-algebra E with nontrivial discriminant d_E such that $w_2(q_E) = [A] + [(-1,-d_E)]$. By [10, Thm. 1], we can find a field extension L/K of degree 4 whose trace form is isometric to q_E, whose Galois closure $\widetilde{L}/K$ has Galois group G. As before, its class in $H^1(K,G)$ corresponds to a faithful G-curve X defined over k with function field $\widetilde{L}$. By Proposition 5.25, it follows that $\widehat{\Delta}(X) = [A] + [(-1,-1)_2] + [(2,d_E)_2]$.

As in Case 1, suppose that there is a G-compression $f\colon X \to X_0$ and let $f'\colon X' \to X_0'$ be the base extension of f to $k' = k(\sqrt{2})$. There exists a

commutative diagram

$$\begin{array}{ccc} \mathrm{Br}_2(k(X_0)^G) & \xrightarrow{i_*} & \mathrm{Br}_2(K) \\ \downarrow{\scriptstyle j_0} & & \downarrow{\scriptstyle j} \\ \mathrm{Br}_2(k'(X_0')^G) & \xrightarrow{i'_*} & \mathrm{Br}_2(k'(x)) \end{array}$$

where the vertical arrows are induced by base extension and the horizontal arrows are induced by f and f'. By Proposition 5.24, we must have $i_*(\widehat{\Delta}(X_0)) = \widehat{\Delta}(X)$ in $\mathrm{Br}_2(K)$. By Proposition 5.27(b), it follows that $j_0(\widehat{\Delta}(X_0)) = [(-1,-1)_2]$, since 2 is a square in k'. Consequently, we conclude that

$$[(-1,-1)_2] = i'_*(j_0(\widehat{\Delta}(X_0))) = j(i_*(\widehat{\Delta}(X_0))) = j(\widehat{\Delta}(X)) = [A]+[(-1,-1)_2],$$

whence A must be split over $k'(x)$. This contradicts our initial assumption.

Since G does not act faithfully on any curve of genus 1, it follows from Lemma 5.1 that there exist strongly incompressible G-curves. □

Chapter 6

Conclusions and open problems

6.1 Finite group actions on conics

Let q be a nondegenerate quadratic form of rank 3 over k. Recall that q defines a (smooth projective) k-curve $X_q \subset \mathbb{P}^2$ of genus 0. Such a curve is usually referred to as a *conic*. It is well known that any smooth projective curve of genus 0 is isomorphic to some conic X_q, where q is unique up to scalar multiplication. Note that $X_q \cong \mathbb{P}^1$ if and only if q is isotropic over k.

Recall that the automorphism group of X_q is isomorphic to the *group of projective similitudes* $\mathrm{PGO}(q)$ (see [8, Cor. 69.6]). Since $\mathrm{rank}(q) = 3$ is odd, there exists an isomorphism of algebraic groups $\mathrm{PGO}(q) \cong \mathrm{SO}(q)$ (cf. [16, Prop. 12.4 and 12.6]), which is an absolutely simple adjoint group of type B_1. The accidental isomorphism of Dynkin diagrams $A_1 = B_1$ implies that

$$\mathrm{SO}(q) \cong \mathrm{PGL}_1(A_q),$$

where A_q is a quaternion algebra with Severi-Brauer conic X_q.

In the case where q is isotropic, we have that $\mathrm{SO}(q) \cong \mathrm{PGL}_2$. The classification, up to conjugacy, of finite subgroups of PGL_2 (or equivalently, finite group actions on the projective line) over an arbitrary field can be found in [2, 11]. In Chapter 3 of this thesis, we classify the finite subgroups of $\mathrm{SO}(q)$ up to conjugacy, for every nondegenerate ternary quadratic form q and every base field of characteristic different from 2.

To complete the classification of finite subgroups of absolutely simple adjoint group of type $B_1 = A_1$, it remains to consider the non-split case over a base field of characteristic 2. To the author's best knowledge, this case remains wide open. To fix ideas, let q be an anisotropic ternary quadratic form over a base field k of characteristic 2. After rescaling, we may assume that $q \simeq \langle 1 \rangle \perp [a, b]$ for some $a, b \in k$, where $[a, b]$ stands for the binary quadratic form $ax^2 + xy + by^2$ (cf. [8, Cor. 7.32]).

