dMFA

ARS MATHEMATICA CONTEMPORANEA

Also available at http://amc.imfm.si
ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 6 (2013) 25–35

Nonorientable regular maps over linear fractional groups

Gareth A. Jones
University of Southampton, Southampton, U.K.

Martin Mačaj
Comenius University, Bratislava, Slovakia

Jozef Širáň
Open University, Milton Keynes, U.K.
Slovak University of Technology Bratislava, Slovakia

Received 28 October 2011, accepted 22 January 2012, published online 1 June 2012

Abstract

It is well known that for any given hyperbolic pair (k, m) there exist infinitely many regular maps of valence k and face length m on an orientable surface, with automorphism group isomorphic to a linear fractional group. A nonorientable analogue of this result was known to be true for all pairs (k, m) as above with at least one even entry. In this paper we establish the existence of such regular maps on nonorientable surfaces for all hyperbolic pairs.

Keywords: Regular map, linear fractional group.

Math. Subj. Class.: 05C10, 05C25, 20G99

1 Introduction

A map on a compact, orientable surface is *orientably regular* if the group of all orientation preserving automorphisms of the map is transitive, and hence regular, on darts of the map. A map on a compact, nonorientable surface is *regular* if its automorphism group is transitive, and hence regular, on flags of the map. In either case, such maps have all vertices of the same degree and all faces of the same length; if these quantities are k and m we speak of a map of *type* $\{m, k\}$. The type is said to be *hyperbolic* if $1/k + 1/m < 1/2$. Regarding type, the following basic fact was rediscovered a number of times in the past.

E-mail addresses: g.a.jones@soton.ac.uk (Gareth A. Jones), macaj@fmph.uniba.sk (Martin Mačaj), j.siran@open.ac.uk (Jozef Širáň)

Theorem 1.1. *For every hyperbolic pair (k, m) there exist infinitely many orientably regular maps of type $\{m, k\}$.*

A brief history of the development around this result together with a list of various proofs can be found in [9]. A particularly important way of proving Theorem 1.1 follows from [8] and implies that all such maps can be chosen to have the orientation preserving automorphism group isomorphic to a linear fractional group over a finite field.

It is quite surprising that a nonorientable analogue of Theorem 1.1 has not been considered. A proof might follow from the study of generation of symmetric and alternating groups by pairs of permutations of given order in [6], but this work does not appear to have a corresponding follow-up and it is not our intention to do so. Instead, motivated by the result of [8] mentioned above, we will be interested in possibilities to prove a stronger form of a nonorientable analogue of Theorem 1.1 for maps with automorphism group isomorphic to a linear fractional group over a finite field. In fact, this has already been done for three quarters of the cases by the third author in [11] where it is shown that for any hyperbolic pair (k, m) with at least one even entry there are infinitely many nonorientable regular maps of type $\{m, k\}$ with automorphism group isomorphic to $PGL(2, F)$ for suitable finite fields F, but the case when both k and m are odd was left untouched.

In this note we fill in this gap, establishing thus the existence of an infinite number of nonorientable regular maps of type $\{m, k\}$ with automorphism group isomorphic to a linear fractional group for any given hyperbolic type $\{m, k\}$. The main results are presented in Section 4, preceded by background information summed up in Section 2 and auxiliary number theoretic results in Section 3.

2 Preliminaries

Foundations of the theory of regular maps have been laid in [4] and [2] and in what follows we just briefly review a few basic facts; for surveys we recommend [7] and [10].

Orientably regular maps of type $\{m, k\}$ can be identified with their orientation preserving automorphism groups and these are in a one-to-one correspondence with the finite groups G presented in the form

$$G = \langle r, s;\ r^k = s^m = (rs)^2 = \ldots = 1 \rangle \tag{2.1}$$

where r and s represent a k-fold rotation about a fixed vertex of the map and an m-fold rotation about the centre of a face incident with the vertex. In particular, we require that k, m and 2 are the true orders of r, s, and rs, respectively. Vertices, faces and edges of the orientably regular map $M_{\rm or}(G)$ corresponding to a presentation of a group G as in (2.1) can be identified with left cosets of the cyclic subgroups $\langle r \rangle$, $\langle s \rangle$ and $\langle rs \rangle$, with incidence determined by non-empty intersection; the group G then acts as the orientation preserving automorphism group of $M_{\rm or}(G)$ by left multiplication.

Regular maps on nonorientable surfaces are also in a one-to-one correspondence with presentations of finite groups as in (2.1) but satisfying the extra condition that G contains an involution t such that $trt = r^{-1}$ and $tst = s^{-1}$. This time, the nonorientable regular map $M_{\rm nor}(G)$ corresponding to such a group G has vertices, faces and edges identified with the left cosets of the dihedral subgroups $\langle r, t \rangle$, $\langle s, t \rangle$ and $\langle rt, ts \rangle$. Incidence is again determined by non-empty intersection and G acts as the automorphism group of $M_{\rm nor}(G)$ by left multiplication.

