J. Math. Soc. Japan
Vol. 31, No. 4, 1979

Finite groups in which two different Sylow p-subgroups have trivial intersection for an odd prime p

By Chat-Yin HO

(Received Jan. 31, 1978)

1. Introduction

Let p be a prime and let G be a finite group which satisfies the following condition.

(TIp): two different Sylow p-groups contain only the identity element in common.

Suzuki [10] treated the case $p=2$. When p is an odd prime, it seems quite difficult to describe all possibilities. Here we treat a restricted case that G posess a p-non-stable faithful representation. More precisely, we say that G is a (Qp)-group if G satisfies the following condition:

(Qp): There exists a finite vector space M over $GF(p)$, the field with p elements, such that M is a faithful $GF(p)(G)$-module and some nontrivial element of G has minimal polynomial $(X-1)^2$ over M.

We remark that the above condition (Qp) is always valid for $p=2$ when G is of even order. This can be seen by taking M to be the group algebra of G over $GF(2)$ and let G act on M naturally. The main result of this paper is the following theorem.

THEOREM 1. *Let p be an odd prime and let G be a finite group satisfy the conditions (TIp) and (Qp). Then one of the following holds:*

(a) *A Sylow p-group of G is a normal subgroup.*

(b) *G contains normal subgroups G_1 and G_2 such that*

$$G \geqq G_1 > G_2 \geqq 1$$

where G_2 is the center of G_1, both G/G_1 and G_2 are of order prime to p and G_1/G_2 is isomorphic to $L_2(p^n)$ or $U_3(p^n)$ for some positive integer n.

(c) *$p=3$ and G contains normal subgroups G_1 and G_2 such that*

$$G \geqq G_1 > G_2 \geqq 1$$

where G_2 is the maximal normal 2-group of G_1, G/G_1 has order prime to p and G_1/G_2 is isomorphic to the cyclic group of order 3 or A_5.

Let K/Ω be an algebraic function field with one variable of genus $g>1$

over the algebraic closed field Ω. If Ω is the complex number or $\mathrm{Char}(\Omega) \nmid |\mathrm{Aut}(K/\Omega)|$ then $|\mathrm{Aut}(K/\Omega)| \leqq 84(g-1)$. Theorem 1 seems to have application to find a bound for $|\mathrm{Aut}(K/\Omega)|$ in the case $\mathrm{Char}(\Omega) \mid |\mathrm{Aut}(K/\Omega)|$. In fact W. Henn suggested that in this case $|\mathrm{Aut}(K/\Omega)| \leqq g^2$ up to some exceptional case.

This work was suggested by Ch. Hering to whom the author would like to express his gratitude.

2. Notation and Definition.

A group is *quasi-simple* if it is perfect and the quotient over its center is simple. For any group H, let $E(H)$ be the central product of all subnormal quasi-simple subgroups of H. These subgroups are called the components of $E(H)$. The *generalized Fitting subgroup* of H is denoted by $F^*(H)$ and is defined by $F^*(H)=E(H)F(H)$, where $F(H)$ is the Fitting subgroup of H.

All groups considered in this paper are of finite order. Most notations are standard and can be found in [2]. We list some of them for the convenience of the reader.

Z_n: the cyclic group of order n.

$Z(H)$: the center of the group H.

$O_p(H)$: the maximal normal p-subgroup of H for the prime p.

$O_{p'}(H)$: the maximal normal subgroup of H of order prime to p.

$C_H(T)$: the centralizer of the subset T in H.

$\langle X, Y\rangle$: subgroup generated by X and Y.

$[X, Y]$: $\langle x^{-1}y^{-1}xy \mid x\in X,\ y\in Y\rangle$.

X^Y: $\langle X^y \mid y\in Y\rangle$.

$S(H)$: the maximal solvable normal subgroup of H.

$K \trianglelefteq H$: K is a normal subset of H.

$H^{(\infty)}$: the terminal member of the derived series of H.