Question 6.1. What are the finite subgroups of $\mathrm{SO}(q)$? What can we say about their conjugacy classes?

We do not even know whether $\mathrm{SO}(q)$ can contain a 2-irregular subgroup (i.e., a subgroup of even order) when q is anisotropic. We showed in Theorem 1.1 that this assertion fails if 2 is replaced by an odd prime p, but the proof relies on Lemma 3.1(b), which breaks down in characteristic 2.

6.2 Geometric Galois embedding problems

In this section, all groups are assumed to be finite. Let M/K be Galois extension with Galois group G, and let $\pi\colon E \twoheadrightarrow G$ be a group epimorphism. The *Galois embedding problem* given by M/K and π asks for the existence of an E-Galois extension F/K, such that $M \subset F$ and π coincides with the natural surjection $E \cong \mathrm{Gal}(F/K) \twoheadrightarrow \mathrm{Gal}(M/K) \cong G$ (cf. [19, §2.2]).

Let X be a geometrically irreducible faithful G-variety defined over a base field k. It is well known that $k(X)/k(X)^G$ is a G-Galois extension. Given this extension and an epimorphism $\pi\colon E \twoheadrightarrow G$, we can then define a Galois embedding problem, which we refer to as the *geometric Galois embedding problem* given by X and π.

How can we interpret a solution to the above problem geometrically? Suppose that $F/k(X)^G$ is such a solution. Then, there exists a faithful E-variety Y/k such that $k(Y) \cong F$ as k-fields with an E-action. (Such an E-variety is commonly referred to as a *model* for F.) In particular, this implies that $Y/\mathrm{Ker}(\pi)$ and X are birationally isomorphic as G-varieties. We have thus proven that the geometric Galois embedding problem given by X and π is equivalent to the following *lifting problem*.

Question 6.2. Determine necessary and sufficient conditions on X/k and $\pi\colon E \twoheadrightarrow G$ for the existence of a faithful E-variety Y/k such that $Y/\mathrm{Ker}(\pi)$ is G-equivariantly birationally isomorphic to X.

In Chapter 4, we completely answered the above question in the case where $X = \mathbb{P}^1$ over an arbitrary field of characteristic 0 and π is any double cover of a Kleinian group G acting on the projective line. That case is particularly interesting because the typical solutions to the lifting problem are hyperelliptic curves endowed with a group action. To the author's best knowledge, the analogous problem is still open over a base field of positive characteristic. Even over an algebraically closed field k, the literature available on the complete classification of automorphism groups of hyperelliptic curves often assumes that $\mathrm{char}(k) = 0$ (cf. [5, 33]).

We illustrate an interesting connection between Galois cohomology and the geometric Galois embedding problem for X and π considered above. Suppose that $N := \mathrm{Ker}(\pi)$ is abelian and consider the exact sequence

$$1 \longrightarrow N \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1.$$

This induces to an exact sequence in cohomology

$$H^1(K, E) \longrightarrow H^1(K, G) \xrightarrow{\Delta} H^2(K, N),$$

where $K := k(X)^G$. Recall that X gives rise to a cohomology class $[X] \in H^1(K, G)$ (see Section 5.1). We claim that the solvability of the lifting problem is closely related to the vanishing of the class $\Delta([X]) \in H^2(K, N)$. Indeed, if Y is a solution to the lifting problem, then $[X]$ is the image of $[Y]$ in the above exact sequence, which implies that $\Delta([X]) = 0$. Conversely, if $\Delta([X]) = 0$, it follows that $[X]$ arises from a class in $c \in H^1(K, E)$. However, a variety Y representing c is *not* necessarily irreducible. (In general, Y is a primitive E-variety, i.e., E permutes the irreducible components of Y.) In the usual language of Galois embedding problems, such a Y would correspond to a *weak* solution to the problem (cf. [19, §2.4]). Under certain mild hypotheses though, one can guarantee that a weak solution is a proper solution as well, e.g., when $N \cong \mu_p$ for some prime $p \neq \mathrm{char}(k)$, and k contains all p-th roots of unity (see [19, Thm. 2.4.1 and Cor. 2.4.2]).

