BULLETIN OF THE
GREEK MATHEMATICAL SOCIETY
Volume 53, 2007 (59–67)

On certain Regular Maps with Automorphism group PSL$(2, p)$

Martin Downs

Received 18/04/2007 Accepted 03/10/2007

Abstract

Let p be any prime greater than three. The unique regular oriented triangular map of valency p with automorphism group isomorphic to PSL$(2, p)$ is constructed combinatorially. In particular, it is shown that the underlying graph has diameter 3 and if a map automorphism preserves one vertex then it also preserves all vertices that are of distance 3 from it. All circuits in the map can be derived from circuits of length six or less. The types of circuits of length six or less are listed and a two-generator, four-relator unified presentation for the groups PSL$(2, p)$ as p varies is stated.

1991 *Mathematics subject classification*: 20B25
Keywords: Regular oriented maps, sets of vertices fixed by an automorphism, projective special groups over finite fields.

1. Introduction

Oriented maps are defined in terms of transitive group actions, but their definition is motivated by 2-cell imbeddings of graphs in oriented topological surfaces. (There are parallel theories for maps imbedded in non-oriented surfaces but as these are not considered in this paper we shall usually abbreviate the term "oriented map" to "map"). Automorphisms of a map will be defined later; regular maps are those for which the automorphism group is transitive. Regular maps are particularly important in that they represent imbeddings with certain maximal symmetry properties. For example regular maps necessarily induce imbeddings where the valency and the number of edges bounding a 2-cell are constants. (However the converse does not hold, see [7, p. 305].) The study of regular maps offers several research directions, some of which we mention now. The most obvious examples of representations of regular maps are the Platonic "solids" of antiquity. These all have genus 0; a program to characterize regular maps with particular "low" genus is a natural one to undertake. This is

This work was done with the financial aid of the State Scholarship Foundation of Greece, Grant Number 707, 2005-2006.

carried out in [7] for genus 1. Another line of examination concerning regular maps is the enumeration of regular maps having an automorphism group of a particular isomorphism type. This task reduces to the determination of the Möbius inversion on the subgroup lattice (see e.g., [5], [6]). A further issue is raised by the fact that a regular map induces an underlying graph; this rouses the question which specific graphs can underlie a regular map? Some results of this kind are reviewed in [9]. A similar aim would be to investigate whether regular maps induce underlying graphs that satisfy certain specified properties; a particular case is dealt with in this paper.

We define a certain type of maps. An extreme-vertex-fixing map of order r is a regular map with an underlying graph of diameter r satisfying:

(i) For any vertex v, there is a unique maximal set S_v of vertices including v such that the distance between any two vertices of S_v equals r.

(ii) For any vertex v, there is a non-identity automorphism of the map that fixes each element of S_v but no other vertices.

For example, the regular octahedron represents an extreme-vertex-fixing map of order 2, the cube and icosahedron are extreme-vertex-fixing maps of order 3, and the dodecahedron is an extreme-vertex-fixing map of order 5. (In each case $|S| = 2$). Given the existence of the automorphism in (ii), the fixed vertices induce invariance properties that will help in the analysis of the structure of the map. The purpose of this paper is to construct an infinite family of extreme-vertex fixing maps of order 3. Specifically, we shall prove:

Proposition 1.1 *For every prime $p > 3$, the unique regular triangular map with automorphism group isomorphic to $PSL(2,p)$ and vertices of valency p is an extreme-vertex fixing map of order* 3.

2. Theoretical Background and specific aims

In this section we outline (oriented) map theory as far as we need it. We follow the treatment (and notation) of [7], rather than that of [2] which is perhaps more widely-known.

An oriented map $\mathbf{M}$ is a set Ω together with permutations x and y of Ω such that x^2 is the identity permutation and the group G generated by x and y is transitive on Ω. We denote $\mathbf{M}$ by the quadruple (G, Ω, x, y) and we term the elements of Ω as the darts of $\mathbf{M}$. Also we abbreviate "oriented map" by "map".

