Canad. J. Math. Vol. 68 (3), 2016 pp. 541–570
http://dx.doi.org/10.4153/CJM-2015-012-3

Strongly Incompressible Curves

Mario Garcia-Armas

Abstract. Let G be a finite group. A faithful G-variety X is called strongly incompressible if every dominant G-equivariant rational map of X onto another faithful G-variety Y is birational. We settle the problem of existence of strongly incompressible G-curves for any finite group G and any base field k of characteristic zero.

1 Introduction

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 [Re04, §2], where the author asks for a classification of strongly incompressible G-varieties (see also [Re10, §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. X. Chen [Ch10] proved that every dominant self-rational map of a very general projective $K3$ surface of genus $g \geq 2$ is birational (see [Ch12] 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 [Re04, Example 6]). In unpublished notes, N. Fakhruddin and R. Pardini have independently proved the existence of strongly incompressible complex G-surfaces for certain finite groups G. To the best of our knowledge, no examples of strongly incompressible varieties are known in higher dimensions.

In this paper, we study the question of the existence of strongly incompressible G-curves for every finite group G and every base field k of characteristic 0 (see Section 2 for more details on our assumption on $\mathrm{char}(k)$). We settle the classification problem for G-curves raised in [Re04], by considering finite groups G that can act on a curve of genus ≤ 1. In Section 3, we show that strongly incompressible G-curves exist if G does not act faithfully on any curve of genus 0.

Theorem 1.1 (see Theorem 3.4) *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.*

Received by the editors September 24, 2014; revised February 25, 2015.
Published electronically March 8, 2016.
The author is partially supported by a Four Year Fellowship, University of British Columbia.
AMS subject classification: **14L30**, 14E07, 14H37.
Keywords: algebraic curves, group actions, Galois cohomology.

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 4 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, 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 6–9. Our results are summarized in the following theorem. In this paper, we denote the dihedral group of $2n$ elements by D_{2n}. For a definition of cohomological 2-dimension of a field k, denoted by $\mathrm{cd}_2(k)$, we refer the reader to [Se02, I.§3]. We remark that k has cohomological 2-dimension zero if and only if every algebraic extension of k is quadratically closed (see [EW87, Lemma 2]).

Theorem 1.2 *Let $n \geq 2$ be an integer and let ω_n be a primitive n-th root of* 1.

- (i) *(Theorem 3.4, Proposition 6.4) 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 $\omega_n + \omega_n^{-1} \notin k$.*
- (ii) *(Theorem 3.4, Propositions 6.3 and 7.1) Suppose that n is even. Then there exist strongly incompressible $\mathbb{Z}/n\mathbb{Z}$-curves if and only if $\omega_n \notin k$.*
- (iii) *(Theorem 3.4, Proposition 8.7) 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* $\mathrm{cd}_2(k) > 0$.
- (iv) *(Propositions 8.1 and 9.6) Let $G = (\mathbb{Z}/2\mathbb{Z})^2$, 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 [Re04].

Corollary 1.3 *Let G be a nontrivial finite group and let k be an algebraically closed base field. 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.*

2 Notation and Preliminaries

Let k denote a base field of characteristic 0 and let $\overline{k}$ be its algebraic closure. A *k-variety* X is a geometrically reduced scheme of finite type over k (not necessarily irreducible). The word "curve" is reserved for a geometrically irreducible smooth projective 1-dimensional variety. A *point* of a variety means a geometric point, unless stated otherwise.

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 defined 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 of the algebra of G-invariant functions $k(X)^G$ into $k(X)$ induces a *rational quotient map* $\pi_X \colon X \dashrightarrow W$, where $k(W) = k(X)^G$ (see [Ros56, Ros63]). 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. 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 corresponding rational quotient maps. The above constructions are detailed in [Re00], where the base field is assumed to be algebraically closed. However, the results there easily carry over to the general case, since the approach in [Re00] builds on the work of M. Rosenlicht [Ros56, Ros63], where the base field is arbitrary.

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 [BF03, Theorem 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.

As we defined in the introduction, a generically free G-variety X is said to be *strongly incompressible* if every G-compression of X is birational. However, as it stands, this definition is not satisfactory over base fields k of characteristic $p > 0$. Indeed, we claim that for every finite group G and every G-variety X defined over k, there exists a non-birational G-compression of X. Indeed, let $F_{X/\operatorname{Spec}(k)} \colon X \to X^{(p)}$ be the relative Frobenius morphism associated to X (see [Liu02, §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 $F_{X/\operatorname{Spec}(k)}$ into a dominant G-equivariant morphism, which has degree $p^{\dim(X)}$ by [Liu02, Corolary 2.27]. To complete the proof of the claim, we must show that the G-action on $X^{(p)}$ is faithful. Let N be the kernel of the action. Then we must have $k(X^{(p)}) \subset k(X)^N \subset k(X)$, where the inclusion $k(X^{(p)}) \subset k(X)$ is the purely inseparable extension induced by $F_{X/\operatorname{Spec}(k)}$. Thus $k(X)/k(X)^N$ is both Galois and purely inseparable, which implies that N is trivial.

In view of the above argument, it seems natural to define strong incompressibility by requiring that only *separable* G-compressions should be birational. The techniques used in the present paper do not carry over easily to that setting, though some results remain true (see Lemma 3.1). We do not pursue this direction any further and assume in the sequel that our base field k has characteristic 0.

