J. Aust. Math. Soc. **85** (2008), 155–175
doi:10.1017/S1446788708000827

REGULAR HYPERMAPS OVER PROJECTIVE LINEAR GROUPS

MARSTON CONDER ✉, PRIMOŽ POTOČNIK and JOZEF ŠIRÁŇ

(Received 23 December 2007; accepted 17 May 2008)

Communicated by Peter M. Neumann

Dedicated to Cheryl Praeger for her sixtieth birthday

Abstract

An enumeration result for orientably regular hypermaps of a given type with automorphism groups isomorphic to $\mathrm{PSL}(2, q)$ or $\mathrm{PGL}(2, q)$ can be extracted from a 1969 paper by Sah. We extend the investigation to orientable reflexible hypermaps and to nonorientable regular hypermaps, providing many more details about the associated computations and explicit generating sets for the associated groups.

2000 *Mathematics subject classification*: primary 57M15; secondary 05C25, 20F05.
Keywords and phrases: hypermap, regular hypermap, triangle group, projective linear group.

1. Introduction

A *regular hypermap* $\mathcal{H}$ is a pair (r, s) of permutations generating a regular permutation group on a finite set, and provides a generalization of the geometric notion of a regular map on a surface, by allowing edges to be replaced by 'hyperedges'. The cycles of r, s and rs correspond to the hypervertices, hyperedges and hyperfaces of $\mathcal{H}$, which determine the embedding of the underlying (and connected) hypergraph into the surface, and their orders give the *type* of $\mathcal{H}$, say $\{k, l, m\}$. The group G generated by r and s induces a group of automorphisms of this hypergraph, preserving the embedding, and acting transitively on the flags (incident hypervertex-hyperedge pairs) of $\mathcal{H}$. When one of the parameters k, l, m is 2, the hypergraph is a graph, and the hypermap is a regular map.

The authors gratefully acknowledge the support from the NZIMA programme on Combinatorics and Its Applications. The first and third authors wish to acknowledge the partial support from the Marsden Fund, and the third author would like to acknowledge the partial support from APVV Grants Nos. 20-000704 and 0040-06.

The theory of such objects is well developed, and has been thoroughly explained in [10, 11]. Without going into too much detail, we need to make a few basic observations. First, the group G has a presentation of the form

$$G = \langle r, s, t \mid r^k = s^l = t^m = rst = \cdots = 1\rangle,$$

and (so) is a finite quotient of the *ordinary* (k, l, m) *triangle group*. For simplicity, we will say that such a group G has *type* (k, l, m), provided that k, l, m are the *true orders* of the corresponding elements r, s, t. There is a bijective correspondence between isomorphism classes of regular hypermaps of a given type $\{k, l, m\}$ and torsion-free normal subgroups of the ordinary (k, l, m) triangle group $\Delta(k, l, m)$, and the number of those with a given group G as 'rotational symmetry group' (or quotient of $\Delta(k, l, m)$) is equal to the number of ways of generating G by a (k, l, m)-triple (r, s, t) up to equivalence under $\mathrm{Aut}(G)$. For further details about representing hypermaps in the form of cellular decomposition of closed two-dimensional surfaces and visualizing the rotational symmetries, and also their association with Riemann surfaces and algebraic number fields (through Grothendieck's theory of *dessins d'enfants*), we refer the reader to [4, 10, 11].

A regular hypermap may admit a symmetry that induces a reversal of some local orientation of the supporting surface. At the group theory level, this is equivalent to the existence of an automorphism ϑ of a (k, l, m)-group G presented as above, such that ϑ inverts two of the three generators. Such regular hypermaps are called *reflexible*. If ϑ is actually given by conjugation of some element of order two in G, then the corresponding (k, l, m)-generating triple for G gives rise to two distinct reflexible hypermaps: one on a nonorientable surface $\mathcal{S}$, with full automorphism group G, and another one on an orientable surface that is a double cover of $\mathcal{S}$, with full automorphism group isomorphic to the direct product of G with the cyclic group of order two. We will call this kind of generating triple *inner reflexible*, since the inverting automorphism is inner. The Euler characteristic χ of the regular hypermap of type (k, l, m) associated with a rotational symmetry group G of type (k, l, m) is given by $\chi = |G|(1/k + 1/l - 1/m)$ in the orientable case, and $\chi = |G|(1/k + 1/l - 1/m)/2$ if the supporting surface of the hypermap is nonorientable.

In 1969, Sah [15] extended some work of Macbeath [14] by enumerating orientably regular hypermaps of a given type (k, l, m) with automorphism groups isomorphic to $\mathrm{PSL}(2, q)$ or $\mathrm{PGL}(2, q)$. Further results in this area were obtained in [12, 13], where certain necessary and sufficient conditions for the existence of an orientably regular map of a given type were found, and in work by Downs [6], Breda and Jones [2], and Glover and Sjerve [7]; see also [1].

The aim of this paper is to extend Sah's investigation to *reflexible* hypermaps, on both orientable and nonorientable surfaces, and provide much more detail about the associated computations, including explicit generating sets for the associated groups. In a forthcoming paper [3] we will apply the results of this refined approach to the classification of all regular maps of Euler characteristic equal to $-p^2$ for some prime p. For completeness, we mention that, to the best of our knowledge, the only other classes of classical groups for which a (partial) classification of regular maps has been considered are the Suzuki groups and Ree groups (see [8, 9]).

A triple (k, l, m) is called *hyperbolic*, *parabolic*, or *elliptic*, according to whether $1/k + 1/l + 1/m - 1$ is negative, zero, or positive. We will restrict ourselves to hyperbolic triples. The reason for this restriction is that in the parabolic case (where $1/k + 1/l + 1/m = 1$), the only case where G is a projective two-dimensional linear group is $G \cong \mathrm{PSL}(2, 3) \cong A_4$ for the triple $(3, 3, 3)$, and for the elliptic type (where $1/k + 1/l + 1/m > 1$), there are only four such cases, namely $G \cong \mathrm{PSL}(2, 2) = \mathrm{PGL}(2, 2) \cong S_3$ for the triple $(3, 2, 2)$, $G \cong \mathrm{PSL}(2, 3) \cong A_4$ for the triple $(3, 3, 2)$, $G \cong \mathrm{PGL}(2, 3) \cong S_4$ for $(4, 3, 2)$, and $G \cong \mathrm{PSL}(2, 4) \cong \mathrm{PGL}(2, 4) \cong \mathrm{PSL}(2, 5) \cong A_5$ for $(5, 3, 2)$. Note that in a hyperbolic triple the smallest element cannot be less than 2; if it is equal to 2, then the remaining entries are at least 3.

In Section 2 we provide a detailed analysis of hyperbolic triples (up to conjugacy) in projective two-dimensional linear groups, and then in Section 3 we consider what happens when an inverting automorphism exists, and determine the groups they generate in Section 4. We re-establish Sah's enumeration [15] for hyperbolic triples for such groups in Section 5, and then apply this to the classification of reflexible hypermaps (on both orientable and nonorientable surfaces) in Section 6, and make some concluding remarks in Section 7.

2. Conjugacy classes of representative triples

Let (k, l, m) be a fixed hyperbolic triple and let f be an isomorphism taking a finite (k, l, m)-group G with a partial presentation of the form

$$G = \langle r, s, t \mid r^k = s^l = t^m = rst = \cdots = 1\rangle$$

onto $\mathrm{PSL}(2, F)$ or $\mathrm{PGL}(2, F')$, where F and F' are fields of characteristic p. From the point of view of the associated computations with projective transformations $f(r)$, $f(s)$ and $f(t)$, it turns out to be of advantage to consider first the situation in the special linear group $\mathrm{SL}(2, K)$ where K is an algebraically closed field of characteristic p (such as the union of an ascending chain of all fields of order a power of p). The results will then be carried over to $\mathrm{PSL}(2, K)$ by the natural projection given by $M \mapsto \overline{M} = \pm M$ for any 2×2 matrix $M \in \mathrm{SL}(2, K)$, which will also help to determine the subfields F and F'. To facilitate the exposition, any of the two matrices $M, -M \in \mathrm{SL}(2, K)$ will be called a *representative* of $\overline{M} \in \mathrm{PSL}(2, K)$.

The next few observations will address orders and conjugacy classes of elements in $\mathrm{SL}(2, K)$. If p is odd, then $\mathrm{SL}(2, K)$ contains exactly one involution, namely, $-I$, where I is the 2×2 identity matrix. All elements of order p and $2p$ in $\mathrm{SL}(2, K)$ are known to be conjugate to the transvections U and $-U$, respectively, where

$$U = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \tag{2.1}$$

and there are no elements of order divisible by p for any other multiple of p. Equivalently, if p is odd, the order of an element $J \in \mathrm{SL}(2, K)$ is p (respectively $2p$)

https://doi.org/10.1017/S1446788708000827 Published online by Cambridge University Press

if and only if $J \neq \pm I$ and the trace $\mathrm{tr}(J)$ of J is equal to 2 (respectively -2). If $p = 2$, then all elements in $\mathrm{SL}(2, K)$ of order two are conjugate to U, and there are no elements there of any even order greater than two. For any prime p, an element of $\mathrm{SL}(2, K)$ of order i, where $i \geq 3$ and $\gcd(i, p) = 1$, is known to be conjugate to one (and hence to both) of the matrices

$$V(\xi) = \begin{bmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{bmatrix} \quad \text{and} \quad W(\omega) = \begin{bmatrix} 0 & -1 \\ 1 & \omega \end{bmatrix}, \tag{2.2}$$

where ξ is a primitive ith root of unity over $K_p = F_p$, and $\omega = \xi + \xi^{-1}$. In other words, an element $J \in \mathrm{SL}(2, K)$ has order i, where i is as above, if and only if $\mathrm{tr}(J) = \omega = \xi + \xi^{-1}$ for some primitive ith root of unity ξ over F_p. Note that, if $i \geq 3$, we have $\omega \notin \{2, -2\}$.

