Bull. Aust. Math. Soc. **89** (2014), 159–165
doi:10.1017/S000497271300049X

PRIMITIVE PERMUTATION GROUPS CONTAINING A CYCLE

GARETH A. JONES

(Received 11 December 2012; accepted 3 March 2013; first published online 18 July 2013)

Abstract

The primitive finite permutation groups containing a cycle are classified. Of these, only the alternating and symmetric groups contain a cycle fixing at least three points. This removes a primality condition from a classical theorem of Jordan. Some applications to monodromy groups are given, and the contributions of Jordan and Marggraff to this topic are briefly discussed.

2010 *Mathematics subject classification*: primary 20B15; secondary 01A55, 20-03, 20B20.
Keywords and phrases: primitive group, cycle, fixed points, alternating group.

1. Introduction

There is a long tradition, going back to Jordan, of proving that a primitive permutation group of degree n, containing an element with a specific cycle structure, must contain A_n. The following theorem of Jordan (see [10, Theorem 3.3E] or [25, Theorem 13.9]) is typical.

THEOREM 1.1. *Let G be a primitive permutation group of finite degree n, containing a cycle of prime length fixing at least three points. Then $G \geq A_n$.*

This result has frequently been used to show that certain permutations generate the alternating or symmetric group: see, for instance, Conder's proof in [8] that alternating groups of degree $n > 167$ are all Hurwitz groups. The following extension of Theorem 1.1, removing the primality condition, is a response to a question raised by Alexander Zvonkin in connection with his work with Fedor Pakovich on polynomials and weighted plane trees, motivated by the Galois theory of pairs of polynomials with a given factorisation pattern and with a minimal degree of their difference. The proof is a surprisingly simple application of the classification of finite simple groups.

THEOREM 1.2. *Let G be a primitive permutation group of finite degree n, not containing the alternating group A_n. Suppose that G contains a cycle fixing k points, where $0 \leq k \leq n-2$. Then one of the following holds:*

(1) $k = 0$ *and either:*
  (a) $C_p \le G \le AGL_1(p)$ *with* $n = p$ *prime; or*
  (b) $\mathrm{PGL}_d(q) \le G \le P\Gamma L_d(q)$ *with* $n = (q^d - 1)/(q - 1)$ *and* $d \ge 2$ *for some prime power* q*; or*
  (c) $G = L_2(11)$, M_{11} *or* M_{23} *with* $n = 11, 11$ *or* 23 *respectively.*

(2) $k = 1$ *and either:*
  (a) $\mathrm{AGL}_d(q) \le G \le A\Gamma L_d(q)$ *with* $n = q^d$ *and* $d \ge 1$ *for some prime power* q*; or*
  (b) $G = L_2(p)$ *or* $PGL_2(p)$ *with* $n = p + 1$ *for some prime* $p \ge 5$*; or*
  (c) $G = M_{11}$, M_{12} *or* M_{24} *with* $n = 12, 12$ *or* 24 *respectively.*

(3) $k = 2$ *and* $\mathrm{PGL}_2(q) \le G \le P\Gamma L_2(q)$ *with* $n = q + 1$ *for some prime power* q.

Corollary 1.3. *Let G be a primitive permutation group of finite degree n, containing a cycle with k fixed points. Then $G \ge A_n$ if $k \ge 3$, or if $k = 0, 1$ or 2 and n avoids the values listed in parts (1), (2) or (3) of Theorem 1.2.*

Remark 1.4. If a permutation g has a cycle of length coprime to all its other cycle lengths, then some power of g is a cycle of the same length, so these results can be applied to it.

Remark 1.5. It is straightforward to check that the groups G listed in Theorem 1.2 all have elements with the appropriate cycle structures. Moreover, they are all primitive. In fact, apart from proper subgroups of $AGL_1(p)$ in (1)(a), they are all doubly transitive.

Remark 1.6. In general, one cannot remove the hypothesis that G is primitive. For instance, if m is a proper divisor of n then the imprimitive group $S_m \wr S_{n/m}$ of degree n contains a cycle g with k fixed points for $k = m, 2m, \ldots, n - 2m$ (permuting the blocks nontrivially), and for $n - m \le k \le n - 2$ (leaving each block invariant). However, if k is coprime to n and less than $n/2$, then any transitive group containing g is primitive, so these results apply.

