SYLOW p-SUBGROUPS OF THE GENERAL LINEAR GROUP OVER FINITE FIELDS OF CHARACTERISTIC p

A. J. WEIR

If K is the finite field $GF(q)$ with $q=p^k$ elements then the general linear group $GL_n(K)$ has order

$$q^{n(n-1)/2}(q-1)\cdots(q^n-1).$$[1]

Let e_{ij} denote the matrix with the 1 of K in the (i, j) position and 0 elsewhere; we shall call any matrix of the form $1+\sum_{i<j} a_{ij}e_{ij}$ 1-*triangular*. The group G_n of all 1-triangular matrices in $GL_n(K)$ is a Sylow p-subgroup of $GL_n(K)$. We shall often write G for G_n if this is unambiguous. p is assumed throughout to be an odd prime.

The generators $1+ae_{i,i+1}$ and the fundamental relations connecting them are studied carefully in a recent paper by Pavlov[2] (for the particular case $q=p$) and we have therefore mentioned them briefly in the opening paragraph.

When $i<j$ the group P_{ij} of all $1+ae_{ij}$ $(a\in K)$ is isomorphic to the additive group of K. Any subgroup P of G generated by these P_{ij} is characterised by a partition diagram $|P|$. These partition diagrams bear a strong resemblance to the row of "hauteurs" which define the "sous-groupes parallélotopiques" of the Sylow p-subgroups of the symmetric groups on p^n symbols, studied by Kaloujnine.[3] A necessary and sufficient condition is given for the partition subgroup P to be normal in G and if $P'=(P, G)$, $P^*/P=$centre of G/P, the duality between P' and P^* is emphasised by constructing their partition diagrams.

Certain "diagonal" automorphisms are introduced and used to prove that any characteristic subgroup of G is a normal partition subgroup. The maximal abelian normal subgroups are fully investigated and used in conjunction with the symmetry about the second diagonal to give a simple combinatorial proof that the characteristic subgroups of G are precisely those given by symmetric normal partitions. In the last section we finally identify the group of automorphisms of G.

Received by the editors February 15, 1954.

[1] Dickson, *Linear groups*.

[2] P. P. Pavlov, *Sylow p-subgroups of the full linear group over a simple field of characteristic p*, Izvestiya Akad. Nauk SSSR, Ser. Mat. vol. 16 (1952) pp. 437–458. [Russian]. Math. Reviews vol. 14 (1953) p. 533.

[3] L. Kaloujnine, *La structure des p-groupes de Sylow des groupes symétriques finis*, Ann. École Norm. vol. 65 (1948) pp. 239–276.

This paper is substantially the content of Chapter 5 of my Cambridge University Ph.D. Thesis (1953) and I should like to acknowledge here my gratitude to Professor Philip Hall who supervised this research in such a kind and encouraging way.

1. Generators of G_n.

$$e_{ij}e_{hk} = \begin{cases} e_{ik} & \text{if } j = h, \\ 0 & \text{if } j \neq h. \end{cases}$$

If $A = 1 + \sum_{i<j} a_{ij}e_{ij}$, then $r_s = \prod_{j>s} (1 + a_{sj}e_{sj}) = 1 + \sum_{j>s} a_{sj}e_{sj}$ has the same sth row as A. Then $r_{n-1}r_{n-2} \cdots r_1 = A$. Thus the set of all $1 + ae_{ij}$ $(a \in K,\ i<j)$ generate G.

Further if $u<v<w$, a, $b \in K$, we have the fundamental commutator relation

$$(1) \qquad (1 + ae_{uv},\ 1 + be_{vw}) = 1 + abe_{uw}.$$

Putting $b=1$; $u=i$, $v=i+1$ and $w=i+2, i+3, \cdots$ in succession we see that the set of elements $1 + ae_{i,i+1}$ $(a \in K;\ i = 1, \cdots, n-1)$ generate the group G_n.