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 $\big(f(x), g(x)\big)_2$ 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 $f(\alpha) = r(\alpha)^2 p(\alpha)^{-2} \in k(\alpha)^{\times 2}$. ∎

3 Strong Incompressibility of Curves

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 G-equivariant surjective finite 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 3.1 ([Re04, 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 the Hurwitz Formula (see [Liu02, Theorem 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 [RY01, Proposition 8.6] (see also [RY01, Remark 9.9]), whose proof depends on the 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 3.2 *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 3.3 *Let E be an elliptic curve defined over a field k.*

(i) *There exists a split exact sequence*

$$1 \longrightarrow E \xrightarrow{i} \mathrm{Aut}(E) \xrightarrow{\pi} \mathrm{Aut}_0(E) \longrightarrow 1\,, \tag{3.1}$$

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

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

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

(iii) *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 k contains a primitive fourth (resp. sixth) root of unity.*

(iv) *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 (i) See [Sil09, §X.5]. Note that in [Sil09] $\mathrm{Aut}(E)$ and $\mathrm{Aut}_0(E)$ are denoted by $\mathrm{Isom}(E)$ and $\mathrm{Aut}(E)$, respectively.

(ii) See [Sil09, Corolary III.10.2].

(iii) This follows directly from part (ii).

(iv) 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 3.4 *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 3.1, 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 [Beau10, Proposition 1.1]). By Theorem 3.2, 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. Extending to 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 (3.1) and the fact that $G \not\simeq \mathbb{Z}/n\mathbb{Z}$ for $n = 1, 2, 3, 4, 6$, we conclude that $G \cap i(E_{\overline{k}}) \neq \varnothing$. 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 element of 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 4 to the study of equivariant rational maps to projective spaces, and we will use these results to understand compressions onto curves of genus 0.

4 Equivariant Maps to Projective Spaces

Let G be an algebraic group defined over a field k. A projective representation $\rho: G \hookrightarrow \mathrm{PGL}(V)$ 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

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{G}_m \arrow[r] & \mathrm{GL}(V) \arrow[r] & \mathrm{PGL}(V) \arrow[r] & 1\,, \\
1 \arrow[r] & \mathbb{G}_m \arrow[r] \arrow[u, equal] & G' \arrow[r] \arrow[u, hook, "\overline{\rho}"'] & G \arrow[r] \arrow[u, hook, "\rho"'] & 1
\end{tikzcd}$$

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

$$\begin{tikzcd}
 & 1 \arrow[r] & H^1(K, \mathrm{PGL}(V)) \arrow[r] & H^2(K, \mathbb{G}_m) \\
1 \arrow[r] & H^1(K, G') \arrow[r, "\phi"] \arrow[u, "\overline{\rho}_*"'] & H^1(K, G) \arrow[r, "\Delta_\rho"] \arrow[u, "\rho_*"'] & H^2(K, \mathbb{G}_m). \arrow[u, equal]
\end{tikzcd}$$

(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

$$\Delta_\rho : H^1(K, G) \to H^2(K, \mathbb{G}_m) = \mathrm{Br}(K).$$

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 4.1 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 4.2 *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

$$\phi\colon H^1(K, G') \to H^1(K, G),$$

where $K = k(Y)^G$. Let $\widetilde{Y}$ be as in Construction 4.1. 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 $\phi([\widetilde{Y}]) = [\widetilde{Y}/\mathbb{G}_m] = [Y]$. ∎

Proposition 4.3 *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.*

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

$$\begin{tikzcd} H^1(K,G) \arrow[r, "\Delta_\rho^K"] \arrow[d, "i_*"'] & H^2(K,\mathbb{G}_m) \arrow[d] \\ H^1(L,G) \arrow[r, "\Delta_\rho^L"] & H^2(L,\mathbb{G}_m). \end{tikzcd}$$

It is well known that in the above situation we must have $i_*([Y]) = [X]$. By Lemma 4.2, we have $\Delta_\rho^K(Y) = 1$. The commutativity of the above diagram then implies that $\Delta_\rho^L(X) = 1$.

Case 2. In the argument below, every point is assumed to be a geometric point unless stated otherwise. Suppose that the G-action on Y has a kernel H. Let $\widetilde{Y}$ be as in Construction 4.1, 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 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 $h \in H$ be arbitrary and let $h^* \in \pi^{-1}(h)$ be any lift. Since h acts trivially on y, there exists an element $\lambda_{h^*} \in \mathbb{G}_m$ 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 $\mathrm{Stab}_{G'}(\widetilde{y}) = H'$. Since $\mathbb{G}_m$ acts freely on $\widetilde{Y}$, it is easy to see that $\lambda_{h^*}^{-1}h^*$ is the unique element in $\pi^{-1}(h)$ contained in H'; in

https://doi.org/10.4153/CJM-2015-012-3 Published online by Cambridge University Press

particular, it is independent of the lift h^*. It follows that the section $s: H \to \pi^{-1}(H)$ 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:

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{G}_m \arrow[r] \arrow[d, equal] & G' \arrow[r, "\pi"] \arrow[d] & G \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathbb{G}_m \arrow[r] & G'/H' \arrow[r] & G/H \arrow[r] & 1.
\end{tikzcd}$$

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 $i: K \hookrightarrow L$. Using the bottom sequence above, we obtain a commutative diagram in cohomology:

$$\begin{tikzcd}
H^1(K, G'/H') \arrow[r] \arrow[d] & H^1(K, G/H) \arrow[r] \arrow[d, "i_*"'] & H^2(K, \mathbb{G}_m) \arrow[d] \\
H^1(L, G'/H') \arrow[r] & H^1(L, G/H) \arrow[r] & H^2(L, \mathbb{G}_m).
\end{tikzcd}$$

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 the commutative diagram

$$\begin{tikzcd}
H^1(L, G') \arrow[r] \arrow[d] & H^1(L, G) \arrow[r, "\Delta_\rho"] \arrow[d] & H^2(L, \mathbb{G}_m) \arrow[d, equal] \\
H^1(L, G'/H') \arrow[r] & H^1(L, G/H) \arrow[r] & H^2(L, \mathbb{G}_m).
\end{tikzcd}$$

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.