Thus, if a group G with presentation (2.1) admits an inner automorphism induced by an involution and inverting r and s, the above correspondences allow one to associate two maps with G, namely, $M_{\rm or}(G)$ and $M_{\rm nor}(G)$. To remove this ambiguity in what follows, for a group G as in (2.1) we define the map $M(G)$ by letting $M(G) = M_{\rm nor}(G)$ if G has an inner automorphism induced by an involution, inverting both r and s, and $M(G) = M_{\rm or}(G)$ if G has no such inner automorphism.

As stated in the Introduction we will be interested in regular maps of a given type with automorphism group isomorphic to a linear fractional group. We begin by recalling the characterisation of such automorphism groups from [8]; for a much more detailed proof we refer to [3].

Proposition 2.1. *Let (k, m) be a hyperbolic pair and let K be an algebraically closed field of a prime characteristic p coprime to km. Let ξ and η be primitive $(\delta k)^{\rm th}$ and $(\delta m)^{\rm th}$ roots of unity in K, where $\delta = 1$ if $p = 2$ and $\delta = 2$ if $p > 2$. Let $D = -(\xi^2 + \xi^{-2} + \eta^2 + \eta^{-2})$ and let*

$$R = \pm \begin{bmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{bmatrix} \quad \text{and} \quad S = \pm(\xi - \xi^{-1})^{-1} \begin{bmatrix} -(\eta + \eta^{-1})\xi^{-1} & D \\ 1 & (\eta + \eta^{-1})\xi \end{bmatrix}$$

be elements of $PSL(2, K)$. Then,

(a) *the orders of R, S, and RS in $PSL(2, K)$ are k, m, and 2, respectively, and*

(b) *if G is a subgroup of $PSL(2, K)$ with presentation (2.1), then there exist primitive $(\delta k)^{\rm th}$ and $(\delta m)^{\rm th}$ roots of unity such that G is conjugate to the subgroup generated by the matrices R and S as above.*

It is therefore sufficient to study the groups $G(\xi, \eta) = \langle R, S\rangle$ with R and S as above. Necessary and sufficient conditions for $G(\xi, \eta)$ to give rise to a nonorientable regular map were given in [3]. Here we present an excerpt sufficient for our purposes.

Theorem 2.2. *Let (k, m) be a hyperbolic pair and let K be an algebraically closed field of a prime characteristic p relatively prime to both k and m. Let ξ and η be primitive $(\delta k)^{\rm th}$ and $(\delta m)^{\rm th}$ roots of unity in K, where $\delta = 1$ if $p = 2$ and $\delta = 2$ if $p > 2$. Let $e = e(k, m)$ be the smallest positive integer j such that $n \mid (p^j - \varepsilon_n)/\delta$ for each $n \in \{k, m\}$ and some $\varepsilon_n \in \{+1, -1\}$. Then:*

(1) *if e is even, $e = 2f$, then $G(\xi, \eta)$ is isomorphic to $PGL(2, p^f)$ if and only if the quantity $D = -(\xi^2 + \xi^{-2} + \eta^2 + \eta^{-2})$ is not equal to zero, and either* (a) *there is an even entry $n \in \{k, m\}$ and an $\varepsilon \in \{+1, -1\}$ such that n divides $(p^f - \varepsilon)$ but $2n$ does not, while the other entry divides $(p^f - \varepsilon')/2$ for some $\varepsilon' \in \{+1, -1\}$, or* (b) *both k and m are even and for any $n \in \{k, m\}$ there exists an ε'_n such that n is a divisor of $(p^f - \varepsilon'_n)$ but $2n$ is not;*

(2) *$G(\xi, \eta)$ is isomorphic to $PSL(2, p^e)$ if and only if $D \neq 0$ and either e is odd, or the pair (k, m) together with an even e do not satisfy any of the above conditions* (a) *and* (b)*; and*

(3) *if $D \neq 0$, the map $M(G(\xi, \eta))$ is nonorientable if and only if either $e = 2f$ and $G(\xi, \eta) \cong PGL(2, p^f)$, or if $G(\xi, \eta) \cong PSL(2, p^e)$ and D is a square in $GF(p^e)$; in particular, in the last case $M(G(\xi, \eta))$ is always nonorientable if $p = 2$ and both k and m are odd.*

From the last part of this result one sees that to obtain nonorientable regular maps it is, for example, sufficient to make sure that $e = 2f$, $D \neq 0$ and $G(\xi, \eta) \cong PGL(2, p^f)$. In [11] it is shown that this can be guaranteed whenever at least one of k and m is even:

