RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

PANAGIOTIS C. SOULES

Construction of finite p-groups with prescribed group of noncentral automorphisms

Rendiconti del Seminario Matematico della Università di Padova, tome 76 (1986), p. 75-88

<http://www.numdam.org/item?id=RSMUP_1986__76__75_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 76 (1986)

Construction of Finite p-Groups with Prescribed Group of Noncentral Automorphisms.

PANAGIOTIS C. SOULES (*)

1. Introduction.

Using graphs, Heineken and Liebeck [3] have proved that there exists for every finite group K and every odd prime p a p-group G of nilpotency class 2 and exponent p^2 such that Aut $G/\mathrm{Aut}_c\, G$ is isomorphic to K. This paper is centred around the following problem: Given a finite group K, find a p-group G such that K is isomorphic to Aut $G/\mathrm{Aut}_c\, G$ and this quotient group operates regularly (instead of semiregularly as in [3]) on the elements of a suitable basis of G/G'. Other work in this direction was done by Zurek [6] who taken G such that $G^{p^2} \leqslant G' = Z(G)$ and $(G')^p = 1$, avoiding the exclusion of $p = 2$. The graphs themselves are not altered, Lawton [4] has changed the graphs using a general statement on graphs, and U. Webb [5] used graphs that are no longer directed. There is no overlap in the arguments of these papers with the present work. The aim of this work is to find out, for which groups K the original method of graphs construction can be used to find a graph with $|K|$ points, making the operation regular instead of semiregular. So one has to choose a set of generators of K, and the operation of right hand multiplication by a generator is described by an arrow. Two problems arise:

(*) Indirizzo dell'A.: Department of Mathematics, University of Athens, Athens, Greece.

(I) Is there a generating set M of K such that Aut $D_M(K) \simeq K$?

(II) Can the digraph $D(K)$ be chosen such that

$$\text{Aut } D(K) \simeq \text{Aut } G/\text{Aut}_c\, G?$$

In this direction we prove Theorem 2.2.1 using Lemma 2.1.1. By arguments of Lemma 2.1.1. it is found that the digraph $D(K)$ is suitable in the sense of (II) if $D(K)$ does not contain closed paths of length 2, 3 or 4. This leads to the modification of problem (II) to

(II*) Can the digraph $D(K)$ be chosen without closed paths of length 2, 3 or 4?

We call a group K *rigid* for shortness if it is a group with simultaneous affirmative answer for (I) and (II*).

Our first application is Lemma 3.1.1. Here we study groups generated by an element of order 5 and another element of higher order, as a consequence we find that every alternating group A_n for $n > 5$ and every symmetric group S_n for $n > 4$ has a suitable graph. Here also the question of distinguishing arrows as belonging to different « families » comes into play such that one arrow of every family begins at a given point.

Our second application is Lemma 4.1.1. Here we examine groups generated by two elements of order 5, and we obtain that the digraph constructed is suitable if there is no automorphism interchanging the two generators.

There are, however, many well known simple groups without any element of order 5, for instance all the projective special linear groups $PSL(2, p)$ with $p \equiv 2, 3 \bmod 5$. Here we use Lemma 5.1.1. and we choose generators x, y of higher orders such that x^2y is of order 2 but xy^2 is not.

From the preceeding it is now clear that noncyclic abelian groups are never rigid groups because of the closed paths of length 4 representing $x^{-1}y^{-1}xy = 1$ in the generators x, y. For high ranks the methods will not lead to substantial improvements compared with the graphs used Heineken and Liebeck. The consideration of the problems (I), (II) for this range of groups leads to structural insights about these groups and may give hints as to how to find a suitable representation of the group K for other purposes.

2. The digraph $D(K)$ of a finite group K and its associated p-group $P(D(K))$.

Given a finite group K we construct the digraph $D(K)$ relative to a specified set of generators. The construction is identical to that described in [3] excluding the auxiliary points and the only condition is that every point belong to a closed path containing at least 5 points. The points of $D(K)$ correspond to group elements of a non-cyclic group K and are adjacent to n points and adjacent from at least n different points. We will have to show that if the orders of generating elements are different and greater than 5 we can distinguish the closed paths on the digraph in many cases. An automorphism of the digraph $D(K)$ preserves closed paths and the Aut $D(K)$ is isomorphic to K. We call *n-circuit* a closed path consisting of n arrows *without considering the direction* and *n-cycle* a closed path consisting of n arrows, *uniformly directed.*

Our terminology for digraphs can be found in [2].