Remark 1.7. A similar result to Theorem 1.2, restricted to the case where n is prime and $k > 0$, has been obtained by Bouw and Osserman [3, Proposition 3.1], who apply it to covers of curves in positive characteristic. (Their proof can be simplified by using the fact that the transitive groups of prime degree n are known: apart from S_n and A_n, they are the groups G in parts (1)(a) or (1)(c) of Theorem 1.2, together with those in (1)(b) for which n is prime.)

Remark 1.8. As in the preceding comment, some of the motivation for results of this type comes from covering space theory. The monodromy group of a covering is the group of permutations of the sheets obtained by lifting closed paths. It is primitive if and only if the covering is not a composition of coverings of smaller degrees. Local branching information provides cycle structures for certain elements of this group, so it is useful to know which primitive groups contain elements with given cycle structures. An application of Theorem 1.2 is given in Section 3.

Remark 1.9. There is a similar situation in Galois theory: the Galois group G of a polynomial $f(t) \in \mathbb{Z}[t]$ acts transitively on the roots if and only if $f(t)$ is irreducible,

https://doi.org/10.1017/S000497271300049X Published online by Cambridge University Press

and it acts primitively if and only if $f(t)$ does not divide a composition $g(h(t))$ of polynomials of smaller degrees, with $g(t)$ irreducible. If p is a prime not dividing the discriminant of $f(t)$, then the degrees of the irreducible factors of the reduction modulo (p) of $f(t)$ give the cycle structure of an element of G. This information can help in identifying G.

Remark 1.10. There is an infinite analogue of Corollary 1.3: [10, Theorem 3.3D] shows that a primitive group on an infinite set, containing a cycle of finite length (or indeed any permutation with nonempty finite support), contains the alternating group, consisting of all the even permutations with finite support.

Remark 1.11. Finally, it should be emphasised that the proof of Theorem 1.2 relies heavily on the classification of finite simple groups—in particular, on the resulting classification of doubly transitive groups. It seems hopeless to expect proofs of results such as this using only the methods available to Jordan and his contemporaries.

2. Proof of Theorem 1.2

The case $k = 0$ has been dealt with by the author in [12], completing work of Feit [11], while the case $k = 1$ has been dealt with by Müller in [19, Theorem 6.2] (see also Theorem 3.2 of [20, 21], and [4]). Both results can be deduced from the classification of doubly transitive groups, stated in [6, 10] for instance. Thus we may assume that $k \geq 2$.

A theorem of Jordan, often attributed to Marggraff (see Section 3) shows that G, being primitive and containing a cycle with k fixed points, is $(k + 1)$-transitive; since $k \geq 2$, G is at least 3-transitive. As a result of the classification of finite simple groups, the multiply transitive finite permutation groups are known. In particular, the 3-transitive groups $G \not\geq A_n$ are as follows:

(1) various groups G such that $L_2(q) \leq G \leq P\Gamma L_2(q)$, with $n = q + 1$ for some prime power q;
(2) various subgroups $G \leq AGL_d(2)$ with $n = 2^d$ and $d \geq 3$;
(3) M_{11} with $n = 11$ or 12, M_{12} with $n = 12$, M_{22} and Aut M_{22} with $n = 22$, M_{23} with $n = 23$, M_{24} with $n = 24$.

All these groups appear in their natural representations, apart from M_{11} acting on the $n = 12$ cosets of a subgroup $L_2(11)$. Of these groups, only M_{11}, M_{12}, M_{23} and M_{24} in their natural representations are 4-transitive, only M_{12} and M_{24} are 5-transitive, and none are 6-transitive. Thus $2 \leq k \leq 4$.

The groups in (3) can be eliminated since inspection of the groups or of their character tables in [9] shows that they do not contain $(n - k)$-cycles for such values of k. The groups G in (1) and (2) are only 3-transitive, so $k = 2$.