Theorem 2.3. *Let (k, m) be a hyperbolic pair with at least one even entry. Then, there is an infinite number of finite, nonorientable, regular maps of type $\{m, k\}$ with automorphism group isomorphic to $PGL(2, F)$ for suitable finite fields F.*

To be able to extend this result to the case when both k and m are odd, by Theorem 2.2 one can only hope to establish the existence of infinitely many regular maps of type $\{m, k\}$ with automorphism group isomorphic to $PSL(2, F)$ for suitable finite fields F. In particular, by part (3) of Theorem 2.2, to achieve this we need to make sure that for an infinite number of primes p one can select primitive $2k$-th and $2m$-th roots of unity ξ and η in $GF(p^e)$ in such a way that the quantity $D = -(\xi^2 + \xi^{-2} + \eta^2 + \eta^{-2})$ is a square in $GF(p^e)$, where $e = e(k, m)$; note that e depends on p as well but this dependence is not shown in our notation. Observe that if k and m are odd, ξ^2 and η^2 are primitive k-th and m-th roots of unity, respectively. Thus, in this case D has the form $D = -(\omega_k + \omega_m)$ where ω_n denotes the sum of an n-th primitive root of unity and its reciprocal in $GF(p^e)$. In what follows we will investigate such quantities in general, first over the field of complex numbers and subsequently over finite fields by considering factor fields of rings of algebraic integers.

3 Auxiliary results involving complex roots of unity

Let ζ_n denote any primitive n-th root of unity, but this time taken in the field $\mathbb{C}$ of complex numbers unless stated otherwise. It is known that all the primitive n-th roots of unity are conjugate over the rationals $\mathbb{Q}$ and their common minimal polynomial is the n-th cyclotomic polynomial Φ_n of degree $\varphi(n)$, the value of the Euler totient function at n. By ω_n we denote any number of the form $\zeta_n + \zeta_n^{-1}$; these quantities are again conjugate over $\mathbb{Q}$ and their common minimal polynomial will be denoted by $\Psi_n(x)$. It is well known that if $n > 2$, then

$$x^{\varphi(n)/2}\Psi_n(x + x^{-1}) = \Phi_n(x). \tag{3.1}$$

Finally, let U_n denote the set of all primitive n-th roots of unity in $\mathbb{C}$ and let $\overline{U}_n$ stand for the set of all the corresponding quantities ω_n.

We continue with some observations. From the fact that $\Phi_1(x) = x - 1$, $\Phi_p(x) = 1 + x + \cdots + x^{p-1}$ and $\Phi_{pn}(x) = \Phi_n(x^p)$ if $p|n$ and $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$ otherwise, we obtain the following auxiliary result by easy calculations.

Lemma 3.1. *Let $\Phi_n(x)$ be the n-th cyclotomic polynomial. Then, $\Phi_1(1) = 0$, $\Phi_{p^k}(1) = p$ for p prime and $k > 0$, and $\Phi_n(1) = 1$ otherwise. Also, $\Phi_1(-1) = -2$, $\Phi_2(-1) = 0$, $\Phi_{2p^k}(-1) = p$ for p prime and $k > 0$, and $\Phi_n(-1) = 1$ otherwise.* □

With the help of these facts we obtain our basic result on products of the quantities $-(\omega_k + \omega_m)$ for any $\omega_k \in \overline{U}_k$ and $\omega_m \in \overline{U}_m$.

Proposition 3.2. *Let k, m be odd positive integers and let*

$$P(k, m) = \prod_{\omega_k \in \overline{U}_k} \prod_{\omega_m \in \overline{U}_m} -(\omega_k + \omega_m)\ .$$

Then, $P(1, 1) = -4$, $P(k, k)^2 = (-2)^{\varphi(k)}$ for $k \geq 3$, and $P(k, m)^2 = 1$ otherwise.

Proof. Obviously $P(k,m) = P(m,k)$ and we will therefore assume that $k \geq m$ in what follows. The values of $P(k,m)$ for $k,m \leq 2$ are trivial. If $k \geq 3$ and $m = 1$, then $P(k,1) = \prod_{\omega_k \in \overline{U}_k} -(2+\omega_k) = \Psi_k(-2) = (-1)^{-\varphi(k)/2}\Phi_k(-1) = (-1)^{\varphi(k)/2}$ and so $P(k,1)^2 = 1$. For the remaining part of the proof we assume that $k \geq m > 1$.