Let the points of $D(K)$ be $P_1, P_2, \ldots, P_n$. Relative to this ordering of points we define the associated p-group $P(D(K)) = P$ of nilpotency class 2 to be generated by canonical generators $x_1, \ldots, x_n$ subject to the conditions:

(i) $[x_a, x_b, x_c] = 1$ for all a, b, c in K;

(ii) for every $h \in K$, $|K| = n$, given that P_h is adjacent to P_{hw}, $P_{hv}, \ldots, P_{hs}$ and to no other points, then the following defining relations holds in $P(D(K))$:

$$x_n^p = [x_h, x_{hw}x_{hv} \ldots x_{hs}] \qquad w, v, \ldots, s \text{ generators of } K .$$

Evidently, given a permutation φ on $\{1, 2, \ldots, n\}$ the map $P_h \to \to P_{h\varphi} (h = 1, \ldots, n)$ is an automorphism of $D(K)$ if and only if the map $x_h \to x_{h\varphi}$ extends to an automorphism of the corresponding p-group P. We intend to establish the Theorem by proving these automorphisms generate Aut P modulo $\mathrm{Aut}_c P$. The proof is based on the following Lemma:

LEMMA 2.1.1. Let $D(K)$ be a connected digraph satisfying the following two conditions:

(i) There is no closed path of length smaller than 5,

(ii) each point of the graph is the beginning of at least two arrows.

Consider an element t of the associated p-group $P(D(K)) = P$. If there is an element u in P such that $t^p = [t, u] \neq 1$, then $t = x_h^m c$ for h in K, $m \in \mathbb{Z}^+$ and $c \in Z(P)$.

REMARK. Lemma 2.1.1 excludes cyclic groups K. For them, however, the statement is true by Lemma of [3] if their order is at least 5.

PROOF. By construction t does not belong to $Z(P)$. So t may be described as a product

$$t = x_1^{a_1} x_2^{a_2} \dots x_n^{a_n} c, \qquad 0 \leqslant a_i < p, \qquad i = 1, 2, \dots, n,$$

such that (without loss of generality) $a_1 \neq 0$. Accordingly

$$t^p = (x_1^{a_1})^p \dots (x_n^{a_n})^p = [x_1^{a_1}, y_1] \dots [x_n^{a_n}, y_n]$$

where $y_i = \prod_{P_j \text{ adjacent to } P_i} x_j$.

If we present each commutator $[x_i^{a_i}, y_i]$ as product of commutators $[x_i, x_k]$ and multiply all these expressions to obtain t^p, we find that

(1) no commutator $[x_i, x_k]$ occurs in more than one expression, making cancellation impossible,

(2) if $[x_i, x_k]$ and $[x_k, x_j]$ occur in t^p, then $[x_i, x_j]$ does not occur in t^p,

(3) there are no quadruples x_h, x_i, x_j, x_k such that all four $[x_h, x_i]$, $[x_i, x_j]$, $[x_j, x_k]$, $[x_k, x_h]$ occur in t^p.

These three statements are in fact the direct consequences of the condition that there are no paths of lenght 2, 3 or 4. By assumption we have $t^p = [t, u] \neq 1$, so u is not contained in $Z(P)$ and there is a representation

$$u = x_1^{b_1} \dots x_n^{b_n} d, \qquad 0 \leqslant b_i < p, \qquad i = 1, \dots, n$$

analogous to that of t. Since $[t, u] = [t, t^k u]$ for all k, we may assume $b_1 = 0$.

Assume now that x_r and x_s occur in y_1 (by condition (ii) there are at least two such generators). Then x_r and x_s also occur in u, that is, $b_r \neq 0 \neq b_s$.

Assume now that t is not of the form stated in the Lemma, then $a_m \neq 0$ for some m different from 1. Either m is equal to r or to s, and we obtain a contradiction to (2), or m is different from both of them and we have a contradiction to (3). This proves the Lemma. □

The above Lemma 2.1.1 holds for any number n of generators of the finite group K. The next Theorem depends on Lemma 2.1.1.

