J. Aust. Math. Soc. **77** (2004), 297–304

FIXED POINT FREE ACTIONS OF GROUPS OF EXPONENT 5

ENRICO JABARA

(Received 8 April 2002; revised 11 April 2003)

Communicated by R. B. Howlett

Abstract

In this paper we prove that if V is a vector space over a field of positive characteristic $p \neq 5$ then any regular subgroup A of exponent 5 of $GL(V)$ is cyclic. As a consequence a conjecture of Gupta and Mazurov is proved to be true.

2000 *Mathematics subject classification*: primary 20E25, 20F50.

1. Introduction

A group G is called *periodic* if any element of G has finite order and *of finite exponent* e if, for any $g \in G$, we have $g^e = 1$. Obviously any group of finite exponent is periodic, but the contrary is not true in general. We also recall that a group G is called *locally finite* if each finite subset of G is contained in a finite subgroup of G.

A well-known conjecture of Burnside says that a finitely generated group of finite exponent e is necessarily finite (or, equivalently, that any group of finite exponent is locally finite).

This conjecture has been proved only for $e = 2$ (in this case the group is abelian), for $e = 3$ (Levi and van der Waerden [4], see also [8, 14.2.2]), for $e = 4$ (Sanov [9], see also [8, 14.2.3]) and for $e = 6$ (Hall [3]), while nothing is known for the case $e = 5$. In some classes of groups Burnside's conjecture is true; for example, Burnside proved that if F is a field of characteristic 0, then any subgroup of finite exponent of $GL(n, F)$ is finite. However Burnside's conjecture is not true in general, as Novikov and Adjan proved in a series of papers of great length. Successively Adjan constructed infinite groups of exponent e with a finite numbers of generators for any odd exponent $e \geq 665$ (see [1]).

It is therefore quite natural to ask if, given a natural number e and a vector space V over a field F of characteristic finite and coprime with e, there exists an infinite subgroup A of $GL(V)$ of exponent e that is regular (that is, with the property that $\alpha(v) \neq v$ for any $v \neq 0$ and any $\alpha \in A$, $\alpha \neq 1$). If e is a prime number, it can be conjectured that A is necessarily cyclic. This conjecture is certainly true if the dimension of V over F is finite (this fact was proved by Burnside; see [8, 10.5.6]).

In this paper, we consider the case $e = 5$ and prove

THEOREM 1.1. *If V is a vector space over a field of positive characteristic $p \neq 5$ then any regular subgroup A of exponent 5 of $GL(V)$ is cyclic.*

We observe that the action of A is regular over V if and only if any non-identity element of A has minimal polynomial that divide $x^4 + x^3 + x^2 + x + 1$. In group-theoretic terms, this means that in the semidirect product of V by A there are not elements of order $5p$.

2. Notation and preliminary results

We fix two distinct primes p and q. Let F be a field of characteristic p, V a vector space over F and A a subgroup of the automorphism group of V of exponent q and such that for any $\alpha \in A$, $\alpha \neq 1$ we have $\mathrm{Fix}_V(\alpha) = \{0\}$. It is easy to verify that for any $\alpha \in A \setminus \{1\}$ and any $v \in V$ we have

$$v + \alpha(v) + \alpha^2(v) + \cdots + \alpha^{q-1}(v) = 0. \tag{1}$$

In the ring $\mathrm{End}_F(V)$ identity (1) can be written as follows

$$1 + \alpha + \alpha^2 + \cdots + \alpha^{q-1} = 0 \tag{2}$$

for any $\alpha \in A \setminus \{1\}$.

REMARK. For any pair of elements $\alpha, \beta \in A \setminus \{1\}$ with $\langle\alpha\rangle \cap \langle\beta\rangle = \{1\}$ we have $[\alpha, \beta] \neq 1$.