By the properties of the polynomials

$$\Psi_m(x) = \prod_{\omega_m \in \overline{U}_m} (x - \omega_m)$$

we obtain, for any $\omega_k = \zeta_k + \zeta_k^{-1} \in \overline{U}_k$, the equality

$$\prod_{\omega_m \in \overline{U}_m} -(\omega_k + \omega_m) = \Psi_m(-\omega_k) = (-\zeta_k)^{-\varphi(m)/2}\Phi_m(-\zeta_k)\ .$$

Let U_k' be a subset of U_k of cardinality $\varphi(k)/2$ such that $\overline{U}_k = \{\zeta_k + \zeta_k^{-1};\ \zeta_k \in U_k'\}$. The previous computation then implies that

$$P(k,m) = \prod_{\zeta_k \in U_k'} (-\zeta_k)^{-\varphi(m)/2}\Phi_m(-\zeta_k)\ .$$

Extending the product above from U_k' to U_k means squaring the last equation; combining this with the fact that the product of all the (even number of) k-th primitive roots of unity is equal to 1 we obtain

$$P(k,m)^2 = \prod_{\zeta_k \in U_k} (-\zeta_k)^{-\varphi(m)/2}\Phi_m(-\zeta_k) = \prod_{\zeta_k \in U_k} \Phi_m(-\zeta_k).$$

Invoking the well known identity $\Phi_m(x) = \prod_{d|m}(x^d - 1)^{\mu(m/d)}$, where μ is the Moebius function, we have

$$\Phi_m(-\zeta_k) = \prod_{d|m}(-\zeta_k^d - 1)^{\mu(m/d)}\ .$$

This product is non-zero since both k and m, and hence all the divisors d, are odd and so $(-\zeta_k)^d \neq 1$; note also that the divisors satisfy $d \leq k$ because of the assumption $m \leq k$.

Let us analyze the system of powers $\mathcal{U} = (\zeta_k^d;\ \zeta_k \in U_k)$ appearing in the last equality. For any positive divisor d of m let $n(d) = k/(d,k)$ and $r(d) = \varphi(k)/\varphi(n(d))$; of course, both quantities depend on k as well. It can now be seen that the system $\mathcal{U}$ is a collection, for any d dividing m, of primitive $n(d)$-th roots of unity, each repeated $r(d)$ times. With the help of all these facts together with $\Phi_t(x) = \prod_{\zeta_t \in U_t}(x - \zeta_t)$ evaluated at $x = -1$ we successively obtain

$$P(k,m)^2 = \prod_{\zeta_k \in U_k} \prod_{d|m}(-\zeta_k^d - 1)^{\mu(m/d)} = \prod_{d|m} \prod_{\zeta_k \in U_k} (-1 - \zeta_k^d)^{\mu(m/d)}$$

$$= \prod_{d|m} \prod_{\zeta_{n(d)} \in U_{n(d)}} (-1 - \zeta_{n(d)})^{r(d)\mu(m/d)} = \prod_{d|m} (\Phi_{n(d)}(-1))^{r(d)\mu(m/d)}\ .$$

As all the values of $n(d)$ are odd here, we have $\Phi_{n(d)}(-1) = 1$ if $d < k$ and $\Phi_{n(d)}(-1) = -2$ if $d = k$, where the second possibility occurs if and only if $m = k$ and then $r(d) = \varphi(k)$ and $\mu(m/d) = 1$. We conclude that for $k \geq 3$ we have $P(k,k)^2 = (-2)^{\varphi(k)}$, and $P(k,m)^2 = 1$ if $1 < m < k$. This completes the proof. □

A different and more powerful approach to the investigation of the quantity D from Theorem 2.2 relies on some known facts on algebraic integers in algebraic number fields. We refer to [1] as a suitable introductory reference and recall here just a few basic concepts and results.

Let K be an algebraic number field, that is, an extension of $\mathbb{Q}$ of a finite degree. Let $O = O_K$ be the ring of algebraic integers in K. The ring O is known to be a Dedekind domain, but apart from a few facts the theory of such domains will not be needed. A basic property of O is that every non-zero ideal $J \subset O$ has a finite index $[O : J]$. Without going into too much detail we recall that the the index $[O : J]$ is the *norm* $N(J)$ of J. Another important property of O is that any prime ideal $J \subset O$ is maximal. Thus, for any such J the quotient ring O/J is a finite field and so there exists a unique rational prime p such that $N(J) = p^j$ for some $j \in \{1, 2, \ldots, d\}$, where $d = [K : \mathbb{Q}]$ is the degree of the extension. Further, it is known that K admits exactly d distinct injective homomorphisms $\sigma_1, \ldots, \sigma_d$ into $\mathbb{C}$. The *norm* $N(z)$ of any element $z \in K$ is defined as the product $N(z) = \sigma_1(z) \ldots \sigma_d(z)$; the elements $\sigma_t(z)$, $1 \le t \le d$, are the *conjugates of* z *over* K. The norm is multiplicative, that is, $N(z_1 z_2) = N(z_1)N(z_2)$ for any $z_1, z_2 \in K$. Norms of elements of O and ideals in O are known to be related by the fact that, for every non-zero algebraic integer $z \in O$, the absolute value of $N(z)$ is equal to the norm of the ideal $(z) \subset O$ generated by z. In particular, the norm of every non-zero element $z \in O$ is a non-zero integer, and it is well known that $|N(z)| = 1$ if and only if z is a unit, that is, an invertible element in the ring O. We will also repeatedly use the fact that if an element $z \in O$ belongs to an ideal I of O, then $N(I)$ divides $N(z)$.