THEOREM 2.2.1. Let θ be an automorphism of the associated p-group P and $t = x_h$ for the $h \in K$ then $t\theta = x_g c$ where $t \in P$ $g \in K$ and $c \in Z(P)$.

PROOF. Let the elements x_h, $x_{hw^{-1}}$ of the group P. By Lemma 2.1.1 we have:

$$x_{hw^{-1}}\theta = x_d^m c_1 \text{ and } x_h\theta = x_g^n c_2$$

where d, $g \in K$, m, $n \in \mathbb{Z}^+$, c_1, $c_2 \in Z(P)$ and from

$$x_{hw^{-1}}^p = [x_{hw^{-1}}, x_h x_{hw^{-1}v}]$$

applying θ we have:

$$(x_{hw^{-1}}\theta)^p = [x_{hw^{-1}}\theta,\ x_h\theta x_{hw^{-1}}\theta] = [x_d^m, x_g^n]\,[x_d^m, z]$$

then from

(1) $$(x_d^p)^m = [x_d, x_g]^{mn}\,[x_d z]^m$$

and

(2) $$(x_d^p)^m = [x_d, x_{dw}]^m\,[x_d, x_{dv}]^m$$

so from (1) and (2) we take:

$$[x_d, x_g]^{mn}\,[x_d, z]^m = [x_d, x_{dw}]^m\,[x_d, x_{dv}]^m$$

and so either $x_g = x_{dw}$ and $z = x_{dv}$ or $x_g = x_{dv}$ and $z = x_{dv}$. Thus $mn = m \Rightarrow n = 1$. □

Since t was chosen arbitrarily among the generators x_h, $h \in K$, we see that an automorphism of the group P modulo $\mathrm{Aut}_c P$ is specified by a permutation on the n numbers of the generating, set, where $n = |K|$.

3. In this section the method used there is simplified for certain classes of groups. For each group of these classes it is necessary to obtain a certain presentation in order that the new method can be used. This presentation is called, *rigid.* For each class of rigid groups a general criterion is given which is satisfied by the groups of the class.

LEMMA 3.1.1. Let G finite group generated by two elements x, y and assume $o(x) = 5$ and $o(y) > 5$. The graph constructed by G using the generators x and y can be used for the construction of a corresponding nilpotent group, if we have:

$$\text{(i)}\ [y^2, x] \neq 1\,, \qquad \text{(ii)}\ (xy)^2 \neq 1\,, \qquad \text{(iii)}\ (xy^{-1})^2 \neq 1\,.$$

PROOF. We have to show two things:

(I) The graph has no circuits of length 4 or less.

(II) The arrows of the graph fall into two different classes.

For (I), we have to check the consequences of short circuits. For length 2 and for length 3 there are no circuits by the given statements, i.e. $xy \neq 1$, $xyx \neq 1$.

For length 4: *a*) $x^3y = 1$ yields $[x, y] = 1$ contradicting (i). The arguments for $x^3y^{-1} = 1$, $xy^3 = 1$, and $xy^{-3} = 1$ are analogous.

b) $x^2y^2 = 1$ yields $[x, y^2] = 1$ contrary to (i). Same for $x^2y^{-2} = 1$. $xyxy = 1$ and $xy^{-1}xy^{-1} = 1$ contradict (ii) and (iii) respectively.

c) $xyxy^{-1} = 1$ means $yxy^{-1} = x^{-1}$ and so $y^2xy^{-2} = x$ contrary to (i).

d) $xyx^{-1}y = 1$ leads to $x^2yx^{-2} = y$, contradiction since x is of order 5.

This shows that there are no circuits of length 4 in the graph. We will now show that the x-arrow is the only arrow occurring in 5-cycles of the graph. For this we have to consider the relations which may lead to a 5-cycle.

$x^5 = 1$ is true, so the x-arrow occurs in 5-cycles.

$x^{5-i}y^i = 1$ with $1 \leqslant i \leqslant 4$ yields $[x^{5-i}, y] = 1$ and so $[x, y] = 1$, contradicting (i). There are two possibilities left:

$$xyxy^2 = 1 \quad \text{and} \quad xyx^2y = 1.$$

We consider the consequences od the first equation. We find

$$xyx = y^{-2} \quad \text{and} \quad xy^2x = y^{-1}$$

and so

$$x^{-1}yx = (xyx)^{-1}(xy^2x) = y,$$

contradicting (i). For the second equation we proceed analogously. No 5-cycle contains an y-arrow, so there are two classes of arrows in the graph, the x-arrow and the y-arrow. □

This statement can be used to simplify the consideration of the groups S_n, A_n further.