(ii) 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 $\pi_V: V \dashrightarrow {}_\rho\mathbb{P}(V)$ 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 [Se03, 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.

https://doi.org/10.4153/CJM-2015-012-3 Published online by Cambridge University Press

Corollary 4.4 *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 4.3(i). 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 4.3(ii), 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 Some Explicit Computations

In this section, we explicitly compute the invariant introduced in Section 4 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 $\mathbb{P}^1$. In what follows, the class of an element $a \in k^\times$ in $k^\times/k^{\times 2}$ will be denoted by $\overline{a}$.

Recall that the conjugacy classes of embeddings of $(\mathbb{Z}/2\mathbb{Z})^2$ into $\mathrm{PGL}_2(k)$ 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 (see [Beau10, Proposition 3.4]). We 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.

- Suppose that both a and b are non-squares. Then we have

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

  where $\lambda^2 - a \equiv b \mod k^{\times 2}$ (we can find such $\lambda \in k$ because $(a,b)_2$ is split).
- Suppose that $\overline{a} = \overline{1}$. Then we have

$$\rho_{(a,b)}\colon e_1 \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} \quad e_2 \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{5.1}$$

- Suppose that $\overline{b} = \overline{1}$. Then we have

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

(If $(\overline{a}, \overline{b}) = (\overline{1}, \overline{1})$, the last two embeddings are conjugate.) 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 5.1 *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 $\rho_{(a,b)*}: (K^\times/K^{\times 2})^2 \to H^1(K, \mathrm{PGL}_2)$ 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

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

where the embedding ϕ is given by $e_1 \mapsto [i]$, $e_2 \mapsto [j]$. We have therefore reduced the problem to showing that $\phi_*: (K^\times/K^{\times 2})^2 \to H^1(K, \mathrm{PGL}_1(\mathcal{A}))$ 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 $\phi_*(\overline{c}, \overline{d})$ 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 $v: \mathrm{Gal}(L/K) \to \mathrm{PGL}_1(\mathcal{A})(L)$ representing $\phi_*(\overline{c}, \overline{d})$ 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

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

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 $\phi_*(\overline{c}, \overline{d})$ 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 $\phi_*(\overline{c}, \overline{d}) = (bd, ac)_2 \cong (ac, bd)_2$. ∎

Recall now that the group $\mathbb{Z}/2\mathbb{Z}$ embeds into $\mathrm{PGL}_2(k)$ over any field k and the possible embeddings are of the form

$$\rho_b: -1 \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix},$$

up to conjugacy (see[Beau10, Theorem 4.2]). We denote ${}_{\rho_b}\mathbb{P}^1$ simply by ${}_b\mathbb{P}^1$. Note that ${}_b\mathbb{P}^1$ and ${}_{b'}\mathbb{P}^1$ are isomorphic as $\mathbb{Z}/2\mathbb{Z}$-varieties if and only if $\overline{b} = \overline{b'}$. By [Le07, Example 6], it follows that ${}_b\mathbb{P}^1$ is versal if and only if $b \in k^{\times 2}$.

Corollary 5.2 *Let ρ_b be defined 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 $\Delta_{\rho_b}(\overline{c}) = [(c, b)_2]$ for all $c \in K^\times$.*

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

to e_1. Therefore we must have $\rho_{b*}(\bar{c}) = \rho_{(1,b)*} \circ \phi_*(\bar{c}) = \rho_{(1,b)*}(\bar{c}, \bar{1}) = (c, b)_2$, where the last equality follows from Lemma 5.1. ∎

6 Cyclic and Dihedral Groups: Compressibility of $\mathbb{P}^1$

We set some notation for the remainder of the paper. Given an integer $n \geq 2$, let ω_n be a choice of a primitive n-th root of unity, let $\alpha_n = (\omega_n + \omega_n^{-1})/2$ and let $\beta_n = \alpha_n^2 - 1$.

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 [Beau10, Ga13] for details). 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 3.4.

Lemma 6.1 *Let $n \geq 3$ be any integer, let k be a field containing α_n, and define the embedding $\rho: D_{2n} \hookrightarrow \mathrm{PGL}_2(k)$ by sending*

$$\sigma \mapsto \begin{pmatrix} \alpha_n + 1 & \beta_n \\ 1 & \alpha_n + 1 \end{pmatrix} \quad \tau \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{6.1}$$

where σ, τ are the usual generators of D_{2n}. Then ${}_\rho\mathbb{P}^1$ is not strongly incompressible.

Proof We need to exhibit a G-equivariant map ${}_\rho\mathbb{P}^1 \to {}_\rho\mathbb{P}^1$ 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

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

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

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

and

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

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

$$u = (x + \beta_n^{1/2} y)^{n+1} + (x - \beta_n^{1/2} y)^{n+1},$$
$$v = \beta_n^{-1/2}\big((x + \beta_n^{1/2} y)^{n+1} - (x - \beta_n^{1/2} y)^{n+1}\big).$$

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 birational. ∎

Remark 6.2 Restricting the embedding (6.1) 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 6.3 *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 [Re04, Example 5]; we supply a short alternative proof. Recall that the embedding $\rho: \mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathrm{PGL}_2(k)$ 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 6.4 *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 introduced in (6.1) is generic for odd n, *i.e.*, the G-variety ${}_\rho\mathbb{P}^1$ is versal (see [Le07, Theorem 8]). It follows that any faithful G-variety can be G-compressed to ${}_\rho\mathbb{P}^1$. It thus suffices to prove that ${}_\rho\mathbb{P}^1$ itself is not strongly incompressible. This follows directly from Lemma 6.1. ■

7 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 the embedding $\rho: G \hookrightarrow \mathrm{PGL}_2(k)$ by sending

$$\sigma \mapsto \begin{pmatrix} \alpha_n + 1 & \beta_n \\ 1 & \alpha_n + 1 \end{pmatrix},$$

where σ is a generator of $\mathbb{Z}/n\mathbb{Z}$. Recall that this embedding is unique up to conjugacy (see [Beau10, Theorem 4.2], [Ga13, Remark 3.4]). By the results in Proposition 6.3, 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.