3. Preliminary results.

3.1. LEMMA. *Let H be a group. Then $C_H(F^*(H)) \leqq F(H)$.*

PROOF. [3, (2.2)].

The following theorem may be of independent interest.

3.2. THEOREM. *Let p be a prime and let G satisfy the condition (TIp).*

(1) *Every subgroup of G also satisfies (TIp).*

(2) *If G is p-solvable, then one of the following holds:*

(2.a) *A Sylow p-group of G is normal.*

(2.b) *A Sylow p-group of G is cyclic.*

(2.c) *$p=2$ and a Sylow 2-group of G is a generalized quaternion.*

(3) *If* $G=\langle g \mid g^p=1\rangle$ *and* $p \mid |S(G)|$, *then one of the following holds:*

(3.a) *G is a p-group.*

(3.b) *A Sylow p-group P of G has order p, $G=PO_{p'}(G)$ and $O_{p'}(G)=[P, O_{p'}(G)]$.*

PROOF. (1) Let H be a subgroup of G. Let Q_1 and Q_2 be two Sylow p-groups of H. Let P_1 and P_2 be two Sylow p-groups of G such that $Q_1 \leqq P_1$ and $Q_2 \leqq P_2$. If $Q_1 \cap Q_2 \neq 1$, then $P_1 \cap P_2 \neq 1$ and so $P_1=P_2$. Therefore $Q_1=P_1 \cap H=P_2 \cap H=Q_2$.

(2) If $O_p(G)\neq 1$, then clearly (2.a) holds. Therefore we may assume $O_p(G)=1$. Applying induction on $|G|$ we may assume that G is generated by its p-elements. Suppose X is an elementary abelian p-subgroup of order p^2 of G. Let P be a Sylow p-group of G containing X and let $N=O_{p'}(G)$. Let $1\neq x \in X$ and let $n \in C_N(x)$. Since $x \in P \cap P^n$, $P=P^n$. Therefore $[n, X] \leqq N \cap P=1$ and so $C_N(x) \leqq C_N(X)$. By [4, Theorem 3.16 on p. 188] we have $N=\prod_{1\neq x \in X} C_N(x)$ and so $N=C_N(X)$. Thus $X \leqq P \cap P^N$ and so $P=P^N$. Therefore $[N, P] \leqq N \cap P=1$. Since G is generated by its p-elements, $N \leqq Z(G)$. As G is p-solvable, $N \lneqq O_{p'p}(G)$. This implies $O_{p'p}(G)=N \times O_p(G)$. Hence $O_p(G)\neq 1$, a contradiction. Therefore G does not contain any non cyclic abelian p-group. By [4, Theorem 4.10, p. 199] we see either (2.b) or (2.c) holds.

(3) If $O_p(G)\neq 1$, then (3.a) holds. Therefore we may assume $O_p(G)=1$. Let $S=S(G)$ and let $N \leqq O_{p'p}(S)$ such that $N/O_{p'}(S)=\Omega_1(O_{p'p}(S)/O_{p'}(S))$. Since $O_p(S)=1$, (1) and (2) imply $|N/O_{p'}(S)|=p$. Let x be an element of order p of G. Suppose $x \notin N$. Let X be a Sylow p-group of $N\langle x\rangle$ containing x. Then X is elementary abelian of order p^2. As in the proof of (2) we see that $[X, O_{p'}(G)]=1$ and so $[x, O_{p'}(G)]=1$. Since x is arbitrary and G is generated by its elements of order p, $O_{p'}(G) \leqq Z(G)$. Since $O_{p'}(S) \leqq O_{p'}(G)$, $O_{p'}(S) \leqq Z(S)$. Therefore $N=O_{p'}(S) \times O_p(N)$ and $|O_p(N)|=p$. Since $O_p(N) \leqq O_p(G)$, $O_p(G)\neq 1$ which is a contradiction. Therefore $x \in N$. This implies $G \leqq N$ and so $G=N$. Let P be a Sylow p-group of G and let $L=O_{p'}(G)$. Then $|P|=p$ and $G=PL$. By [4, Theorem 3.5, p. 180] we have $L=C_L(P)[P, L]$. Therefore $P[P, L]$ is a normal subgroup of index prime to p. Since G is generated by its element of order p, $G=P[P, L]$. By comparing orders we see that $L=[P, L]$ as required.