The above interpretation can be used to solve the lifting problem in certain cases. To fix ideas, let us assume that N is cyclic, i.e., $N = \mu_m$. Then, we can interpret $H^2(K, \mu_m)$ as the m-th torsion part of the Brauer group $\mathrm{Br}(K)$, and therefore $\Delta([X])$ represents the Brauer class of some central simple algebra of period dividing m.

In this thesis, we compute such Brauer class in certain instances. For example, suppose that we can find a diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathrm{GL}(V) & \longrightarrow & \mathrm{PGL}(V) & \longrightarrow & 1 \\ & & \uparrow & & \uparrow{\scriptstyle \overline{\rho}} & & \uparrow{\scriptstyle \rho} & & \\ 1 & \longrightarrow & N & \longrightarrow & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \end{array}$$

Then Lemma 5.6 implies the lifting problem for ${}_{\rho}\mathbb{P}(V)$ and π is (weakly) solvable. (Recall that ${}_{\rho}\mathbb{P}(V)$ is simply the projective space $\mathbb{P}(V)$ endowed with a G-action via ρ.) In the case where $N = \mu_2$ and $\dim(V) = 2$, we recover some of the results in Chapter 4. Unfortunately, the technique above

does not work for all exact sequences $1 \to N \to E \to G \to 1$, as they might not fit into the required commutative diagram (see, e.g., Remark 5.26).

A more systematic method to compute the class $\Delta([X])$ based on geometric properties of the G-variety X would be very desirable.

6.3 Strongly incompressible varieties

Let G be an algebraic group. Recall that a *G-compression* of a generically free G-variety X is a dominant G-equivariant rational map onto another generically free G-variety. We say that X is *strongly incompressible* if every G-compression of X is birational.

It is natural to pose the following question.

Question 6.3. Let k be a base field, let G/k be an algebraic group and let n be a positive integer. Does there exist a strongly incompressible G-variety of dimension n defined over k? If so, can one construct explicit examples of such G-varieties?

In dimension 1, Z. Reichstein ([24]) showed the existence of strongly incompressible G-curves for finite groups G that cannot act faithfully on curves of genus ≤ 1. In Chapter 5 of this thesis, we answer the existence part of the above question for every field of characteristic 0 and every finite group G. Roughly, the classification goes as follows: There always exist strongly incompressible G-curves if G cannot act faithfully on a curve of genus 0. If, on the contrary, G has a faithful action on a curve of genus 0, then the existence of strongly incompressible G-curves depends on the arithmetic of the field k. In particular, after a large enough algebraic extension of k, one can prove that all G-curves are compressible.

In higher dimensions, the situation is largely unexplored. However, some progress has been made in dimension 2. N. Fakhruddin proved in an unpublished note that if G is a finite group that does not act faithfully on a rational surface or a surface of Kodaira dimension 0 or 1 with finite fundamental group, then there exist a strongly incompressible complex G-surface. In particular, his results imply that all but finitely many non-abelian simple groups have strongly incompressible actions on complex surfaces. Also, R. Pardini has shown that any group containing $(\mathbb{Z}/2\mathbb{Z})^6$ or $(\mathbb{Z}/p\mathbb{Z})^5$ (p an odd prime) acts strongly incompressibly on some complex surface. Perhaps more importantly, she produces an explicit example of a strongly incompressible complex surface: if C is a Hurwitz curve of genus $g \geq 2$, then $(\mathrm{Aut}(C))^2 \rtimes (\mathbb{Z}/2\mathbb{Z})$ acts strongly incompressibly on $C \times C$.

In most cases, the problem of constructing examples of strongly incompressible G-varieties remains open, even in dimension 1. Our argument in Lemma 5.1 is essentially non-constructive and though in Chapter 5 we give several examples of G-curves that compress to some strongly incompressible curve, we do not know if they are strongly incompressible themselves.