Proposition 7.1 *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 Our goal is to construct a hyperelliptic curve endowed with a faithful G-action that cannot be G-compressed to any curve of genus ≤ 1. The result then follows from Lemma 3.1.

Let $m = n/2$, let $K = k(t)$ be the rational function field, and consider the exact sequence $1 \to \mathbb{Z}/2\mathbb{Z} \to G \to \mathbb{Z}/m\mathbb{Z} \to 1$. Then we obtain an exact sequence in cohomology

$$1 \longrightarrow H^1(K, \mathbb{Z}/2\mathbb{Z}) \longrightarrow H^1(K, G) \longrightarrow H^1(K, \mathbb{Z}/m\mathbb{Z}).$$

Consider the class $[{}_\rho\mathbb{P}^1] \in H^1(K, G)$. Its image in $H^1(K, \mathbb{Z}/m\mathbb{Z})$ is equal to the class of the $\mathbb{Z}/m\mathbb{Z}$-variety $Y = {}_\rho\mathbb{P}^1/(\mathbb{Z}/2\mathbb{Z})$ (which is abstractly isomorphic to $\mathbb{P}^1$). Recall that σ^m maps to $\left(\begin{smallmatrix} 0 & \beta_n \\ 1 & 0 \end{smallmatrix}\right)$ under the embedding ρ. It thus follows that the quotient map ${}_\rho\mathbb{P}^1 \to Y$ is given by $(x:y) \mapsto (x^2+\beta_n y^2 : 2xy)$.

Note that $H^1(K,\mathbb{Z}/2\mathbb{Z}) = K^\times/K^{\times 2}$ acts on the fiber of $[Y]$. To describe this action, write $L = k({}_\rho\mathbb{P}^1) = k(u)$, which is a G-Galois extension of K. Then the subextension $L_0 = k(Y) = k(x)$ of L, where $x = \frac{u^2+\beta_n}{2u}$, corresponds to the $\mathbb{Z}/m\mathbb{Z}$-torsor $Y \to Y/(\mathbb{Z}/m\mathbb{Z})$. A short computation shows that L can be obtained from L_0 by adjoining $\sqrt{x^2-\beta_n}$. An element $c \in K^\times/K^{\times 2}$ acts on the torsor L/K by replacing $L = L_0(\sqrt{x^2-\beta_n})$ with $L_0(\sqrt{(x^2-\beta_n)f(t)})$, where $f(t) \in K$ is any representative of the class c. Recall that t is a rational function of x, say $t = p(x)/q(x)$. Thus, in general we obtain the function field of a hyperelliptic curve X, which is naturally endowed with a faithful G-action. Our goal is to make a clever selection of the class c. Fix $a \in k$, not a zero of either q or $qp' - pq'$, and let c be the class of $f(t) = q(a)t - p(a)$. An explicit hyperelliptic equation for X is given by $y^2 = s(x)$, where $s(x)$ is the square-free part of $(x^2-\beta_n)(q(a)p(x)-p(a)q(x))q(x)$. By assumption, $s(a) = 0$, whence $(x,y) = (a,0)$ is a k-rational point of X.

We claim that X 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 X has k-rational points. For the sake of contradiction, suppose that there exists a G-compression $X \to {}_\rho\mathbb{P}^1$. Regard this map as a $\mathbb{Z}/2\mathbb{Z}$-compression. As we saw before, ${}_\rho\mathbb{P}^1$ is isomorphic to ${}_{\beta_n}\mathbb{P}^1$ as a $\mathbb{Z}/2\mathbb{Z}$-variety. On the other hand, if we regard X as a $\mathbb{Z}/2\mathbb{Z}$-variety, its class $[X] \in H^1(L_0,\mathbb{Z}/2\mathbb{Z}) = L_0^\times/L_0^{\times 2}$ is given by $\overline{s(x)}$. If we denote the restriction of ρ to $\mathbb{Z}/2\mathbb{Z}$ by ρ', we conclude using Corollary 5.2 that $\Delta_{\rho'}(X) = [(s(x),\beta_n)_2]$. This class must be trivial over $L_0 = k(x)$ by Corollary 4.4. 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 prove that X cannot be G-compressed to any G-curve of genus 1. Since X has k-rational points, it suffices to prove that there is no G-compression $X \to E$, 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 3.3(i), 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 3.3(iv), 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 3.3(iii), 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 X, namely $(x,y) = (a,0)$. Hence, it must also fix a point in E. This contradiction completes the proof. ∎

Example 7.2 We will explicitly construct the curve X from the above proposition when $n = 4$. In this case, $\alpha_4 = (\omega_4 + \omega_4^{-1})/2 = 0$ and $\beta_4 = -1$. It suffices to construct

X over the field of rational numbers. Note that the field extension L_0/K satisfies $L_0 = k(x)$, $K = k(t)$, and $t = \frac{x^2-1}{2x}$. Taking $a = 1$, the above construction yields the function field

$$k(X) = L_0\Big(\sqrt{(x^2+1)\frac{x^2-1}{x}}\Big),$$

whose corresponding hyperelliptic equation is $y^2 = x^5 - x$. The $\mathbb{Z}/4\mathbb{Z}$-action on X is given by $\sigma\cdot(x, y) \mapsto (-1/x, y/x^3)$, where σ is a generator of $\mathbb{Z}/4\mathbb{Z}$. Note that this curve has genus 2 and it was proved above that it does not map G-equivariantly to any curve of genus ≤ 1. Hence it is an explicit example of a strongly incompressible $\mathbb{Z}/4\mathbb{Z}$-curve (recall that we are assuming $\omega_4 \notin k$ throughout). In general, this procedure will not necessarily yield a strongly incompressible G-curve, but a G-curve that can be G-compressed to a strongly incompressible one.