EXAMPLE 3.2.1. Symetric groupb S_n, $n > 4$. We treat the groups differently for odd and for even n.

(i) S_n, $n > 5$ odd. The group S_n is generated by two generators $a = (1, 2, 3, 4, 5)$, $b = (1, 2)(3, 4, 5, \ldots, n)$. We construct the graph $D(S_n)$ by the elements $a = (1, 2, 3, 4, 5,)$ and $b = (1, 2)(3, 4, 5, \ldots, n)$ where $o(a) = 5$ and $o(b) = 2n - 4$. The graph by Lemma 3.1.1. is constructing since $\langle b^2, a\rangle$ non abelian and the orders of (ab) and (ab^{-1}) are no 2. For $n = 5$ we take $b = (13)(245)$.

(ii) S_n, n even. The group S_n is generated by two generators $a = (1, 2, 3, 4, 4)$ and $b = (2, 3)(4, 5, 6, \ldots, n)$. We construct the graph $D(S_n)$ by the elements $a = (1, 2, 3, 4, 5)$ and $b = (2, 3)(4, 5, 6, \ldots, n)$ where n is an even number, and the graph $D(S_n)$ is constructing by Lemma 3.1.1.

EXAMPLE 3.2.2. The alternating group A_n, $n > 5$. Also, we treat the groups A_n differently for odd and for even n.

(i) A_n, n odd. The alternating group A_n is generated by $a = = (1, 2, 3, 4, 5)$ and $b = (1, 2)(3, 4)(5, 6, 7, \ldots, n)$ and the graph $D(A_n)$ is constructing by Lemma 3.1.1. since the subgroup $\langle b^2, a\rangle$ is non-abelian and the orders of (ab) and (ab^{-1}) are no 2.

(ii) A_n, n even. The group A_n is generated by two elements $a = (1, 2, 3, 4, 5)$ and $b = (1, 2)(3, 4, \ldots, n)$ and the graph $D(A_n)$ is constructing by Lemma 3.1.1.

LEMMA 4.1.1. Assume that G is finite and is generated by two elements of order 5 e.g. x and y such that $(xy)^2 \neq 1$ $(xy^{-1})^2 \neq 1$ and G is non-abelian. The graph constructed by x and y is suitable, if and only if there is no automorphism of G interchanging x and y.

PROOF. By the given statements there are no circuits of length 4 or smaller. Every x-arrow and every y-arrow is contained in exactly one 5-cycle and all arrows belonging to a given 5-cycle are x-arrows or all of them are y-arrows.

Beginning at any point P of the graph, we can construct two classes of arrows in the following way:

(i) one of the arrows beginning in P is defined as belonging to class A, the other to class B.

(ii) An arrow belonging to a 5-cycle in which one arrow is member of class A is itself member of class A.

(iii) As in (ii) but for class B.

(iv) Two arrows beginning at the same point are always members of different classes.

Since the graph is constructed by G, every arrow is eventually defined as belonging to class A or B. Any automorphism of the graph which is not defined by group multiplication can be changed by group multiplication to an automorphism fixing some point P and hence interchanging the two classes of arrows. But that means that every relation $F(x, y) = 1$ is also true after that change i.e. $F(y, x) = 1$ if $\sigma \in \mathrm{Aut}\, G$, $\sigma(x) = y$ and $\sigma(y) = x$ and then G possesses the automorphism mentioned. The other direction is clear.

EXAMPLE 4.1.2. Let G be the group:

$$G = \langle a, b | a^5 = b^2 = [b, a^{-i}ba^i] = (ab)^5 = 1, \quad i = 1, 2, 3, 4 \rangle$$

then the graph $D(G)$ is to be constructed. The order of G is 5.2^4. Since b has order 2, we should try to change the set of generators. We take $x = a$ and $y = a^2b$. The order of y is 5, because $y^5 = (a^2b)^5 = (ab)^5 = 1$.