If $\alpha, \beta \in A \setminus \{1\}$ with $\langle\alpha\rangle \cap \langle\beta\rangle = \{1\}$ commute, then $\alpha\beta^i$ ($i = 0, 1, \ldots, q-1$) are all non identity elements of A. If we write the fundamental relation (2) for these elements, we get $1 + \alpha\beta^i + \cdots + (\alpha\beta^i)^{q-1} = 0$ for $i = 0, 1, \ldots, q-1$. Summing term by term and using the fact $[\alpha, \beta] = 1$ we get

$$q + \alpha(1 + \beta + \cdots + \beta^{q-1}) + \cdots + \alpha^{q-1}(1 + \beta + \cdots + \beta^{q-1}) = 0$$

but, by (2), $1 + \beta + \cdots + \beta^{q-1} = 0$, and therefore $q = 0$ while $p \neq q$. This contradiction proves the statement.

The preceding remark shows that any finite subgroup of A must have order q. We observe that infinite groups in which any proper (non trivial) subgroup has order q have been constructed by Ol'šanskiĭ ([7]). Groups of this type are called *Tarski monsters*.

Before proving Theorem 1.1, we want to expose the ideas behind the proof. We suppose for a moment that $q = 3$ (and not knowing the theorem of Levi and van der Warden [4]); then we can write (2) as

$$1 + \alpha + \alpha^{-1} = 0 \quad \text{for all } \alpha \in A \setminus \{1\}. \tag{3}$$

If A is not cyclic, there exist $\alpha, \beta \in A \setminus \{1\}$ with $\langle\alpha\rangle \cap \langle\beta\rangle = \{1\}$ and from (3) we get

$$\begin{cases} 1 + \alpha + \alpha^{-1} = 0, \\ 1 + \alpha\beta + \beta^{-1}\alpha^{-1} = 0, \\ 1 + \alpha\beta^{-1} + \beta\alpha^{-1} = 0, \end{cases}$$

summing each member we obtain

$$3 + \alpha(1 + \beta + \beta^{-1}) + (1 + \beta + \beta^{-1})\alpha^{-1} = 0$$

but, from (3), $1 + \beta + \beta^{-1} = 0$. From this we get the contradiction $3 = 0$ while $p \neq 3$.

3. Proof of Theorem 1.1 ($p = 2$)

We suppose $q = 5$; to prove Theorem 1.1 we suppose that there exists a counterexample, that is, a vector space V over a field F of characteristic $p \neq 5$ and a non cyclic group A of exponent 5 acting regularly on V.

We fix the following notation: the indices in the sums will always be from 0 to 4 and considered mod 5. We shall often use the fundamental relation (2) in the form

$$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^{-1} = 0 \tag{4}$$

or in the form

$$1 + \alpha + \alpha^2 + \alpha^{-2} + \alpha^{-1} = 0. \tag{5}$$

We shall always denote by α and β two non identity elements of A with $\langle\alpha\rangle \cap \langle\beta\rangle = \{1\}$.

The proof is in various steps.

STEP 1. We have $\sum_{i,j} \beta^{i+j}\alpha\, \beta^{i+2j}\alpha\beta^{i+j} = 0$.

PROOF. If we put $i+j=r$ we obtain

$$\sum_{i,j}\beta^{i+j}\alpha\beta^{i+2j}\alpha\beta^{i+j}=\sum_r\left\{\beta^r\alpha\beta^r\left(\sum_j\beta^j\right)\alpha\beta^r\right\}$$

and we conclude because $\sum_j\beta^j=0$. □

We put $\overline{\sigma}=\sum_i\beta^i\alpha\beta^i$ and $\underline{\sigma}=\sum_i\beta^i\alpha^{-1}\beta^i$.

STEP 2. $\overline{\sigma}+\underline{\sigma}=0$.

PROOF. If $i=0,1,\dots 4$, by (4) we get

$$1+\alpha\beta^i+\alpha\beta^i\alpha\beta^i+\alpha\beta^i\alpha\beta^i\alpha\beta^i+\beta^{-i}\alpha^{-1}=0$$

summing the five preceding equalities and recalling that

$$\alpha\left(\sum_i\beta^i\right)=0\quad\text{and}\quad\left(\sum_i\beta^{-i}\right)\alpha^{-1}=0$$

we get

$$\alpha\left(\sum_i\beta^i\alpha\beta^i\right)+\alpha\left(\sum_i\beta^i\alpha\beta^i\alpha\beta^i\right)=-5 \tag{6}$$

and

$$\sum_i\beta^i\alpha\beta^i+\sum_i\beta^i\alpha\beta^i\alpha\beta^i=-5\alpha^{-1}. \tag{7}$$