4. Proof of Theorem 1.

In this section let p be an odd prime and let G be a group satisfy (TIp) and (Qp) for the vector space M. For any subspace U of M we write $\dim U$ to mean the dimension of U over $GF(p)$.

Let $Q=\{g \in G \mid g\neq 1 \text{ and } M(g-1)^2=0\}$. For any $\sigma \in Q$, we have $\sigma^p=1$.

Let $Q_d=\{\tau\in Q\,|\,\dim(M(\tau-1))=\min_{\sigma\in Q}\dim(M(\sigma-1))\}$. For $\sigma\in Q_d$, let $E(\sigma)=\{\tau\in Q\,|\,C_M(\tau)=C_M(\sigma)$ and $M(\tau-1)=M(\sigma-1)\}\cup\{1\}$. Then $E(\sigma)$ is an elementary abelian p-group [8, Lemma 2.2]. Let $\Sigma=\{E\,|\,E=E(\sigma)$ for some $\sigma\in Q_d\}$.

4.1. LEMMA. *Let $E\in\Sigma$ and let $F=E^g$ for some g. Suppose $E\neq F$. Set $S=\langle E, F\rangle$.*

(a) *If $p\geqq 5$ and S is not a p-group, then $S\cong SL(2, |E|)$.*

(b) *If $p=3$, $|E|>3$ and S is not a 3-group, then $S\cong SL(2, |E|)$.*

(c) *If $p=3$, $|E|=3$, then S is isomorphic to one of the following groups: $Z_3\times Z_3$, 3^{1+2}, $SL(2, 3)$, $SL(2,3)\times Z_3$, $SL(2,5)$, where 3^{1+2} is the extra special 3-group of order 27, exponent 3.*

PROOF. (a) [8, Theorem 2.6].

(b) [6, Theorem 4.2].

(c) [5, Theorem 4.3].

4.2. THEOREM. *Let $H=\langle\sigma\,|\,\sigma\in Q\rangle$. Then one of the following holds:*

(a) *H is a p-group.*

(b) *H is a quasi-simple group such that $Z(H)$ has order prime to p and $H/Z(H)\cong L_2(p^n)$ or $U_3(p^n)$ for some positive integer n.*

(c) *$p=3$, $[H, O_2(H)]=O_2(H)$ and $H/O_2(H)\cong Z_3$ or A_5.*

PROOF. Since an element in Q has order p, H is generated by its elements of order p. By Theorem 3.2.(1) we see that H satisfies (TIp). If $O_p(H)\neq 1$, then (a) holds, by Theorem 3.2.(3). Therefore we may assume $O_p(H)=1$. We use induction on $|H|+|M|$ in the rest of the proof. Let $K=\langle\sigma\,|\,\sigma\in Q_d\rangle$. Then K is a normal subgroup of H. Hence $O_p(K)=1$. Suppose $K\subsetneqq H$. Induction implies that conclusion (b) or (c) holds when replace H by K. Since $K\trianglelefteq H$, H induces only inner automorphisms of $K/Z(K)$ when case (b) holds (or $K/O_2(K)$ when (c) holds) as H satisfies (TIp). If $K/O_2(K)\cong Z_3$, then as in the proof of Theorem 3.2.(3) we see that $H=K$ which is impossible. Let $C=C_H(K/Z(K))$ when (b) holds and let $C=C_H(K/O_2(K))$ when $K/O_2(K)\cong A_5$. Then $H=KC$. Since $O_p(H)=1$, C is a p'-group. Since H is generated by elements of order p, $H=K$ a contradiction. Therefore $H=\langle\sigma\,|\,\sigma\in Q_d\rangle$. Similarly we have $H=E^H$ for any $E\in\Sigma$.

