On p-strongly embedded subgroups of A_n and $PSL(n, q)$

By Kensaku GOMI

(Communicated by Y. Kawada)

§ 1. Introduction.

Let G be a finite group and let p be a prime. A subgroup H of G is called a p-strongly embedded subgroup of G if (1) p divides the order of H and (2) p does not divide the order of $H \cap H^g$ whenever g is in $G-H$. The purpose of this note is to determine all the p-strongly embedded subgroups of A_n and of $PSL(n, q)$. Here we understand by A_n and $PSL(n, q)$, the alternating group of degree n, and the n-dimensional projective special linear group over the field $GF(q)$ of q elements, respectively.

Bender [1] classified finite groups with a 2-strongly embedded proper subgroup and showed that a p-strongly embedded subgroup of a finite group G is closely related to an equivalence relation defined among Sylow p-subgroups of G. That is, G has a p-strongly embedded proper subgroup if and only if G is p-isolated in the sense of Goldschmidt [2]. In [2], he improved Alperin's theorem on fusion and showed that fusion of p-elements in G is determined by p-local subgroups L of G such that $L/O_p(L)$ is p-isolated. Hence it is desirable to classify finite groups with p-strongly embedded proper subgroups for odd p. Though Bender classified 2-isolated groups and Goldschmidt showed that Sylow p-subgroups of a p-isolated p-solvable group are cyclic or generalized quaternion, classification of p-isolated nonsolvable groups, p an odd prime, seems to be very difficult. So the author wished to know more about p-strongly embedded subgroups of known nonsolvable groups. This is the motivation of this work.

It is easily seen that if a Sylow p-subgroup of G is cyclic, p-strongly embedded subgroups of G are exactly those which contain the normalizer of a subgroup of order p (see § 2). So we may state our results in the following form.

THEOREM A. *Let H be a p-strongly embedded proper subgroup of A_n, p an odd prime. Then one of the following statements holds:*

(1) *$n=2p$, and H is a conjugate of the subgroup*

$$\{g \,;\, g \in A_{2p} \text{ and } \{1, 2, \cdots, p\}g=\{1, 2, \cdots, p\} \text{ or } \{p+1, p+2, \cdots, 2p\}\}$$

(2) *$p \leqq n < 2p$, and a Sylow p-subgroup of A_n is cyclic of order p.*

THEOREM B. *Let H be a p-strongly embedded proper subgroup of $PSL(n, q)$, p an odd prime. Then one of the following statements holds:*

(1) *$n=2$, q is a power of p, and H is the normalizer of a Sylow p-subgroup of $PSL(2, q)$.*

(2) *$p=n=3$, $q=4$, and H is a conjugate of the subgroup $PSU(3, 2)$, the 3-dimensional projective special unitary group over $GF(4)$.*

(3) *A Sylow p-subgroup of $PSL(n, q)$ is cyclic.*

A restatement of Theorem B will be given in §4 Theorem B* (see also the remark following Theorem B*).

Bender's classification theorem asserts that simple groups with a 2-strongly embedded proper subgroup necessarily have independent Sylow 2-subgroups, i.e. distinct Sylow 2-subgroups intersect in the identity element (Finite groups with independent Sylow 2-subgroups have been classified by M. Suzuki.). On the contrary, simple groups with a p-strongly embedded proper subgroup for odd p not necessarily have independent Sylow p-subgroups, even if Sylow p-subgroups are noncyclic. For instance, Sylow p-subgroups of A_{2p}, p an odd prime, are elementary abelian of order p^2, but are not independent. Note that $PSL(3, 4)$ has independent elementary abelian Sylow 3-subgroups of order 9.

In finite groups having a 2-strongly embedded proper subgroup, elements of order 2 form one conjugacy class. On the contrary, finite groups having a p-strongly embedded proper subgroup for odd p may have more than one conjugacy classes of elements of order p. In fact, A_{2p} and $PSL(2, p^m)$, p an odd prime, have two conjugacy classes of elements of order p.

The proofs of Theorems A and B are elementary, but in one place we must use the deep results of [3], [4] and [6]. It is desirable to avoid using them. In §4, we will assume familiarity with the structure and embedding of the Sylow subgroups of $GL(n, q)$. A good description of them was provided by Weir [5]. We note that if $2 \neq p | q-1$ or $p=2$ and $4 | q-1$, the subgroup of monomial matrices contains a Sylow p-subgroup of $GL(n, q)$.

The author would like to thank Professors M. Suzuki, T. Kondo and Mr. H. Enomoto for suggesting the present forms of the proofs of lemmas (2.3) and (4.1).

§2. Properties of a p-strongly embedded subgroup.

Throughout this section, let G denote a finite group, and let p be a prime dividing the order of G. We define an equivalence relation among Sylow p-subgroups of G by: $P_0 \sim P$ if and only if there exist Sylow p-subgroups $P_1, P_2, \cdots, P_n = P$ of G such that $P_{i-1} \cap P_i \neq 1$ for $i=1, 2, \cdots, n$. For each Sylow p-subgroup

P of G we define $G(P)=\{g\,;\,g\in G$ and $P\sim P^g\}$. We also define an equivalence relation among elements of order p of G by: $x_0\sim x$ if and only if there exist elements $x_1, x_2, \cdots, x_n=x$ of order p such that $x_{i-1}x_i=x_ix_{i-1}$ for $i=1, 2, \cdots, n$. For each element x of order p we define $G(x)=\{g\,;\,g\in G$ and $x\sim x^g\}$. Then both $G(P)$ and $G(x)$ are subgroups, $G(P)=G(x)$ if $x\in P$, $G(P)^g=G(P^g)$ for any $g\in G$, and $G(P)=G(Q)$ if $P\sim Q$. Clearly, $G(P)\supseteq N_G(P)$, and $G(P)=N_G(P)$ if and only if G has independent Sylow p-subgroups. The number of equivalence classes of Sylow p-subgroups coincides with that of equivalence classes of elements of order p, and both are equal to the index $|G:G(P)|$.

Almost all of the following propositions were stated implicitly in [1]. But we will furnish the complete proof here.