8 Strongly Incompressible Curves for Even Dihedral Groups

8.1 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 8.1 *The following are equivalent.*

(i) *There are no strongly incompressible G-curves over k.*
(ii) $\mathrm{cd}_2(k) = 0$.

Proof of (ii) ⇒ (i) Suppose that k has cohomological 2-dimension 0 and let X be any faithful G-curve. The fixed field $K = k(X)^G$ is a transcendence degree 1 extension of k, whence $\mathrm{cd}_2(K) \leq 1$ by [Se02, Proposition II.4.2.11]. Then, by [Se02, Proposition II.2.3.4], it follows that $\mathrm{Br}_2(K)$ is trivial. Let $\rho\colon (\mathbb{Z}/2\mathbb{Z})^2 \hookrightarrow \mathrm{PGL}_2(k)$ 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 4.4. 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 (5.1) with $b = 1$. 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) ⇒ (ii). To achieve this, we need the following result.

Proposition 8.2 *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 a rational function field, 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

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

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 these coordinates. Any point in $Y' \cap U_1$ must satisfy the equations

$$y - uP(yu) = 0 \quad \text{and} \quad yv^2 - uQ(yu) = 0.$$

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

$$P_1(x) = (P(x) - P(0))/x \quad \text{and} \quad Q_1(x) = (Q(x) - Q(0))/x.$$

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 $e_1 e_2$ has a fixed point in X. ∎

Lemma 8.3 *Let X be any (smooth projective) G-curve obtained from Proposition 8.2. 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 (i) and (ii) of Lemma 3.3, 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 8.1. 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 8.2. The following well-known lemma provides more manageable conditions on k.

Lemma 8.4 *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 [EW87, Lemma 2]. We now prove that (i) ⇒ (iv). If $\mathrm{cd}_2(k) = 0$, it follows from [Se02, Proposition II.4.1.11] that $\mathrm{cd}_2(k(x)) \le 1$. Then we conclude that $\mathrm{Br}_2(k(x)) = 0$ by [Se02, Proposition 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 $\big(x, h(x)\big)_2$ 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 8.5 In view of Lemma 8.4, given that $\mathrm{cd}_2(k) \ne 0$, 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

$$P(x) = (x-\alpha)\Big(\frac{(x-\alpha-1)h(x-\alpha) + (\alpha+1)h(-\alpha)}{(\alpha+1)h(-\alpha)x}\Big),$$
$$Q(x) = \alpha(\alpha+1-x)h(0)h(x-\alpha),$$

where $\alpha \in k$ is taken such that P has no multiple roots, $P(0) \ne 0$, and $Q(0) \ne 0$. (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 8.2. In what follows, let X denote the corresponding curve.

https://doi.org/10.4153/CJM-2015-012-3 Published online by Cambridge University Press

Lemma 8.6 *Let X be the curve obtained in Construction 8.5. Then there is no G-compression $X \to Y$, where Y is a curve of genus 0.*

Proof By construction, X has k-rational points. Hence, such a G-compression could only be possible if $Y \cong {}_{\rho}\mathbb{P}^1$ for some embedding $\rho: G \hookrightarrow \mathrm{PGL}_2(k)$. From Proposition 8.2, we observe that $k(X)^G = K = k(x)$. Moreover, note that 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 5.1, we obtain that $\Delta_\rho(X) = [(axP(x), bxQ(x))_2] \in \mathrm{Br}(K)$ for some $(\overline{a}, \overline{b}) \in (k^\times/k^{\times 2})^2$ such that $(a,b)_2$ is split.

Suppose that there exists a G-compression $X \to {}_{\rho}\mathbb{P}^1$. Then by Corollary 4.4 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 8.1, we use Lemma 8.3 and Lemma 8.6 to conclude that X cannot be G-compressed to any curve of genus ≤ 1. Thus, it follows from Lemma 3.1 that there exist strongly incompressible G-curves if $\mathrm{cd}_2(k) > 0$. The proof is now complete.

8.2 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 8.1 holds in this case.

Proposition 8.7 *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 8.1, it follows that any faithful G-curve X can be G-compressed to ${}_{\rho}\mathbb{P}^1$, where the embedding $\rho: G \hookrightarrow \mathrm{PGL}_2(k)$ is as in (6.1). Moreover, it follows from Lemma 6.1 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 7.1. Using the cohomology sequence associated to the central exact sequence $1 \to \mathbb{Z}/2\mathbb{Z} \to G \to D_n \to 1$, one can construct a hyperelliptic G-curve X, having a k-rational point fixed by the hyperelliptic involution. Suppose that X can be G-compressed to ${}_{\eta}\mathbb{P}^1$, where η is any embedding $G \hookrightarrow \mathrm{PGL}_2(k)$. 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 7.1, we must have $\beta_n \in k^{\times 2}$, contradicting our assumption. Similarly, it follows that X cannot be G-compressed to any curve of genus 1. By Lemma 3.1, there exists a strongly incompressible G-curve in this case.