If $G \leq AGL_d(2)$ as in (2), the subgroup G_0 fixing 0 contains a cycle g of length $n - 2$, so $h := g^{(n-2)/2}$ is an involution in $GL_d(2)$ fixing just two points. Thus $(h - 1)^2 = 0$ and $\dim \ker(h - 1) = 1$, so $d \leq 2$, contradicting (2).

https://doi.org/10.1017/S000497271300049X Published online by Cambridge University Press

Finally, let $G \leq P\Gamma L_2(q)$ as in (1). We can take the $(q-1)$-cycle to fix 0 and ∞. Their stabiliser in $P\Gamma L_2(q)$ consists of the semilinear transformations $g : t \mapsto at^\gamma$, where $a \in \mathbb{F}_q^*$ and $\gamma \in \mathrm{Gal}\,\mathbb{F}_q$. This has a normal subgroup $N = \{g \mid \gamma = 1\} \cong \mathbb{F}_q^* \cong C_{q-1}$, complemented by a subgroup $\{g \mid a = 1\} \cong \mathrm{Gal}\,\mathbb{F}_q \cong C_e$, where $q = p^e$ with p prime. Replacing g with a suitable power of the same order, we may assume that $\gamma : t \mapsto t^{p^f}$ for some f dividing e, so γ has order $d := e/f$. Then

$$g^d : t \mapsto a^{1+p^f+p^{2f}+\cdots+p^{(d-1)f}} t$$

is an element of N, and if this has order m then g has order dm. Now $1 + p^f + p^{2f} + \cdots + p^{(d-1)f}$ divides $p^e - 1 = q - 1$, so m divides

$$\frac{q-1}{1 + p^f + p^{2f} + \cdots + p^{(d-1)f}}.$$

Clearly $1 + p^f + p^{2f} + \cdots + p^{(d-1)f} \geq d$, so $dm \leq q - 1$, with equality only if $d = 1$, that is, $g \in N$. It follows that the only $(q-1)$-cycles $g \in P\Gamma L_2(q)$ are those in $PGL_2(q)$; since they satisfy $\langle L_2(q), g\rangle = PGL_2(q)$, the only groups G containing $(q-1)$-cycles are those containing $PGL_2(q)$.

3. Application to monodromy groups

Let X be a projective algebraic curve over $\mathbb{C}$ (equivalently a compact Riemann surface), and $f : X \to \mathbb{P}^1(\mathbb{C})$ a rational function of degree n which is indecomposable as a composition, so that its monodromy group G is a primitive subgroup of S_n (see Remark 1.8 in Section 1). Suppose that f has k simple poles, and one of multiplicity $m = n - k$. Then the corresponding monodromy element $g_\infty \in G$, induced by analytic continuation around ∞, is a single cycle of length m, with k fixed points, so Theorem 1.2 applies to G. In particular, if $G \not\geq A_n$ then $k \leq 2$ and G is one of the groups listed there.

For each of these listed groups G, and for each integer $r \geq 3$, one can extend g_∞ to a set of r generators for G with product (in some order) equal to 1. It is sufficient to prove this when $r = 3$: the maximal subgroups of each G are known, and those containing g_∞ do not cover G; one can therefore choose any g_1 not in their union and define $g_0 = (g_1 g_\infty)^{-1}$, so that $G = \langle g_0, g_1, g_\infty\rangle$ with $g_0 g_1 g_\infty = 1$. The Riemann existence theorem then implies that for any r-element subset $R \subset \mathbb{P}^1(\mathbb{C})$ there is a covering $f : X \to \mathbb{P}^1(\mathbb{C})$ by some curve X, ramified over R, with the chosen generators as the local monodromy permutations.

If $r = 3$ then by applying a Möbius transformation one can assume that $R = \{0, 1, \infty\}$, with g_0, g_1 and g_∞ the monodromy permutations at these points. In this case, Belyĭ's theorem [2] implies that X and f are defined over an algebraic number field, though in practice it is rarely possible to find explicit equations for them.

Example 3.1. Let $k = 0$, $n = p$ and $G \leq AGL_1(p)$ as in part (1)(a) of Theorem 1.2, where p is an odd prime. Then G is a semidirect product of C_p by C_q for some divisor q

https://doi.org/10.1017/S000497271300049X Published online by Cambridge University Press

of $p-1$. If $q>1$ then in order to generate G we must take g_1 and hence also g_0 to have order q, so they each have one fixed point and $(p-1)/q$ cycles of length q. Thus 0 and 1 are each covered by one simple point in X and $(p-1)/q$ points of multiplicity q. The total order of branching of f is therefore

$$B = 2\frac{(p-1)}{q}(q-1) + (p-1) = \frac{(p-1)(3q-2)}{q},$$

so the Riemann–Hurwitz formula implies that X has genus

$$1 - p + \frac{B}{2} = \frac{(p-1)(q-2)}{2q}.$$

For instance, if $q=2$ then $X=\mathbb{P}^1(\mathbb{C})$ and $f=(1+T_p)/2$, where T_p is the Chebyshev polynomial $z\mapsto\cos(p\cos^{-1}z)$ of degree p, while G is the dihedral group of order $2p$.