(2.1) *$G(P)$ is a minimal p-strongly embedded subgroup of G. Conversely, if H is a minimal p-strongly embedded subgroup of G, there exists a Sylow p-subgroup P of G such that $H=G(P)$.*

PROOF. Set $H=G(P)$. By the definition of $G(P)$ and Sylow's theorem, the equivalence class of P is the set of Sylow p-subgroups of H. Assume that $g\in G$ and that p divides the order of $H\cap H^g$. Then there exist Sylow p-subgroups P_1 and P_2 of H such that $P_1\cap P_2^g\neq 1$. Hence, $g\in G(P_2)=H$.

Conversely, let H be a p-strongly embedded subgroup of G. Clearly H satisfies the following condition:

(*) $N_G(X)\subseteq H$ for each nonidentity p-subgroup X of H.

In particular, H contains a Sylow p-subgroup P_0 of G. We will show that $G(P_0)\subseteq H$. Let $g\in G(P_0)$. By definition, there exist Sylow p-subgroups $P_1, P_2, \cdots, P_n=P_0^g$ of G such that $P_{i-1}\cap P_i\neq 1$ for $i=1, 2, \cdots n$. By Sylow's theorem, $P_i=P_{i-1}^{g_i}$ for some $g_i\in G$, $i=1, 2, \cdots, n$. Since $H\cap H^{g_1}\supseteq P_0\cap P_0^{g_1}\neq 1$, it follows that $g_1\in H$ and that $P_1\subseteq H$. Proceeding by induction, we conclude that $g_i\in H$ for $i=1, 2, \cdots, n$. Since $P_0^{g_1g_2\cdots g_n}=P_0^g$, it follows that $g\in N_G(P_0)H\subseteq H$. The proof is complete.

(2.2) *Assume that a Sylow p-subgroup of G is cyclic or a generalized quaternion. Then for each subgroup P of order p, $N_G(P)$ is a minimal p-strongly embedded subgroup of G.*

PROOF. Let S_0 be a Sylow p-subgroup of G containing P. We will prove that $G(S_0)=N_G(P)$. Clearly, $N_G(P)\subseteq G(S_0)$. Let $g\in G(S_0)$. Then there exist Sylow p-subgroups $S_1, S_2, \cdots, S_n=S_0^g$ of G such that $S_{i-1}\cap S_i\neq 1$ for $i=1, 2, \cdots, n$. Since each Sylow p-subgroup of G has a unique subgroup of order p, it follows that $P\subseteq S_i$ for $i=1, 2, \cdots n$. In particular $P\subseteq S_0^g$. Hence, $P=P^g$, q.e.d.

(2.3) *Let H be a p-strongly embedded subgroup of G. Then any subgroup* *of G containing H is also p-strongly embedded in G.*

PROOF. Let K be a subgroup of G containing H. Since H contains a Sylow p-subgroup of G and satisfies (*), K also satisfies (*) where H is replaced by K. Assume that $g\in G$ and that p divides the order of $K\cap K^g$. Let S be a Sylow p-subgroup of $K\cap K^g$. By (*), S is a Sylow p-subgroup of G. Since $S, S^{g^{-1}}\subseteq K$, $S^k=S^{g^{-1}}$ for some $k\in K$. Hence, $g\in KN_G(S)\subseteq K$, q.e.d.

Proposition (2.3) has an obvious corollary, which is not used in this paper.

COROLLARY. *Let H be a p-strongly embedded subgroup of G, and let N be a normal subgroup of G. If $p\mid |N|$, then $G=HN$. If $p\nmid |N|$, then HN/N is a p-strongly embedded subgroup of G/N, and HN/N is minimal if H is minimal.*

(2.4) *Let H be a p-strongly embedded subgroup of G. Then $H/O^p(H)$ is a homomorphic image of $G/O^p(G)$, where $O^p(X)$ denotes the subgroup of X generated by the elements of orders prime to p.*

PROOF. By assumption, $H\cap H^g\subseteq O^p(H)$ for every $g\in G-H$. By a theorem of Wielandt [6], H has a normal complement over $O^p(H)$. Hence the assertion follows.

(2.5) *Let H be a p-strongly embedded subgroup of G, and let p^n be the highest power of p dividing the order of G. Then $|G:H|\equiv 1 \pmod{p^n}$.*

PROOF. The number of the right cosets of H contained in the double coset HgH is equal to $|H:H\cap H^g|$ which is divisible by p^n if $g\in G-H$, q.e.d.

§3. The proof of Theorem A.

Let p be an odd prime, n an integer greater than or equal to $2p$, $N=\{1, 2, \cdots, n\}$ and let M denote the set of subsets of p distinct elements of N.

(3.1) *Assume $n\geqq 2p+1$. Then for any two elements α_0, β of M there exist elements $\alpha_1, \alpha_2, \cdots, \alpha_r=\beta$ of M such that $\alpha_{i-1}\cap\alpha_i=\emptyset$ for $i=1, 2, \cdots, r$.*

PROOF. If $\alpha_0\cap\beta=\emptyset$, there is nothing to prove. We argue by induction on $|\alpha_0\cap\beta|$. Assume $|\alpha_0\cap\beta|=m\geqq 1$, and that $\alpha_0=\{a_1, \cdots, a_{p-m}, c_1, \cdots, c_m\}$ and $\beta=\{b_1, \cdots, b_{p-m}, c_1, \cdots, c_m\}$. Since $n-|\alpha_0\cup\beta|\geqq m+1$, there exist $m+1$ distinct elements $d_1, \cdots, d_{m+1}$ of N not contained in $\alpha_0\cup\beta$. Set $\gamma=\{b_1, \cdots, b_{p-m}, d_1, \cdots, d_m\}$ and $\alpha_1=\{a_1, \cdots, a_{p-m}, c_1, \cdots, c_{m-1}, d_{m+1}\}$. Then $\alpha_0\cap\gamma=\emptyset$, $\gamma\cap\alpha_1=\emptyset$ and $|\alpha_1\cap\beta|=m-1$. The proof is complete by induction.

