SYLOW $p$-SUBGROUPS OF THE CLASSICAL GROUPS OVER FINITE FIELDS WITH CHARACTERISTIC PRIME TO $p$

A. J. WEIR

If $S_n$ is a Sylow $p$-subgroup of the symmetric group of degree $p^n$, then any group of order $p^n$ may be imbedded in $S_n$. We may express $S_n$ as the complete product\(^1\) $C \circ C \circ \cdots \circ C$ of $n$ cyclic groups of order $p$ and the purpose of this paper is to show that any Sylow $p$-subgroup of a classical group (see §1) over the finite field $GF(q)$ with $q$ elements, where $(q, p) = 1$, is expressible as a direct product of basic subgroups $S_n \cong C \circ C \circ \cdots \circ C$ ($n$ factors), where $C$ is cyclic of order $p^r$. (We assume always that $p \neq 2$.) Since $C$ may be imbedded in $S_r$, we see that $S_n$ is imbedded in $S_{n+r-1}$ in a particularly simple way. The above $r$ is defined by the equation $q^r - 1 = p^r \cdot \ast$ where $q^r$ is the first power of $q$ which is congruent to 1 mod $p$ and $\ast$ denotes some unspecified number prime to $p$. The case $r = 1$ is therefore of frequent occurrence, and then clearly $S_n \cong S_n$.

Professor Philip Hall was my research supervisor in Cambridge (England) during the years 1949–1952 and it is a pleasure to acknowledge here my indebtedness to him for his generous encouragement.

1. We shall refer to the following groups as the Classical Groups:\(^2\)

I. The general linear group $GL(n, q)$ is the group of all nonsingular $(n \times n)$ matrices with coefficients in $GF(q)$. The order of $GL(n, q)$ is

$$q^n(n-1)/2(q-1)(q^2-1) \cdots (q^n-1).$$

II. The symplectic group (Komplexgruppe) $C(2m, q)$ is the group of all $(2m \times 2m)$ matrices with coefficients in $GF(q)$ which leave invariant a given nonsingular skew-symmetric form. For different choices of skew-symmetric form all the symplectic groups are isomorphic and their order is

$$q^m(q^2-1)(q^4-1) \cdots (q^{2m}-1).$$

III. The unitary group $U(n, q^2)$ is the group of all $(n \times n)$ matrices with coefficients in $GF(q^2)$ which leave invariant a given nonsingular Hermitian form. (Hermitian has its usual meaning if we write $\bar{a} = a^q$)

\(^1\) The notion of complete product is carefully discussed in [1] and a summary given in [2]. A discussion of the groups $S_n$ in these terms will be found in [3].

\(^2\) See [4] and [5]. We use here the notation of [5].

Received by the editors April 5, 1954.
in $GF(q^2)$. Again there is essentially only one $U(n, q^2)$. The order is

$$q^{n(n-1)/2}(q + 1)(q^2 - 1)(q^3 + 1) \cdots (q^n - (-1)^n).$$

IV. The orthogonal groups $O_D(n, q)$ are the groups of all $(n \times n)$ matrices with coefficients in $GF(q)$ which leave invariant a given nonsingular quadratic form with discriminant $D$. For $n = 2m + 1$ there is essentially only one $O_D(n, q)$. The order is $q^m(q^2 - 1)(q^4 - 1) \cdots (q^{2m} - 1)$.

For $n = 2m$, there are two types, $O_1(n, q)$ and $O_2(n, q)$, depending on whether or not $D$ is a square in $GF(q)$. The symbol $\nu$ denotes a nonsquare in $GF(q)$. Their orders are

$$q^{m(m-1)}(q^2 - 1)(q^4 - 1) \cdots (q^{2m-2} - 1)(q^m - \nu^m)$$

where $\epsilon = (-1)^{m-1/2}$ and $\sigma = 1$ for $O_1$, $\sigma = -1$ for $O_2$.