In what follows, assume that $\omega_n \in k$. By Lemma 8.4, 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 X that cannot be G-compressed to any curve of genus ≤ 1. Let $m = n/2$, and define X

to be the hyperelliptic curve with equation

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

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

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

It is not hard to see that

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

Recall that $(x^m + x^{-m})/2 = T_m((x + x^{-1})/2)$ for some polynomial T_m. For simplicity, write $s = (x + x^{-1})/2$. Then note that

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

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

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 $x^2 - \beta_n y^2$ (see [Ga13, Theorem 1.3]). 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

$$\rho_a: \sigma \mapsto \begin{pmatrix} \alpha_n + 1 & \beta_n \\ 1 & \alpha_n + 1 \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} x & -y\beta_n \\ y & -x \end{pmatrix}, \tag{8.1}$$

where $\sigma, \tau \in D_{2n}$ satisfy $\sigma^n = \tau^2 = (\sigma\tau)^2 = 1$. We claim that X cannot be G-equivariantly compressed to ${}_\eta\mathbb{P}^1$, where η is the embedding (8.1) 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, $\overline{a}$ can be any element of $k^\times/k^{\times 2}$. Since we have $\omega_n \in k$, the embedding η can be conjugated to

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

so we may assume that η is of this form. It follows that ${}_\eta\mathbb{P}^1 \cong {}_{(a,1)}\mathbb{P}^1$ as $(\mathbb{Z}/2\mathbb{Z})^2$-varieties. Using Lemma 5.1, we compute $\Delta_{\rho_{(a,1)}}(X) = [(2a(s + 1)f(T_m(s)), s^2 - 1)_2]$. If we regard the assumed G-compression $X \to {}_\eta\mathbb{P}^1$ as a $(\mathbb{Z}/2\mathbb{Z})^2$-compression, then we conclude that $\Delta_{\rho_{(a,1)}}(X)$ is trivial in $\mathrm{Br}(k(s))$.

We will now select f to arrive at 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 $X \to {}_\eta\mathbb{P}^1$ is not possible.

It remains to prove that X cannot be G-compressed to any curve of genus 1. Suppose there is such a G-compression $X \to E$. By construction, the hyperelliptic involution of X, namely σ^m, fixes some k-rational point of X. 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 3.3(i) 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. By Lemma 3.3(i), we may write $\sigma = \tau_{P_0} \circ \alpha$, where τ_{P_0} denotes the translation by $P_0 \in E$ and $\alpha \in \mathrm{Aut}_0(E)$. Since σ^2 is 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 $P \mapsto -P$. This implies 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. ■

9 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.

9.1 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 disjoint transpositions lift to elements of order 4. (This is not the double cover studied in [Se84], 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 $\widehat{\Delta}: H^1(K,G) \to H^2(K,\mathbb{Z}/2\mathbb{Z}) = \mathrm{Br}_2(K)$ 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 9.1 *Let X, Y be faithful primitive G-varieties and suppose that there exists a G-compression $f: X \dashrightarrow Y$. Let $i: k(Y)^G \hookrightarrow k(X)^G$ be the natural inclusion induced by f and define $i_*: \mathrm{Br}_2(k(Y)^G) \to \mathrm{Br}_2(k(X)^G)$ 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 9.2 (cf. [Se84, Theorem 1]) *Let q_E be 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 [Se84, Theorem 1] or [Vi88, §2]. ∎

Remark 9.3 If the field k satisfies some additional conditions, we may view $\widehat{\Delta}$ as a particular case of the cohomological invariant defined in Section 4. Suppose that the following assumptions hold.

(i) There exists an embedding $\rho: G \hookrightarrow \mathrm{PGL}_2$. 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 [Beau10, Proposition 1.1]).

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

$$\begin{tikzcd} 1 \arrow[r] & \mathbb{G}_m \arrow[r] & \mathrm{GL}_2 \arrow[r] & \mathrm{PGL}_2 \arrow[r] & 1 \\ 1 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] \arrow[u, hook] & \widehat{G} \arrow[r] \arrow[u, hook, "\overline{\rho}"'] & G \arrow[r] \arrow[u, hook, "\rho"'] & 1. \end{tikzcd}$$

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.

9.2 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 (see *e.g.*, [Ga13, Theorem 1.2 and 1.3]). 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 9.4

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

(ii) *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 (i) 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 9.3 that $\widehat{\Delta}(X_0') = \Delta_\rho(X_0') = \Delta_\rho({}_\rho\mathbb{P}^1)$, which is trivial by Lemma 4.2. This completes the proof of the claim.

Let E be the étale algebra corresponding to the class $[X_0] \in H^1(K, G)$. 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 [Lam05, Theorem 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

https://doi.org/10.4153/CJM-2015-012-3 Published online by Cambridge University Press

follows that $\widehat{X_0}$ is a hyperelliptic curve (in the sense that its canonical divisor is not very ample). Moreover, note that $\mathrm{Aut}(\widehat{X_0})(\bar{k})$ 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 [Sh03, 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.*, [Me91, §2.1]), which is equivalent to the splitting of $(-1,-1)_2$ over the field k. This contradiction concludes the proof of (i).

(ii) 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 inside 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 $k(X_0)^H = K[Y]/\big(p(Y)\big)$. By a simple computation, it is not hard to see that the trace form of $K[Y]/\big(p(Y)\big)$ 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 9.5 *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.*

(i) *The Jacobian $E \cong \mathrm{Pic}^0(C)$ has j-invariant 0.*
(ii) *The elliptic curve E can be endowed with a faithful A_4-action defined over k.*
(iii) *The curve C is A_4-equivariantly isomorphic to E over some extension k'/k of odd degree.*
(iv) *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 [Sil09, §X.3] (see also [LT58]). Recall that C is a principal homogeneous space under E. A k-automorphism $g: C \to C$ induces a group automorphism of $\mathrm{Pic}^0(C)$, hence also a k-automorphism $\hat{g}: E \to E$ 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 3.3(ii), it follows that $j(E) = 0$.