(3.2) *Assume $n\geqq 2p+1$. Then A_n has no p-strongly embedded proper subgroups.*

PROOF. This is an immediate consequence of (2.1) and (3.1), for each element of order p of A_n commutes with a p-cycle and any two p-cycles are equivalent in A_n by (3.1).

(3.3) *Let x be a p-cycle. Then the centralizer of x consists of permutations of the form $x^k y$, where k is an integer, and x and y are disjoint permutations (i.e. their cycle decompositions contain no common letters).*

PROOF. We may assume $x=(1, 2, \cdots, p)$. If z centralizes x, z fixes the unique nontrivial orbit $\{1, 2, \cdots, p\}$ of x. Suppose that $(1)z=(1)x^k$. It can be shown by induction on i that $(i)z=(i)x^k$ for $i=1, 2, \cdots, p$, q.e.d.

By a similar argument we have:

(3.4) *Let $z=xy$ where x and y are disjoint p-cycles. Then each permutation of odd order in the centralizer of z is of the form $x^h y^k u$, where h and k are integers, and x, y and u are disjoint.*

Suppose $n=2p$. (3.3) and (3.4) imply that if $(1, 2, \cdots, p)\sim(a_1, a_2, \cdots, a_p)$, then either $\{1, 2, \cdots, p\}=\{a_1, a_2, \cdots, a_p\}$ or $\{1, 2, \cdots, p\}\cap\{a_1, a_2, \cdots, a_p\}=\varnothing$. Thus, the subgroup described in Theorem A is one of the minimal p-strongly embedded subgroups of A_{2p}. As is well known, it is a maximal subgroup of A_{2p}, whence p-strongly embedded proper subgroups of A_{2p} are exactly its conjugates. The proof is complete.

§4. The proof of Theorem B.

We restate the assertion of Theorem B in a slightly different form.

THEOREM B*. *Let p be an odd prime, n be a positive integer, and q be a prime power. Then the following holds:*

(1) *In case $p|q$ and $n\geqq 3$, $PSL(n, q)$ has no p-strongly embedded proper subgroups.*

(2) *In case $p|q-1$ and $n\geqq 3$, $PSL(n, q)$ has no p-strongly embedded proper subgroups unless $p=n=3$ and $q=4$.*

(3) *$PSU(3, 2)$ is a minimal 3-strongly embedded subgroup of $PSL(3, 4)$.*

(4) *In case $p\nmid q(q-1)$, let k be the smallest positive integer such that $q^k\equiv 1 \pmod p$, and set $t=[n/k]$, the largest integer not greater than n/k. If $t\geqq 2$, $PSL(n, q)$ has no p-strongly embedded proper subgroups.*

REMARK. Sylow p-subgroups of $PSL(2, p^m)$ are independent and their normalizers are maximal subgroups of $PSL(2, p^m)$. If $p|q-1$, p an odd prime, a Sylow p-subgroup of $PSL(2, q)$ is cyclic. $PSU(3, 2)$ is a maximal subgroup of $PSL(3, 4)$. Let p, q, k and t be as in B* (4). If $t\leqq 1$, a Sylow p-subgroup of $PSL(n, q)$ is cyclic. Hence Theorem B can be obtained from Theorem B*.

4.1. The proof of B* (1).

To prove B* (1), it suffices to show that if $n\geqq 3$ and $p|q$, Sylow p-subgroups of

$\mathfrak{G}=GL(n, q)$ are all equivalent.

Let V be a vector space of dimension n over $GF(q)$. If we identify $\mathfrak{G}$ with the group of linear transformations of V, each Sylow p-subgroup of $\mathfrak{G}$ is characterized as the stability group of a composition series of V. Let $\mathfrak{P}$ and $\mathfrak{Q}$ be the stability groups of the composition series $V=V_n \supseteq V_{n-1} \supseteq \cdots \supseteq V_1 \supseteq 0$ and of $V=W_n \supseteq W_{n-1} \supseteq \cdots \supseteq W_1 \supseteq 0$, respectively. If $V_i=W_i$ for some i with $1 \leqq i \leqq n-1$, then $\mathfrak{P} \cap \mathfrak{Q} \neq 1$ since the stability group of the series $V \supseteq V_i \supseteq 0$ is contained in $\mathfrak{P} \cap \mathfrak{Q}$.

If $V_1 \neq W_1$, take the stability group $\mathfrak{R}$ of a composition series $0 \subseteq V_1 \subseteq V_1+W_1 \subseteq \cdots \subseteq V$ and the stability group $\mathfrak{S}$ of a composition series $0 \subseteq W_1 \subseteq V_1+W_1 \subseteq \cdots \subseteq V$. By the preceding paragraph we have $\mathfrak{P} \cap \mathfrak{R} \neq 1$, $\mathfrak{R} \cap \mathfrak{S} \neq 1$ and $\mathfrak{S} \cap \mathfrak{Q} \neq 1$. Hence $\mathfrak{P} \sim \mathfrak{Q}$, q.e.d.[1]

4.2. Necessary lemmas.

In this subsection, we will prove two lemmas needed in proving B* (2) and B* (4). Notations introduced in this subsection will be used throughout the remainder of this paper.

Let V be an n-dimensional vector space over an arbitrary field K. Let $n=d_1+d_2+\cdots+d_m$ be a partition of n, where d_i is a positive integer for $i=1, 2, \cdots, m$, and let $\mathfrak{X}=\mathfrak{X}(d_1, d_2, \cdots, d_m)$ denote the set of all unordered m-tuples $(V_1, V_2, \cdots, V_m)$ of subspaces of V such that V is the direct sum of $V_1, V_2, \cdots, V_m$ and that after a suitable renumbering of V_i's we have $\dim_K V_i=d_i$ for $i=1, 2, \cdots, m$. Clearly, $GL(V)$ acts on $\mathfrak{X}$ by $(V_1, V_2, \cdots, V_m)g=(V_1g, V_2g, \cdots, V_mg)$ for each $g \in GL(V)$. For each element $x=(V_1, V_2, \cdots, V_m)$ of $\mathfrak{X}$ we define:

$$\mathfrak{M}(x)=\{g\,;\, g \in GL(V), \text{ and } xg=x\}\,.$$

$$\mathfrak{D}(x)=\{g\,;\, g \in GL(V), \text{ and } V_ig=V_i \text{ for } i=1, 2, \cdots, m\}\,.$$

We define a reflexive and symmetric relation in $\mathfrak{X}$ by: $(V_1, V_2, \cdots, V_m) \approx (W_1, W_2, \cdots, W_m)$ if and only if, after suitable renumberings of V_i's and of W_i's, we have $V_i=W_i$ for $i \geqq 2$ and $V_1+V_2=W_1+W_2$.