In order to aply Lemma 4.1.1. we must have

$$(xy)^2 = (aa^2b)^2 = (a^3b)^2 = a^3ba^3b \neq 1$$

$$(xy^{-1})^2 = (ab^{-1}a^{-2})^2 \neq 1 .$$

But there is no automorphism of the group interchanging x and y since:

$$(x^3y)^2 = (a^3a^2b)^2 = 1 \neq (y^3x)^2 = \big((a^2b)^3a\big)^2$$

and if the order of $(a^2b)^3a$ is 2 then $b = 1$ contradiction.

EXAMPLE 4.1.3. The group $C_5 \sim C_5$. The group $C_5 \sim C_5$ is generated by two elements $x = (a, 1)$, and $y = \big(1, (a, 1, 1, 1, 1)\big)$. We can apply Lemma 4.1.1. since $xy = \big(a, (a, 1, 1, 1, 1)\big)$ and $xy^{-1} = \big(a, (a^{-1}, 1, 1, 1, 1)\big)$ with orders $\neq 2$.

There is no automorphism of the group $C_5 \sim C_5$ interchanging x and y since the relation: $[y, x^{-1}yx] = \big(1, (1, 1, 1, 1, 1)\big)$ but $[x, y^{-1}xy] = \big(1, (a, a^{-2}, a, 1, 1)\big) \neq 1$ hence the group $C_5 \sim C_5$ is a rigid group by Lemma 4.1.1.

LEMMA 5.1.1. If G is finite group generated by two elements x and y such that $o(x) > 5$, $o(y) > 6$, $o(xy) \neq 2$, $o(xy^2) \neq 2$, $o(x^2y) = 2$ and $[x^2, y^2] \neq 1$, then the graph constructed by x and y has as only automorphisms those induced by G, and the graph can be used for our group constructions.

PROOF. We have to show that the arrows describing the action of x and y can be distinguished; we also have to show the regularity conditions. Since $[x^2, y^2] \neq 1$, G is not commutative and not cyclic. So, in particular, there are no circuits of length 2 or 3.

For length 4 we have to consider the relations: $xyxy = 1$, $xyxy^{-1} = 1$, $xyx^{-1}y = 1$, $xyx^{-1}y^{-1} = 1$. These relations and all other relations e.g. $x^4 = 1$, $x^{-1}yx^{-1}y = 1$ are also not valid. The first and the last relation can not hold by hypothesis. The second relation yields $x^{-1} = yxy^{-1}$ so $y^2xy^{-2} = x$, $[x, y^2] = 1$, which contracts $[x^2, y^2] \neq 1$. The argument for the third relation is analogous. This shows that the graph can be used for the group constructions. Now we check the cycles of higher length. The cycles of length 5 would yield one of the following relations:

$$x^5 = 1,\ y^5 = 1,\ xyyxy = 1,\ xxyxy = 1$$

the other relations

$$xy^4 = 1,\ x^2y^3 = 1,\ x^3y^2 = 1,\ x^4y = 1$$

are also not valid. The first two relations are impossible by assumption. The third relation yields $xy^2x = y^{-1}$ and $xyx = y^{-2}$ so $x^{-1}yx = (xyx)^{-1}(xy^2x) = y^2y^{-1} = y$ and $[x, y] = 1$, a contradiction. By symmetry, the fourth relation is impossible, too. We have found that there exists no cycle of length 5 in the graph. Since we have the relation $xxyxxy = 1$ there are 6-cycles. By assumption, we may have $x^6 = 1$, but we know also $y^6 = 1$. We want to show that the x-arrows occur in more 6-cycles than the y-arrows. If $(x^2y)^2 = 1$ is the only relation valid of this length, then the x arrows are contained in two different 6-cycles and y-cycles only in one. Because:

Case 1: The y-arrows contained in more 6-cycles than the x-arrows. Then, the cycles of length 6 would yield one of the following relations: $xy^5 = 1,\ x^2y^4 = 1,\ xyxy^3 = 1,\ xy^2xy^2 = 1$.

We find:

$$xy^5 \neq 1$$

because G is not cyclic.

If $x^2y^4 = 1$, from $(x^2y)^2 = 1$ we have $(y^{-4}y)^2 = 1,\ y^6 = 1$ which contradicts the hypothesis.

The relation $xyxy^3 = 1$ is impossible since $(x^2y)^2 = (xyx)^2 = 1$ implies $y^6 = 1$, a contradiction.