Every map is faithfully represented as a 2-cell imbedding of a graph in an oriented surface and vice-versa. Details of this association may be found in [7]. For this paper, only an informal outline of how an imbedding induces a map is required. Let $\mathbf{G}$ be a graph imbedding. Then we define Ω, i.e., the darts, as the set of pairs (v, e) where e is an edge of $\mathbf{G}$ incident with the vertex v of $\mathbf{G}$. The positioning of the darts in $\mathbf{G}$

follows these rules: If $\delta = (v, e)$ is a dart, then $x(\delta)$ is the other dart on the same edge e, and $y(\delta)$ is the next dart (following orientation) in the cycle of darts at the same vertex v. Having determined the permutations x and y on Ω, we define $G := \langle x, y \rangle$. As **G** is connected, it is clear that G acts transitively. Then (G, Ω, x, y) is a map.

From the orientation of the surface, any dart δ is naturally associated with a unique 2-cell F (where if $\delta = (v, e)$, e is part of the boundary of F). Note that letting $z := xy^{-1}$, then $z(\delta) = x(y^{-1}(\delta))$ is the next dart (following orientation) in the cycle of darts associated with F. It is natural to define the vertices, edges and faces of **M** as the cycles of the permutations y, x and z on Ω respectively. If the order of z is three, we call **M** triangular.

An automorphism of the map $\mathbf{M} := (G, \Omega, x, y)$ is a permutation of Ω which commutes with all elements of G. The automorphism group of **M** always acts semi-regularly; if further it acts transitively we term **M** as regular. Examples of regular maps are those of the form $(G, |G|, x, y)$, where $|G|$ denotes the underlying set of the group G and x and y act on $|G|$ by left-hand multiplication in G. (Multiplying $g \in G$ on the right of elements of $|G|$ constitutes an automorphism of **M**.) In fact every regular map is isomorphic to a map of this form.

If **M** is regular and the constant number of darts incident to a vertex is d, **M** is said to be of valency d. This paper will give enough information to form an explicit construction of the unique regular triangular map of valency p with automorphism group isomorphic to PSL$(2, p)$ (where p is any prime). We shall denote this map as $M(2, p, 3)$. It will be shown that for all $p > 3$, the underlying graph of $M(2, p, 3)$ has diameter three, and the family of maps $M(2, p, 3)$ are extreme-vertex-fixing maps of order 3.

A particular two generator set of PSL$(2, p)$ will be associated with the map $M(2, p, 3)$ and, broadly speaking, the relators in these two generators can be "read off" from the circuits that occur in $M(2, p, 3)$. Hence our construction of $M(2, p, 3)$ is a good vehicle to examine presentations of the groups PSL$(2, p)$ in these specific generators. The small diameter of these maps allow us to consider only relators associated with circuits of length six or less. In the paper a list of such circuits is given. A process of derivation of circuits from others (analogous to derivation of relators from other relators) allows the deduction of the following unified presentation for the groups PSL$(2, p)$:

$$\langle X, Y \mid X^2 = Y^p = (XY^{-1})^3 = I, Y = W^{-1}(X, Y) Y^{\alpha^2} W(X, Y) \rangle$$

where α is any primitive root of GF(p) (i.e., any generator of the cyclic group $\{1, 2, \ldots p-1\}$ under multiplication mod(p)), and

$$W(X, Y) = XY^{\alpha^{-1}} XY^{\alpha} X.$$

The argument for this result is omitted, as other presentations are extant in previous papers. In [1], for example, a similar two generator, 4 relator presentation is given. However this presentation was obtained indirectly by first obtaining a particular presentation of the group $\mathrm{SL}(2, \mathbf{Z}^{(2)})$, where $\mathbf{Z}^{(2)} = \{x/2^t : x, t \in \mathbf{Z}\}$, and then by employing an homomorphism onto $\mathrm{SL}(2, p)$. The authors of [1] state that it would be desirable to have a direct demonstration of their presentation. The presentation stated above was acquired directly. (Any reader interested in the proof may contact the author.)

3. Some definitions concerning circuits of a map M

For this section, we suppose that $\mathbf{M}$ is a map without loops (edges whose vertices coincide), and given any two vertices there is at most one edge between them (i.e., there are no multiple edges). G will be assumed to be finite. Also forthwith we shall not distinguish a map from its corresponding imbedding.