(4.1) *For any two elements x_0 and x of $\mathfrak{X}$, there exist elements $x_1, x_2, \cdots, x_s=x$ of $\mathfrak{X}$ such that $x_{i-1} \approx x_i$ for $i=1, 2, \cdots, s$.*

PROOF. To prove this, it suffices to consider the case $d_1=d_2=\cdots=d_m=1$. Assume that $x_0=(V_1, V_2, \cdots, V_n)$ and $x=(W_1, W_2, \cdots, W_n)$. Let $0 \neq v_i \in V_i$ and $0 \neq w_i \in W_i$ for $i=1, 2, \cdots n$. Define an element g of $GL(V)$ by $v_ig=w_i$ for $i=1, 2, \cdots, n$. Then $x_0g=x$. Let G be a matrix of g with respect to the basis $v_1, v_2,$

[1] It can be proved by another method that groups of Lie type of characteristic p and of rank greater than 1 have no p-strongly embedded proper subgroup.

$\cdots, v_n$. If G is diagonal, then $V_i=W_i$ for each i and $x_0\approx x$. If G is an elementary transformation, we also have $x_0\approx x$. In general, G can be represented as the product of diagonal or elementary transformations: $G=A_sA_{s-1}\cdots A_2A_1$. Let $g_i\in GL(V)$ correspond to $(A_{i-1}\cdots A_2A_1)^{-1}A_i(A_{i-1}\cdots A_2A_1)$ with respect to the basis $v_1, v_2, \cdots, v_n$. Then the matrix of $g_1g_2\cdots g_i$ is $A_i\cdots A_2A_1$. In particular, $g=g_1g_2\cdots g_s$. Since A_i is the matrix of g_i with respect to the basis $v_jg_1g_2\cdots g_{i-1}$, $j=1, 2, \cdots, n$, we have $x_0g_1g_2\cdots g_{i-1}\approx x_0g_1g_2\cdots g_i$, $i=1, 2, \cdots, s$. The proof is complete.

(4.2) *Let W be a subspace of V such that* $\dim_K W\geqq n/2$. *Let $\mathfrak{Y}$ denote the set of all subspaces U of V such that $V=U+W$ (direct sum). For any two distinct elements U_0 and U of $\mathfrak{Y}$, there exist elements $U_1, U_2, \cdots, U_s=U$ of $\mathfrak{Y}$ such that $U_{i-1}\cap U_i=0$ for $i=1, 2, \cdots, s$.*

PROOF. If $n-\dim_K W=1$, the assertion is clear. Assume that $n-\dim_K W=k\geqq 2$. Let $u_1, u_2, \cdots, u_k$ be a basis of U and $w_1, w_2, \cdots, w_k$ be linearly independent elements of W, and set $U'=\langle u_1+w_1, u_2+w_2, \cdots, u_k+w_k\rangle$, subspace of V generated by u_i+w_i, $i=1, 2, \cdots, k$. Then clearly $U'\in\mathfrak{Y}$ and $U\cap U'=0$.

If $U_0\cap U=0$, there is nothing to prove. So we may assume that $U_0\cap U\neq 0$. We proceed by induction on $k-\dim_K U_0\cap U$. Since $U_0\neq U$, there exists an element u of U such that $u=u_0+w$ with $u_0\in U_0-U$ and $w\in W-U$. Choose a basis $u_1, \cdots, u_m$ of $U_0\cap U$ and extend it to a basis $u_1, \cdots, u_m, u_{m+1}=u_0, \cdots, u_k$ of U_0. Let z be an element of W independent of w, and let $w_1, \cdots, w_m=w, w_{m+1}=w+z, \cdots, w_k$ be linearly independent elements of W, and set $U_1=\langle u_1+w_1, \cdots, u_k+w_k\rangle$. Then by the preceding paragraph, $U_1\in\mathfrak{Y}$ and $U_0\cap U_1=0$.

Let $-w_1, \cdots, -w_m, -z, z_{m+2}, \cdots, z_k$ be linearly independent elements of W, and set $U_2=\langle u_1, \cdots, u_m, u, u_{m+2}+w_{m+2}+z_{m+2}, \cdots, u_k+w_k+z_k\rangle$. Since $u_i=(u_i+w_i)-w_i$ and $u=(u_{m+1}+w_{m+1})-z$, it follows that $U_2\in\mathfrak{Y}$ and that $U_1\cap U_2=0$. Furthermore $\dim_K U_0\cap U<\dim_K U_2\cap U$. The proof is complete by induction.

4.3. The proof of B* (4).

Let V be an n-dimensional vector space over $GF(q)$, and set $\mathfrak{G}=GL(V)$. Let p be an odd prime number prime to $q(q-1)$, and let k be the smallest positive integer such that $q^k\equiv 1 \pmod p$. Set $t=[n/k]$, $n=kt+r$ and $m=t+r$. Set $\mathfrak{X}=\mathfrak{X}(\underbrace{k, \cdots, k}_{t}, \underbrace{1, \cdots, 1}_{r})$.