Returning to the isomorphism f introduced at the beginning, let $\overline{R}$, $\overline{S}$, $\overline{T} \in \mathrm{PSL}(2, K)$ be the images of r, s, t under f; in particular, $\overline{RST} = \overline{I}$ where I is the 2×2 identity matrix. We will refer to the orders (k, l, m) of $\overline{R}$, $\overline{S}$, $\overline{T}$ as the *projective orders*. Our aim is now to specify which representatives $R, S, T \in \mathrm{SL}(2, K)$ of $\overline{R}$, $\overline{S}$, $\overline{T}$ we will be working with. This will depend on the projective orders in the following way. Suppose, for example, that p is odd and k is even. Since k was assumed to be the order of $\overline{R} \in \mathrm{PSL}(2, K)$, it is plain that the order of both R and $-R$ in $\mathrm{SL}(2, K)$ must be $2k$. On the other hand, if both p and k are odd, then the orders of R and $-R$ form the set $\{k, 2k\}$. Of course, the same holds for $\overline{S}$ and $\overline{T}$. It follows that if p is odd and one of the entries k, l, m is even, then by suitably combining signs we may choose the representatives $R, S, T \in \mathrm{SL}(2, K)$ in such a way that the orders of R, S and T are $2k$, $2l$ and $2m$, respectively, and $RST = I$. If p and all of k, l, m are odd, then we may choose the representatives R, S, T in such a way that $RST = I$ and their orders are either (k, l, m) or $(2k, 2l, 2m)$; these two cases are mutually exclusive. If $p = 2$ then $\mathrm{SL}(2, K) \cong \mathrm{PSL}(2, K)$ and R, S, T simply have orders k, l, m.

Triples of matrices (R, S, T) in $\mathrm{SL}(2, K)$ with $RST = I$ and with the orders specified as above will be called *representative triples*, and the orders of R, S, T in $\mathrm{SL}(2, K)$ will be called *representative orders* and denoted by (κ, λ, μ). Representative orders are therefore related to projective orders as follows. We have: $(\kappa, \lambda, \mu) = (2k, 2l, 2m)$ if p is odd and at least one of k, l, m is even; $(\kappa, \lambda, \mu) = (k, l, m)$ or $(2k, 2l, 2m)$ if p and all of k, l, m are odd; and $(\kappa, \lambda, \mu) = (k, l, m)$ if $p = 2$. Note that if one of the orders, say k, is a multiple of p, then it follows from Dickson's classification [5] of subgroups of $\mathrm{PSL}(2, K)$ that $k = p$. We can therefore confine ourselves to triples (k, l, m) with $\gcd(j, p) = 1$ or $j = p$ whenever $j \in \{k, l, m\}$; such triples will be called *p-restricted*. For the corresponding representative order, we have $\kappa \in \{p, 2p\}$ if p is odd, and $\kappa = p$ if $p = 2$. In particular, if p divides all of k, l, m, then $(k, l, m) = (p, p, p)$ for all p, and $(\kappa, \lambda, \mu) = (p, p, p)$ or $(2p, 2p, 2p)$ if p is odd, while $(\kappa, \lambda, \mu) = (p, p, p)$ if $p = 2$.

In general there can be many distinct conjugacy classes of representative triples (R, S, T) having the same p-restricted projective orders (k, l, m) and the same representative orders (κ, λ, μ). Later we will show that it is possible to determine the number of such conjugacy classes by means of counting the corresponding *trace triples* $(\mathrm{tr}(R), \mathrm{tr}(S), \mathrm{tr}(T))$. Earlier in this section we saw that if p is odd and ν is the order of an element $M \in \mathrm{SL}(2, K)$ with $M \neq \pm I$, then one of the following three possibilities occurs:

(1) $\nu \geq 3$ and $(\nu, p) = 1$, which happens if and only if $\mathrm{tr}(M) = \omega_\nu = \xi_\nu + \xi_\nu^{-1}$, where ξ_ν is a νth primitive root of unity;
(2) $\nu = p$, which happens if and only if $\mathrm{tr}(M) = 2$; or
(3) $\nu = 2p$, which happens if and only if $\mathrm{tr}(M) = -2$.

To capture this in a single formula, we extend the definition of ω_ν also to $\nu = p$ and $\nu = 2p$ by stipulating that $\omega_\nu = \xi_\nu + \xi_\nu^{-1}$, where ξ_ν is the (ν/p)th primitive root of unity $\exp(2\pi i \nu/p)$; this gives $\omega_p = 2$ and $\omega_{2p} = -2$. If $p = 2$, then we just change 2 to 0 in part (2) of the above, and omit part (3) (where $\nu = 2p$). With this all applied to $\nu = \kappa$, λ and μ, the trace triple corresponding to the above representative triple (R, S, T) is simply $(\omega_\kappa, \omega_\lambda, \omega_\mu)$.

In the remaining part of this section we prove the important fact that, up to a certain small class of exceptions, any two representative triples having both the same projective and representative orders *and* the same trace triple are conjugate in $\mathrm{SL}(2, K)$.

It will be of advantage to consider first the case where at least two of k, l, m are equal to p. If $p = 2$, the projective group $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ is dihedral and therefore out of the scope of our interest. We will therefore assume without loss of generality that $(k, l, m) = (p, p, m)$ where p is an odd prime.

PROPOSITION 2.1. *Let p be an odd prime and let (k, l, m) be a p-restricted hyperbolic triple such that $k = l = p$ and $m \geq 2$. Let (R, S, T) be a representative triple corresponding to the representative orders $(\kappa, \lambda, \mu) = (\varepsilon p, \varepsilon p, \varepsilon m)$ for suitable $\varepsilon \in \{1, 2\}$. Assume that the group $\langle R, S, T \rangle$ is not abelian. Then, $(\kappa, \lambda, \mu) \neq (p, p, p)$, and the triple (R, S, T) is conjugate in $\mathrm{SL}(2, K)$ to the triple (R_1, S_1, T_1), where*

$$R_1 = \pm \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad S_1 = \pm \begin{bmatrix} 1 & 0 \\ \omega_\mu - 2 & 1 \end{bmatrix} \quad \text{and} \quad T_1 = \begin{bmatrix} 1 & -1 \\ 2 - \omega_\mu & \omega_\mu - 1 \end{bmatrix},$$

and the signs are taken simultaneously (with $+$ for $\varepsilon = 1$, and $-$ for $\varepsilon = 2$).

PROOF. We know that any element $M \in \mathrm{SL}(2, K)$ of order p $(2p)$ is conjugate to the matrix U $(-U)$ given in (2.1). Without loss of generality we therefore may assume that

$$R = \pm \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad S = \pm \begin{bmatrix} a & b \\ c & 2 - a \end{bmatrix},$$

where $(a - 1)^2 + bc = 0$ (the determinant condition) and the positive (negative) signs are taken simultaneously if $\kappa = \lambda = p$ or $2p$, respectively, giving the traces 2 and -2.

https://doi.org/10.1017/S1446788708000827 Published online by Cambridge University Press

From $RST = I$ we obtain $\mathrm{tr}(T) = 2 + c$. It can be checked that $RS = SR$ if and only if $c = 0$. Since the group $\langle R, S, T\rangle = \langle R, S\rangle$ is assumed to be nonabelian, we have $c \neq 0$. Let $M = (m_{ij}) \in \mathrm{SL}(2, K)$ be the 2×2 matrix such that $m_{11} = m_{22} = 1$, $m_{21} = 0$ and $m_{12} = (1 - a)c^{-1}$. It can be checked that $MRM^{-1} = R$ while also

$$MSM^{-1} = \pm \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} \quad \text{and} \quad MTM^{-1} = \begin{bmatrix} 1 & -1 \\ -c & 1 + c \end{bmatrix}.$$

Since conjugation preserves traces, $\mathrm{tr}(T) = 2 + c \neq 2$, and therefore $(\kappa, \lambda, \mu) \neq (p, p, p)$. In our notation, we have $\mathrm{tr}(T) = \omega_\mu$ with $\omega_\mu = \xi_\mu + \xi_\mu^{-1}$, where ξ_μ is a primitive μth root of unity over F_p if $(\mu, p) = 1$ and a primitive (μ/p)th root of unity if $\mu = 2p$. This gives $c = \omega_\mu - 2$ and leads to the three matrices in our statement. $\square$

It remains for us to consider the case where at most one of the projective orders is p. We may assume without loss of generality that both k and l are coprime to p, and $k \geq 3$. At this point our approach will vary from Sah's [15], leading to a different form of matrices representing the generators R, S and T.

PROPOSITION 2.2. *Let p be a prime and let (k, l, m) be a p-restricted hyperbolic triple such that $k \geq 3$ and $k, l \neq p$. Let (R, S, T) be a representative triple associated with the projective orders (k, l, m) and representative orders (κ, λ, μ). Let $(\omega_\kappa, \omega_\lambda, \omega_\mu)$ be the corresponding trace triple, let ξ_κ be a κth primitive root of unity such that $\omega_\kappa = \xi_\kappa + \xi_\kappa^{-1}$, and let $D = \omega_\kappa^2 + \omega_\lambda^2 + \omega_\mu^2 - \omega_\kappa\omega_\lambda\omega_\mu - 4$. Assume that $\langle R, S, T\rangle$ is not isomorphic to a subgroup of the upper triangular subgroup of* $\mathrm{SL}(2, K)$. *Then $D \neq 0$ and the triple (R, S, T) is conjugate in* $\mathrm{SL}(2, K)$ *to the following triple (R_2, S_2, T_2), with $\eta = (\xi_\kappa - \xi_\kappa^{-1})^{-1}$:*

$$R_2 = \begin{bmatrix} \xi_\kappa & 0 \\ 0 & \xi_\kappa^{-1} \end{bmatrix},$$

$$S_2 = \eta \begin{bmatrix} \omega_\mu - \omega_\lambda\xi_\kappa^{-1} & -D \\ 1 & \omega_\lambda\xi_\kappa - \omega_\mu \end{bmatrix},$$

$$T_2 = \eta \begin{bmatrix} \omega_\lambda - \omega_\mu\xi_\kappa^{-1} & \xi_\kappa D \\ -\xi_\kappa^{-1} & \omega_\mu\xi_\kappa - \omega_\lambda \end{bmatrix}.$$

REMARK. Later we will show that, whenever $D \neq 0$, the projective images of the matrices given in the proposition above generate a group isomorphic to $\mathrm{PSL}(2, F)$ or $\mathrm{PGL}(2, F)$ for some finite field F of characteristic p.