For illustration we present some of the consequences of Proposition 3.2 in the language of algebraic number theory. Let $\alpha = \zeta_{2k}$ and $\beta = \zeta_{2m}$ be complex primitive $2k$-th and $2m$-th roots of unity, respectively, and let $A = -(\alpha^2 + \alpha^{-2} + \beta^2 + \beta^{-2})$. In what follows, let K denote the algebraic number field $\mathbb{Q}[\alpha, \beta]$. Since the generators α and β of K are roots of unity in $\mathbb{C}$, every injective homomorphism $\sigma : K \to \mathbb{C}$ is uniquely determined by positive integers i and j, relatively prime to k and m, such that $\sigma(\alpha) = \alpha^i$ and $\sigma(\beta) = \beta^j$. Observe, however, that whether particular i and j give rise to such an injective homomorphism may also depend on α and β and not just on k and m. As before, let $O = O_K$ be the ring of algebraic integers of K. Since α and β themselves are algebraic integers in K, we have $A \in O$; in particular, the norm $N(A)$ in O is an integer.

Lemma 3.3. *If $\alpha \ne \beta$, then A is a unit in O, and if $\alpha = \beta$, then $|N(A)|$ is a power of 2.*

Proof. Observe that all factors in the product $P(k, m)$ in Proposition 3.2 are algebraic integers, with all conjugates of A being among the factors. By the same Proposition we have $P(k, m) = \pm 1$ if $k \ne m$, while $P(k, k)^2 = (-2)^{\varphi(k)}$ for $k \ge 3$. Since algebraic integers have integral norm, it follows that A is a unit in O if $k \ne m$. In the case when $k = m$ and $\alpha = \beta$, the absolute value of the norm of $-2(\alpha^2 + \alpha^{-2})$ is equal to $(-2)^{\varphi(k)/2}$, and therefore for $\alpha \ne \beta$ the absolute value of the norm of A must be 1. □

Returning to our main theme, until the end of this section we will assume that (k, m) is a fixed hyperbolic pair with no restriction on the parity of the two entries. We begin by an elementary observation that will turn out to be crucial later.

Lemma 3.4. *The quantity $A - n^2$ is never a unit in O for any integer $n > 2$.*

Proof. We recall the known fact that K is isomorphic to the cyclotomic field $\mathbb{Q}[\gamma]$, where $\gamma = \cos(\frac{2\pi}{\ell}) + i \sin(\frac{2\pi}{\ell})$ is a primitive ℓ-th root of unity for $\ell = \operatorname{lcm}\{2, k, m\}$. The

conjugates of γ over K have the form $\cos(\frac{2\pi}{\ell}j) + i\sin(\frac{2\pi}{\ell}j)$, where $1 \le j < \ell$ and $(j,\ell) = 1$. All the $\varphi(\ell)$ distinct injective homomorphisms $\sigma_t : K \to \mathbb{C}$ preserve the rationals pointwise. Since the explicit form of the conjugates of γ over K implies that $|\sigma_t(A)| < 4$, we have $|\sigma_t(A - n^2)| = |\sigma_t(A) - n^2| \ge n^2 - |\sigma_t(A)| > n^2 - 4$ for any t such that $1 \le t \le \varphi(\ell)$. Thus, by the definition of the norm, for $n > 2$ we have $|N(A - n^2)| > 1$, which means that $A - n^2$ is not invertible in O. □

It is useful to realise that our considerations before Lemma 3.1 did not depend on the parity of k and m and hence we may use them in what follows. Observe that in the general case we want to deal with, the value of A could be equal to zero in K, which happens precisely if $i\beta \in \{\pm\alpha, \pm\alpha^{-1}\}$. If, however, $\{k, m\}$ is a hyperbolic pair, it is easy to see that we can choose α and β avoiding this condition. Keeping to the notation introduced above, for any $n \ge 3$ let $I = I_n$ be a maximal ideal in O containing the element $A - n^2$ and let $p = p_n$ be the characteristic of the field $F = O/I$. Letting $\xi = \alpha + I$, $\eta = \beta + I$, and $D = A + I$, we have:

Lemma 3.5. *If n is relatively prime to $N(A)$, then the element $D = -(\xi^2 + \xi^{-2} + \eta^2 + \eta^{-2})$ is a non-zero square in F and p does not divide n. Moreover, if p is not a divisor of $2km$, then ξ and η are primitive $2k$-th and $2m$-th root of unity in F.*

Proof. Since $A - n^2 \in I$, that is, $A + I = n^2 + I$, the element $D = A + I$ is a square in F. As $p \in I$ and I is a prime ideal, by our earlier remarks on norms of elements and ideals of the Dedekind ring O the condition $A \in I$ is equivalent to each of the conditions $n^2 \in I$, $n \in I$, and $p|n$. Hence p divides both n and $N(A)$, contrary to our assumption on their relative primeness.