(4.3) *Assume that $t\geqq 2$. Then for any two elements x_0 and x, of $\mathfrak{X}$, there exist elements $x_1, \cdots, x_s=x$ of $\mathfrak{X}$ such that $\mathfrak{D}(x_{i-1})\cap\mathfrak{D}(x_i)$ contains a nonidentity p-element for $i=1, \cdots, s$.*

PROOF. By (4.1), we may assume that $x_0=(V_1, V_2, \cdots, V_m)$, $x=(W_1, V_2, \cdots, V_m)$

and that $V_1+V_2=W_1+V_2$. If either V_1 or V_2 is one-dimensional, it follows that $m\geqq 3$ and that at least one of $V_3, \cdots, V_m$ is of dimension k. Since $GL(k, q)$ contains a nonidentity p-element, we conclude that $\mathfrak{D}(x_0)\cap\mathfrak{D}(x)$ contains a nonidentity p-element. If both V_1 and V_2 are of dimension k, we may assume $V_1\cap W_1=0$ (see (4.2)). Let $w_1, \cdots, w_k$ be a basis of W_1 and write $w_i=e_i+f_i$ with $e_i\in V_1$ and $f_i\in V_2$. Then clearly $e_1, \cdots, e_k$ and $f_1, \cdots, f_k$ are bases of V_1 and V_2, respectively. There exists nonidentity p-element g in $\mathfrak{D}(x_0)$ such that the matrix of $g|V_1$ coincides with that of $g|V_2$, i.e. a p-element g in $\mathfrak{D}(x_0)$ such that $e_ig=\sum g_{ij}e_j$ and $f_ig=\sum g_{ij}f_j$ for $i=1, \cdots, k$ with the same coefficients $g_{ij}\in GF(q)$. Clearly g is contained in $\mathfrak{D}(x)$. The proof is complete.

It is now easy to prove B* (4). We use the same notation as in (4.3). It suffices to show that Sylow p-subgroups of $\mathfrak{G}$ are all equivalent. We first note that each Sylow p-subgroup of $\mathfrak{G}$ contains a Sylow p-subgroup of $\mathfrak{D}(x)$ for some $x\in\mathfrak{X}$. Let $\mathfrak{P}_0$, $\mathfrak{P}$ be Sylow p-subgroups of $\mathfrak{G}$, and suppose that $\mathfrak{P}_0$, $\mathfrak{P}$ contain Sylow p-subgroups of $\mathfrak{D}(x_0)$ and $\mathfrak{D}(x)$, respectively. If $t\geqq 2$, then by (4.3), there exist elements $x_1, \cdots, x_s=x$ of $\mathfrak{X}$ such that $\mathfrak{D}(x_{i-1})\cap\mathfrak{D}(x_i)$ contains a nonidentity p-element. Since $t\geqq 2$, Sylow p-subgroups of $\mathfrak{D}(y)$ are all equivalent in $\mathfrak{D}(y)$ for every $y\in\mathfrak{X}$. Therefore $\mathfrak{P}_0\sim\mathfrak{P}$. The proof is complete.

4.4. The proof of B* (2) and B* (3).

Let V be a vector space of dimension n over $GF(q)$, and let p be an odd prime dividing $q-1$. Let $\mathfrak{G}'$ denote the special linear group $SL(V)$, $\mathfrak{Z}$ the center of $\mathfrak{G}'$, and set $\mathfrak{X}=\mathfrak{X}(\underbrace{1, 1, \cdots, 1}_{n})$. For each element $x=(V_1, \cdots, V_n)$ of $\mathfrak{X}$, we define $\mathfrak{D}'(x)=\mathfrak{D}(x)\cap\mathfrak{G}'$. $\mathfrak{D}'(x)$ is an abelian group of order $(q-1)^{n-1}$, and so has a unique Sylow p-subgroup $\mathfrak{D}'_p(x)$.

(4.4) *Assume $n\geqq 3$. Then for any two elements x_0 and x of $\mathfrak{X}$, there exist elements $x_1, \cdots, x_s=x$ of $\mathfrak{X}$ such that $\mathfrak{D}'_p(x_{i-1})\cap\mathfrak{D}'_p(x_i)\not\subseteq\mathfrak{Z}$ for $i=1, \cdots, s$, unless $p=n=3$ and $9\nmid q-1$.*

Proof. As in the proof of (4.3), we may assume that $x_0=(V_1, V_2, \cdots, V_n)$ and $x=(W_1, V_2, \cdots, V_n)$ with $W_1\subseteq V_1+V_2$. Let v_i be a nonzero element of V_i for each i. The assumption guarantees the existence of an element δ in $\mathfrak{D}'_p(x_0)$ such that $v_1\delta=av_1$, $v_2\delta=av_2$, $v_3\delta=bv_3, \cdots$, where a and b are distinct nonzero elements of $GF(q)$. Clearly δ is contained in $\mathfrak{D}'_p(x)$, but not in $\mathfrak{Z}$, q.e.d.

(4.5) *Let q be a prime power, and let p be an odd prime dividing $q-1$. If $n\geqq 3$, $PSL(n, q)$ has no p-strongly embedded proper subgroups unless $p=n=3$ and $9\nmid q-1$.*

PROOF. This is an immediate corollary of (4.4). We will show that Sylow p-subgroups of $PSL(n, q)$ are all equivalent. We use the same notation as in (4.4). Note that each Sylow p-subgroup of $\mathfrak{G}'$ contains $\mathfrak{D}'_p(x)$ for some $x \in \mathfrak{X}$. Let $\mathfrak{P}_0$, $\mathfrak{P}$ be Sylow p-subgroups of $\mathfrak{G}'$, and suppose that $\mathfrak{P}_0 \supseteq \mathfrak{D}'_p(x_0)$ and $\mathfrak{P} \supseteq \mathfrak{D}'_p(x)$. By (4.4), there exist elements $x_1, \cdots, x_s = x$ of $\mathfrak{X}$ such that $\mathfrak{D}'_p(x_{i-1}) \cap \mathfrak{D}'_p(x_i) \nsubseteq \mathfrak{Z}$ for $i=1, \cdots, s$. Choose a Sylow p-subgroup $\mathfrak{P}_i$ of $\mathfrak{G}'$ containing $\mathfrak{D}'_p(x_i)$ for $i=1, \cdots, s-1$, and set $\mathfrak{P}_s = \mathfrak{P}$. If we denote the image of $\mathfrak{P}_i$ in $PSL(V)$ by $\bar{\mathfrak{P}}_i$, $\bar{\mathfrak{P}}_{i-1}$ intersects $\bar{\mathfrak{P}}_i$ nontrivially for $i=1, \cdots, s$. Hence, $\bar{\mathfrak{P}}_0 \sim \bar{\mathfrak{P}}$, q.e.d.