PROOF. Since any element $M \in \mathrm{SL}(2, K)$ of order κ coprime to p is conjugate to the matrix $V(\xi_\kappa)$ in (2.2) for a suitable primitive κth root of unity ξ_κ, we may assume that

$$R = \begin{bmatrix} \xi_\kappa & 0 \\ 0 & \xi_\kappa^{-1} \end{bmatrix}, \quad S = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{and} \quad T = \begin{bmatrix} d\xi_\kappa^{-1} & -b\xi_\kappa \\ -c\xi_\kappa^{-1} & a\xi_\kappa \end{bmatrix},$$

where $ad - bc = 1$, $\mathrm{tr}(S) = a + d = \omega_\lambda$, and $\mathrm{tr}(T) = a\xi_\kappa + d\xi_\kappa^{-1} = \omega_\mu$; the reader should be aware of the subtleties in the definition of ω_μ in the case where $\mu \in \{p, 2p\}$.

Since $k \geq 3$ and $\gcd(k, p) = 1$, we have $\xi_\kappa - \xi_\kappa^{-1} \neq 0$. The two equations coming from the traces have the unique solution $a = \eta(\omega_\mu - \omega_\lambda \xi_\kappa^{-1})$ and $d = \eta(\omega_\lambda \xi_\kappa - \omega_\mu)$, where $\eta = (\xi_\kappa - \xi_\kappa^{-1})^{-1}$. A computation shows that the determinant condition turns into $bc = -\eta^2 D$, which is the only condition on b and c we have. If $D = 0$, then $\langle R, S\rangle = \langle R, S, T\rangle$ is clearly isomorphic to a subgroup of the upper triangular subgroup of $\mathrm{SL}(2, K)$, contrary to our assumptions. Hence we have $D \neq 0$. It can be checked that, if $M = \mathrm{diag}(u, u^{-1})$ where $0 \neq u \in K$, then

$$MRM^{-1} = R \quad \text{and} \quad MSM^{-1} = \begin{bmatrix} a & u^2 b \\ u^{-2} c & d \end{bmatrix}.$$

We may choose $u \in K$ such that $u^2 b = -\eta D$ and $u^{-2} c = \eta$. Equivalently, up to conjugation, we may assume that $b = -\eta D$ and $c = \eta$. This gives the matrices in the statement of the proposition. □

Summing up the two results yields the announced one-to-one correspondence between conjugacy classes of representative triples and their trace triples. The formulation is universal and depends only on the values of $D = D(\omega_\kappa, \omega_\lambda, \omega_\mu)$. Note that if $k = l = p$, then $\omega_\kappa = \omega_\lambda$ and they both are equal to the sum of the (κ/p)th root of unity and its reciprocal, which is 2 or -2, and the expression for D then simplifies to $D = (\omega_\mu - 2)^2$.

PROPOSITION 2.3. *Let p be a prime and let (k, l, m) be a p-restricted, hyperbolic triple. Assume that $D = D(\omega_\kappa, \omega_\lambda, \omega_\mu) \neq 0$ for any triple (κ, λ, μ) of representative orders and any trace triple $(\omega_\kappa, \omega_\lambda, \omega_\mu)$. Then the conjugacy classes of representative triples (R, S, T) associated with the projective orders (k, l, m) and the representative orders (κ, λ, μ) are in a bijective correspondence with the trace triples $(\omega_\kappa, \omega_\lambda, \omega_\mu)$.*

PROOF. What remains to be proved is that, given a trace ω, the pair $\{\xi, \xi^{-1}\}$ of primitive roots such that $\omega = \xi + \xi^{-1}$ is uniquely determined. This follows from the observation that ξ and ξ^{-1} are roots of the polynomial $x^2 - \omega x + 1$. □

We now derive a necessary and sufficient condition for $D = D(\omega_\kappa, \omega_\lambda, \omega_\mu)$ to be zero. Recall that if ν is any of κ, λ, μ, then $\omega_\nu = \xi_\nu + \xi_\nu^{-1}$ where $\xi_\nu \neq 0$ is the corresponding νth root of unity. Substituting this into the expression for D, multiplying by ξ_κ^2 and simplifying, we obtain the factorization

$$\xi_\kappa^2 D = (\xi_\kappa - \xi_\lambda \xi_\mu)(\xi_\kappa - \xi_\lambda^{-1} \xi_\mu^{-1})(\xi_\kappa - \xi_\lambda^{-1} \xi_\mu)(\xi_\kappa - \xi_\lambda \xi_\mu^{-1}).$$

Since $\xi_\kappa \neq 0$, this shows that $D = 0$ if and only if $\xi_\kappa \xi_\lambda^\varepsilon \xi_\mu^\delta = 1$ for some $\varepsilon, \delta \in \{\pm 1\}$. Raising the last equation to the power of $[\lambda, \mu]$ gives $\xi_\kappa^{[\lambda, \mu]} = 1$, which shows that κ divides $[\lambda, \mu]$. Moreover, also λ divides $[\kappa, \mu]$, and μ divides $[\kappa, \lambda]$, by the symmetry of the function D. It is easy to see that these three conditions are satisfied simultaneously if and only if, for each prime p', the largest power of p' dividing one of κ, λ, μ divides at least two of them. We summarize this in the following lemma.

https://doi.org/10.1017/S1446788708000827 Published online by Cambridge University Press

LEMMA 2.4. *In the above notation, $D = 0$ if and only if $\xi_\kappa \xi_\lambda^\varepsilon \xi_\mu^\delta = 1$ for some $\varepsilon, \delta \in \{\pm 1\}$. In particular, if there exists a prime p' such that the largest power of p' dividing one of k, l, m divides none of the remaining entries, then $D \neq 0$ for any choice of representative triples (κ, λ, μ) and primitive roots $(\xi_\kappa, \xi_\lambda, \xi_\mu)$.*

Finally, we note that, for any triple (k, l, m) of projective orders, the number of all triples of primitive roots $(\xi_\kappa, \xi_\lambda, \xi_\mu)$ associated with the representative orders (κ, λ, μ) and such that $D = D(\omega_\kappa, \omega_\lambda, \omega_\mu) \neq 0$ has been determined in [1].

3. Adjoining an involution that inverts two generators

Let (k, l, m) be a hyperbolic triple and let H be a group with presentation

$$H = \langle x, y, z \mid x^2 = y^2 = z^2 = (yz)^k = (zx)^l = (xy)^m \cdots = 1\rangle.$$

Keeping the same terminology and notation as introduced before, let H be a subgroup of $\mathrm{PSL}(2, K)$, where K is an algebraically closed field of characteristic p. Taking $r = yz$, $s = zx$ and $t = xy$, we see that H contains a subgroup G with presentation

$$G = \langle r, s, t \mid r^k = s^l = t^m = rst = \cdots = 1\rangle$$

of index at most two in H. We can therefore use results of the previous section and study the ways G can be extended by adjoining an involution z such that both rz and zs are involutions.

We first show that, if such a z exists, then it is unique. Indeed, let z and z' be two involutions such that the elements $u = rz$, $v = zs$, $u' = rz'$ and $v' = z's$ are all involutions. Then, $z'z = u'u = v'v$; denote this common element by w. A simple calculation shows that $rw = u'z' \cdot z'z = u'z = u'u \cdot uz = wr$, and, similarly, $sw = ws$. It follows that w centralises G. But G has trivial centre (since G is isomorphic to $\mathrm{PSL}(2, K)$ or $\mathrm{PGL}(2, K)$), and thus $w = 1$, and $z' = z$. Hence the extension of G by z is unique, if it exists.

The existence of such an extension has been known as folklore; however, we need to derive an explicit form for z suitable for later consideration. Assume that the group G has been mapped onto a subgroup of $\mathrm{PSL}(2, F)$ where $F = F_p(\omega_\kappa, \omega_\lambda, \omega_\mu) < K$ as before, via the generating triples $R, S, T \in \mathrm{SL}(2, F)$ listed in Propositions 2.1 and 2.2. In $\mathrm{SL}(2, K)$, we are therefore looking for an element $Z \in \mathrm{SL}(2, K)$ such that each of Z, $Y = RZ$ and $X = ZS$ has order four if p is odd, or order two if $p = 2$. We begin with the situation where two of the projective orders are equal to p, in which case p must be odd.

PROPOSITION 3.1. *Let p be an odd prime and let (k, l, m) be a p-restricted hyperbolic triple such that $k = l = p$ and $m \geq 2$. Let (R, S, T) be a representative triple corresponding to the representative orders $(\kappa, \lambda, \mu) = (\varepsilon p, \varepsilon p, \varepsilon m)$ for a suitable $\varepsilon \in \{1, 2\}$. Assume that the group $\langle R, S, T\rangle$ is not abelian. Then $(\kappa, \lambda, \mu) \neq (p, p, p)$, and there exists some $Z \in \mathrm{SL}(2, K)$ such that each of Z,*

https://doi.org/10.1017/S1446788708000827 Published online by Cambridge University Press

$Y = RZ$ and $X = ZS$ has order four. Moreover, the triple (X, Y, Z) is conjugate in $\mathrm{SL}(2, K)$ *to the triple (X_1, Y_1, Z_1), where*

$$X_1 = \pm\alpha \begin{bmatrix} 1 & 0 \\ 2-\omega_\mu & -1 \end{bmatrix}, \quad Y_1 = \pm\alpha \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix} \quad \text{and} \quad Z_1 = \alpha \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

with $\alpha^2 = -1$ and the signs taken simultaneously ($+$ for $\varepsilon = 1$, and $-$ for $\varepsilon = 2$).