2. The general linear group. Let $e$ be the least positive integer for which $p$ divides $q^e - 1$ and suppose that $q^e = 1 + p^{e^*}$ where $e^*$ denotes some unspecified number prime to $p$. It follows that

$$q^{te} = 1 + tp^{e^*} + C_{1,t} p^{2e^*} + \cdots \quad (t \text{ integer } > 1).$$

If $t = p^{e^*}$ where $s$ is an integer $> 0$,

$$q^{te} = 1 + p^{e^*} + C_{1,t} p^{2e^*} + \cdots .$$

Now $p \neq 2$, so that $C_{1,t}$ is divisible by $p^{e^*}$ and the subsequent terms are divisible by $p^{e^*+1}$. Hence,

$$q^{te} = 1 + p^{e^*} \quad \text{where } t = p^{e^*}. \quad \text{[True even if } s = 0].$$

Suppose $n = c + ea$ ($0 \leq c < e$) and $a = a_0 + a_1 p + \cdots + a_e p^e$ ($0 \leq a_i < p$). The factors of the order of $GL(n, q)$ which are divisible by $p$ are $q^e - 1, q^{2e} - 1, \cdots, q^{ae} - 1$. The number of these factors which are divisible by $p^{e^*}$ is $[a/p^s]$. (See (1).) Hence $p$ divides the order of $GL(n, q)$ $N$ times where $N = ra + [a/p] + [a/p^2] + \cdots$, i.e.

$$N = ra + \sum a_i \mu_i(p) \text{ where } \mu_i(p) = 1 + p + \cdots + p^{i-1}.$$

In particular when $n = e, ep, \cdots, ep^i$ we obtain $N_0 = r, N_1 = rp + 1, \cdots, N_i = rp^{i+1} + \mu_i(p)$. If $G_0, G_1, \cdots$ are the corresponding Sylow $p$-subgroups, $N = \sum a_i N_i$ so the direct product $\Pi = \prod G_i$ is a group of order $p^N$ and degree $\sum a_i e^{p^i} = ea$. By introducing a diagonal block $1_e$ we imbed $\Pi$ in a Sylow $p$-subgroup of $GL(n, q)$.

Consider the Sylow $p$-subgroup $G_0$ of $GL(e, q)$. We may regard $GF(q^e)$ as a vector space of dimension $e$ over the field $GF(q)$ and so we can find a basis $a_1, \cdots, a_e$. Given $x \in GF(q^e)$ we define the matrix

\[ There is a term $q^{e^*}$ missing after $e^*$ in the formula in [5, §6]. \]
(x_{ij}) by the equation \( x = \sum x_{ij} a_j \) and then the mapping \( x \rightarrow (x_{ij}) \) is an isomorphism of the multiplicative group of \( GF(q^e) \) into \( GL(e, q) \). Hence \( GL(e, q) \) contains a cyclic subgroup of order \( q^e - 1 = p^r \star \) and \( G_0 \) is therefore cyclic of order \( p^r \). We write \( C = G_0 \).

If \( A, B \) are groups of permutation matrices of degrees \( m, n \) respectively and orders \( a, b \) respectively, then \( A \circ B \) is a group of permutation matrices of degree \( mn \) and order \( a^n b^r \).

We may define \( G_i \) inductively: \( G_0 = C, G_i = G_{i-1} \circ C \) for then \( G_i \) has order \( p^{N_i} \) and degree \( e^i \). In the special case \( r = 1, G_i \cong S_{e^{i+1}} \) and so we rename \( G_i = S_{e^{i+1}} \). In other words \( S_n \cong C \circ C \circ \cdots \circ C \) (\( n \) factors).

3. The symplectic group. If \( e \) is even, the factors of the order of \( C(2m, q) \) which are divisible by \( p \) are again \( q^e - 1, q^{2e} - 1, \cdots \) and so a Sylow \( p \)-subgroup of \( C(2m, q) \) is already a Sylow \( p \)-subgroup of \( GL(2m, q) \).

If \( e \) is odd, the factors which are divisible by \( p \) are \( q^{2e} - 1, q^{4e} - 1, \cdots, q^{2ne} - 1 \) where \( 2m = d + 2eb \) (\( 0 \leq d < 2e \)). Since \( p \neq 2 \), the number of these factors which are divisible by \( p^{r+1} \) is \( \lceil b/p^e \rceil \) and if \( b = b_0 + b_1 p + \cdots + b_r p^r \) (\( 0 \leq b_i < p \)) the order of a Sylow \( p \)-subgroup is \( p^M \) where \( M = rb + \sum b_i \mu_i(p) \). The particular values \( 2m = 2e, 2ep, \cdots \) again give Sylow \( p \)-subgroups \( G_0, G_1, \cdots \) of orders \( N_0, N_1, \cdots \) and a Sylow \( p \)-subgroup of \( C(2m, q) \) is of the form \( \Pi = \prod G_i \). [The matrix of the skew-symmetric form left invariant by \( \Pi \) is a diagonal sum of constituent blocks \( J_i \) belonging to the \( G_i \).]