In the rest of this paper, let q be a prime power such that $3 \| q-1$, i.e. $3 | q-1$ and $9 \nmid q-1$, and V be a 3-dimensional vector space over $GF(q)$. Set $\mathfrak{G} = GL(V)$, $\mathfrak{G}' = SL(V)$ and $\bar{\mathfrak{G}}' = PSL(V)$. Set $\mathfrak{X} = \mathfrak{X}(1, 1, 1)$. We define an equivalence relation in $\mathfrak{X}$ by: $x_0 \sim x$ if and only if there exist elements $x_1, \cdots x_s = x$ of $\mathfrak{X}$ such that, for $i=1, \cdots, s$, $\mathfrak{G}' \cap \mathfrak{M}(x_{i-1}) \cap \mathfrak{M}(x_i)$ contains a 3-element not contained in the center $\mathfrak{Z}$ of $\mathfrak{G}'$ (such an element is called a noncentral 3-element).

Let $\mathfrak{P}_0$, $\mathfrak{P}$ be Sylow 3-subgroups of $\mathfrak{G}'$. If there exist Sylow 3-subgroups $\mathfrak{P}_1, \cdots, \mathfrak{P}_t = \mathfrak{P}$ of $\mathfrak{G}'$ such that $\mathfrak{P}_{i-1} \cap \mathfrak{P}_i \neq \mathfrak{Z}$ for $i=1, \cdots, t$, we write $\mathfrak{P}_0 \approx \mathfrak{P}$. Let $\bar{\mathfrak{S}}$ denote the image in $\bar{\mathfrak{G}} = \mathfrak{G}/\mathfrak{Z}$ of a subset $\mathfrak{S}$ of $\mathfrak{G}$. Clearly, $\bar{\mathfrak{P}}_0$ is equivalent to $\bar{\mathfrak{P}}$ in $\bar{\mathfrak{G}}' = PSL(V)$ if and only if $\mathfrak{P}_0 \approx \mathfrak{P}$, for $\mathfrak{Z}$ is of order 3.

Since $3 | q-1$, $\mathfrak{P}$ is contained in $\mathfrak{M}(x)$ for some $x \in \mathfrak{X}$. Let $g \in \mathfrak{G}$. We will show that $\mathfrak{P} \approx \mathfrak{P}^g$ if and only if $x \sim xg$. Assume that $\mathfrak{P} \approx \mathfrak{P}^g$. By definition, there exist Sylow 3-subgroups $\mathfrak{P}_0 = \mathfrak{P}, \mathfrak{P}_1, \cdots, \mathfrak{P}_t = \mathfrak{P}^g$ of $\mathfrak{G}'$ such that $\mathfrak{P}_{i-1} \cap \mathfrak{P}_i \neq \mathfrak{Z}$ for $i=1, 2, \cdots, t$. For each i, $1 \leq i \leq t-1$, choose an $x_i \in \mathfrak{X}$ such that $\mathfrak{P}_i \subseteq \mathfrak{M}(x_i)$ and set $x_0 = x$, $x_t = xg$. Then $\mathfrak{P}_i \subseteq \mathfrak{M}(x_i)$ for $i=0, 1, \cdots, t$. Since $\mathfrak{G}' \cap \mathfrak{M}(x_{i-1}) \cap \mathfrak{M}(x_i) \supseteq \mathfrak{P}_{i-1} \cap \mathfrak{P}_i$, we have $x \sim xg$. Conversely, assume that $x \sim xg$. By definition, there exist elements $x_0 = x, x_1, x_2, \cdots, x_s = xg$ of $\mathfrak{X}$ such that $\mathfrak{G}' \cap \mathfrak{M}(x_{i-1}) \cap \mathfrak{M}(x_i)$ contains a noncentral 3-element g_i for $i=1, 2, \cdots, s$. Choose a Sylow 3-subgroup $\mathfrak{P}_{i-1}$ of $\mathfrak{G}' \cap \mathfrak{M}(x_{i-1})$ containing g_i, and a Sylow 3-subgroup $\mathfrak{Q}_i$ of $\mathfrak{G}' \cap \mathfrak{M}(x_i)$ containing g_i. For each $y \in \mathfrak{X}$, Sylow 3-subgroups of $\mathfrak{G}' \cap \mathfrak{M}(y)$ contain the unique Sylow 3-subgroup of $\mathfrak{D}' \cap \mathfrak{D}(y)$ which is elementary abelian of order 9. Hence $\mathfrak{P}_i \approx \mathfrak{Q}_i$ for $i=1, \cdots, s-1$, $\mathfrak{P}_0 \approx \mathfrak{P}$ and $\mathfrak{Q}_s \approx \mathfrak{P}^g$. Since $g_i \in \mathfrak{P}_{i-1} \cap \mathfrak{Q}_i - \mathfrak{Z}$, we conclude that $\mathfrak{P} \approx \mathfrak{P}^g$.

Thus, if we denote by $\mathfrak{S}(x)$ the subset of $\mathfrak{G}$ consisting of $g \in \mathfrak{G}$ such that $x \sim xg$, $\overline{\mathfrak{S}(x) \cap \mathfrak{G}'}$ becomes one of the minimal 3-strongly embedded subgroups of $\bar{\mathfrak{G}}' = PSL(V)$. Let $\mathfrak{M}$ denote the set of monomial matrices in $GL(3, q)$, and $\mathfrak{N}$ the set of all nonsingular matrices of the form:

$$\begin{bmatrix} a, & b, & c \\ c, & a, & b \\ b, & c, & a \end{bmatrix}, \quad a, b, c \in GF(q) . \tag{4.6}$$

Let $\mathfrak{H}$ be the subgroup of $GL(3, q)$ generated by $\mathfrak{M}$ and $\mathfrak{N}$: $\mathfrak{H}=\langle\mathfrak{M}, \mathfrak{N}\rangle$.