The relation $(xy^2)^2 = 1$ is excluded by hypothesis.

Case 2: The y-arrows are contained in equal 6-cycles with x-arrows. The cycles of length 6 would yield one of following relations:

$$x^3y^3 = 1,\ x^2y^2xy = 1,\ (xy)^5 = 1,\ y^2xyx^2 = 1\,.$$

$$x^3y^3 = 1 \quad \text{or} \quad x^2yy^2x = 1 \quad (y^2x)^2 = 1\,,$$

contradicting the hypothesis.

$$x^2y^2xy = 1 \quad \text{or} \quad yxyx^2y = 1 \quad \text{with } x^2y = y^{-1}x^{-2}$$

yields $yxyy^{-1}x^{-2} = 1$ and $y = x$, contradiction.

$$(xy)^3 = 1 \quad \text{or} \quad xy(xyx)y = 1$$

with

$$xyx = (xyx)^{-1} \quad \text{and} \quad yxy = xyx\,,$$

but $o(xyx) = 2$ so $o(yxy) = 2$, a contradiction because $yxyyxy \neq 1$ from $(xy^2)^2 \neq 1$ by hypothesis.

So, the possible 6-cycles are $x^2yx^2y = 1$, $xyxyx^2 = 1$ and if furthermore $x^6 = 1$, the x-arrows are contained in three different 6-cycles, while nothing is changed for the y-arrows. We conclude that the number of 6-cycles containing a given x-arrow is always greater than the corresponding number for a given y-arrow, and this method of distinction proves the Lemma. □

EXAMPLE 5.1.2. The groups $PGL(2, p)$ and $PSL(2, p)$. The projective linear group is the factor group:

$$PGL(2, p) = GL(2, p)/Z(GL(2, p))$$

and can be identified in a natural way with the group of projective transformations

$$\alpha\colon\ z' = \frac{az + b}{cz + d}\,, \qquad a, b, c, d \in GF(p) \text{ and } ad - bc \neq 0$$

of projective line L of $q + 1$ points coordinatized by the elements of $GF(p)$ and the symbol ∞.

The projective special linear group is the factor group: $PSL(2, p) = SL(2, p)/Z(SL(2, p))$ and the element α lies in $PSL(2, p)$ precisely when $ad - bc = 1$ in $GF(p)$.

The elements of $PGL(2, p)$ are of the form:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} Z(G) \qquad (\mathrm{mod}\ p)$$

where $G = GL(2, p)$ and the centre $Z(G)$ consists of all matrices αI, where α is any mark of $GF(p)$ different from 0, i.e. the centre is generated by αI, where α is a primitive mark of the field.

In general the groups $PSL(n, q)$ have three properties that are useful in discussing the Mathieu groups. The first property is $PSL(n, q)$ is a simple group except for the two following cases: $n = 2$, $q = 2$, $q = 3$ [1]. The second property is $PSL(2, q)$ and $PSL(3, q)$ are doubly transitive on sets of $q + 1$ and $q^2 + q + 1$ points respectively [1]. The third property is stated in the following theorem:

THEOREM A: For the values $q = 2, 3, 5, 7, 9$ and 11, $PSL(2, q)$ has a subgroup of index $q + 1$, but $PSL(2, q)$ also has subgroups of minimal index 2, 3, 5, 7, 6 and 11 respectively [1].

Consider:

$$x = \begin{pmatrix} u & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{and} \qquad y = \begin{pmatrix} 1 + t & t \\ -t & 1 - t \end{pmatrix}$$

as representatives of $GL(2, p)/Z(GL(2, p))$.

The order of x is the (multiplicative) order of u in Z_p. If $t \neq 0$, the representative of y is a matrix of determinant 1 and trace 2, which is different from the unit matrix. The order of y is p. We take $u^2 \neq 1$ and t will be chosen dependent on u. Now we have to show that:

PROPOSITION 5.1.3. The elements x and y, suitable chosen, will generate $PGL(2, p)$ and $PSL(2, p)$ respectively.