We may again define the \( G_i \) inductively: \( G_i = G_{i-1} \circ C \). (The matrix \( J_i \) of \( G_i \) is the diagonal sum of \( p \) matrices \( J_{i-1} \).)

It remains to show that \( G_0 \) is cyclic. Consider the subgroup \( R \) of \( GL_{2e}(q) \) of all

\[
T = \begin{pmatrix}
A & 0 \\
0 & B
\end{pmatrix}
\]

satisfying \( T^t J T = J \) where \( A, B \subseteq S_1 \subseteq GL_e(q) \) and

\[
J = \begin{pmatrix}
0 & 1 \\
-1 & 0
\end{pmatrix}.
\]

The condition on \( A, B \) is \( A^t B = 1 \) so that \( R \) is isomorphic to \( S_1 \) and is cyclic of order \( p^r \). Hence \( G_0 \) is cyclic of order \( p^r \).

If we write \( G_0 = \overline{C} \) (now of degree \( 2e \)), the Sylow \( p \)-subgroups of \( C(2m, q) \) may be expressed as direct products of \( \overline{S}_e \cong \overline{C} \circ C \circ \cdots \circ C \).

4. The unitary group. Suppose \( e \) is odd. If \( f \) is odd then \( q^f + 1 \) is

* See [3, §2]. It is shown there that the operation \( \circ \) is associative.
prime to $p$ (otherwise $q^{t_{e}} \equiv -1 \pmod{p}$ ($p \neq 2$)). The factors of the order of $U(n, q^{2})$ which are divisible by $p$ are

$$q^{2e} - 1, q^{4e} - 1, \ldots, q^{2be} - 1$$

where $n = d + 2eb$ ($0 \leq d < 2e$), and so in this case we are reduced to the same type of construction as in §3. $G_{0}$ is again of degree $2e$ and by using the matrix

$$J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

as above we verify that $G_{0}$ is cyclic of order $p^{r}$.

Suppose $e = 2e$. Now $q^{e} = 1 + p^{r} \cdot s$ and $q^{e} - 1$ is prime to $p$ (by the definition of $e$); hence $q^{e} = -1 + p^{r} \cdot s$. If $t$ is an integer greater than 1 then

$$q^{t_{e}} = (-1)^{t} \left[ 1 - t p^{r} \cdot s + C_{t,2} p^{2r} \cdot s \ldots \right].$$

There are two cases to consider:

(i) If $e$ is odd, $q^{t_{e}} - (-1)^{t_{e}} = p^{r} \cdot s$ where $t = p^{r} \cdot s$, and also $q^{2t_{e}} - 1 = p^{r} \cdot s$ so that a Sylow $p$-subgroup of $U(n, q^{2})$ is already a Sylow $p$-subgroup of $GL(n, q^{2})$.

(ii) If $e$ is even, the factors of the order of $U(n, q^{2})$ which are divisible by $p$ are $q^{e} - 1$, $q^{2e} - 1$, $\ldots$, $q^{ae} - 1$ where $n = c + ea$ ($0 \leq c < e$), and we may use the construction of §2.

With

$$J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{(of degree $e$)},$$

we may verify that $G_{0}$ is cyclic of order $p^{r}$.

5. The orthogonal groups. If $e$ is even, a Sylow $p$-subgroup of $O(2m + 1, q)$ is already a Sylow $p$-subgroup of $GL(2m + 1, q)$.

If $e$ is odd, we may use the construction of §3 and verify that $G_{0}$ is cyclic of order $p^{r}$ using

$$J = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1. \\ 0 & 1. & 0 \end{pmatrix} \quad \text{(of degree $2e + 1$).}$$

If $L \in O_{D}(n, q)$ then

$$\begin{pmatrix} 1 & 0 \\ 0 & L \end{pmatrix} \in O_{D}(n + 1, q).$$
and so we may imbed $O_D(n, q)$ in $O_D(n+1, q)$ in a natural way.

Consider $q^m+1, q^m-1$. One at least is prime to $p$, and their product is $q^{2m}-1$. In terms of the above imbedding a Sylow $p$-subgroup of $O_D(2m, q)$ is already a Sylow $p$-subgroup of $O_D(2m+1, q)$ or of $O_D(2m-1, q)$.

Finally we may sum up the results of §2–§5: The Sylow $p$-subgroups of the classical groups over $GF(q)$ ($q$ prime to $p$) are all expressible as direct products of the basic subgroups $S_n \cong C \circ C \circ \cdots \circ C$.

**Bibliography**


**Princeton University**