(4.7) *Let $x=(V_1, V_2, V_3)$ be an element of $\mathfrak{X}$, and let v_i be a nonzero element of V_i for $i=1, 2, 3$. Let g be an element of $\mathfrak{G}$. Then $x\sim xg$ if and only if the matrix of g with respect to the basis v_1, v_2, v_3 of V is contained in $\mathfrak{H}$.*

PROOF. First assume that $x\sim xg$. Let G denote the matrix of g with respect to the basis v_1, v_2, v_3. To show $G\in\mathfrak{H}$, it suffices to consider the case that $\mathfrak{G}'\cap\mathfrak{M}(x)\cap\mathfrak{M}(xg)$ contains a noncentral 3-element f. Set $W_i=V_ig$ and $w_i=v_ig$. Since f is of odd order, there are four possibilities for the action of f on V_i's and on W_i's. Namely, (i) $f\in\mathfrak{D}(x)\cap\mathfrak{D}(xg)$, (ii) $f\in\mathfrak{D}(x)$ but f permutes W_i's regularly, (iii) $f\in\mathfrak{D}(xg)$ but f permutes V_i's regularly or (iv) f acts regularly on both V_i's and on W_i's.

Case (i). In this case G must be contained in $\mathfrak{M}$, or equivalently $g\in\mathfrak{M}(x)$. For, if one of the W_i's, say W_1, differs from V_i's, w_1 is expressed in the form $w_1=b_1v_1+b_2v_2+b_3v_3$ where at least two of the b_i's, say b_1 and b_2, are not zero. Since f leaves W_1 invariant, $w_1f=cw_1$ for some c with $c^3=1$ because f is a 3-element and $3\|q-1$. Since f also leaves V_i's invariant and $\det(f)=1$, we have $v_if=a_iv_i$ for some a_i with $a_1a_2a_3=1$. It follows that $a_1=a_2=c$ whence $a_3=c^{-2}=c$. But this is not the case, since f is noncentral.

Case (ii). Since f leaves V_i invariant, we have $v_if=a_iv_i$ for some a_i with $a_i^3=1$. Suppose that f permutes w_1, w_2, w_3 cyclically and that $w_1=av_1+bv_2+cv_3$. Then G is of the form

$$\begin{bmatrix} 1, & 1, & 1 \\ a_1, & a_2, & a_3 \\ a_1^2, & a_2^2, & a_3^2 \end{bmatrix}\begin{bmatrix} a & & \\ & b & \\ & & c \end{bmatrix}. \tag{4.8}$$

Let ε be a primitive cube root of unity in $GF(q)$, and set

$$\begin{bmatrix} 1, & 1, & 1 \\ 1, & \varepsilon, & \varepsilon^2 \\ 1, & \varepsilon^2, & \varepsilon \end{bmatrix}=C. \tag{4.9}$$

The matrix on the left in the above expression of G is obtained by multiplying C by permutation matrices. But C is contained in $\mathfrak{H}$, for

$$C\begin{bmatrix} \varepsilon & & \\ & 1 & \\ & & 1 \end{bmatrix}=\begin{bmatrix} 1 & & \\ & & \varepsilon \\ & \varepsilon & \end{bmatrix}\begin{bmatrix} \varepsilon, & 1, & 1 \\ 1, & \varepsilon, & 1 \\ 1, & 1, & \varepsilon \end{bmatrix}.$$

Hence, G is contained in $\mathfrak{H}$. In general case, G is obtained by multiplying a matrix of the form (4.8) by monomial matrices.

Case (iii). By the above argument, the matrix of g^{-1} with respect to the basis w_1, w_2, w_3 is contained in $\mathfrak{H}$. Hence, $G\in\mathfrak{H}$.

Case (iv). Suppose that f permutes both v_1, v_2, v_3 and w_1, w_2, w_3 cyclically, and that $w_1=av_1+bv_2+cv_3$. Then G is of the form (4.6). In general case, G is obtained by multiplying a matrix of the form (4.6) by monomial matrices.

Conversely, assume that $G\in\mathfrak{H}$. As in the proof of (4.1), we may assume that $G\in\mathfrak{M}\cup\mathfrak{N}$. If $G\in\mathfrak{M}$, then $g\in\mathfrak{M}(x)$ or $x=xg$. If $G\in\mathfrak{N}$, the element of $\mathfrak{G}$ which permutes v_1, v_2, v_3 cyclically is a noncentral 3-element in $\mathfrak{G}'\cap\mathfrak{M}(x)\cap\mathfrak{M}(xg)$. The proof is complete.

(4.10) *If* $q=4$, *then* $\mathfrak{H}=U(3,2)$, *the general unitary group.*

PROOF. Let C be the matrix defined in (4.9) and set

$$A=\begin{bmatrix}\varepsilon, & 1, & 1\\ 1, & \varepsilon, & 1\\ 1, & 1, & \varepsilon\end{bmatrix}, \quad B=\begin{bmatrix}\varepsilon^2, & 1, & 1\\ 1, & \varepsilon^2, & 1\\ 1, & 1, & \varepsilon^2\end{bmatrix}=A^{-1}.$$

Let T be a matrix of the form (4.6) not contained in $\mathfrak{M}$, and set $d=\det(T)$. Then $d=(a+b+c)(a^2+b^2+c^2-ab-bc-ca)$. In order that $d\neq 0$, a, b and c must be non-zero elements of $GF(4)$ two of which coincide. For, if $a=0$, then $d=(b+c)(b^2+c^2-bc)$. Since $T\in\mathfrak{M}$, $bc\neq 0$ and $b\neq c$. If $c=1$, then $d=(b+1)(b^2+b+1)=0$. So $b\neq 1\neq c$ and $c=b^2$. But then $d=(b+b^2)(b^2+b+1)=0$, a contradiction. This implies that $T\in\langle\mathfrak{M}, A, B\rangle$. Clearly $\mathfrak{M}$ and A are contained in $GU(3,2)$. Comparing the order we conclude that $\mathfrak{H}=GU(3,2)$ or $|\mathfrak{H}:\mathfrak{M}|=2$. The latter case does not occur since

$$A^{-1}\begin{bmatrix}\varepsilon & & \\ & 1 & \\ & & 1\end{bmatrix}A=\begin{bmatrix}\varepsilon & & \\ & 1 & \\ & & 1\end{bmatrix}C.$$