Case (i) $p\geqq 5$ or $p=3$ and there exists $E\in\Sigma$ such that $|E|>3$.

By 4.1. (a) we see that $O_{p'}(H)\leqq Z(H)$. If $E(H)=1$, then $F^*(H)=F(H)$. Since $O_p(H)=1$, $F(H)\leqq O_{p'}(H)\leqq Z(H)$. Hence $H\leqq C_H(F(H))=C_H(F^*(H))\leqq F(H)$ by 3.1. This is impossible as H is generated by its elements of order p. Therefore $E(H)\neq 1$. Theorem 3.2 implies that $E(H)$ is quasi-simple. Let $X\in\Sigma$ and let $Y=XE(H)$. Since $F(H)\leqq Z(H)$, $C_H(E(H))\leqq F(H)$. Since $O_p(H)=1$, $X\nleqq C_H(E(H))$. Therefore $X\nleqq O_p(Y)$. Therefore there exists $g\in G$ such that $L=\langle X, X^g\rangle$ is not a p-group by [4, Theorem 8.2, p. 105]. Therefore $L\cong SL(2, |X|)$ by 4.1. Hence $X\leqq L=L^{(\infty)}\leqq Y^{(\infty)}\leqq E(H)$. This shows that $H=E(H)$

is quasi-simple. Since H satisfies (TIp), we see that (b) holds by [**7**, Theorem 1].

Case (ii) $p=3$ and $|E|=3$ for all $E\in\Sigma$.

Let $E\in\Sigma$ and let $F=E^h\neq E$ for some $h\in H$. Let $S=\langle E, F\rangle$. Since H satisfies (TIp), $S\not\cong SL(2, 3)\times Z_3$. Suppose $\langle E, F\rangle\cong 3^{1+2}$. Let $X=[E, F]$. Then $X\in\Sigma$ by [**2**, Theorem 1]. Let $Y\in\Sigma$ such that $\langle X, Y\rangle\cong SL(2, 3)$ and let $w\in\langle X, Y\rangle$ such that $X^w=Y$ and $w^4=1$. By [**5**, Theorem 4.4] and a direct calculation of matrices we see that $\langle E, E^w\rangle\cong Z_3\times Z_3$ and $\langle X, Y\rangle$ normalizes $\langle E, E^w\rangle$. This contradicts to the fact that H satisfies (TIp). Therefore $S\not\cong 3^{1+2}$. By 4.1 $S\cong Z_3\times Z_3$, $SL(2, 3)$ or $SL(2, 5)$.

Suppose $3\,|\,|S(H)|$. Theorem 3.2.(3) implies that $H=O_{p'}(H)P$, where P is a Sylow 3-group of order 3. In particular the possibilities $Z_3\times Z_3$ and $SL(2, 5)$ for S cannot occur in this case. [**1**, Theorem 3.7] implies that $|H/O_2(H)|=3$ and (c) holds. Therefore we may assume that $3\nmid|S(H)|$.

Let $X\in\Sigma$. Let q be a prime such that $q\notin\{2, 3\}$. Let R be a q-group normalized by X. Then $[R, X]=1$ by 4.1. This shows that $O_{2'}(O_{3'}(H))\leqq Z(H)$.