A path in $\mathbf{M}$ is a finite sequence of vertices such that every pair of consecutive vertices is joined by an edge. The length of a path is the number of vertices in the sequence minus one. The distance $d(v, v')$ between two vertices is the minimal length of the paths linking them. The diameter of $\mathbf{M}$ is the maximum distance found in $\mathbf{M}$.

A circuit in $\mathbf{M}$ is a cycle of at least two vertices such that every pair of consecutive vertices of the cycle is joined by an edge and that each vertex appears in the cycle at most once. For all positive integers n, an n-circuit is a circuit with n vertices in its cycle. (In the case of $n = 2$, the cycle involves taking the joining edge twice.)

A circuit C_0 in $\mathbf{M}$ and a path linking two vertices of C_0 naturally determine two circuits, C_1 and C_2 say. Then we say that any one circuit from C_0, C_1, C_2 is simply derivable from the other two. Whether a circuit is derivable from a given set E of circuits $\{E_1, \ldots, E_n\}$, $n \geq 2$, is determined by the following inductive definition:

- if $n = 2$, then C is derivable from E iff C is simply derivable from E_1 and E_2,
- if $n > 2$, then C is derivable from E iff there exists $E_i, E_j \in \mathsf{E}$ s.t. $\exists$ circuit F (simply) derivable from E_i and E_j, and C is derivable from the set $\mathsf{E} \cup \{F\} \setminus \{E_i, E_j\}$.

Let v_1, v_2, v_3 be successive vertices of a path, with e_1 joining v_1 to v_2 and e_2 joining v_2 to v_3. Let d_1 be the dart (v_2, e_1) and d_2 the dart (v_2, e_2). Then we define the angle $\angle v_1 v_2 v_3$ to be the least natural integer k satisfying $y^k(d_1) = d_2$. If v_1 and v_3 are understood we will abbreviate $\angle v_1 v_2 v_3$ by $\angle v_2$. For a circuit $C := (v_1, \ldots, v_n)$, we call the cycle of integers $(\angle v_1, \ldots, \angle v_n)$ the cycle of angles of C.

We suppose that $\mathbf{M} := (G, |G|, x, y)$ is regular. Two circuits are called equivalent if they share the same cycle of angles. An (equivalence) class of circuits of $\mathbf{M}$ corresponds to a conjugacy class of words in the symbols x and y reducing in G to the identity.

Suppose that P is a presentation of G in the generators x and y, and that J is a subset of the relators of P. Let $C \in \mathsf{J}$ and $\mathsf{E} = \mathsf{J} \setminus \{C\}$. We suppose also that C (as a circuit of $\mathbf{M}$) is derivable from a set of circuits all elements of which are equivalent to elements of E. Then P' obtained from P by deleting the single relator C is also a presentation of G.

4. Some information about the groups $\mathbf{PSL}(2,p)$, p odd prime

$\mathrm{GL}(2,p)$ is the group of invertible 2×2 matrices with entries in the finite field $\mathrm{GF}(p)$ of order p, p odd prime. $\mathrm{SL}(2,p)$ is the set of elements of $\mathrm{GL}(2,p)$ with determinant 1. $\mathrm{PSL}(2,p)$ is the quotient of $\mathrm{SL}(2,p)$ by its centre, i.e., $\{I,-I\}$. The subgroup structure of $\mathrm{PSL}(2,p)$ is described in Chapter 12 of [3]. The order of $\mathrm{PSL}(2,p)$ is $p(p^2-1)/2$.

$G := \mathrm{PSL}(2,p)$ acts doubly transitively on the points of the projective line $\mathrm{GF}(p)\cup\{\infty\}$ by

$$\pm\begin{pmatrix} a & b\\ c & d\end{pmatrix} : v \to \frac{av+b}{cv+d}$$

The stabilizer of any point in this action is a Frobenius group F, with the complements cyclic of order $(p-1)/2$ and the kernel K cyclic of order p. The normaliser of K in G is F, the centraliser of any $y\in K\setminus\{I\}$ in G is K. Further y^r is conjugate to y in G is equivalent to r is a non-zero square in $\mathrm{GF}(p)$.