Bibliography

[1] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen. Finiteness results for modular curves of genus at least 2. *Amer. J. Math.*, 127(6):1325–1387, 2005.

[2] Arnaud Beauville. Finite subgroups of $\mathrm{PGL}_2(K)$. In *Vector bundles and complex geometry*, volume 522 of *Contemp. Math.*, pages 23–29. Amer. Math. Soc., Providence, RI, 2010.

[3] Grégory Berhuy and Giordano Favi. Essential dimension: a functorial point of view (after A. Merkurjev). *Doc. Math.*, 8:279–330 (electronic), 2003.

[4] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1991.

[5] Rolf Brandt and Henning Stichtenoth. Die Automorphismengruppen hyperelliptischer Kurven. *Manuscripta Math.*, 55(1):83–92, 1986.

[6] Xi Chen. Self rational maps of $k3$ surfaces. arXiv:1008.1619 [math.AG], 2010.

[7] Xi Chen. Rational self maps of Calabi-Yau manifolds. In *A celebration of algebraic geometry*, volume 18 of *Clay Math. Proc.*, pages 171–184. Amer. Math. Soc., Providence, RI, 2013.

[8] Richard Elman, Nikita Karpenko, and Alexander Merkurjev. *The algebraic and geometric theory of quadratic forms*, volume 56 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2008.

[9] Richard Elman and Adrian R. Wadsworth. Hereditarily quadratically closed fields. *J. Algebra*, 111(2):475–482, 1987.

[10] Martin Epkenhans and Martin Krüskemper. On trace forms of étale algebras and field extensions. *Math. Z.*, 217(3):421–434, 1994.

[11] Xander Faber. Finite p-irregular subgroups of $\mathrm{PGL}_2(k)$. arXiv:1112.1999 [math.NT], 2011.

[12] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.

[13] Skip Garibaldi, Alexander Merkurjev, and Jean-Pierre Serre. *Cohomological invariants in Galois cohomology*, volume 28 of *University Lecture Series*. American Mathematical Society, Providence, RI, 2003.

[14] Nikita A. Karpenko and Alexander S. Merkurjev. Essential dimension of finite p-groups. *Invent. Math.*, 172(3):491–508, 2008.

[15] Felix Klein. *Lectures on the icosahedron and the solution of equations of the fifth degree*. Dover Publications, Inc., New York, N.Y., revised edition, 1956. Translated into English by George Gavin Morrice.

[16] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol. *The book of involutions*, volume 44 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1998. With a preface in French by J. Tits.

[17] Tsit Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.

[18] Serge Lang and John Tate. Principal homogeneous spaces over abelian varieties. *Amer. J. Math.*, 80:659–684, 1958.

[19] Arne Ledet. *Brauer type embedding problems*, volume 21 of *Fields Institute Monographs*. American Mathematical Society, Providence, RI, 2005.

[20] Arne Ledet. Finite groups of essential dimension one. *J. Algebra*, 311(1):31–37, 2007.

[21] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[22] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser Boston, Boston, MA, 1991.

[23] Zinovy Reichstein. On the notion of essential dimension for algebraic groups. *Transform. Groups*, 5(3):265–304, 2000.

[24] Zinovy Reichstein. Compressions of group actions. In *Invariant theory in all characteristics*, volume 35 of *CRM Proc. Lecture Notes*, pages 199–202. Amer. Math. Soc., Providence, RI, 2004.

[25] Zinovy Reichstein. Essential dimension. In *Proceedings of the International Congress of Mathematicians. Volume II*, pages 162–188. Hindustan Book Agency, New Delhi, 2010.

[26] Zinovy Reichstein and Angelo Vistoli. Birational isomorphisms between twisted group actions. *J. Lie Theory*, 16(4):791–802, 2006.

[27] Zinovy Reichstein and Boris Youssin. Splitting fields of G-varieties. *Pacific J. Math.*, 200(1):207–249, 2001.