Example 3.2. Let $k=1$, $n=24$ and $G=M_{24}$, as in part (2)(c) of Theorem 1.2. The maximal subgroups of M_{24} have been determined by Choi [7], and they are also given in [9]. The only maximal subgroups containing elements g_∞ of order $m=23$ are isomorphic to M_{23} or $L_2(23)$; these have no elements of order 10, so if we take $g_1\in G$ to be any element of order 10 then $G=\langle g_1, g_\infty\rangle$, as required. Since g_1 has cycle structure $2^2\,10^2$, the resulting function f takes the value 1 at four points in X, with multiplicities 2, 2, 10 and 10. The Frobenius triple-counting formula [24, Theorem 7.2.1] shows that one can choose g_1 and g_∞ as above so that g_0 is any nonidentity element of G, allowing various different ramification patterns for f over 0. For instance, an involution $g_0\in G$ is a product of eight or twelve transpositions as it is in the conjugacy class $2A$ or $2B$ respectively, so f has either eight double and eight simple zeros, or twelve double zeros; the Riemann–Hurwitz formula then shows that X has genus 2 or 4, respectively.

4. Jordan and Marggraff

Following Burnside [5, Section 159] and Wielandt [25, Theorem 13.8], the result that a primitive permutation group containing a cycle with k fixed points must be $(k+1)$-transitive has often been attributed to Marggraff (or Marggraf or Marggraaf). Both authors state the result without proof, referring to his dissertation [17]. Dixon and Mortimer [10, Exercise 7.4.11] set it as an exercise, without attribution or solution, though in a later hint they refer to a proof by Levingston and Taylor [16]. In his scholarly review of that paper, Neumann [22] points out that an earlier paper by Atkinson [1] contains a similar proof due to Alan Williamson.

In fact Neumann, clearly one of the few who have read Marggraff's dissertation or his subsequent paper [18], argues in [22] and in more detail in [23] that this theorem should really be attributed to Jordan. Here is Jordan's Théorème I from page 384 of [13] (see also [15, page 314]), with the incorrect '$n-p-2q+3$ *fois primitif*' in his first sentence amended to '$n-p-2q+3$ *fois transitif*', the phrase he surely intended. (See [23, page 272] for Neumann's comments on this, including an English translation of Théorème I using modern terminology.)

https://doi.org/10.1017/S000497271300049X Published online by Cambridge University Press

Si un groupe G, primitif et de degré n, contient un groupe Γ *dont les substitutions ne déplacent que p lettres et les permutent transitivement (p étant un entier quelconque), il sera au moins* $n - p - 2q + 3$ *fois transitif, q étant le plus grand diviseur de p tel que l'on puisse répartir les lettres de* Γ *de deux manières différentes en systèmes de q lettres jouissant de la propriété que chaque substitution de* Γ *remplace les lettres de chaque système par celles d'un même système.*

Si aucun des diviseurs de p ne jouit de cette propriété (ce qui arrivera notamment si Γ *est primitif, ou formé des puissances d'une seule substitution circulaire), G sera* $n - p + 1$ *fois transitif.*

Note in particular the last sentence, which includes the case where Γ is generated by a cycle. Neumann also finds no clear justification for the date of 1892 assigned by Burnside and Wielandt to Marggraff's dissertation, arguing that the rather sketchy evidence available suggests that it was probably written in 1889 or 1890. Again, see [23] for more on Marggraff's work and its relationship with that of Jordan.