2. The lower central series of G_n. We define H_k to be the set of all A for which $a_{ij} = 0$ for $0 < j - i < k$. If we write $\theta_0 > \theta_1 > \cdots$ for the derived series of G we have the following

THEOREM 1. (i) *The lower central series of G_n coincides with the series $H_1 > H_2 > \cdots > H_n = 1$.*

(ii) $(H_k, H_m) = H_{k+m}$.

(iii) $\theta_k = H_{2^k}$.

PROOF. Let V_k be the set of all L for which $1 + L \in H_k$. We verify immediately that $V_k V_m \subset V_{k+m}$. It follows that H_k is a group. Moreover if $1 + L \in G$, then $1 - L + L^2 \cdots$ terminates and must therefore be $(1+L)^{-1}$.

Say $A = 1 + L \in H_k$ and $B = 1 + M \in H_m$ then

$$\begin{aligned}(A, B) &= (1 + L)^{-1}\{(1 + M)^{-1} + L - ML + O_{2m+k}\}(1 + M) \\ &= (1 + L)^{-1}\{1 + L + LM - ML + O_{2m+k}\} \\ &= 1 + LM - ML + O_{2m+k} + O_{2k+m} \\ &= 1 + O_{k+m}, \qquad \text{where } O_k \text{ denotes "some element of } V_k\text{."}\end{aligned}$$

In other word $(H_k, H_m) \subset H_{k+m}$.

H_k is generated (with some generators to spare, in general) by the set of all $1 + a_{ij}e_{ij}$ $(a_{ij} \in K,\ j - i \geqq k)$. If now $w - u \geqq k + m$ we may find v so that $v - u \geqq k$ and $w - v \geqq m$, and we obtain the generators of

H_{k+m} in the form $1+ae_{uw}=(1+ae_{uv}, 1+e_{vw})$. Hence $(H_k, H_m)\supset H_{k+m}$, and so finally $(H_k, H_m)=H_{k+m}$.

In particular $(H_m, H_1)=H_{m+1}$. Since $H_1=G$, $H_1>H_2>\cdots>H_n=1$ is the lower central series of G_n.

The third part of the theorem follows immediately from the second by induction.

3. **The partition subgroups.** If $i<j$ the group P_{ij} of all $1+ae_{ij}$ ($a\in K$) is isomorphic to the additive group of K and so is elementary abelian of order q. Any subgroup P of G generated by a selection of these P_{ij} is called a *partition subgroup*. Such a subgroup may be characterised by a "partition" diagram $|P|$ in the natural way. For example (if $n\geqq 4$) the group generated by P_{12} and P_{24} contains also the subgroup P_{14} and $|P|$ consists of the squares $(1, 2)$, $(2, 4)$, $(1, 4)$. The sequence of diagrams for the lower central series is obtained from the whole diagram (representing G) by removing successive diagonals $j-i=1, 2, \cdots$.

THEOREM 2. *A necessary and sufficient condition for the partition subgroup P to be normal in G is that the boundary of $|P|$ should move monotonically downward and to the right.*

PROOF. If N is the least normal subgroup containing $1+ae_{ij}$, by the identity (1) it is clear that N must also contain P_{uj} and P_{iv} where $u<i$ and $v>j$. Further since $P_{iv}\subset N$ we have $P_{uv}\subset N$ where $u<i$, $v>j$. If $|N_{ij}|$ consists of the squares (u, v) with $u\leqq i$, $v\geqq j$ and if $|N'_{ij}|$ is $|N_{ij}|$ omitting (i, j), then N must contain N'_{ij}. The least normal subgroup containing P_{ij} is N_{ij}. We shall find it convenient to refer to this process as "completing the rectangle." Now if P is any normal partition subgroup and if (i, j) is any square in $|P|$, then P must contain N_{ij}. Conversely, the product of several N_{ij} is a normal subgroup of G. These remarks are equivalent to the statement of the theorem.