[28] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[29] Jean-Pierre Serre. Extensions icosaédriques. In *Seminar on Number Theory, 1979–1980 (French)*, pages Exp. No. 19, 7. Univ. Bordeaux I, Talence, 1980.

[30] Jean-Pierre Serre. L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$. *Comment. Math. Helv.*, 59(4):651–676, 1984.

[31] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.

[32] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, second edition, 2008. With notes by Henri Darmon.

[33] Tanush Shaska. Determining the automorphism group of a hyperelliptic curve. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 248–254 (electronic). ACM, New York, 2003.

[34] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[35] Núria Vila. On stem extensions of S_n as Galois group over number fields. *J. Algebra*, 116(1):251–260, 1988.

Appendix A

Proof of Theorem 5.2

Lemma A.1. *Let P, Q be two polynomials in $k[x]$, not both zero, and let $A \subset \overline{k}$ be the set of their common roots. Then for all but finitely many $c \in k$, the polynomial $P + cQ$ has no multiple roots outside of A.*

Proof. It suffices to show that given two coprime polynomials $P, Q \in k[x]$, the polynomial $P + cQ$ has simple roots for all but finitely many $c \in k$. If both polynomials are constant, the result is immediate, so we may assume that is not the case. Note that $\xi \in \overline{k}$ is a multiple root of $P + cQ$ if and only if $P(\xi) + cQ(\xi) = P'(\xi) + cQ'(\xi) = 0$, which implies that $P(\xi)Q'(\xi) - P'(\xi)Q(\xi) = 0$. The polynomial $PQ' - P'Q$ cannot be identically zero because P and Q are coprime and not both constant, so it has finitely many roots. If we take $c \in k$ outside the finite set

$$\{-P(\xi)/Q(\xi) \mid \xi \in \overline{k} \text{ satisfies } P(\xi)Q'(\xi) - P'(\xi)Q(\xi) = 0,\ Q(\xi) \neq 0\},$$

it follows that $P + cQ$ has simple roots. The proof is complete. □

Definition A.2. We define a *ramification condition* to be an l-tuple of integers $\mathcal{P} = (b_1, \ldots, b_l)$, where $l \geq 1$ and $b_i \geq 2$ for all i. We say that $P \in k[x]$ has a *local decomposition of type $\mathcal{P}$ at $\beta \in k$*, if there exists a factorization

$$P(x) - \beta = a(x - \alpha_1)^{b_1} \ldots (x - \alpha_l)^{b_l}(x - \alpha_{l+1}) \ldots (x - \alpha_r),$$

where a is the leading coefficient of P, and $\alpha_1, \ldots, \alpha_r$ are distinct elements in $\overline{k}$.

Proposition A.3. *Let $\mathcal{P}_i = (b_{i,1}, \ldots, b_{i,l_i})$ $(1 \leq i \leq n)$ be a collection of ramification conditions (not necessarily distinct), and let $\beta_1, \ldots, \beta_n$ be distinct points in k. Then there exists a polynomial $P \in k[x]$ that satisfies local decompositions of type $\mathcal{P}_i$ at β_i for $1 \leq i \leq n$. Moreover, we can choose* $\deg(P)$ *to be any sufficiently large positive integer.*

Proof. Choose distinct points $a_{ij} \in k$ for $1 \leq i \leq n$, $1 \leq j \leq l_i$. By the Chinese Remainder Theorem, there exists $Q \in k[x]$ such that

$$Q(x) \equiv \beta_i + (x - a_{ij})^{b_{ij}} \mod (x - a_{ij})^{b_{ij}+1},$$

for $1 \leq i \leq n$, $1 \leq j \leq l_i$. We define

$$H(x) = \prod_{i,j} (x - a_{ij})^{b_{ij}+1}$$

and we let $A = \{a_{ij}\}_{i,j}$ be the set of its roots. Applying Lemma A.1 to $g_i = Q - \beta_i$ and H for $1 \leq i \leq n$, we conclude that there exists a finite set $S \subset k$ such that if $c \in k$ lies outside S, the polynomials $g_i + c\,H$ contain no multiple roots outside of A for $1 \leq i \leq n$. Choose any such c and define $P = Q + c\,H$. We claim that P satisfies the desired conditions. Indeed, note that the following properties hold.