It is obvious that ξ is a $2k$-th root of unity in F. Assume that $\alpha^u - 1 \in I$, where α^u is a primitive c-th root of unity in $\mathbb{C}$ for a proper divisor c of $2k$. As the ideal generated by the algebraic integer $\alpha^u - 1$ is contained in I, the norm of I divides the norm of $\alpha^u - 1$, which implies that the norm of $\alpha^u - 1$ is divisible by p. On the other hand, all conjugates of α^u are c-th primitive roots of unity in $\mathbb{C}$. Arguments analogous to those used in the proof of Proposition 3.2 imply that, up to sign, the norm of $\alpha^u - 1$ is a power of $\Phi_c(1)$. Thus, by Lemma 3.1, c is a power of p, contrary to the assumption that $p \nmid 2k$. It follows that ξ is a primitive $2k$-th root of unity in F. By the same token, η is a primitive $2m$-th root of unity in F. □

By suitably varying the parameter n one obtains an infinite sequence of primes as in Lemma 3.5.

Lemma 3.6. *If $A \neq 0$, then there exists an infinite set of values n and an infinite sequence of prime ideals I_n of O containing the element $A - n^2$ such that the fields O/I_n have pairwise distinct prime characteristic p_n.*

Proof. Referring to the way the primes p_n have been introduced for any $n > 2$, let us define an infinite sequence n_j of integers by letting $n_1 = 2|N(A)| + 1$ and $n_j = \prod_{i=1}^{j-1} p_{n_i}$ for $j > 1$. Applying Lemma 3.5 inductively we deduce that p_{n_j} does not divide n_j for any $j \ge 1$. By our construction, for any $j \ge 2$ the prime p_{n_j} differs from all the previous primes p_{n_i} for $i < j$. □

4 Results

Two immediate consequences in the direction of our interest can be obtained by exploring earlier results. Firstly, there is a much more general version of Theorem 2.2 in which the prime p is not necessarily coprime to k and m, in particular, covering the case when both k and m are equal to p and $G \cong PSL(2,p)$; see Propositions 3.1, 3.2, 4.6 and 6.1 of [3]. In order to avoid a rather long re-statement of these facts we invite the reader to check that part (2) of Proposition 6.1 combined with Proposition 3.1 of [3] imply:

Theorem 4.1. *If p is a prime congruent to 1 mod 4, then there exists a nonorientable regular map of type (p,p) with automorphism group isomorphic to $PSL(2,p)$.* □

Secondly, if both k and m are odd and $p = 2$, part (3) of Theorem 2.2 directly yields the following result, where $e = e(k,m)$ is as introduced in the statement of Theorem 2.2.

Theorem 4.2. *Let (k,m) be a hyperbolic pair consisting of odd entries. Then there is a nonorientable regular map of type $\{m,k\}$ with automorphism group isomorphic to $PSL(2,2^e)$ for $e = e(k,m)$.* □

Together with the earlier findings this gives at least an existence result of the sought kind on regular maps over linear fractional groups.

Corollary 4.3. *For any hyperbolic pair (k,m) there exists a nonorientable regular map of type $\{m,k\}$ with automorphism group isomorphic to a linear fractional group over a finite field.* □

In the light of Theorem 2.3, the question of existence of an infinite number of such maps of any given type hyperbolic type is settled by the following result. Although we are interested mainly in the case when k and m are odd, we give a more general formulation which yields an alternative proof of Theorem 2 of [11].

Theorem 4.4. *For every hyperbolic pair (k,m) there is an infinite number of finite, nonorientable, regular maps of type $\{m,k\}$ with automorphism group isomorphic to $PSL(2,F)$ or $PGL(2,F)$ for suitable finite fields F.*

Proof. We will refer to the notation introduced in Section 3. For a fixed hyperbolic pair (k,m) and a non-zero $A = -(\alpha^2 + \alpha^{-2} + \beta^2 + \beta^{-2})$ with let $p = p_n$ be any prime from Lemma 3.6 relatively prime to $2km$, and let $G = G(\xi,\eta)$ be the corresponding group. By Theorem 2.2, G is isomorphic to $PSL(2,F)$ or $PGL(2,F')$. As D is a square, the corresponding regular map $M(G)$ is nonorientable in both cases. □

We also present two more results based on residue techniques which, although applicable only to a very restricted infinite set of types with both entries odd, may be useful in future investigations.