The sum $\overline{\sigma}=\sum_i\beta^i\alpha\beta^i$ is invariant with respect to the substitutions $\alpha\rightsquigarrow\beta^j\alpha\beta^j$ with $j=0,1,\dots,4$. If we make these substitutions in (7) and we take a sum, we get

$$5\sum_i\beta^i\alpha\beta^i+\sum_{i,j}\beta^{i+j}\alpha\beta^{i+2j}\alpha\beta^{i+j}=-5\sum_j\beta^{-j}\alpha^{-1}\beta^{-j}.$$

By Step 1 we have $\sum_{i,j}\beta^{i+j}\alpha\beta^{i+2j}\alpha\beta^{i+j}=0$ and since $\operatorname{char}F=p\neq 5$ we obtain the relation we wanted. □

STEP 3. $\alpha\overline{\sigma}+\underline{\sigma}\alpha^{-1}=-5$.

PROOF. We observe that, since A has exponent 5, the relation (6) can be written as $\alpha\big(\sum_i\beta^i\alpha\beta^i\big)+\big(\sum_i\beta^{-i}\alpha^{-1}\beta^{-i}\big)\alpha^{-1}=-5$. □

STEP 4. $\overline{\sigma}^2+\underline{\sigma}^2=-25$.

PROOF. We have observed before that $\overline{\sigma}$ and $\underline{\sigma}$ are invariant with respect to the substitutions $\alpha \rightsquigarrow \beta^j \alpha \beta^j$ with $j = 0, 1, \ldots, 4$. So we make these substitutions in $\alpha\overline{\sigma} + \underline{\sigma}\alpha^{-1} = -5$, we sum the five equalities and we get the desired result. □

STEP 5. Theorem 1.1 is true if $p = 2$.

PROOF. Let $p = 2$. By Step 2 we have $\overline{\sigma} = \underline{\sigma}$ and, recalling Step 4 we obtain the following contradiction $0 = 2\overline{\sigma}^2 = \overline{\sigma}^2 + \underline{\sigma}^2 = -25$. □

4. Proof of Theorem 1.1 ($p = 3$)

From now on, we suppose that $p = 3$ and therefore the relations obtained in Steps 2–4 have the form:

$$\begin{cases} \overline{\sigma} + \underline{\sigma} = 0, \\ \alpha\overline{\sigma} + \underline{\sigma}\alpha^{-1} = 1, \\ \overline{\sigma}^2 + \underline{\sigma}^2 = 2. \end{cases}$$

In particular, $\overline{\sigma}^2 = \underline{\sigma}^2 = 1$.

STEP 6. We have

(a) $\alpha\overline{\sigma} = 1 + \overline{\sigma}\alpha^{-1}$;
(b) $\alpha^{-1}\overline{\sigma} = \overline{\sigma}\alpha - 1$.

PROOF. From $\overline{\sigma} = -\underline{\sigma}$ and from $\alpha\overline{\sigma} + \underline{\sigma}\alpha^{-1} = 1$ we get (a).

Multiplying $\alpha\overline{\sigma} + \underline{\sigma}\alpha^{-1} = 1$ on the left by α^{-1} and on the right by α we obtain $\alpha^{-1}\underline{\sigma} + \overline{\sigma}\alpha = 1$ that gives (b). □

STEP 7. If we put $\rho = \alpha + \alpha^{-1}$ and $\varphi = \alpha\overline{\sigma}$ we get

(a) $\rho \in GL(V)$ has order 8 and $\rho^2 = 1 - \rho$;
(b) $\varphi \in GL(V)$ has order 8 and $\varphi^2 = 1 + \varphi$;
(c) $[\rho, \varphi] = 1$.