Let $X\in\Sigma$ and let U be the subgroup of H which stabilizes the chain of subspaces: $0\leqq\langle M(x-1)\,|\,x\in X\rangle\leqq C_M(X)\leqq M$. Then U has exponent p and $X\leqq Z(U)$. Suppose $X\neq U$. Then there exists an elementary subgroup B of order p^2 such that $X\leqq B$. As in the poof of Theorem 3.2. (2) we see that $[O_{p'}(H), B]=1$ and so $[O_{p'}(H), X]=1$. Since X is arbitrary, $O_{p'}(H)\leqq Z(H)$. As in the proof of (i) we see that $E(H)\neq 1$ and $E(H)$ is quasi-simple. Suppose $X\not\leqq E(H)$. Let $D=\{X^g\,|\,g\in E(H)\}$ and let $K=\langle Z\,|\,Z\in D\rangle$. Let $A, B\in D$. If $\langle A, B\rangle\cong SL(2, 5)$, then $A\leqq\langle A, B\rangle=\langle A, B\rangle^{(\infty)}\leqq(XE(H))^{(\infty)}\leqq E(H)$. This implies $X\leqq E(G)$, a contradiction. Therefore $\langle A, B\rangle$ is isomorphic to $Z_3\times Z_3$, or $SL(2, 3)$. If K is a perfect group, then $X\leqq K^{(\infty)}\leqq(XE(H))^{(\infty)}\leqq E(H)$ a contradiction. By [**1**], K must be solvable. Therefore $[K, E(H)]$ is a normal solvable subgroup of $E(K)$ and so $E(H)$ centralizes K. In particular $X\leqq C_G(E(H))=C_G(F^*(H))\leqq F(H)$ which is impossible as $F(H)$ is a p'-group. Therefore $X\leqq E(H)$. Since X is arbitrary, $H=E(H)$ is quasi-simple. By [**7**, Theorem 1] and condition (TIp) we see that $H/Z(H)$ is isomorphic to A_5 or $U_3(3)$. Therefore we may assume $U=X$. Suppose there exists $Y\in\Sigma$ such that $\langle X, Y\rangle\cong SL(2, 5)$. Then $H'=H$. Let $I_l(X)=\{i\,|\,i^2=1, \dim M(i-1)=2d$ and there exists $Z\in\Sigma$ such that $i\in\langle X, Z\rangle\}$. Let $i, j\in I_l(X)$. Then $ij\in U$ by [**5**, Lemma 5.1 and Corollary 5.2]. Since $U=X$, $I_l(X)=\{i\}$. Let $R(i)=\{E\,|\,E\in\Sigma$ and $i\in I_l(E)\}$. Let $\Sigma_1=\{X^h\,|\,h\in H\}$. Then H is generated by the elements in Σ_1. We claim $R(i)\geqq\Sigma_1$. Suppose $[Z, S]=1$ for all $S\in R(i)$ and all $Z\in\Sigma_1\cdot R(i)$. Then $R(i)$ is H invariant as $H=\langle\Sigma_1\rangle$. Since H is transitive on Σ_1, $R(i)\geqq\Sigma_1$ in this case. Hence we may assume that there exist $S_1\in R(i)$ and $\langle z\rangle=Z\in\Sigma_1\backslash R(i)$ such that $[S_1, Z]\neq 1$. Since $\langle S_1, Z\rangle\not\cong 3^{1+2}$, so there is an involution $j\in\langle S_1, Z\rangle$. If $j\in I_l(S_1)$, then $j=i$ and so $i\in I_l(Z)$. This implies $Z\in R(i)$, a contradiction. Therefore $j\neq i$. Hence dim $M(j-1)\leqq 2d$. Suppose $[Z, i]=1$. Then $C_M(i)$ and $M(i-1)$ are Z-submodules. Let $s\in S_1$ such that s is conjugate to z in $\langle S_1, Z\rangle$. Since $S_1\in R(i)$, the restriction of S_1 on $C_M(i)$ is the identity transformation. Hence $s^{-1}z$ and z have the same restriction on $C_M(i)$. However $(s^{-1}z)^2=j$ is an involution. This shows that the restriction of Z on $C_M(i)$ is also the identity transformation. Since $[Z, i]=1$, i acts on $I_l(Z)=\{k\}$ by conjugation. Hence $[i, k]=1$. Therefore $M(i-1)$ and $C_M(i)$ are $\langle k\rangle$-submodules. [**5**, Lemma 2.6] implies that k induces -1 on $M(i-1)$. By comparing dimension, we see that $k=i$. This implies $Z\in R(i)$, a contradiction. Thus we may assume $[Z, i]\neq 1$. Let $T\in R(i)$ such that $i\in\langle S_1, T\rangle$ and $\langle S_1, T\rangle\cong SL(2, 3)$. If $[Z, T]=1$, then $i^z\in\langle (S_1)^z, T^z\rangle =\langle (S_1)^z, T\rangle$. Hence $i^z\in I_l(T)=\{i\}$. This implies that $i^z=i$, which is impossible. Therefore $[Z, T]\neq 1$˙ If $\langle Z, T\rangle\cong SL(2, 5)$, then [**5**, Lemma 4.6] implies that $I_l(Z)=I_l(T)=\{i\}$. Thus $Z\in R(i)$, a contradiction. Therefore $\langle Z, T\rangle\cong SL(2, 3)$. Similary we have $\langle T_1, Z\rangle\cong SL(2, 3)$ for each $T_1\in\Sigma_1\cap\langle S, T\rangle$. Thus [**9**, (1.1.1)] implies that i is conjugate to j, a contradiction. Therefore $\Sigma_1\backslash R(i)$ is empty and $R(i)\geqq\Sigma_1$ as required. Since H is generated by elements of Σ_1, $i\in Z(H)$. Let $\bar{H}=H/O_2(H)Z(H)$. Since $3\nmid |S(H)|$ and $O_{2'}(O_{3'}(H))\leqq Z(H)$, $O_2(\bar{H})=Z(\bar{H})=1$. By condition (TIp) and [**9**, Satz] we see that $\bar{H}\cong A_5$. Since $H'=H$ and the Schur multiplier of A_5 has order 2, $H/O_2(H)\cong A_5$ as $Z(H)$ is a $3'$-subgroup.