We now proceed with the proof of part (ii). 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 3.3 (ii), we conclude from part (i) 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 (iii), 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 [Sil09, Theorem X.3.6], it follows that the class $\{C/k\} \in H^1(k, E)$ belongs to the kernel of the map $(1-\alpha)_*: H^1(k, E) \to H^1(k, E)$ 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 [LT58, Proposition 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 $\phi: C \to E$ defined by $q \mapsto q - q_0$ is A_4-equivariant. Since it clearly commutes with translations, it suffices to show that $\phi(g(q)) = \alpha\big(\phi(q)\big)$. We compute $\phi(g(q)) = g(q) - q_0 = g(q) - g(q_0) = \alpha\big(\phi(q)\big)$, which completes the proof of the claim.

It remains to prove part (iv). 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 (iii), 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 9.2, 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. ∎

9.3 Strong Incompressibility

Proposition 9.6 *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 8.4, it follows that k satisfies the hypotheses of Lemma 9.7 below. In particular, there exists an embedding $\rho: G \hookrightarrow \mathrm{PGL}_2$ 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 4.4. To finish the proof, we must show that ${}_\rho\mathbb{P}^1$ is not strongly incompressible. This is achieved in Lemma 9.7. ∎

Lemma 9.7 *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 $\rho: G \hookrightarrow \mathrm{PGL}_2$ 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 $\mathrm{PGL}_2(k)$, whence we may assume that $\rho(G)$ is this particular subgroup. Then an easy 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 9.6. The following lemma will be useful in the sequel.

Lemma 9.8 *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.*

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

(ii) *If $(a,b)_2 \not\simeq (-1,-1)_2$, there exists an n-dimensional étale k-algebra E_2 with non-trivial 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 [Se03, 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

$$\langle 1, A, A^2 - B, AB(A^2 - B) \rangle.$$

An easy computation shows that

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

To prove part (i), 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 (ii), 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 9.9 The conclusion in part (ii) of the above theorem might fail if $(a,b)_2 \cong (-1,-1)_2$. Indeed, suppose that $k = \mathbb{R}$. By [Se03, Theorem 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

$$w_2(q_E) = [(-A, -B(A^2 - B))_2] + [(-1, -B)_2].$$

For 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) Suppose that $\mathrm{cd}_2(k) > 0$ and let $K = k(x)$. Note in particular that the field K is Hilbertian (see [FJ08, Prop. 13.2.1]).

Case 1. Suppose that $G = A_n$, where $n = 4$ or 5. By Lemma 8.4, there exists a nonsplit quaternion algebra A defined over K. Using Lemma 9.8(i), we can construct an n-dimensional étale K-algebra E with trivial discriminant such that $w_2(q_E) = [A] + [(-1,-1)_2]$. By [EK94, Theorem. 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 9.2, we must have $\widehat{\Delta}(X) = [A] + [(-1,-1)_2]$.

We claim that X cannot be G-compressed to any curve of genus ≤ 1. Recall that any faithful G-curve of genus 0 is G-equivariantly isomorphic to the quadric associated to $\langle 1,1,1\rangle$, which we denoted earlier by X_0. Suppose that there exists a G-compression $X \to X_0$. By Proposition 9.1, 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 9.4(i), 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 an 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 9.5(iv) contradicts the fact that A is not split. This completes the proof of the claim. By Lemma 3.1, 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 8.4. 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',

https://doi.org/10.4153/CJM-2015-012-3 Published online by Cambridge University Press

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

$$\langle 1,1,1\rangle \quad \text{and} \quad \langle -x, -(x^2-4x+2), x(x^2-4x+2)\rangle$$

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 9.8(ii), we can construct a 4-dimensional étale K-algebra E with non-trivial discriminant d_E such that $w_2(q_E) = [A] + [(-1,-d_E)]$. By [EK94, Theorem 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 9.2, 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

$$\begin{tikzcd}
\mathrm{Br}_2(k(X_0)^G) \arrow[r, "i_*"] \arrow[d, "j_0"'] & \mathrm{Br}_2(K) \arrow[d, "j"] \\
\mathrm{Br}_2(k'(X_0')^G) \arrow[r, "i_*'"] & \mathrm{Br}_2(k'(x)),
\end{tikzcd}$$

where the vertical arrows are induced by base extension and the horizontal arrows are induced by f and f'. By Proposition 9.1, we must have $i_*(\widehat{\Delta}(X_0)) = \widehat{\Delta}(X)$ in $\mathrm{Br}_2(K)$. By Proposition 9.4(ii), 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 3.1 that there exist strongly incompressible G-curves. ∎

Appendix A Proof of Theorem 3.2

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

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

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 $\mathcal{P} = (b_1, \dots, b_l)$, 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