Theorem 4.5. *Let k and m be prime powers congruent to 3 mod 4. Then, there exist infinitely many nonorientable regular maps of type $\{m,k\}$ with automorphism group isomorphic to $PSL(2,F)$ for suitable finite fields F.*

Proof. Let p be a prime congruent to 1 mod 8 and let $e = \min\{n; k|p^n \pm 1 \text{ and } m|p^n \pm 1\}$. Then, p does not divide $2km$ and the equality from Proposition 3.2 holds also in $GF(p^e)$, with appropriate interpretation of the primitive roots. Since $p \equiv 1 \bmod 8$, the four

elements ± 1 and ± 2 are all quadratic residues in $GF(p)$ and hence also in $GF(p^e)$. By Proposition 3.2, the element $P(k,m)$ is a quadratic residue in $GF(p^e)$; note that in the case $k \neq m$ it would have been sufficient to assume $p \equiv 1 \bmod 4$ to obtain the same conclusion. By our assumptions, both $\varphi(k)/2$ and $\varphi(m)/2$ are odd. The product $P(k,m)$ has therefore an odd number of factors and so at least one of them must be a quadratic residue in $GF(p^e)$. That is, there exist $\omega_k \in \overline{U}_k$ and $\omega_m \in \overline{U}_m$ such that the value $D = -(\omega_k + \omega_m)$ is a square in $GF(p^e)$. This gives, by Theorem 2.2 and the remark after Theorem 2.3, a nonorientable regular map of type $\{m,k\}$. Since there are infinitely many primes p as above, our result follows. □

Theorem 4.6. *Let k and m be odd integers forming a hyperbolic pair such that the number $\varphi(k)\varphi(m)/4$ is even, that is, at least one of k, m is not a prime power congruent to 3 mod 4. If $P(k,m) < 0$, then there are infinitely many finite, nonorientable, regular maps of type $\{m,k\}$ with automorphism group isomorphic to $PGL(2,F)$ for suitable finite fields F.*

Proof. Let $p \equiv 3 \bmod 4$ be a prime such that e is odd (e.g., any $p \equiv \pm 1 \bmod km$). If $k \neq m$, then $P(k,m) = -1$ not only in $\mathbb{C}$ but also in $GF(p^e)$. Similarly if $k = m$, then we have $P(k,m) = (-2)^{\varphi(k)/2}$ both in $\mathbb{C}$ and in $GF(p^e)$. Note that if $k = m$, then $\varphi(k)/2$ is even and $2^{\varphi(k)/2}$ is a quadratic residue in $GF(p)$. As $p \equiv 3 \bmod 4$ and e is odd, the product $P(k,m)$ is a quadratic nonresidue in both $GF(p)$ and $GF(p^e)$. On the other hand, $P(k,m)$ has an even number of factors, and therefore at least one of them is a quadratic residue in $GF(p^e)$. □

5 Remarks

By Theorem 4.4, for any given hyperbolic pair (k,m) there exists an infinite number of nonorientable regular maps of type $\{m,k\}$ with automorphism group isomorphic to linear fractional groups over finite fields. Our approach was based on developing some results obtained in [3] in the course of analysing regular maps over linear fractional groups. The scope of [3] is, however, broader and covers regular hypermaps. For a general theory of hypermaps and their surface representations we recommend [5]. Here we just recall that a finite regular hypermap of type (k,m,l) can be identified with a finite quotient group of the triangle group $T(k,m,l) = \langle r,s,t;\ r^k = s^m = (rs)^l = 1\rangle$. Thus, regular hypermaps are a natural generalisation of regular maps (corresponding to the case when $l = 2$). Facts collected in [8, 3] imply that for any hyperbolic triple (k,m,l), that is, such that $1/k + 1/m + 1/l < 1$, there exist infinitely many regular hypermaps of type (k,m,l) on orientable surfaces, with automorphism group isomorphic to a linear fractional group over a finite field. By the theory developed in [3] combined with the findings in this paper, to establish a nonorientable analogue of this result requires analysing conditions under which the quantity $A' = 4+(\alpha+\alpha^{-1})(\beta+\beta^{-1})(\gamma+\gamma^{-1})-(\alpha+\alpha^{-1})^2-(\beta+\beta^{-1})^2-(\gamma+\gamma^{-1})^2$, where α, β and γ are primitive $2k$-th, $2m$-th, and $2l$-th roots of unity in $\mathbb{C}$, projects onto a non-zero square in a quotient field of the ring of algebraic integers of $\mathbb{Q}[\alpha,\beta,\gamma]$ generated by a suitable prime ideal; note that for $l = 2$ we have $\gamma^2 = 1$ and $\gamma + \gamma^{-1} = 0$ and then A' reduces to the quantity A introduced earlier. In fact, methods of Section 3 can be adapted in an obvious way to construct, for any hyperbolic triple (k,m,l) and for suitable triples (α,β,γ) of primitive roots of unity as above, an infinite number of nonorientable regular hypermaps of type (k,l,m) over linear fractional groups.