Let $g\in G$; we denote the order of g in G as $\mathrm{o}(g)$. An element of G has order 2 if and only if its trace is 0, has order 3 if and only if its trace is ±1, and has order p if and only if its trace is ±2 and is not the identity element. By Theorem 3 of [8] there is exactly one conjugacy class under $\mathrm{PGL}(2,p)$ of pairs (x,y) of elements of G satisfying $\mathrm{o}(x)=2$, $\mathrm{o}(y)=p$ and $\mathrm{o}(xy^{-1})=3$. By Theorem 4 of [8], any such pair (x,y) generates G.

Now taking $x := \pm\begin{pmatrix} 0 & -1\\ 1 & 0\end{pmatrix}$ and $y := \pm\begin{pmatrix} 1 & 1\\ 0 & 1\end{pmatrix}$, we have $xy^{-1} = \pm\begin{pmatrix} 0 & -1\\ 1 & -1\end{pmatrix}$ so we deduce that, up to isomorphism, $(G,|G|,x,y)$ is the unique regular map of valency p with the automorphism group $\mathrm{PSL}(2,p)$. We denote this map by $M(2,p,3)$.

5. The construction of the map $M(2,p,3)$

Proposition 5.1 *Let* $\mathbf{M} := (G,|G|,x,y)$ *be a regular triangular map with* $G = PSL(2,q)$ *or* $PGL(2,q)$*, these being matrix groups over* $GF(q)$*,* q *any prime power. We suppose that* $q>3$ *and the order of* y *to be* d*. Then*

(i) $y^i x \neq I$ *for every* $i\in\mathbf{Z}_d$,

(ii) $y^i x y^j x = I \Rightarrow i\equiv j\equiv 0 \mod d$,

(iii) $y^i x y^j x y^k x = I \Rightarrow i\equiv j\equiv k\equiv \pm1 \mod d$.

(The geometric interpretation of these results is $\mathbf{M}$ *does not possess loops or multiple edges, and does not contain 3-circuits except those forming the triangular faces of the imbedding.)*

Proof. In general, the proof may be found in [4, p. 183-191]. For the sole case which concerns us, i.e., $\mathbf{M} = M(2,p,3)$, the results are easily checked by setting $x = \pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $y = \pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. □

Let $\mathbf{M} := (G, |G|, x, y)$ be any regular map. Then the correspondence $\alpha : g \to gy$ for all g in G is an automorphism of $\mathbf{M}$ and α fixes the vertex v if and only if for some $i \in \mathbf{Z}$,

$$\alpha(g) = y^i g, \quad \forall\, g \in v.$$

Thus the fixed vertices of α are determined from the solutions for g in $gy = y^i g$ as i varies. Let N be the number of fixed vertices of α, M the number of powers of y conjugate to y, and d the order of y. Then we have:

$$N = \big(M.|C_G(y)|\big)/d$$

where $C_G(y)$ is the centraliser in G of y. Applying the above to $M(2,p,3)$ we have $d = p$, $M = (p-1)/2$ and $|C_G(y)| = p$. (Refer to section 4 for these facts.) Hence

Proposition 5.2 *For p odd, the automorphism $\alpha : g \to gy$ of $M(2,p,3)$ fixes exactly $(p-1)/2$ vertices.*

Definitions. Let V be the set of vertices of a graph Γ and $V' \subset V$. Then the induced subgraph on V' is the graph with V' as its set of vertices, and there is an edge between $u', v' \in V'(u' \neq v')$ iff u' and v' have an edge between them as vertices in Γ.

The span $S(v)$ of a vertex v of Γ is the induced subgraph on the vertices adjacent to v in Γ; the web $W(v)$ is the induced subgraph on v and its adjacent vertices.

Lemma 5.3 *The webs of the fixed vertices under $\alpha : g \to gy$ are mutually disjoint for any $M(2,p,3)$, p prime > 3.*

Proof. Let $v_1 \neq v_2$ be two fixed vertices under α. We suppose that the webs of v_1 and v_2 intersect non-trivially; then $S(v_1) \cap S(v_2)$ contains at least a vertex. By applying α repeatedly we see that the vertices of $S(v_1)$ are the same as the vertices of $S(v_2)$. Further, if $S(v_1) \cap S(v_2)$ contains an edge, then $S(v_1) = S(v_2)$ and $M(2,p,3)$ is of valency 4 contravening p prime. Suppose now that $S(v_1) \cap S(v_2)$ only contains vertices. Necessarily there are vertices a, b such that (v_1, a, b) is a 3-circuit. Then (v_2, a, b) is also a 3-circuit; thus the edge (a, b) is in both $S(v_1)$ and $S(v_2)$, a contradiction. □