Concerning Jordan's Theorem 1.1, although Wielandt [25, Theorem 13.9] refers to [14], it is not explicitly stated there. However, it follows easily from [13, Théorème I], stated above, together with [14, Théorème I]:

Soit p un nombre premier impair. Un groupe de degré $p + k$ *ne pourra être plus de k fois transitif, si* $k > 2$*, à moins de contenir le groupe alterné.*

Acknowledgements

The author thanks Alexander Zvonkin for raising the issue discussed here, the organisers of the conference Groups and Riemann Surfaces, Madrid, September 2012, where this conversation took place, and Peter Müller and Peter Neumann for some very helpful mathematical, stylistic and historical comments on early drafts of this paper.

References

[1] M. D. Atkinson, 'Doubly transitive but not doubly primitive permutation groups II', *J. Lond. Math. Soc.* (2) **10** (1975), 53–60.
[2] G. V. Belyĭ, 'On Galois extensions of a maximal cyclotomic field', *Izv. Akad. Nauk SSSR Ser. Mat.* **43** (1979), 267–276, 479.
[3] I. I. Bouw and B. Osserman, 'Some 4-point Hurwitz numbers in positive characteristic', *Trans. Amer. Math. Soc.* **363** (2011), 6685–6711.
[4] D. Bubboloni and C. E. Praeger, 'Normal coverings of finite symmetric and alternating groups', *J. Combin. Theory Ser. A* **118** (2011), 2000–2024.
[5] W. Burnside, *Theory of Groups of Finite Order*, 2nd edn. (Cambridge University Press, Cambridge, 1911), reprinted (Dover, New York, 1955).
[6] P. J. Cameron, 'Permutation groups and finite simple groups', *Bull. Lond. Math. Soc.* **13** (1981), 1–22.
[7] C. Choi, 'On subgroups of M_{24}. II: The maximal subgroups of M_{24}', *Trans. Amer. Math. Soc.* **167** (1972), 29–47.
[8] M. D. E. Conder, 'Generators for alternating and symmetric groups', *J. Lond. Math. Soc.* (2) **22** (1980), 75–86.

[9] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups* (Clarendon Press, Oxford, 1985).
[10] J. D. Dixon and B. Mortimer, *Permutation Groups* (Springer, New York, 1996).
[11] W. Feit, 'On symmetric balanced incomplete block designs with doubly transitive automorphism groups', *J. Combin. Theory Ser. A* **14** (1973), 221–247.
[12] G. A. Jones, 'Cyclic regular subgroups of primitive permutation groups', *J. Group Theory* **5** (2002), 403–407.
[13] C. Jordan, 'Théorèmes sur les groupes primitifs', *J. Math. Pures Appl.* (2) **16** (1871), 383–408.
[14] C. Jordan, 'Sur la limite de transitivité des groupes non alternés', *Bull. Soc. Math. France* **1** (1873), 40–71.
[15] C. Jordan, *Oeuvres de Camille Jordan, Tome I* (Gauthiers-Villars, Paris, 1961).
[16] R. Levingston and D. E. Taylor, 'The theorem of Marggraff on primitive permutation groups which contain a cycle', *Bull. Aust. Math. Soc.* **15** (1976), 125–128.
[17] B. Marggraff, *Über primitive Gruppen mit transitiven Untergruppen geringeren Grades*, Inaugural Dissertation, Univ. Giessen, c. 1890.
[18] B. Marggraff, 'Primitive Gruppen, welche eine transitive Gruppe geringeren Grades enthalten', *Wissenschaftliche Beilage zum Jahresberichte des Sophien-Gymnasiums zu Berlin*, 1895.
[19] P. Müller, 'Reducibility behavior of polynomials with varying coefficients', *Israel J. Math.* **94** (1996), 59–91.
[20] P. Müller, Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Siegel functions, arXiv:math/01110060 (2001).
[21] P. Müller, 'Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials', *Ann. Sci. Norm. Super. Pisa Cl. Sci.*, to appear, doi:10.2422/2036-2145.201012_002.
[22] P. M. Neumann, Review of [16], *Math. Rev.* **54**, 12870.
[23] P. M. Neumann, 'Some primitive permutation groups', *Proc. Lond. Math. Soc* (3) **50** (1985), 265–281.
[24] J.-P. Serre, *Topics in Galois Theory* (Jones and Bartlett, Boston, 1992).
[25] H. Wielandt, *Finite Permutation Groups* (Academic Press, New York, 1964).

GARETH A. JONES, School of Mathematics,
University of Southampton, Southampton SO17 1BJ, UK
e-mail: G.A.Jones@maths.soton.ac.uk