PROOF. The element x is contained in the normalize of two p-Sylow subgroups, namely those generated by:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{and by} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

It is known that an element $\neq 1$ is contained in at most two different p-Sylow subgroups of $PSL(2, p)$ it is therefore not contained in the Normalizer of the subgroup generated by y,

$$y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-t} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Therefore $\langle x, y \rangle$ and $PSL(2, p) \cap \langle x, y \rangle$ contains all $p + 1$ p-Sylow subgroups because contains the all conjugate class and the order of $PSL(, p)$ is $\frac{1}{2}\ p(p^2 - 1)$.

The intersection is a subgroup of the group $PSL(2, p)$ of index

$$\frac{|PSL(2, p)|}{|PSL(2, p) \cap \langle x, y\rangle|} = k \qquad \text{dividing } p-1 .$$

Since $PSL(2, p)$ is simple for $p > 6$ and of order divisible by the prime p, we find that $PSL(2, p) \cap \langle x, y\rangle = PSL(2, p)$ because the group $PSL(2, p)$ has no proper subgroup of index p-1. But the intersection of $\langle x, y\rangle$ with the group $PSL(2, p)$ would have such an index, therefore:

$$PSL(2, p) \cap \langle x, y\rangle = PSL(2, p) \quad \text{and} \quad \langle x, y\rangle = PSL(2, p)$$

if and only if x is not contained in $PSL(2, p)$ then $\langle x, y\rangle = PGL(2, p)$. Consequently if $p > 7$ and u is a generate of Z_p^*, $\langle x, y\rangle = PGL(2, p)$, and this basis is suitable by Lemma 5.1.1. If, on the other hand, $p \geqslant 13$ and u is the square of a generator of Z_p^*, then $x \in PSL(2, p)$ and $\langle x, y\rangle = PSL(2, p)$ and this provides a suitable graph. So, we check all the conditions of Lemma 5.1.1. Before checking all the conditions of Lemma we have:

$$x^2 = \begin{pmatrix} u^2 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad y^2 = \begin{pmatrix} 1+2t & 2t \\ -2t & 1-2t \end{pmatrix}$$

and a matrix, taken mod $Z(PGL(2, p))$ has order 2 if and only if its trace is zero. So, $u^2 = 1$ and $u = -1$ since $u \neq 1$. Now the conditions of Lemma 5.1.1. lead to $o(u) > 5$ and from this $p > 6$ so,

$$\operatorname{tr}(xy) = \operatorname{tr}\begin{pmatrix} (1+t)u & ut \\ -t & 1-t \end{pmatrix} = (1+t)u + (1-t) \neq 0 ,$$

$$\operatorname{tr}(xy^2) = \operatorname{tr}\begin{pmatrix} (1+2t)u & 2tu \\ -2t & 1-2t \end{pmatrix} = (1+2t)u + (1-2t) \neq 0 ,$$

$$\operatorname{tr}(x^2 y) = (1+t)u^2 + (1-t) = 0 ,$$

and from $[x^2, y^2] \neq 1$ we take $2tu^2 \neq 2t$.

The only equality yields $t = (1+u^2)/(1-u^2)$ this is defined if $u^2 \neq 1$ and all the inequalites are satisfied.

Acknowledgement. This paper is a part of the author's thesis, written with the suppport of Professor Dr. H. Heineken, Wurzburg University, and accepted for a Ph. D. degree at the University of Athens in November, 1984. The author wishes to thank Professor Dr. H. Heineken for his help and for his kind encouragement during the preparation of the thesis. I have also to express my sincere thanks to Prof. S. Andreadakis, University of Athens, for his whole contribution to my scientific formulation.

REFERENCES

[1] L. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Dover Publications, N.Y., 1958.

[2] F. Harary, *Graph Theory*, Addison Wesley, 1969.

[3] H. Heineken - H. Liebeck, *On the occurence of finite groups in the automorphism group of nilpotent groups of class* 2, Arch. Math., **25** (1974), pp. 8-16.

[4] R. Lawton, *A note on a theorem of Heineken and Liebeck*, Arch. Math., **31** (1978), pp. 520-523.

[5] U.H.M. Webb, *The occurence of groups as automorphisms of nilpotent p-groups*, Arch. Math., **37** (1981), pp. 481-498.

[6] G. Zurek, *Eine Bemerkung zu einer Arbeit von Heineken und Liebeck*, Arch. Math., **38** (1982), pp. 206-207.

Manoscritto pervenuto in redazione il 6 febbraio 1985.