Given two distinct squares (i, j), (u, v) in $|G|$; if $u\leqq i$, $v\geqq j$ we shall say (i, j) *covers* (u, v). When $|P|$ is a normal partition we shall say $|P|$ *covers* (u, v) if some square of $|P|$ covers (u, v). If (u, v) covers some square outside $|P|$ we shall say (u, v) *avoids* $|P|$.

When P is a normal partition subgroup we may define the groups $P'=(P, G)$ and P^* where $P^*/P=$centre of G/P. Then P' and P^* are again normal partition subgroups. More precisely

THEOREM 3. *$|P'|$ consists of the squares covered by $|P|$, and $|P^*|$ consists of the squares which do not avoid $|P|$.*

PROOF. Let $|N|$ be the set of squares covered by $|P|$. By the process of completing the rectangle we see that P' contains N.

Now N is the product of normal subgroups N'_{ij} and so is normal. If $(i, j)\in|P|$, then $(1+ae_{ij}, 1+be_{km})\in N$. Any commutator (z, t) where $z\in P$, $t\in G$ may be expanded by application of the rule $(xy, rs) =(x, s)^y(x, r)^{sy}(y, r)^{sy}(y, s)$.[4] Hence $(P, G)\subset N$.

Let $|\overline{P}|$ be the set of squares which do not avoid $|P|$. We obtain $|\overline{P}|$ by adding one square to each row of $|P|$ except when this new square covers a square outside $|P|$. Clearly $(\overline{P}, G)\subset P$. If $A=1+\sum_{i<j} a_{ij}e_{ij}\notin\overline{P}$ then $a_{ij}\neq 0$ for some (i, j) avoiding $|P|$ and $(A, G)\not\subset P$. Hence $\overline{P}=P^*$. [We notice that the notation N'_{ij} already used is consistent with that of Theorem 3.]

Theorem 3 shows how strong is the duality between the groups P' and P^*. In particular we have as an immediate corollary

THEOREM 4. *The upper and lower central series of G coincide.*

4. The diagonal automorphisms. If W is the diagonal matrix

$$\begin{pmatrix} w_1 & & & & \\ & w_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & & w_n \end{pmatrix}$$

in $GL_n(K)$ and $A=1+\sum_{i<j} a_{ij}e_{ij}\in G_n$, then $W^{-1}AW=1+\sum_{i<j} a^*_{ij}e_{ij}$ where $a^*_{ij}=w_i^{-1}a_{ij}w_j$. Let D be the group of all such W.

PROPOSITION. *DG_n is the normalizer of G_n in $GL_n(K)$.*

PROOF. Clearly DG_n is contained in this normalizer.

Suppose $M=\sum_{i,j} b_{ij}e_{ij}$ where $b_{uv}\neq 0$ $(u>v)$, and v is as small as possible with respect to this property.

On the one hand $(1+e_{vu})M=M+\sum_j b_{uj}e_{vj}$ and this differs from M in the (v, v) position. On the other hand $M(1+\sum_{r<s} a_{rs}e_{rs})$ has in the (v, v) position the element $b_{vv}+\sum b_{vr}\sum_{r<v} a_{rv}=b_{vv}$ since the choice of b_{uv} implies that $b_{vr}=0$ for all $r<v$. Now $1+e_{vu}\in G_n$ and we have shown that $M^{-1}(1+e_{vu})M\notin G_n$. Thus M does not belong to the normalizer of G_n in $GL_n(K)$.

Any automorphism of G of the form $A\to W^{-1}AW$ where $W\in D$ is called a *diagonal* automorphism. Let $\mathcal{D}$ be the group of all diagonal automorphisms.

5. The normal partition subgroups. It is now possible to prove the following

---

[4] P. Hall, *A contribution to the theory of groups of prime-power order*, Proc. London Math. Soc. vol. 36 (1933).