PROOF. If p is odd, then an element $Z \in \mathrm{SL}(2, K)$ has order four if and only if its trace is equal to zero, that is,

$$Z = \begin{bmatrix} A & B \\ C & -A \end{bmatrix},$$

where $A^2 + BC = -1$; this is the determinant-one condition. Let R_1 and S_1 be the matrices from Proposition 2.1. Then,

$$Y = R_1 Z = \pm \begin{bmatrix} A+C & B-A \\ C & -A \end{bmatrix},$$

which shows that Y has order four if and only if $C = 0$. Using this in evaluating $X = ZS_1$, we obtain

$$X = ZS_1 = \pm \begin{bmatrix} A + B(\omega_\mu - 2) & B \\ A(2-\omega_\mu) & -A \end{bmatrix},$$

and therefore X has order four if and only if $B(\omega_\mu - 2) = 0$. In the proof of Proposition 2.1 we saw that $\omega_\mu \neq 2$, and so X has order four if and only if $B = 0$. Therefore $Z = \mathrm{diag}(A, -A)$ where $A^2 = -1$. Letting $Z_1 = Z$, $Y_1 = Y$, $X_1 = X$ and $\alpha = A$ gives our statement. □

We now clarify the situation for the remaining hyperbolic triples.

PROPOSITION 3.2. *Let p be a prime and let (k, l, m) be a p-restricted hyperbolic triple such that $k \geq 3$ and both k and l are coprime to p. Let (R, S, T) be a representative triple associated with the projective orders (k, l, m) and representative orders (κ, λ, μ). Let $(\omega_\kappa, \omega_\lambda, \omega_\mu)$ be the corresponding trace triple, let ξ_κ be a κth primitive root of unity such that $\omega_\kappa = \xi_\kappa + \xi_\kappa^{-1}$, and let*

$$D = \omega_\kappa^2 + \omega_\lambda^2 + \omega_\mu^2 - \omega_\kappa\omega_\lambda\omega_\mu - 4 \neq 0.$$

Then there exists a $Z \in \mathrm{SL}(2, K)$ such that each of Z, $Y = RZ$ and $X = ZS$ has order four. Moreover, the triple (X, Y, Z) is conjugate in $\mathrm{SL}(2, K)$ *to the triple (X_2, Y_2, Z_2), where*

https://doi.org/10.1017/S1446788708000827 Published online by Cambridge University Press

$$X_2 = \eta\beta \begin{bmatrix} D & D(\omega_\lambda \xi_\kappa - \omega_\mu) \\ \omega_\mu - \omega_\lambda \xi_\kappa^{-1} & -D \end{bmatrix},$$
$$Y_2 = \beta \begin{bmatrix} 0 & \xi_\kappa D \\ \xi_\kappa^{-1} & 0 \end{bmatrix},$$
$$Z_2 = \beta \begin{bmatrix} 0 & D \\ 1 & 0 \end{bmatrix},$$

with $\beta = -1/\sqrt{-D}$ *and* $\eta = (\xi_\kappa - \xi_\kappa^{-1})^{-1}$.

PROOF. First, let p be odd. Take the same general $Z \in \mathrm{SL}(2, K)$ of order four as at the beginning of the previous proof. Let R_2 and S_2 be the matrices from Proposition 2.2. Then

$$Y = R_2 Z = \begin{bmatrix} \xi_\kappa A & \xi_\kappa B \\ \xi_\kappa^{-1} C & -\xi_\kappa^{-1} A \end{bmatrix},$$

which implies that Y has order four if and only if $A = 0$. We use this in determining $X = ZS_1$ and obtain

$$X = ZS_1 = \eta \begin{bmatrix} B & B(\omega_\lambda \xi_\kappa - \omega_\mu) \\ B^{-1}(\omega_\lambda \xi_\kappa^{-1} - \omega_\mu) & B^{-1} D \end{bmatrix};$$

note that $\eta \neq 0$. It follows that X has order four if and only if $B^2 = -D$. Letting $Z_1 = Z$, $Y_1 = Y$, $X_1 = X$ and $\beta = -B^{-1}$, we obtain the matrices as in the statement of our proposition.

If $p = 2$, then $Z \in \mathrm{SL}(2, K) = \mathrm{PSL}(2, K)$ has order two if and only if it has the same form as used in the previous proof, and hence the above conclusion for X_1, Y_1 and Z_1 is valid also in this case. □

We note that, in the notation of the previous two propositions, conjugation by Z_i inverts R_i and S_i, and, similarly, conjugation by Y_i and X_i invert R_i, T_i and S_i, T_i, respectively, for $i = 1, 2$.

4. Groups generated by representative triples

In order to determine exactly the projective group $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ arising from a representative triple (R, S, T) of elements of $\mathrm{SL}(2, K)$, we first determine the smallest field $F < K$ with the property that $\langle R, S, T \rangle$ is isomorphic to a subgroup of $\mathrm{SL}(2, F)$. Let K have prime characteristic p. If F is any field of characteristic p, we denote by $F_p \cong GF(p)$ the prime field of F. For any collection $\alpha, \beta, \ldots$ of elements of K let $F_p(\alpha, \beta, \ldots)$ denote the smallest subfield of K containing all of $\alpha, \beta, \ldots$.

PROPOSITION 4.1. *Let p be a prime and let (k, l, m) be a p-restricted hyperbolic triple. Let (R, S, T) be a representative triple corresponding to projective orders (k, l, m) and representative orders (κ, λ, μ). Let ω_κ, ω_λ and ω_μ be such that $D \neq 0$. Let F_0 be the smallest field of characteristic p such that the group $\langle R, S, T \rangle$ is isomorphic to a subgroup of* $\mathrm{SL}(2, F)$. *Then $F_0 = F_p(\omega_\kappa, \omega_\lambda, \omega_\mu)$.*

PROOF. Let $F = F_p(\omega_\kappa, \omega_\lambda, \omega_\mu)$. Observe that the traces ω_κ, ω_λ and ω_μ of R, S and T must be contained in the minimal field F_0 of characteristic p such that $\langle R, S, T\rangle$ is isomorphic to a subgroup of $\mathrm{SL}(2, F_0)$. This shows that $F_0 \geq F$. We need to establish the reverse inclusion.

By Proposition 2.1 we have $F_0 = F$ if at least two of the entries k, l, m are equal to p. Consider therefore the situation where $k \geq 3$, and k and l are coprime to p, and either $m = p$ or $\gcd(m, p) = 1$. Proposition 2.2 now shows that the group $\langle R, S, T\rangle$ is isomorphic to a subgroup of $\mathrm{SL}(2, F^*)$ where $F^* = F_p(\xi_\kappa, \omega_\lambda, \omega_\mu)$. Since ξ_κ and ξ_κ^{-1} are roots of the polynomial $x^2 - \omega_\kappa x + 1$, the degree of F^* over F is at most two. Assume that $\xi_\kappa \notin F$ (for otherwise there is nothing to prove). Let ρ^* be the unique nontrivial (involutory) automorphism of F^* that fixes F pointwise; it follows that $\rho^*(\xi_\kappa) = \xi_\kappa^{-1}$. A direct calculation using the matrices $R = R_2$ and $S = S_2$ from Proposition 2.2 shows that $\rho^*(R) = R^{-1}$ and $\rho^*(S) = S^{-1}$. The same effect on R and S, however, arises when conjugating by the matrix $Z = Z_2$ from Proposition 3.2; that is, $Z^{-1}RZ = R^{-1}$ and $Z^{-1}SZ = S^{-1}$. It follows that ρ^* and conjugation $A \mapsto Z^{-1}AZ$ induce the same automorphisms of the group $\langle R, S\rangle = \langle R, S, T\rangle$.

Consider now the subgroup H^* of all the elements $A \in \mathrm{SL}(2, F^*)$ such that $\rho^*(A) = A$. It is well known that $H^* \simeq \mathrm{SL}(2, F)$. Let H_Z^* be the subgroup of all the matrices $B \in \mathrm{SL}(2, F^*)$ such that $\rho^*(B) = Z^{-1}BZ$. From what we saw above we may deduce that $\langle R, S, T\rangle$ is a subgroup of H_Z^*. Our strategy now will be to prove that $H^* \cong H_Z^*$. Having established this, it is sufficient to observe that $\mathrm{SL}(2, F) \leq \langle R, S, T\rangle \leq H_Z^* \cong H^* \cong \mathrm{SL}(2, F)$, which implies that $F_0 = F$.

We prove that $H^* \cong H_Z^*$ by exhibiting a matrix $V \in \mathrm{GL}(2, \hat{F})$, where either $\hat{F} = F^*$ or $[\hat{F} : F^*] = 2$, such that $VZ = \rho^*(V)$. Then it is easy to see that $V^{-1}H^*V = H_Z^*$. Let β be the element we have from Proposition 3.2. If $\beta \notin F$, then $\beta \in F^*$ and $\rho^*(\beta) = -\beta$. In this case we may set

$$V = \begin{bmatrix} 1 & \beta^{-1} \\ \beta & -1 \end{bmatrix}$$

and check that

$$VZ = \begin{bmatrix} 1 & -\beta^{-1} \\ -\beta & -1 \end{bmatrix} = \rho^*(V).$$

On the other hand, if $\beta \in F$, that is, if $\rho^*(\beta) = \beta$, then we need to go beyond F^*. Let $\hat{F}$ be an extension of F^* of degree two, let θ be a primitive element of $\hat{F}$, and let $a = \theta^{(q^2-1)/2}$, where $q = |F|$. Then the automorphism $\hat{\rho}$ of $\hat{F}$ given by $x \mapsto x^q$ has the property that $\hat{\rho}\restriction_{F^*} = \rho^*$ and $\hat{\rho}^2(a) = -a$. Now for the matrix V we may take

$$V = \begin{bmatrix} a & \beta^{-1}\hat{\rho}(a) \\ \beta\hat{\rho}(a) & -a \end{bmatrix}.$$

We leave the remaining details of the calculation to the reader. □

https://doi.org/10.1017/S1446788708000827 Published online by Cambridge University Press

We will now show that the degree of $F_p(\omega_\kappa, \omega_\lambda, \omega_\mu)$ depends only on p, κ, λ and μ, and is independent of the particular choice of primitive roots of unity. As we know, representative orders κ, λ and μ have the property that, if an entry is a multiple of p, then it is equal to p or $2p$ (with the second possibility out of consideration when $p = 2$).