Thus we may assume that $\langle X, Y\rangle\not\cong SL(2, 5)$ for all $Y\in\Sigma$. Therefore for $E\neq F\in\Sigma$ we have $\langle E, F\rangle\cong Z_3\times Z_3$ or $SL(2, 3)$. We can now appeal to [**1**] and applying condition (TIp) to conclude the proof.

By using the condition (TIp), Theorem 1 is now a consequence of 4.2.

References

[1] M. Aschbacher, Groups generated by a class of elements of order 3, J. Algebra, **24** (1973), 591-612.
[2] G. Glauberman, Quadratic elements in unipotent linear groups, J. Algebra, **20** (1972), 637-654.
[3] D. Goldschmidt, 2-Fusion in finite groups, Ann. of Math. II. Ser., **99** (1974), 70-117.
[4] D. Gorenstein, Finite groups, New York, Harper and Row, 1968.
[5] C. Y. Ho, On the quadratic pair whose root group has order 3, Bull. Inst. Math. Acad. Sinica, Republic of China, **1** (1973), 155-180.
[6] C. Y. Ho, Quadratic pair for 3 whose root group has order greater than 3, I. Comm. in Algebra, **3**(11) (1975), 961-1029.
[7] C. Y. Ho, On the quadratic pairs, J. Algebra, **43** (1976) 338-358.
[8] C. Y. Ho, A characterization of $SL(2, p^n)$, $p\geqq 5$, to appear in J. Algebra.
[9] B. Stellmacher, Einfache Gruppen, die von einer Konjugiertenklasse von elementen der ordnung drei erzugt werden, J. Algebra, **30** (1974), 320-354.

[10] M. Suzuki, Finite groups of even order in which Sylow 2-subgroups are independent, Ann. of Math., (2) **80** (1964), 58-77.

Chat-Yin Ho
Departamento de Matemática
Universidade de Brasília
Brasília, Brasil
and
Department of Mathematics
The University of Tsukuba
Ibaraki 300-31
Japan