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

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

Proposition A.3 *Let $\mathcal{P}_i = (b_{i,1}, \dots, b_{i,l_i})$ $(1 \leq i \leq n)$ be a collection of ramification conditions (not necessarily distinct), and let $\beta_1, \dots, \beta_n$ 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 $g_i + cH$ contain no multiple roots outside of A for $1 \leq i \leq n$. Choose any such c and define $P = Q + cH$. 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 3.2 Without loss of generality, we may assume that $G = S_m$ for some $m \geq 2$. Given a partition $b_1 + \cdots + b_s$ of m, where $b_1 \geq \cdots \geq b_l > 1 = b_{l+1} = \cdots = b_s$ for some $l \geq 1$, we can define a ramification condition $\mathcal{P} = (b_1, \dots, b_l)$. Let $\mathcal{P}_1, \dots, \mathcal{P}_n$ be the ramification conditions obtained as we range over all possible partitions of m, except for $1 + \cdots + 1$. 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 $\mathrm{Gal}\big(L/k(t)\big)$ is a transitive subgroup of S_p; we claim that equality holds. Since $\mathrm{Gal}\big(L\overline{k}/\overline{k}(t)\big)$ is a subgroup of $\mathrm{Gal}\big(L/k(t)\big)$, 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 [Se08, Theorem 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 $\mathcal{P}_i = (b^{(i)}{}_1, \dots, b^{(i)}{}_{l_i})$, the inertia subgroup at β_i is generated by an element of S_p of cycle type $(b^{(i)}{}_1, \dots, b^{(i)}{}_{l_i}, 1, \dots, 1)$, 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 $(b^{(i)}{}_1, \dots, b^{(i)}{}_{l_i}, 1, \dots, 1)$. 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. ■

Acknowledgements I am extremely grateful to Z. Reichstein for introducing me to the subject. This work would not have been possible without his helpful comments and suggestions. I also thank Bob Guralnick for useful conversations and an anonymous referee for helpful comments.

References

[Beau10] A. Beauville, *Finite subgroups of* $\mathrm{PGL}_2(K)$, Vector bundles and complex geometry, 23–29, Contemp. Math., 522, Amer. Math. Soc., Providence, RI, 2010.

[BF03] G. Berhuy and G. Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*. Doc. Math. **8** (2003), 279–330.

[Ch10] X. Chen, *Self rational maps of K3 surfaces*, 2010, arXiv:1008.1619v1 [math.AG].

[Ch12] ———, *Rational self maps of Calabi-Yau manifolds*. To appear. (Available online at http://www.math.ualberta.ca/ xichen/paper/cyself.pdf)

[EW87] R. Elman and A. R. Wadsworth, *Hereditarily quadratically closed fields*. J. Algebra **111**(1987), no. 2, 475–482. http://dx.doi.org/10.1016/0021-8693(87)90231-6

[EK94] M. Epkenhans and M. Krüskemper, *On trace forms of étale algebras and field extensions*. Math. Z. **217**(1994), no. 3, 421–434. http://dx.doi.org/10.1007/BF02571952

[FJ08] M. D. Fried and M. Jarden, *Field arithmetic*. Third edition. Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, A Series of Modern Surveys in Mathematics, 11, Springer-Verlag, Berlin, 2008.

[Ga13] M. Garcia-Armas, *Finite group actions on curves of genus zero*. J. Algebra **394**(2012), 173–181. http://dx.doi.org/10.1016/j.jalgebra.2013.07.018

[Lam05] T. Y. Lam, *Introduction to quadratic forms over fields*. Graduate Studies in Mathematics 67, American Mathematical Society, Providence, RI, 2005.

[LT58] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*. Amer. J. Math. **80**(1958), 659–684. http://dx.doi.org/10.2307/2372778

[Le07] A. Ledet, *Finite groups of essential dimension one*. J. Algebra **311**(2007), no. 1, 31–37. http://dx.doi.org/10.1016/j.jalgebra.2006.12.027

[Liu02] Q. Liu, *Algebraic geometry and arithmetic curves*. Oxford Graduate Texts in Mathematics 6, Oxford University Press, Oxford, 2002.

[Me91] J.-F. Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*. Effective methods in algebraic geometry (Castiglioncello, 1990), 313–334, Progr. Math. **94**, Birkhäuser Boston, Boston, MA, 1991.

[Re00] Z. Reichstein, *On the notion of essential dimension for algebraic groups*. Transform. Groups **5**(2000), no. 3, 265–304. http://dx.doi.org/10.1007/BF01679716

[Re04] ———, *Compressions of group actions*. Invariant theory in all characteristics, 199–202, CRM Proc. Lecture Notes, 35, Amer. Math. Soc., Providence, RI, 2004.

[Re10] ———, *Essential dimension*. Proceedings of the International Congress of Mathematicians 2010 (ICM 2010), 162–188.

[RY01] Z. Reichstein and B. Youssin, *Splitting fields of G-varieties*. Pacific J. Math. **200**(2001), no. 1, 207Â249. http://dx.doi.org/10.2140/pjm.2001.200.207

[Ros56] M. Rosenlicht, *Some basic theorems on algebraic groups*. Amer. J. Math. **78**(1956), 401–443. http://dx.doi.org/10.2307/2372523

[Ros63] ———, *A remark on quotient spaces*. An. Acad. Brasil. Ci. **35**(1963), 487–489.

[Se84] J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$. Comment. Math. Helv. **59**(1984), no. 4, 651–676.

[Se02] ———, *Galois cohomology*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.

[Se03] ———, *Cohomological invariants, Witt invariants, and trace forms*. Notes by Skip Garibaldi. Univ. Lecture Ser., 28, Cohomological invariants in Galois cohomology, 1–100, Amer. Math. Soc., Providence, RI, 2003.

[Se08] ———, *Topics in Galois theory*. Second edition, With notes by Henri Darmon, Research Notes in Mathematics 1. A K Peters, Ltd., Wellesley, MA, 2008.

[Sh03] T. Shaska, *Determining the automorphism group of a hyperelliptic curve*. Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2003, pp. 248–254 (electronic).

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*. Second edition, Graduate Texts in Mathematics 106. Springer, Dordrecht, 2009.

[Vi88] N. Vila, *On stem extensions of S_n as Galois group over number fields*. J. Algebra **116**(1988), no. 1, 251–260. http://dx.doi.org/10.1016/0021-8693(88)90205-0

Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada
e-mail: marioga@math.ubc.ca