LEMMA 4.2. *Let i be a positive integer coprime to p, let ξ be a primitive ith root of unity, and let $\omega = \xi + \xi^{-1}$. Then the degree of $F_p(\omega)$ over F_p is the smallest positive integer j such that i divides $p^j - 1$ or $p^j + 1$.*

PROOF. Let $\delta = [F_p(\omega) : F_p]$, and note that the degree $d = [F_p(\xi) : F_p]$ is the smallest positive integer j for which i divides $p^j - 1$. Observe that ξ is a root of the quadratic polynomial $x^2 - \omega x + 1$ over $F_p(\omega)$, and so the degree $[F_p(\xi) : F_p(\omega)]$ is either one or two. If d is odd, then $[F_p(\xi) : F_p(\omega)] = 1$, which implies that $\delta = d$. Let now d be even. Then $[F_p(\xi) : F_p(\omega)] = 2$ if and only if the unique nontrivial Galois automorphism of $F_p(\xi)$ over $F_p(\omega)$ of order two fixes the element ω. We know that this Galois automorphism is given by $z \mapsto z^q$ where $q = p^{d/2}$. It is readily verified that $(\xi + \xi^{-1})^q = \xi + \xi^{-1}$ if and only if $(\xi^{q+1} - 1)(\xi^{q-1} - 1) = 0$, which is equivalent to the condition that i divides $q + 1$ or $q - 1$. In both cases, δ is the smallest j such that i divides $p^j + 1$ or $p^j - 1$. □

For a p-restricted hyperbolic triple (k, l, m), let $e(k, l, m)$ be the smallest positive integer e such that each $n \in \{k, l, m\} \setminus \{p\}$ divides $(p^e + 1)/2^\epsilon$ or $(p^e - 1)/2^\epsilon$, where ϵ is 0 or 1 depending on whether p is even or odd, respectively.

PROPOSITION 4.3. *In the above notation, the degree of $F_p(\omega_\kappa, \omega_\lambda, \omega_\mu)$ over F_p is equal to $e(k, l, m)$. In particular, $F_p(\omega_\kappa, \omega_\lambda, \omega_\mu)$ depends only on the projective orders (k, l, m) and not on the choice of representative orders (κ, λ, μ).*

PROOF. Since ω_ν is $\pm 2 \in F_p$ if p divides ν, by Lemma 4.2 it suffices to show that the statement of the proposition is equivalent to the claim that the degree of $F_p(\omega_\kappa, \omega_\lambda, \omega_\mu)$ over F_p is the smallest e such that each $\nu \in \{\kappa, \lambda, \mu\} \setminus \{p, 2p\}$ divides either $p^e - 1$ or $p^e + 1$.

This is clearly true whenever $p = 2$, or p is odd and one of κ, λ, μ is divisible by 4, since in these two cases $(\kappa, \lambda, \mu) = (2k, 2l, 2m)$ or (k, l, m), respectively.

We may thus assume that p is odd and none of κ, λ, μ is divisible by 4. Then k, l, m are all odd, and $(\kappa, \lambda, \mu) = (2k, 2l, 2m)$ or (k, l, m). For an odd integer n, however, the conditions that $2n$ divides $p^e \pm 1$ and that n divides $p^e \pm 1$ are equivalent, and the statement of the proposition is again equivalent to the above claim. □

For brevity, in the remaining part of this section we set $F = F_p(\omega_\kappa, \omega_\lambda, \omega_\mu)$. From the analysis done up to this point we conclude that, under the assumptions of either Proposition 2.1 or 2.2, the subgroup $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ of $\mathrm{PSL}(2, K)$ is actually a subgroup of $\mathrm{PSL}(2, F)$, not contained in any $\mathrm{PSL}(2, F')$, where F' is a proper subfield of F. We then have only two possibilities: either we may have $\langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \mathrm{PSL}(2, F)$, or, if p is odd and $[F : F_p]$ is even, we may have $\langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \mathrm{PGL}(2, F')$, where F' is the unique subfield of F such that $[F : F'] = 2$. In what follows we will identify the conditions under which the second case occurs. We will assume henceforth that p is an odd prime.

Assume that the order of $|F|$ is q^2 where q is a power of p. Let F' be the subfield of F such that $[F : F'] = 2$, that is, $|F'| = q$, and let $\rho : x \mapsto x^q$ be the unique nontrivial Galois automorphism of F that fixes F' pointwise. Clearly, ρ extends to elements of $\mathrm{SL}(2, F)$ and $\mathrm{PSL}(2, F)$ in the obvious way, and we will use the same symbol ρ for these extensions. Soon we will need the following observation regarding changing signs by ρ.

For convenience, we will write $c \mid_2 (2d)$ if c divides $2d$ but not d. Then, referring to the above notation, we have the following result.

LEMMA 4.4. *Let $\omega = \xi + \xi^{-1}$ where ξ is an ith primitive root of unity in some field containing F. Then, $\rho(\omega) = -\omega$ if and only if $\rho(\xi) = -\xi$ or $\rho(\xi) = -\xi^{-1}$, which is equivalent to $i \mid_2 (2q - 2)$ or $i \mid_2 (2q + 2)$, respectively. In particular, if $\rho(\xi) = -\xi$ for some ith primitive root of unity, then this holds for all the ith primitive roots of unity; the same applies to the relation $\rho(\xi) = -\xi^{-1}$.*

PROOF. Since $\rho(x) = x^q$, we have $\rho(\omega) = -\omega$ if and only if $\xi^q + \xi^{-q} = -\xi - \xi^{-1}$, which is equivalent to $(\xi^{q-1} + 1)(\xi^{q+1} + 1) = 0$, and this is easily seen to be the same as stating that $\rho(\xi) = -\xi$ or $\rho(\xi) = -\xi^{-1}$. The factorization, together with the fact that the order of ξ is i, shows that the above occurs if and only if $i \mid_2 (2q - 2)$ or $i \mid_2 (2q + 2)$, respectively. The last statement in the lemma follows from the fact that the conditions on i are arithmetic and do not refer to a particular ith primitive root. □

We return to our discussion about a possible isomorphism of $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ with the group $\mathrm{PGL}(2, F')$. There is a 'canonical' copy H of $\mathrm{PGL}(2, F')$ in $\mathrm{PSL}(2, F)$ given by $H = \{\overline{A} \in \mathrm{PSL}(2, F) \mid \rho(\overline{A}) = \overline{A}\}$. Let $H_Z = \{\overline{A} \in \mathrm{PSL}(2, F) \mid \rho(\overline{A}) = \overline{ZAZ}\}$. The fact that $H \cong H_Z$ can be derived in exactly the same way as shown at the end of the proof of Proposition 4.1. With the help of this we prove the following convenient criterion for deciding if $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ is isomorphic to $\mathrm{PGL}(2, F')$.

PROPOSITION 4.5. *In the notation of the preceding paragraph, we have $\langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \mathrm{PGL}(2, F')$ if and only if the set $\{R, S, T\}$ has a two-element subset $\mathcal{A}$ such that $\rho(\mathrm{tr}(A)) = -\mathrm{tr}(A)$ for $A \in \mathcal{A}$ and $\rho(\mathrm{tr}(A)) = \mathrm{tr}(A)$ for $A \in \{R, S, T\} \setminus \mathcal{A}$.*

REMARK. Note that if an element $\overline{A} \in \{\overline{R}, \overline{S}, \overline{T}\}$ is an involution, then the corresponding trace is zero, and is thus both preserved and taken to its negative by ρ. Hence if one of the projective orders is two, then we may have more than one choice for the set $\mathcal{A}$.

PROOF. Let (R, S, T) be a representative triple with $\langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \mathrm{PGL}(2, F')$. We know that the group $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ is conjugate in $\mathrm{PGL}(2, F)$ to H. Let (R', S', T') be a representative triple such that $\overline{R}', \overline{S}', \overline{T}'$ are images of $\overline{R}, \overline{S}, \overline{T}$ under such a conjugation. Then by the definition of H we have $\rho(R') \in \{R', -R'\}$, and for traces we then obtain $\rho(\mathrm{tr}(R)) = \rho(\mathrm{tr}(R')) = \pm\mathrm{tr}(R') = \pm\mathrm{tr}(R)$; the same holds when R is

https://doi.org/10.1017/S1446788708000827 Published online by Cambridge University Press

replaced with S and T. Since $R'S'T' = I$ and ρ maps each of R', S', T' either to itself or to its negative, it follows that either ρ preserves the traces of all of R', S', T', or it changes the trace signs on two of them while preserving the third; by the above equalities, the same applies to R, S, T. But ρ cannot preserve all three traces, since then we would have $F' = F$, a contradiction.

For the sufficiency, let R, S, T and F, F' be as before; in particular, the group $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ properly contains $\mathrm{PSL}(2, F')$. Also, we may assume that R, S and T have the form as in Propositions 2.1 and 2.2. Suppose now that ρ changes the sign of the traces of two of R, S, T and preserves the sign of the third, as specified by the subset $\mathcal{A}$. This immediately rules out the case of (R, S, T) described in Proposition 2.1, since there the (nonzero) traces of R and S belong to F', the field pointwise fixed by ρ, and hence at most one of k, l, m can be equal to p. If $k, l, m \neq p$, then without loss of generality we may assume that $\mathcal{A} = \{R, S\}$. If precisely one of k, l, m is equal to p, then (as argued before Proposition 2.2) we may assume that $m = p$. But then, since p is odd, we have $0 \neq \omega_\mu \in F'$, and therefore ρ has to change the sign of the traces of R and S. We conclude that in all cases, we may assume that $\mathcal{A} = \{R, S\}$.

Accordingly, suppose that $\rho(\omega_\kappa) = -\omega_\kappa$ and $\rho(\omega_\lambda) = -\omega_\lambda$ while $\rho(\omega_\mu) = \omega_\mu$. From Lemma 4.4 we know that $\rho(\xi_\kappa) \in \{-\xi_\kappa, -\xi_\kappa^{-1}\}$. By inspection of the matrices R and S in the statement of Proposition 2.2 one may check that, if $\rho(\xi_\kappa) = -\xi_\kappa$, then $\rho(R) = -R$ and $\rho(S) = -S$, and if $\rho(\xi_\kappa) = -\xi_\kappa^{-1}$, then $\rho(R) = -R^{-1}$ and $\rho(S) = -S^{-1}$. Recall now the canonical copy H of $\mathrm{PGL}(2, F')$ in $\mathrm{PSL}(2, F)$ and its isomorphic copy H_Z. If ρ changes the signs of R and S, then $\overline{R}, \overline{S} \in H$. In the second case, where ρ inverts R and S and changes signs, we have $\overline{R}, \overline{S} \in H_Z$ since conjugation by $\overline{Z}$ inverts both $\overline{R}$ and $\overline{S}$. Since $\overline{R}$ and $\overline{S}$ generate $\langle \overline{R}, \overline{S}, \overline{T} \rangle$, we conclude that $\langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \mathrm{PGL}(2, F')$. $\square$

We are now in position to show that deciding whether $\langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \mathrm{PGL}(2, F')$ can be reduced to checking certain divisibility conditions. For brevity, we will write $a \mid_2 (2b \pm 2)$ if either $a \mid_2 (2b + 2)$ or $a \mid_2 (2b - 2)$; and we will let $c \mid (d \pm 1)$ have the analogous meaning.