Corollary 5.4 *Each vertex of $M(2,p,3)$ is contained in the web of a unique fixed point of α.*

Proof. Each web contains $(p+1)$ vertices, and there are $(p-1)/2$ vertices fixed by α. By lemma 5.3, there are exactly $(p^2-1)/2$ vertices contained in some web of the fixed points of α, accounting for all vertices of $M(2,p,3)$. □

Now let b be any vertex of $M(2,p,3)$ not fixed by α. Then $b \in S(u)$ for some fixed vertex u of α. For any $r \in \mathrm{GF}(p) \setminus \{0, \pm 1\}$, let c be the vertex such that $\angle ubc$ is r. Then c is in the span of a fixed point v of α where $v \neq u$. Hence we have the path (u,b,c,v) in $M(2,p,3)$, as we have the path $(u,\alpha(b),\alpha(c),v)$. These combined form a 6-circuit $(u,b,c,v,\alpha(c),\alpha(b))$ with cycle of angles being $(1,r,s,t,-s,-r)$. (The "first" angle may be assumed to be 1 because instead of α one might as well have employed any power of α.) The unknowns s and t are easily determined as r^{-1} and $-r^2$ respectively, by simple matrix algebra using $x = \pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $y = \pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Corollary 5.5 *For all primes $p > 3$, and $r \in GF(p) \setminus \{0, \pm 1\}$, the following relation in $PSL(2,p)$ with generators x and y:*

$$y^{-1}xy^{-r}xy^{-r^{-1}}xy^{r^2}xy^{r^{-1}}xy^{r}x = I$$

holds and is a 6-circuit of $M(2,p,3)$.

Definition. Let v_1 and v_2 be fixed vertices of α. Let d and e be darts of v_1 and v_2 respectively. Suppose that $\alpha(d) = y^i d$ and $\alpha(e) = y^j e$. Then, for any $k \in \mathrm{GF}(p) \setminus \{0\}$, we say that v_2 spins kj as v_1 spins ki.

Using the same notation in the argument for Corollary 5.5, if $\angle ubc$ is r, then as u spins once, v spins r^2. Hence, as r is varied over $\{2,\ldots,p-2\}$, we see that u is linked with $(p-3)/2$ other vertices fixed by α; this accounts for all fixed points of α by Proposition 5.2. If (u,b,c) and (u,b,c') with $c' \neq c$ both are in $S(v)$, then $\angle ubc' = -r$.

Corollary 5.6 *Consider $M(2,p,3)$ for any prime $p \geq 3$. Every vertex not fixed by α belongs to the span of a unique fixed vertex of α, and has exactly two adjacent vertices in the span of any other fixed vertex of α.*

Corollary 5.7 *The diameter of the underlying graph of $M(2,p,3)$ for all primes $p > 3$ is three.*

Proof. Consider three cases: (i) $v_1 \neq v_2$ are both fixed vertices of α, (ii) v_1 is a fixed vertex, v_2 is not, (iii) neither v_1 nor v_2 are fixed by α. Trivial applications of Corollary 5.6 yield $d(v_1,v_2) = 3$ in case (i) and $d(v_1,v_2) \leq 3$ in case (iii). In case (ii) it is clear that $d(v_1,v_2) \leq 4$, but applying a suitable power of α ensures that a path between v_1 and v_2 of length two (or one) exists. □

Note. $M(2,3,3)$ is the tetrahedron and $M(2,2,3)$ has an underlying graph of three vertices for which each pair is connected by an edge, so both have diameter 1.