(i) For $1 \leq i \leq n$, $1 \leq j \leq l_i$, the polynomial $P - \beta_i$ has a root of multiplicity b_{ij} at the point a_{ij}.

(ii) If $i' \neq i$, we have $P(a_{i'j}) = \beta_{i'} \neq \beta_i$ and therefore $P - \beta_i$ cannot have any root of the form $a_{i'j}$.

(iii) By construction, $P - \beta_i$ does not have multiple roots outside of A.

It remains to prove that we can take $\deg(P)$ to be any sufficiently large positive integer d. To show this, take $n = \max(\deg(Q), \deg(H))$. We claim that there exists P satisfying the desired properties such that $\deg(P) = d$ for any $d > n$. Indeed, if we replace $H(x)$ by $(x - a_{11})^{d - \deg H} H(x)$ and ensure that $c \neq 0$ in the definition of P, it follows easily that $\deg(P) = d$. □

Proof of Theorem 5.2. Without loss of generality, we may assume that $G = S_m$ for some $m \geq 2$. Given a partition $b_1 + \ldots + b_s$ of m, where $b_1 \geq \ldots \geq b_l > 1 = b_{l+1} = \ldots = b_s$ for some $l \geq 1$, we can define a ramification condition $\mathcal{P} = (b_1, \ldots, b_l)$. Let $\mathcal{P}_1, \ldots, \mathcal{P}_n$ be the ramification conditions obtained as we range over all possible partitions of m, except for $1 + \ldots + 1$. By Proposition A.3, we can construct a polynomial $P \in k[x]$ satisfying local decompositions of type $\mathcal{P}_i$ at distinct points β_i for $1 \leq i \leq n$. Moreover, we may assume that $\deg(P)$ is some sufficiently large prime number p.

Let the group S_p act on p letters and embed S_m inside S_p as the subgroup that fixes the last $p - m$ letters. We want to construct X as a ramified S_p-cover of $\mathbb{P}^1$. Let $P_t(x) = P(x) - t$, where t is an indeterminate, and define L as the splitting field of P_t over $k(t)$. It is clear that $\mathrm{Gal}(L/k(t))$ is a

transitive subgroup of S_p; we claim that equality holds. Since $\mathrm{Gal}(L\overline{k}/\overline{k}(t))$ is a subgroup of $\mathrm{Gal}(L/k(t))$, it suffices to prove that the former is isomorphic to S_p. (Note that this also implies that L is regular, i.e., $L \cap \overline{k} = k$.) We use a technique similar to [32, Thm. 4.4.5]. We may view the polynomial P_t as a ramified cover $\mathbb{P}^1 \to \mathbb{P}^1$ of degree p. Note that $\beta_1, \dots, \beta_n, \infty$ are among the ramification points. If $\mathcal{P}_i = (b_1^{(i)}, \dots, b_{l_i}^{(i)})$, the inertia subgroup at β_i is generated by an element of S_p of cycle type $(b_1^{(i)}, \dots, b_{l_i}^{(i)}, 1, \dots, 1)$, while the inertia group at ∞ is a p-cycle. In particular, $\mathrm{Gal}(L\overline{k}/\overline{k}(t))$ contains the subgroup generated by a p-cycle and a transposition, which is all of S_p since p is prime. The claim follows immediately.

Let X be the (unique) smooth projective curve defined over k with function field L, which is geometrically irreducible since L/k is regular. Note that X can be endowed with a natural faithful S_p-action via the Galois action on L. If Q is a closed point in $X_{\overline{k}}$ lying above β_i, then its stabilizer is a cyclic subgroup generated by an element of S_p of cycle type $(b_1^{(i)}, \dots, b_{l_i}^{(i)}, 1, \dots, 1)$. Since any two subgroups of this form are conjugate, they all occur as stabilizers of points in the fibre above β_i. Clearly, any nontrivial element of S_m has one of the above cycle types inside S_p, so it fixes at least one geometric point in X. The proof is complete. □