In Proposition 4.3 we saw that $e(k, l, m)$ is equal to the degree of the field $F_p(\omega_\kappa, \omega_\lambda, \omega_\mu)$ over F_p, which is the smallest positive integer e such that each κ, λ, μ coprime to p divides $p^e \pm 1$.

PROPOSITION 4.6. *Let p be an odd prime, let (k, l, m) be a p-restricted hyperbolic triple, and let (R, S, T) be a representative triple with projective orders (k, l, m) and representative orders (κ, λ, μ). Let $(\omega_\kappa, \omega_\lambda, \omega_\mu)$ be the corresponding trace triple, and let*

$$D = \omega_\kappa^2 + \omega_\lambda^2 + \omega_\mu^2 - \omega_\kappa\omega_\lambda\omega_\mu - 4.$$

Then $\langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \mathrm{PGL}(2, p^f)$ for some $f \geq 1$ if and only if $D \neq 0$ and the condition (C) *below is fulfilled:*

(C) *either the condition* $n \mid_2 (p^f \pm 1)$ *holds for exactly two of the three orders* k, l, m*, while the third order is* p *or divides* $\frac{1}{2}(p^f \pm 1)$*; or otherwise* $2 \in \{k, l, m\}$ *and the condition* $n \mid_2 (p^f \pm 1)$ *holds for all* $n \in \{k, l, m\}$.

REMARK. Note that the condition (C) above implies that at least two of k, l, m are even, and that $e(k, l, m) = 2f$.

PROOF. Suppose that $\langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \mathrm{PGL}(2, F')$ for some field of order p^f. Note first that, by Proposition 2.2, $D \neq 0$. Let K be the algebraic closure of F', and let F be the smallest subfield of K such that $\langle \overline{R}, \overline{S}, \overline{T} \rangle \leq \mathrm{PSL}(2, F)$. By Propositions 4.1 and 4.3, the order of F is $p^{e(k,l,m)}$. Since $[F : F'] = 2$, we have $e(k, l, m) = 2f$.

By Proposition 4.5, the Galois automorphism $\rho \in \mathrm{Gal}(F : F')$ takes two of the traces $\{\mathrm{tr}(R), \mathrm{tr}(S), \mathrm{tr}(T)\}$ to their negatives and preserves the third. Note that the trace of any element of order p is ± 2 and is thus preserved by ρ, and that the trace of an element of order two is zero, and is thus both preserved and taken to its negative by ρ. In particular, at most one of the orders k, l, m can be equal to p. If we now apply Lemma 4.4, we see that the condition $\nu \mid_2 (2p^f \pm 2)$ must hold for at least two of the entries κ, λ, μ. Note that any integer ν satisfying $\nu \mid_2 (2p^f \pm 2)$ is divisible by 4, showing that $(\kappa, \lambda, \mu) = (2k, 2l, 2m)$ and that at least two of the entries k, l, m are even. Hence the condition $n \mid_2 (p^f \pm 1)$ holds for at least two of the entries k, l, m. Moreover, if the third entry is not p, then by Lemma 4.2, we see that it must divide $\frac{1}{2}(p^f \pm 1)$. Note also that, if $n \mid_2 (p^f \pm 1)$ holds for all three of k, l, m, then ρ takes the traces of all three elements R, T, S to their negatives, implying that one of k, l, m is 2. This proves (C).

Conversely, assume that all the conditions on D, k, l, m, e (where $e = e(k, l, m)$) listed in the statement of our proposition are fulfilled. Then the generating triple (R, S, T) is conjugate to the triple (R_2, S_2, T_2) as in Proposition 2.2. If the condition $n \mid_2 (p^f \pm 1)$ holds for exactly two of the three orders k, l, m and the third order is p or divides $\frac{1}{2}(p^f \pm 1)$, then, by Lemma 4.4, ρ takes the traces of two of R, S, T to their negatives and fixes the third. The same holds if one of k, l, m is 2 and the other two satisfy the condition $n \mid_2 (p^f \pm 1)$. Proposition 4.5 now shows that the group $\langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \langle \overline{R}_2, \overline{S}_2, \overline{T}_2 \rangle$ is isomorphic to $\mathrm{PGL}(2, F')$ where $[F : F'] = 2$. □

5. Enumeration

In this section we re-establish the enumeration result of Sah [15, Theorem 1.6] for regular hypermaps over projective linear groups. Let p be a prime and let (k, l, m) be a p-restricted hyperbolic triple. We know that if exactly one or exactly two of k, l, m are equal to p, then we may assume that $m = p$ or $m = l = p$, respectively. We need to recall briefly some of the facts we proved in Section 2. Let $(k, l, m)^*$ be the *set* of all representative orders (κ, λ, μ) associated with (k, l, m), so that $(k, l, m)^*$ is either $\{(k, l, m)\}$, or $\{(2k, 2l, 2m)\}$, or $\{(k, l, m), (2k, 2l, 2m)\}$, depending on whether $p = 2$, or $p \geq 3$ and at least one of k, l, m is even, or all of p, k, l, m are odd, respectively. We will say that the triple (k, l, m) is *proper* if $D = D(\omega_\kappa, \omega_\lambda, \omega_\mu) \neq 0$

for any $(\kappa, \lambda, \mu) \in (k, l, m)^*$ and for any choice of ω_κ, ω_λ and ω_μ. Finally, for a hyperbolic, p-restricted, proper triple (k, l, m), let $T(k, l, m)$ be the set of all possible trace triples $(\omega_\kappa, \omega_\lambda, \omega_\mu)$ where $(\kappa, \lambda, \mu) \in (\kappa, \lambda, \mu)^*$. Proposition 2.3 can now be restated in a form that refers just to the projective orders as follows.

PROPOSITION 5.1. *Let p be a prime and let (k, l, m) be a hyperbolic, p-restricted, proper triple. Then there is a bijection between the set $T(k, l, m)$ and the set of conjugacy classes of representative triples (R, S, T) associated with the projective orders (k, l, m).*

New representative triples (R, S, T) with $RST = I$ in $\mathrm{SL}(2, K)$ associated with the same projective orders (k, l, m) can sometimes be obtained from old ones simply by changing signs. To see this, suppose, for instance, that both k and l are even. Then, the orders of both R and $-R$ and of both S and $-S$ are $2k$ and $2l$, respectively, and both (R, S, T) and $(-R, -S, T)$ are representative triples. It is clear that the converse holds as well, that is, if both (R, S, T) and $(-R, -S, T)$ are representative triples, then both k and l are even. Thus, if all k, l, m are even, we may define an equivalence relation on the set of representative triples with equivalence classes of size four formed by the four triples (R, S, T), $(-R, -S, T)$, $(-R, S, -T)$ and $(R, -S, -T)$. If exactly two of the k, l, m are even, then the representative triples come in pairs as we saw above and we again regard the pairs as equivalence classes. Another way to say this is that, when all of k, l, m are even, the quadruples are just orbits of a free action of $Z_2 \times Z_2$ on the set of representative triples; if exactly one of k, l, m is odd then we have a free action of Z_2 representing the sign change. We will refer to this action of $Z_2 \times Z_2$ or of Z_2 as the *sign change action*.

Obviously, the sign change action carries over from the set of representative triples (R, S, T) associated with the projective orders (k, l, m) to the set of the corresponding trace triples $T(k, l, m)$ in a natural way; we will use the symbol $\sim_{\mathrm{S}}$ to denote the corresponding equivalence relation on $T(k, l, m)$. Another natural equivalence relation to be considered on $T(k, l, m)$ is the relation $\sim_{\mathrm{G}}$ induced by the Galois action arising from application of the Galois automorphisms of the fields $F = F_p(\omega_\kappa, \omega_\lambda, \omega_\mu)$ over F_p for $(\kappa, \lambda, \mu) \in (k, l, m)^*$. Indeed, the computations made in the previous section show that the classes of $\sim_{\mathrm{G}}$ are in a one-to-one correspondence with orbits of the Galois action extended to the conjugacy classes of generating triples $(\overline{R}, \overline{S}, \overline{T})$. Let $\sim$ denote the join of $\sim_{\mathrm{S}}$ and $\sim_{\mathrm{G}}$ on $T(k, l, m)$. Since the automorphism group of both $\mathrm{PSL}(2, q)$ and $\mathrm{PGL}(2, q)$ is isomorphic to a semi-direct product of $\mathrm{PGL}(2, q)$ by the Galois group of F over its prime field, we have the following result.