We are now in a position to prove Proposition 1.1:

Theorem 5.8 *The map $M(2,p,3)$ for any prime $p > 3$ is an extreme-vertex fixing map of order 3.*

Proof. Let v be a vertex of $M(2,p,3)$. By regularity, we may suppose that v is fixed by α. Then by Proposition 5.2, there is a non-identity automorphism that fixes a set S of vertices including v where $|S| =$ (p-1)/2. By cases (i) and (ii) in the proof of Corollary 5.7, S forms a maximal set such that the distance between any two elements is three. Furthermore, by case (ii) , it is also clear that S is the unique maximal set containing v. □

Theorem 5.9 *For any prime p, there is a presentation of $PSL(2,p)$ in x and y such that all the relators when considered as circuits of $M(2,p,3)$ have length strictly less than seven.*

Proof. The theorem clearly holds for $p = 2$ or 3, so we may suppose that $p > 3$. As the diameter of $M(2,p,3)$ is three, any circuit of length ≥ 8 is derivable from circuits of length ≤ 7. It remains only to show that any 7-circuit $(v_1,\ldots,v_7)$ in $M(2,p,3)$ is derivable from circuits of length ≤ 6. If either $d(v_1,v_4)$ or $d(v_1,v_5)$ is less than three then the 7-circuit is derivable from two circuits of length ≤ 6. From the regularity of $M(2,p,3)$, we may assume that v_1 is a fixed point of α. If $d(v_1,v_4) = d(v_1,v_5) = 3$ then the adjacent vertices v_4 and v_5 are fixed vertices of α implying $d(v_4,v_5) = 3$, that is a contradiction. □

By Proposition 5.1, the 2-circuits are adjacent vertices with a unique edge connecting them, and the 3-circuits represent the triangular faces of $M(2,3,p)$. We tabulate below the 4-circuits and 5-circuits, and those 6-circuits which possess vertices v, v' satisfying $d(v,v') = 3$. (All other 6-circuits are obviously derivable from circuits of smaller length and so do not have to be considered). The results are easily obtained either by using the structure of $M(2,3,p)$ determined above or by using matrix multiplication with x and y.

	Cycle of angles	$\forall r,s \in$ GF(p) excepting:
4-circuits	$(r, 2r^{-1}, r, 2r^{-1})$	$r \neq 0$
5-circuits: Type 1	$(s, s^{-1}(1-r), r^{-1}(1-s), r, r^{-1}s^{-1}(r+s-1))$	$r, s \neq 0, 1; r+s \neq 1$
Type 2	$(s, s^{-1}(1+r), r^{-1}(1+s), r, r^{-1}s^{-1}(r+s+1))$	$r, s \neq 0, -1; r+s \neq -1$
6-circuits: Type 1	$(r, r^{-1}, -sr^2, -r^{-1}, -r, s)$	$r \neq 0, \pm 1; s \neq 0$
Type 2	$(r, r^{-1}, -sr^2, r^{-1}, r, s+2r^{-1})$	$r \neq 0, \pm 1; s \neq 0$

A process of “eliminating” circuits can be performed by identifying them as derivable from the “remaining” circuits such that the presentation stated in section 2 may be obtained.

References

[1] H. Behr and J. Mennicke, *A presentation of the groups $PSL(2,q)$*, Canad. J. Math. **20** (1968), 1432–1438.

[2] H.S.M Coxeter and W.O.J. Moser, *Generators and relations for discrete groups*, 4th ed., Springer-Verlag, New York, 1980.

[3] L.E. Dickson, *Linear groups with an exposition of the Galois theory*, Dover, New York, 1984.

[4] M.L.N. Downs, *Möbius inversion of some classical groups and their application to the enumeration of regular hypermaps*, Ph.d. dissertation, Southampton, 1988.

[5] M.L.N. Downs, *Möbius function of $PSL(2,q)$, with application to the maximal normal subgroups of the modular group*, J. London Math. Soc. **43** (1991), no. 2, 61–75.

[6] P. Hall, *The Eulerian functions of a group*, Quart. J. Math. (Oxford) **7** (1936), 134–151.

[7] G.A. Jones and D. Singerman, *Theory on maps on orientable surfaces*, Proc. London Math. Soc. **37** (1978), no. 3, 273–307.

[8] A.M. Macbeath, *Generators of the linear fractional groups*, Proc. Sympos. Pure Math. XII, (Amer. Math. Soc., Providence, R.I., 1967), pp. 273–307.

[9] S. Wilson, *Families of regular graphs in regular maps*, J. Comb. Theory, Series B 85 (2002), 269–289.

◇ Martin Downs
25 N. Kalapodi Street,
Rio 26504,
Patras, Greece
`mamona@upatras.gr`