THEOREM 5. *Any subgroup of G which is invariant under the inner and diagonal automorphisms is a normal partition subgroup.*

PROOF. Any matrix of G_{n+1} is expressible in the form

$$\begin{pmatrix} 1 & a \\ 0 & A \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = UV, \quad \text{say}$$

where $A \in G_n$ and a is a row with elements in K.

The group of all V is elementary abelian of order q^n and is normal in G_{n+1}. In this way it is possible to express G_{n+1} as the split extension $G_{n+1} \cong G_n H$ ($G_n \cap H = 1$).

The theorem is true for G_2 and we assume it to be true for G_n. Suppose R is a subgroup of G_{n+1} which is invariant under the inner and diagonal automorphisms of G_{n+1}. Then $R \cap G_n$ is a subgroup of G_n which is invariant under the inner and diagonal automorphisms of G_n and so by the induction hypothesis is a normal partition subgroup of G_n.

$R \cap H$ is a subgroup of H which is normal in G_{n+1} and invariant under diagonal automorphisms. Hence H is of the form N_{1j}. $\{$If $a = (\alpha_2, \cdots, \alpha_{n+1})$ and $\alpha_j \neq 0$ then H contains $P_{1,n+1}, P_{1n}, \cdots, P_{1j}.\}$

It is now sufficient to show that $R = (R \cap G_n)(R \cap H)$ for then the theorem follows by induction.

Clearly $R \supset (R \cap G_n)(R \cap H)$. The most general element of R is of the form

$$\begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = UV, \quad \text{say.}$$

If

$$W = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

then

$$W^{-1}UVW = UV^2 \in R \qquad (p \neq 2).$$

Hence $U, V \in R$. In other words $R \subset (R \cap G_n)(R \cap H)$.

REMARK. Since the diagonal automorphisms clearly leave invariant any partition subgroup, the converse of Theorem 5 is also true and so we may characterise the normal partition subgroups as those which are left invariant by the inner and diagonal automorphisms.

There is a further important automorphism of G_n which we may regard as a symmetry about the second diagonal:

$$\tau: \quad 1 + \sum a_{ij}e_{ij} \to 1 + \sum b_{ij}e_{ij} \quad \text{where} \quad b_{ij} = a_{n+1-j,n+1-i}.$$

In view of this we have the important

COROLLARY. *Every characteristic subgroup of G is a "symmetric" normal partition subgroup.*

6. The maximal abelian normal subgroups. The derived group θ_1 of G gives the maximal abelian quotient group. A natural dual of θ_1 would be a maximal abelian normal subgroup.[5] We shall determine the set of all maximal abelian normal subgroups of G.

If $A_i = N_{i,i+1}$ $(i=1, 2, \cdots, n-1)$ then A_i is clearly a normal (partition) subgroup. If (u, v) and $(u', v') \in |A_i|$ then $u' \leqq i < v$ and $(P_{uv}, P_{u'v'}) = 1$. Hence A_i is abelian. If $z \notin A_i$, that is if

$$z = 1 + \sum_{u<v} a_{uv}e_{uv}$$

and some $a_{uv} \neq 0$ where $u > i$ or $v \leqq i$, then $Gp[z, A_i]$ is not abelian.

(i) Say $u > i$. $(1 - e_{iu})z(1 + e_{iu})$ differs from z in (i, v) position.

(ii) Say $v \leqq i$. $(1 - e_{v,i+1})z(1 + e_{v,i+1})$ differs from z in the $(u, i+1)$ position.

We have now shown that A_i is a maximal abelian normal subgroup of G_n $(i=1, 2, \cdots, n-1)$.

A necessary and sufficient condition for $x \in G$ to belong to a maximal abelian normal subgroup of G is that x should commute with all its conjugates in G.