PROPOSITION 5.2. *The number of nonisomorphic regular hypermaps of a proper, hyperbolic, p-restricted type (k, l, m) with automorphism group isomorphic to a subgroup of* $\mathrm{PSL}(2, F)$ *is equal to the number of equivalence classes of the relation $\sim$ on $T(k, l, m)$.* □

For any j such that $j = p$ or $j = 2p$ or otherwise $\gcd(j, p) = 1$, define a modification φ_p of the Euler totient function φ by letting $\varphi_p(j) = 1$ in the first two cases and $\varphi_p(j) = \varphi(j)$ otherwise. The number of distinct elements ω_j (as defined prior to Proposition 2.1) is then equal to $\varphi_p(j)$ or $\varphi_p(j)/2$ according to whether j is a multiple of p or not. Let u be the number of entries k, l, m coprime to p. If at least one of k, l, m is even, then it is easy to see that

$$|T(k, l, m)| = \varphi_p(2k)\varphi_p(2l)\varphi_p(2m)/2^u.$$

In the case where all of k, l, m are odd,

$$\begin{aligned}|T(k, l, m)| &= \varphi_p(k)\varphi_p(l)\varphi_p(m)/2^u + \varphi_p(2k)\varphi_p(2l)\varphi_p(2m)/2^u \\ &= 2\varphi_p(2k)\varphi_p(2l)\varphi_p(2m)/2^u.\end{aligned}$$

Observe that the equivalence classes of the sign change equivalence $\sim_{\mathrm{S}}$ have size one, two or four, depending on whether $u = 1$, 2 or 3. Hence the number of equivalence classes of $\sim_{\mathrm{S}}$ on $T(k, l, m)$ is $\varphi_p(2k)\varphi_p(2l)\varphi_p(2m)/2^{u+v-1}$. As regards the equivalence $\sim_{\mathrm{G}}$ on $T(k, l, m)$ induced by the Galois action, the number of the corresponding classes is equal to $|T(k, l, m)|/e$, where $e = e(k, l, m)$ is the degree of the field $F_p(\omega_\kappa, \omega_\lambda, \omega_\mu)$ over F_p. It remains for us to determine when two trace triples are equivalent under both $\sim_{\mathrm{S}}$ and $\sim_{\mathrm{G}}$. By the analysis in the previous section, this can happen if and only if both the sign change action as well as the Galois action changes signs on precisely two of the entries in a trace triple. But by Lemma 4.5 and in the associated notation, this occurs if and only if $\langle \overline{R}, \overline{S}, \overline{T}\rangle \simeq \mathrm{PGL}(2, F')$. Thus, the number of equivalence classes of $\sim$ on $T(k, l, m)$ is equal to $\varphi_p(2k)\varphi_p(2l)\varphi_p(2m)/(2^{u+v-1}e)$ if $\langle \overline{R}, \overline{S}, \overline{T}\rangle \simeq \mathrm{PSL}(2, F)$, and to $2\varphi_p(2k)\varphi_p(2l)\varphi_p(2m)/(2^{u+v-1}e)$ in the case where $\langle \overline{R}, \overline{S}, \overline{T}\rangle \simeq \mathrm{PGL}(2, F')$. Combining this with Proposition 4.6 yields the enumeration result of Sah (see [15, Theorem 1.6]).

THEOREM 5.3. *Let p be a prime and let (k, l, m) be a p-restricted, hyperbolic, proper triple. Let $e = e(k, l, m)$, and let u and v be the number of entries coprime to p and the number of even entries among k, l, m, respectively.*

(1) *If p is odd and condition* (C) *of Proposition 4.6 is fulfilled, then all the corresponding groups $\langle \overline{R}, \overline{S}, \overline{T}\rangle$ are isomorphic to* $\mathrm{PGL}(2, F')$ *where F' is the index-two subfield of $F_p(\omega_\kappa, \omega_\lambda, \omega_\mu) \simeq F_p(p^e)$, and the number of all the corresponding pairwise nonisomorphic hypermaps of type (k, l, m) is equal to*

$$2\varphi_p(2k)\varphi_p(2l)\varphi_p(2m)/(2^{u+v-1}e).$$

(2) *In all other cases we have $\langle \overline{R}, \overline{S}, \overline{T}\rangle \simeq \mathrm{PSL}(2, F)$ where $F = F_p(\omega_\kappa, \omega_\lambda, \omega_\mu) \simeq F_p(p^e)$, and then the number of all such nonisomorphic hypermaps of type (k, l, m) is equal to*

$$\varphi_p(2k)\varphi_p(2l)\varphi_p(2m)/(2^{u+v-1}e).$$

https://doi.org/10.1017/S1446788708000827 Published online by Cambridge University Press

6. Nonorientable and reflexible regular hypermaps

We now discuss applications of the preceding results to regular hypermaps on non-orientable surfaces and regular reflexible hypermaps on orientable surfaces. Keeping to the notation introduced in the previous sections, this amounts to comparing the group $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ with the group $\langle \overline{X}, \overline{Y}, \overline{Z} \rangle$ where $\overline{Z}$ is given by Proposition 3.1 or 3.2. The existence of $\overline{Z}$ in all cases shows that such hypermaps are all reflexible. Also, from the outline in the introduction it is clear that a reflexible hypermap with rotational symmetry group $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ is nonorientable if and only if $\langle \overline{R}, \overline{S}, \overline{T} \rangle = \langle \overline{X}, \overline{Y}, \overline{Z} \rangle$. We now identify exactly when this happens.

PROPOSITION 6.1. *Let p be a prime and let (k, l, m) be a p-restricted hyperbolic triple. Suppose that ω_κ, ω_λ and ω_μ are such that $D \neq 0$. Let F and F' be as in Theorem 5.3. Then all of the corresponding regular hypermaps of type (k, l, m) with rotation group $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ isomorphic to* $\mathrm{PSL}(2, F)$ *or* $\mathrm{PGL}(2, F')$ *are reflexible. Moreover, the following cases hold.*

(1) *If $\langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \mathrm{PGL}(2, F')$, then the triple $(\overline{R}, \overline{S}, \overline{T})$ is inner reflexible so always gives rise to a nonorientable regular hypermap.*
(2) *If $\langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \mathrm{PSL}(2, F)$ and if two of k, l, m are equal to p, then the triple $(\overline{R}, \overline{S}, \overline{T})$ gives rise to a nonorientable regular hypermap if and only if $|F| \equiv 1 \pmod 4$.*
(3) *If $\langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \mathrm{PSL}(2, F)$ and if at most one of k, l, m is equal to p, then the triple $(\overline{R}, \overline{S}, \overline{T})$ gives rise to a nonorientable regular hypermap if and only if $-D$ is a square in F.*

PROOF. Let us begin with the case where the rotational symmetry group $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ of a hypermap of type (k, l, m) is isomorphic to $\mathrm{PGL}(2, F')$, where $[F : F'] = 2$ and $F = F_p(\omega_\kappa, \omega_\lambda, \omega_\mu)$ for some prime $p \neq 2$. Generators R, S, T as elements of $\mathrm{SL}(2, F)$ are now given by Proposition 2.2, and the inverting involution $\overline{Z} = \overline{Z}_2$ is as in Proposition 3.2. Then, $\langle \overline{X}, \overline{Y}, \overline{Z} \rangle = \langle \overline{R}, \overline{S}, \overline{T}, \overline{Z} \rangle$ is a proper subgroup of $\mathrm{PSL}(2, F)$ of order at least $|\mathrm{PGL}(2, F')|$. By Dickson's classification of subgroups of $\mathrm{PSL}(2, F)$ we have $\langle \overline{R}, \overline{S}, \overline{T} \rangle = \langle \overline{X}, \overline{Y}, \overline{Z} \rangle$. We conclude that in this case $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ is the automorphism group of a nonorientable regular hypermap of type (k, l, m). Note that the same can be obtained by the following more intrinsic argument. By the proof of Proposition 4.5 we know that we may assume that the elements $\overline{R}$ and $\overline{S}$ given by Proposition 2.2 lie either in the canonical copy $H \simeq \mathrm{PGL}(2, F')$ contained in $\mathrm{PSL}(2, F)$ or in its isomorphic copy H_Z. For the nontrivial Galois automorphism ρ of the extension F over F' applied to the explicit form of the matrix Z_2 we have $\rho(D) = D$, and $\rho(\beta) = \beta$ or $\rho(\beta) = -\beta$ according to whether $-D$ is a square in F' or not. At any rate, we have $\rho(\overline{Z}) = \overline{Z}$ and hence $\overline{Z}$ lies in both H, $H_Z \simeq \mathrm{PGL}(2, F')$, that is, $\langle \overline{R}, \overline{S}, \overline{T} \rangle = \langle \overline{X}, \overline{Y}, \overline{Z} \rangle$.

Suppose now that the group $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ is isomorphic to $\mathrm{PSL}(2, F)$. If $k = m = p$, then p is odd and $F = F_p(\omega_\mu)$. Proposition 3.1 implies that for $\overline{Z} = \overline{Z}_1$ we have $\overline{Z} \in \mathrm{PSL}(2, F)$ if and only if -1 is a square in F, which occurs if and only if

https://doi.org/10.1017/S1446788708000827 Published online by Cambridge University Press

$|F| \equiv 1 \pmod 4$. If $k, m \neq p$, then $F = F_p(\omega_\kappa, \omega_\lambda, \omega_\mu)$ and the inverting involution is $\overline{Z} = \overline{Z}_2$, given by Proposition 3.2. An inspection of the form of $\overline{Z}$ and of the groups H^* and H_Z^* (for odd p) that appear in the second part of the proof of Proposition 4.1 shows that $\overline{Z} \in \mathrm{PSL}(2, F)$ if and only if $-D$ is a square in F. □

A regular hypermap of type (k, l, m) is said to be a *regular map* if one of the parameters k, l, m is equal to 2. For specific applications we will be particularly interested in regular maps with the groups $\langle \overline{X}, \overline{Y}, \overline{Z} \rangle$ isomorphic to *general* projective linear two-dimensional groups. Proposition 6.1 lists necessary and sufficient conditions for a regular hypermap (and hence also for a regular map) to have such a group. In the case of maps, however, we will need for our applications a much more detailed knowledge about the membership of the involutory generators $\overline{X}, \overline{Y}, \overline{Z}$ in the unique subgroup of index two in $\langle \overline{X}, \overline{Y}, \overline{Z} \rangle$. The result we need for regular maps can actually be formulated for hypermaps, which we will do (with pointing out the situation for maps in appropriate places).

We begin with the easy case where the group $\langle \overline{X}, \overline{Y}, \overline{Z} \rangle \cong \mathrm{PGL}(2, F)$ contains $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ as a proper subgroup of index two (isomorphic to the unique copy K of $\mathrm{PSL}(2, F)$ in $\mathrm{PGL}(2, F)$). We obviously have $\overline{Z} \notin K$, and since $\overline{R}, \overline{S} \in K$, we must also have $\overline{X}, \overline{Y} \notin K$.