PROOF. From the relations obtained in Step 6, we get

$$\rho\overline{\sigma} = (\alpha + \alpha^{-1})\overline{\sigma} = 1 + \overline{\sigma}\alpha^{-1} + \overline{\sigma}\alpha - 1 = \overline{\sigma}(\alpha + \alpha^{-1}) = \overline{\sigma}\rho$$

and therefore $[\rho, \overline{\sigma}] = 1$; since $[\rho, \alpha] = 1$ we also have $[\rho, \varphi] = 1$. Then

$$\rho^2 = (\alpha + \alpha^{-1})^2 = \alpha^2 + \alpha^{-2} + 2 = -1 - \alpha - \alpha^{-1} + 2 = 1 - \rho \quad \text{and}$$
$$\rho^4 = (1 - \rho)^2 = 1 - 2\rho + \rho^2 = 1 - 2\rho + 1 - \rho = -1.$$

In particular, $\rho \in GL(V)$ and $\rho^8 = 1$. Moreover,

$$\varphi^2 = \alpha\overline{\sigma}\alpha\overline{\sigma} = \alpha(1+\alpha^{-1}\overline{\sigma})\overline{\sigma} = 1+\alpha\overline{\sigma} = 1+\varphi \quad \text{and}$$
$$\varphi^4 = (1+\varphi)^2 = 1+2\varphi+\varphi^2 = 1+2\varphi+1+\varphi = -1.$$

In particular, $\varphi \in GL(V)$ and $\varphi^8 = 1$. □

STEP 8. The group $B = \langle \rho^2, \varphi^2 \rangle \leq GL(V)$ is abelian and $|B| \leq 4$.

PROOF. By Step 7, B is certainly abelian, moreover ρ^2 and φ^2 have order 4 and therefore, since $\rho^4 = -1 = \varphi^4$, $|B| \leq 8$. We prove that B has order (at most) 4 showing that $\rho^2\varphi^{-2}$, which has order 2, acts fixed points freely over V and it is therefore equal to -1.

If we put $V_0 = \mathrm{Fix}_V(\rho^2\varphi^{-2})$ we have that V_0 is a $\langle \rho, \varphi \rangle$-invariant subspace of V (because $\langle \rho, \varphi \rangle$ is abelian).

If, by contradiction, $V_0 \neq \{0\}$ and using the same symbols for the restrictions of the automorphisms to V_0, from Step 7 we get $1-\rho = \rho^2 = \varphi^2 = 1+\varphi$, that is, $\alpha\overline{\sigma} = \varphi = -\rho = -\alpha-\alpha^{-1}$. Using Step 6 (a) we get $1+\overline{\sigma}\alpha^{-1} = -\alpha-\alpha^{-1}$ and $\overline{\sigma} = -1-\alpha-\alpha^2$ and $1 = \overline{\sigma}^2 = 1+\alpha+\alpha^2+\alpha^4+2\alpha+2\alpha^2+2\alpha^3 = 1+2\alpha+2\alpha^3+\alpha^4$, that is, $\alpha^4 = \alpha+\alpha^3$ and $\alpha^2 = \alpha+\alpha^{-1} = \rho$ which gives the required contradiction: $1 = \rho^8 = (\alpha^2)^8 = \alpha$. □

STEP 9. Theorem 1.1 is true if $p = 3$.

PROOF. By Step 8 we have $|B| \leq 4$ and since $\rho^4 = -1 = \varphi^4$, this is possible only in two ways:

(I) $\rho^2 = \varphi^2$ but this gives a contradiction, because in the proof of Step 8 we have seen that $\rho^2\varphi^{-2}$ acts fixed points freely on V.

(II) $\rho^2 = -\varphi^2$ then, by Step 7, $1-\rho = -1-\varphi$ and $\varphi = 1+\rho$. Then, recalling Step 6, $1+\overline{\sigma}\alpha^{-1} = \alpha\overline{\sigma} = \varphi = 1+\rho$ and $\overline{\sigma} = \rho\alpha = 1+\alpha^2$; this implies $1 = \overline{\sigma}^2 = (1+\alpha^2)^2 = 1+2\alpha^2+\alpha^4$ and $\alpha^2 = 1$: a contradiction. □

5. Sketch of the proof of Theorem 1.1 for $p \geq 7$

We remark that if char $F = p \geq 7$, we can obtain the same result in a way similar to the one used for $p = 3$, but using arguments *ad hoc* for any prime number p.