(4.11) *If* $3\|q-1$ *and* $q\neq 4$, *then* $PSL(3,q)$ *has no* 3-*strongly embedded proper subgroups.*

PROOF. It has been shown that $\overline{\mathfrak{G}'\cap\mathfrak{H}}$ is one of the minimal 3-strongly embedded subgroups of $PSL(V)$. We will derive a contradiction by assuming $\overline{\mathfrak{G}'\cap\mathfrak{H}}\subsetneqq PSL(V)$. Let $\mathfrak{K}$ be a maximal subgroup of $PSL(V)$ containing $\overline{\mathfrak{G}'\cap\mathfrak{H}}$. Since $\mathfrak{K}$ properly contains $\overline{\mathfrak{G}'\cap\mathfrak{M}}$, $\mathfrak{K}$ satisfies the condition

(1) $$2(q-1)^2|k=|\mathfrak{K}| \text{ and } 2(q-1)^2\neq k.$$

By (2.3), (2.4) and the simplicity of $PSL(3,q)$, we have

(2) $$O^3(\mathfrak{K})=\mathfrak{K}.$$

On the other hand, candidates for the maximal subgroups of $PSL(3,q)$ have been obtained by Mitchell [4] and Hartley [3]. Quoting their results, we see that $\mathfrak{K}$ must be of one of the following types.

Set $q=p^m$, where p is a prime.

Type 1. $k=(p^m+1)p^{3m}(p^m-1)^2/3$.

Type 2. $k=p^{2m}+p^m+1$

Type 3. $k=(p^m+1)p^m(p^m-1)$

Type 4. $\mathfrak{K}\simeq PSL(3, p^r)$, m/r is a prime.

Type 5. $\mathfrak{K}$ contains a normal subgroup of index 3.

Type 6. $\mathfrak{K}\simeq PSU(3, p^r)$, $2r=m$.

Type 7. $k=36$, 72 or 168, $p\neq 2$.

Type 8. $k=360$, $p\neq 2$, m is even or m is odd and $p\geqq 17$.

Type 9. $k=720$ or 2520, $p=5$, m is even.

If $\mathfrak{K}$ is of type 1, 2 or 3, then $3\| k$, contrary to (1). Assume that $\mathfrak{K}$ is of type 4. Then $k=p^{3r}(p^r-1)^2(p^r+1)(p^{2r}+p^r+1)/(3, p^r-1)$. Set $m=rl$. Then, $(p^m-1)=(p^r-1)((p^r)^{l-1}+\cdots+p^r+1)$. By (1), we have $\{(p^r)^{l-1}+\cdots+p^r+1\}^2|(p^r+1)(p^{2r}+p^r+1)$. Hence $l=2$ and $(p^r+1)|(p^{2r}+p^r+1)=(p^r+1)^2-p^r$, a contradiction. If $\mathfrak{K}$ is of type 5, $\mathfrak{K}$ does not satisfy (2). Assume that $\mathfrak{K}$ is of type 6. Then $k=p^{3r}(p^r-1)(p^r+1)^2(p^{2r}-p^r+1)/(p^r+1, 3)$. Since $m=2r$, we have $(p^r-1)|(p^{2r}-p^r+1)=(p^r-1)^2+p^r$. This contradicts the assumption that $p^m\neq 4$. Assume that $\mathfrak{K}$ is of type 7. If $k=72$, then $(p^m-1)|6$ and (1) does not hold. If $k=36$, then $(p^m-1)|3$ and $p^m=2$ or 4, a contradiction. If $k=168$, then $(p^m-1)|2$ and $p^m=2$ or 3, a contradiction. Assume that $\mathfrak{K}$ is of type 8. Then $(p^m-1)|6$ and $p^m=2$, 3, 4 or 7, a contradiction. If $\mathfrak{K}$ is of type 9, then $(p^m=1)|6$, again a contradiction. The proof is complete.

Lemma (4.11) completes the proof of Theorem B*.

REMARK. By a similar method and by using (2.5), it can be shown that $PSU(3, 2)$ is a maximal subgroup of $PSL(3, 4)$. Let $\mathfrak{K}$ be a maximal subgroup of $PSL(3, 4)$ containing $PSU(3, 2)$. Then $\mathfrak{K}$ is of type i, $1\leqq i\leqq 6$, with $p^m=4$, or $k=|\mathfrak{K}|=360$. Since $PSU(3, 2)$ is a 3-strongly embedded subgroup of $PSL(3, 4)$, (1) and (2) hold. If $k=360$, then the index of $\mathfrak{K}$ in $PSL(3, 4)$ is 14. This contradicts (2.5). Hence $\mathfrak{K}=PSU(3, 2)$.

References

[1] Bender, H., Transitive Gruppen gerader Ordnung, in denen jede Involution genau einen Punkt festläßt, J. Algebra **17** (1971), 527-554.

[2] Goldschmidt, D. M., A conjugation family for finite groups, J. Algebra **16** (1970), 138-142.

[3] Hartley, R. W., Determination of the ternary collineation groups whose coefficients

lie in the $GF(2^n)$, Ann. of Math. **27** (1926), 140-158.
[4] Mitchell, H. H., Determination of the ordinary and modular ternary linear groups, Trans. Amer. Math. Soc. **12** (1911), 207-242.
[5] Weir, A., Sylow p-subgroups of the classical groups over finite fields with characteristic prime to p, Proc. Amer. Math. Soc. **6** (1955), 529-533.
[6] Wielandt, H., Die Existenz von Normalteilern in endlichen Gruppen, Math. Nachr. **18** (1959), 274-280.

(Received October 25, 1971)

Departmeat of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo
113 Japan