It remains for us to consider the case where the group satisfies $\langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \langle \overline{X}, \overline{Y}, \overline{Z} \rangle \cong \mathrm{PGL}(2, F')$. Recall that the group $\langle \overline{X}, \overline{Y}, \overline{Z} \rangle$ and the corresponding rotation group $\langle \overline{R}, \overline{S}, \overline{T} \rangle$ are related by $R = YZ$, $S = ZX$ and $T = XY$. We know that now p is odd, and among the orders k, l, m of $\overline{R}, \overline{S}, \overline{T}$ we cannot have both k and l equal to p. Hence we may assume that either $k, l, m \neq p$, with $m = 2$ in the category of maps, or else $k, l \neq p$ and $m = p$, with $l = 2$ in the case of maps. Our goal is to clarify which of $\overline{X}, \overline{Y}, \overline{Z}$ are contained in the unique subgroup of $\mathrm{PGL}(2, F')$ isomorphic to $\mathrm{PSL}(2, F')$. To this end it is sufficient to assume that we are in the situation described in Proposition 4.5, where R, S, T are as listed in Proposition 2.2 and X, Y, Z are as given by Proposition 3.2.

PROPOSITION 6.2. *Let $\langle \overline{X}, \overline{Y}, \overline{Z} \rangle = \langle \overline{R}, \overline{S}, \overline{T} \rangle \cong \mathrm{PGL}(2, F')$ and let K be the (unique) subgroup of $\langle \overline{X}, \overline{Y}, \overline{Z} \rangle$ isomorphic to $\mathrm{PSL}(2, F')$. Let $\mathrm{sq}(F')$ be the set of nonzero squares of F'. Also let $\mathcal{A}$ be a two-element subset of $\{R, S, T\}$ such that $\rho(\mathrm{tr}(A)) = -\mathrm{tr}(A)$ for $A \in \mathcal{A}$ and $\rho(\mathrm{tr}(A)) = \mathrm{tr}(A)$ for $A \in \{R, S, T\} \setminus \mathcal{A}$. For $k, l, m \neq p$, we have the following cases.*

(1) *If $\mathcal{A} = \{R, S\}$, then $Z \in K$ and $X, Y \notin K$ if $-D \in \mathrm{sq}(F')$, while $Z \notin K$ and $X, Y \in K$ if $-D \notin \mathrm{sq}(F')$.*
(2) *If $\mathcal{A} = \{S, T\}$, then $X \in K$ and $Y, Z \notin K$ if $-D \in \mathrm{sq}(F')$, while $X \notin K$ and $Y, Z \in K$ if $-D \notin \mathrm{sq}(F')$.*
(3) *If $\mathcal{A} = \{T, R\}$, then $Y \in K$ and $Z, X \notin K$ if $-D \in \mathrm{sq}(F')$, while $Y \notin K$ and $Z, X \in K$ if $-D \notin \mathrm{sq}(F')$.*

In all these cases, if $m = 2$, then the elements X and Y commute. On the other hand, if $k, l \neq p$ and $m = p$, we have the following case.

https://doi.org/10.1017/S1446788708000827 Published online by Cambridge University Press

(4) $\mathcal{A} = \{R, S\}$, *and* $Z \in K$ *and* $X, Y \notin K$ *if* $-D \in \mathrm{sq}(F')$, *while* $Z \notin K$ *and* $X, Y \in K$ *if* $-D \notin \mathrm{sq}(F')$.

Moreover, if $l = 2$, *then* X *and* Z *commute.*

PROOF. Suppose first that $\mathcal{A} = \{R, S\}$, that is, $\rho(\mathrm{tr}(R)) = -\mathrm{tr}(R)$ and $\rho(\mathrm{tr}(S)) = -\mathrm{tr}(S)$. By the arguments developed in the proofs of Propositions 4.1, 4.5 and 6.1, we conclude that $Z \in K$ if and only if $-D \in \mathrm{sq}(F')$; by the same token we have $R, S \notin K$. It follows that $X, Y \notin K$ if and only if $Z \in K$. Bearing in mind the conditions for k, l, m, this proves cases (1) and (4). Now, let $k, l \neq p$ and $m = 2$; then, $k, l \geq 3$. If $\mathcal{A} = \{S, T\}$, then we set $R' = S$, $S' = T$, $T' = R$, $X' = Y$, $Y' = Z$ and $Z' = X$. Since the order of R' is at least three, we may apply the above to the dashed symbols and conclude a dashed version of case (1), which gives case (2). Finally, if $\mathcal{A} = \{S, T\}$, we set $R' = R^{-1}$, $S' = T^{-1}$, $T' = S^{-1}$, $X' = X$, $Y' = Z$ and $Z' = Y$. Again, we may apply case (1) to the dashed symbols, which translates to case (3). The claims about commuting elements are obvious. □

7. Concluding remarks

The explicit form of generating matrices given in Propositions 2.1, 2.2, 3.1 and 3.2 make it possible to perform computations with the associated groups using software packages such as `gap` or MAGMA. Also, our approach clarifies a large number of details not covered in [15] and furnishes a different proof of identification of the minimal field (Proposition 4.1).

It is not clear whether an enumeration result such as the one in Theorem 5.3 could be proved for regular hypermaps on nonorientable surfaces. While the regular hypermaps with rotational symmetry group isomorphic to $\mathrm{PGL}(2, F')$ all come from inner reflexible triples (and so are either nonorientable hypermaps or their orientable double covers) and are enumerated by part (1) of Theorem 5.3, the hypermaps with rotation group isomorphic to $\mathrm{PSL}(2, F)$ seem to present difficulties. By part (3) of Proposition 6.1, a nonorientable regular hypermap of type (k, l, m) can occur for a particular choice of ω_κ, ω_λ, ω_μ with $D \neq 0$ if and only if $-D$ is a square in F. The problem here is that, for a fixed type (k, l, m), different choices of values of $\omega_\kappa, \omega_\lambda, \omega_\mu$ can give all kinds of different values of D: squares, nonsquares, and even zero. To see this, let $F = GF(17)$ and let $(k, l, m) = (4, 8, 8)$, so that $(\kappa, \lambda, \mu) = (8, 16, 16)$. It can be checked that 2 is a primitive eighth root of unity in F, while 3 and 5 are primitive 16th roots of unity in F. In all our examples we set $\omega_\kappa = 2 + 2^{-1} = 2 - 8 = -6$. If $\omega_\lambda = \omega_\mu = 3 + 3^{-1} = 3 + 6 = -8$, then we obtain $D = 0$. Choosing $\omega_\lambda = \omega_\mu = 5 + 5^{-1} = 5 + 7 = -5$ gives $-D = 6$, a nonsquare in F. Finally, letting $\omega_\lambda = -8$ and $\omega_\mu = -5$ leads to $-D = -4$, which is a square in F.

Acknowledgements

The research for this paper was carried out while the second and third authors were affiliated with the University of Auckland.

References

[1] N. M. Adrianov, 'Regular maps with automorphism groups $PSL_2(q)$', *Russian Math. Surveys* **52**(4) (1997), 819–821.

[2] Antonio J. Breda d'Azevedo and Gareth A. Jones, 'Platonic hypermaps', *Beiträge Algebra Geom.* **42**(1) (2001), 1–37.

[3] Marston Conder, Primož Potočnik and Jozef Širáň, Regular maps with almost Sylow-cyclic automorphism groups, and classification of regular maps with Euler characteristic $-p^2$, Preprint.

[4] Robert Cori and Antonio Machì, 'Maps, hypermaps and their automorphisms: a survey, I, II, III', *Exposition. Math.* **10** (1992), 403–427, 429–447, 449–467.

[5] Leonard Eugene Dickson, *Linear Groups: With an Exposition of the Galois Field Theory* (Dover, New York, 1958).

[6] Martin Downs, 'Some enumerations of regular hypermaps with automorphism group isomorphic to $PSL_2(q)$', *Quart. J. Math. Oxford Ser.* (2) **48** (1997), 39–58.

[7] Henry Glover and Denis Sjerve, 'The genus of $PSl_2(q)$', *J. Reine Angew. Math.* **380** (1987), 59–86.

[8] Gareth A. Jones, 'Ree groups and Riemann surfaces', *J. Algebra* **165** (1994), 41–62.

[9] Gareth A. Jones and Stephen A. Silver, 'Suzuki groups and surfaces', *J. London Math. Soc.* (2) **48** (1993), 117–125.

[10] Gareth Jones and David Singerman, 'Maps, hypermaps and triangle groups', in: *The Grothendieck Theory of Dessins d'Enfants (Luminy, 1993)*, London Mathematical Society Lecture Note Series, 200 (Cambridge University Press, Cambridge, 1994), pp. 115–145.

[11] ———, 'Belyĭ functions, hypermaps, and Galois groups', *Bull. London Math. Soc.* **28** (1996), 561–590.

[12] Ulrich Langer and Gerhard Rosenberger, 'Erzeugende endlicher projektiver linearer Gruppen', *Results Math.* **15** (1989), 119–148.

[13] Frank Levin and Gerhard Rosenberger, 'Generators of finite projective linear groups II', *Results Math.* **17** (1990), 120–127.

[14] A. M. Macbeath, 'Generators of the linear fractional groups', in: *Number Theory, Proc. Sympos. Pure Math., Houston, TX*, Vol. XII (American Mathematical Society, Providence, RI, 1967), pp. 14–32.

[15] Chih-han Sah, 'Groups related to compact Riemann surfaces', *Acta Math.* **123** (1969), 13–42.

MARSTON CONDER, Department of Mathematics, University of Auckland, Private Bag 92019, Auckland 1142, New Zealand
e-mail: m.conder@auckland.ac.nz

PRIMOŽ POTOČNIK, Faculty of Mathematics and Physics, University of Ljubljana, and Institute of Mathematics, Physics and Mechanics, Jadranska 19, SI-1000 Ljubljana, Slovenia
e-mail: primoz.potocnik@fmf.uni-lj.si

JOZEF ŠIRÁŇ, Open University, Milton Keynes, MK7 6AA, UK, and Slovak Technical University, Radlinskeho 11, 81368, Bratislava, Slovakia
e-mail: j.siran@open.ac.uk

https://doi.org/10.1017/S1446788708000827 Published online by Cambridge University Press