We can always find commuting elements ρ and φ (as defined in Step 7), satisfying $\rho^2+\rho-1 = 0$ and $\varphi^2+5\varphi+2^{-1}\cdot 25 = 0$. The orders of these automorphisms are divisors of p^2-1 and depends on the prime p, as Table 1 shows, but we haven't been able to find a method of proof valid for any p.

It seems hard to prove the same conjecture for A in the case in which $q = 7$ (or greater), with the methods used in this paper.

TABLE 1.

p	3	7	11	13	17	19
$\lvert\rho\rvert$	8	16	10	28	36	18
$\lvert\varphi\rvert$	8	24	40	12	4	72

6. An application

If G is a periodic group, we denote by $\omega(G)$ the set of the orders of the elements of G. In [2] Gupta and Mazurov proved that if $\omega(G)$ is a proper subset of $\{1, 2, 3, 4, 5\}$, then either G is locally finite or there exists a normal nilpotent $5'$-subgroup N of G such that G/N is a group of exponent 5. The same authors have conjectured that if $N \neq \{1\}$ then G is locally finite. This conjecture is equivalent to

CONJECTURE ([2]). *Let A be an automorphism group of an elementary abelian $\{2, 3\}$-group G such that every non-trivial element of A fixes in G only the trivial element. If A is of exponent 5 then A is cyclic.*

The conjecture is true by Theorem 1.1; hence we have proved:

THEOREM 6.1. *If $\omega(G) \subseteq \{1, 2, 3, 4, 5\}$ and $\omega(G) \neq \{1, 5\}$ then the group G is locally finite.*

To establish Theorem 6.1, we need (in addition to the results of [2]) the following facts:

- The groups of exponent 4 are locally finite ([9]).
- If $\omega(G) = \{1, 2, 3, 4, 5\}$ then G is locally finite ([5]).
- If $\omega(G) = \{1, 2, 3, 5\}$ then $G \simeq A_5$ ([10]).

We recall that if $\omega(G) = \{1, 2\}$ then G is elementary abelian, if $\omega(G) = \{1, 3\}$ then G is nilpotent of class at most 3 ([4]), and that the groups G with $\omega(G) = \{1, 2, 3\}$ are described in [6].

References

[1] S. I. Adyan, 'Periodic groups of odd exponent', in: *Proceedings of the Second International Conference on the Theory of Groups, Australian Nat. Univ., 1973*, Lecture Notes in Math. 372 (Springer, Berlin, 1974) pp. 8–12.

[2] N. D. Gupta and V. D. Mazurov, 'On groups with small orders of elements', *Bull. Austral. Math. Soc.* **60** (1999), 197–205.

[3] M. Hall, 'Solution of the Burnside problem for exponent six', *Illinois J. Math.* **2** (1958), 764–786.

[4] F. W. Levi and B. L. van der Waerden, 'Über eine besondere Klasse von Gruppen', *Abh. Math. Sem. Univ. Hamburg* **9** (1932), 154–158.

[5] V. D. Mazurov, 'Groups of exponent 60 with prescribed orders of elements', *Algebra i Logika* **39** (2000), 329–346; English translation: *Algebra and Logic* **39** (2000), 189–198.

[6] B. H. Neumann, 'Groups whose elements have bounded orders', *J. London Math. Soc.* **12** (1937), 195–198.

[7] A. Ju. Ol'šanskiĭ, 'An infinite group with subgroups of prime order', *Izv. Akad. Nauk SSSR Ser. Mat.* **44** (1980), 309–321.

[8] D. J. S. Robinson, *A course in the theory of groups* (Springer, Berlin, 1982).

[9] I. N. Sanov, 'Solution of Burnside's problem for exponent 4', *Leningrad Univ. Ann. Math. Ser.* **10** (1940), 166–170.

[10] A. K. Zhurtov and V. D. Mazurov, 'A recognition of simple groups $L_2(2^m)$ in the class of all groups', *Sibirsk. Math. Zh.* **40** (1999), 75–78; English translation: *Siberian Math. J.* **40** (1999), 62–64.

Dipartimento di Informatica
Universitá di Ca' Foscari
Via Torino 155–30174 Venezia
Italy
e-mail: jabara@dsi.unive.it