A comparison of Theorems 4.4, 4.5 and 4.6 reveals their different nature. Theorem 4.4 is more universal since it applies to all hyperbolic pairs and it is, in essence, constructive,

but it yields no information on the corresponding set of primes. On the other hand, Theorems 4.5 and 4.6 apply to a very restricted set of hyperbolic pairs and are, in essence, existential, but the sets of primes for which they guarantee the existence of nonorientable regular maps have positive density in the set of all primes. This leaves the intriguing question of whether it is possible, for any given hyperbolic pair (k, m), to determine all primes p such that there exists a nonorientable regular map of type $\{m, k\}$ with its automorphism group isomorphic to a linear fractional group over a field of characteristic p.

For possible further interest we present a table of values of the product $P(k, m)$ for odd k, m such that $3 \leq k, m \leq 41$. Observe that for $k \neq m$ the table shows negative entries only if both k and m are powers of primes congruent to 3 mod 4. If this observation carries through to all odd k and m, Theorem 4.6 would be applicable only in the case when $k = m$, and the values 5, 13, 25, 29 and 37 show that this Theorem is not void.

3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41
2	1	-1	-1	-1	1	1	1	-1	1	-1	1	-1	1	-1	1	1	1	1	1
1	-2^2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
-1	1	-2^3	-1	-1	1	1	1	-1	1	-1	1	-1	1	-1	1	1	1	1	1
-1	1	-1	2^3	-1	1	1	1	-1	1	-1	1	-1	1	-1	1	1	1	1	1
-1	1	-1	-1	2^5	1	1	1	-1	1	-1	1	-1	1	-1	1	1	1	1	1
1	1	1	1	1	-2^6	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	2^4	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	2^8	1	1	1	1	1	1	1	1	1	1	1	1
-1	1	-1	-1	-1	1	1	1	2^9	1	-1	1	-1	1	-1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	2^6	1	1	1	1	1	1	1	1	1	1
-1	1	-1	-1	-1	1	1	1	-1	1	-2^{11}	1	-1	1	-1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	-2^{10}	1	1	1	1	1	1	1	1
-1	1	-1	-1	-1	1	1	1	-1	1	-1	1	2^9	1	-1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	-2^{14}	1	1	1	1	1	1
-1	1	-1	-1	-1	1	1	1	-1	1	-1	1	-1	1	-2^{15}	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2^{10}	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2^{12}	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	-2^{18}	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2^{12}	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2^{20}

Acknowledgement

Research of the second author was supported by the APVV Research Grants 0111-07 and 0223-10, and the VEGA Research Grants 1/0588/09 and 1/0406/09. The third author acknowledges support by the APVV Research Grants 0104-07 and 0223-10, and the VEGA Research Grants 1/0280/10 and 1/0781/11. Both the second and the third authors also acknowledge the APVV support as part of the EUROCORES Programme EUROGIGA (project GREGAS, ESF-EC-0009-10) of the European Science Foundation.

References

[1] S. Alaca and K. S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, Cambridge, 2004.

[2] R. P. Bryant and D. Singerman, Foundations of the theory of maps on surfaces with boundary, *Quart. J. Math. Oxford Ser.* **141** (1985), 17–41.

[3] M. Conder, P. Potočnik and J. Širáň, Regular hypermaps over projective linear groups, *J. Australian Math. Soc.* **85** (2008), 155–175.

[4] G. A. Jones and D. Singerman, Theory of maps on orientable surfaces, *Proc. London Math. Soc.* **37** (1978), 273–307.

[5] G. A. Jones and D. Singerman, Belyĭfunctions, hypermaps, and Galois groups, *Bull. London Math. Soc.* **28** (1996), 561–590.

[6] Q. Mushtaq and H. Servatius, Permutation representations of the symmetry groups of regular hyperbolic tessellations, *J. London Math. Soc.* **48** (1993), 77–86.

[7] R.Nedela, Regular maps – combinatorial objects relating different fields of mathematics, *J. Korean Math. Soc.* **38** (2001), 1069–1105.

[8] Ch.-H. Sah, Groups related to compact Riemann surfaces, *Acta Math.* **123** (1969), 13–42.

[9] J. Širáň, Triangle group representations and their applications to graphs and maps, *Discrete Math.* **229** (2001), 341–358.

[10] J. Širáň, *Regular maps on a given surface: a survey, Topics in Discrete Mathematics*, Algorithms Combin. 26, Springer, 2006, 591–609.

[11] J. Širáň, Non-orientable regular maps of a given type over linear fractional groups, *Graphs and Combinatorics* **26** (2010), 597–602.