Consider G_3: if $x = 1 + e_{12} + e_{23}$ then x commutes with its conjugates all of which have the form $x + ae_{13}$ and so x is in a maximal abelian normal subgroup (clearly neither A_1 nor A_2). Though the A_i are the only partition subgroups which are maximal abelian normal we must expect other types of maximal abelian normal subgroups in general.

Suppose

$$1 + L = 1 + \sum_{u<v} a_{uv}e_{uv} \qquad (a_{uv} \in K),$$

$$1 + M = 1 + \sum_{u<v} b_{uv}e_{uv} \qquad (b_{uv} \in K)$$

then $(1+L)(1+M) = 1 + L + M + LM$ and so $1+L$, $1+M$ commute if and only if L, M commute.

Now

$$(1 - e_{ij})(1 + L)(1 + e_{ij}) = 1 + L + Le_{ij} - e_{ij}L$$

[5] H. Zassenhaus, *The theory of groups*, Chelsea, 1949, Chap. IV, 3.4, p. 115.

since $e_{ij}Le_{ij}=0$. Suppose $1+L$ belongs to a maximal abelian normal subgroup; then we require L to commute with $Le_{ij}-e_{ij}L$, in other words we require $Le_{ij}L-e_{ij}L^2-L^2e_{ij}+Le_{ij}L=0$ or $2Le_{ij}L=e_{ij}L^2+L^2e_{ij}$. Now

$$Le_{ij} = \sum_{u<i} a_{ui}e_{uj}, \qquad e_{ij}L = \sum_{j<v} a_{jv}e_{iv}.$$

Hence we require

$$2\sum_{j<t}\sum_{u<i} a_{ui}a_{jt}e_{ut} = \sum_{j<v<t} a_{jv}a_{vt}e_{it} + \sum_{w<u<i} a_{wu}a_{ui}e_{wj}.$$

Each of these three sums belongs to a separate part of the partition diagram of G, and so they all vanish $[p\neq 2]$.

We thus have the following three sets of equations:

$$\text{(i)} \quad \begin{aligned} a_{1i}\cdot a_{j,j+1} &= a_{1i}\cdot a_{j,j+2} = \cdots = a_{1i}\cdot a_{jn} = 0, \\ a_{2i}\cdot a_{j,j+1} &= a_{2i}\cdot a_{j,j+2} = \cdots = a_{2i}\cdot a_{jn} = 0, \\ &\cdots\cdots\cdots\cdots, \\ a_{i-2,i}a_{j,j+1} &= a_{i-2,i}a_{j,j+2} = \cdots = a_{i-2,i}a_{jn} = 0, \\ a_{i-1,i}a_{j,j+1} &= a_{i-1,i}a_{j,j+2} = \cdots = a_{i-1,i}a_{jn} = 0, \end{aligned}$$

$$\text{(ii)} \quad \begin{aligned} &a_{j,j+1}a_{j+1,j+2} = 0, \\ &a_{j,j+1}a_{j+1,j+3} + a_{j,j+2}a_{j+2,j+3} = 0, \\ &\cdots\cdots\cdots\cdots, \\ &a_{j,j+1}a_{j+1,n} + a_{j,j+2}a_{j+2,n} + \cdots + a_{j,n-1}a_{n-1,n} = 0, \end{aligned}$$

$$\text{(iii)} \quad \begin{aligned} a_{12}a_{2i} + a_{13}a_{3i} + \cdots \qquad & + a_{1,i-1}a_{i-1,i} = 0, \\ a_{23}a_{3i} + \cdots \qquad & + a_{2,i-1}a_{i-1,i} = 0, \\ \cdots\cdots\cdots\cdots&, \\ a_{i-3,i-2}a_{i-2,i} & + a_{i-3,i-1}a_{i-1,i} = 0, \\ & a_{i-2,i-1}\, a_{i-1,i} = 0, \end{aligned}$$

If there is one element a_{uv} in the diagonal $v-u=1$ which does not vanish, then by the last equation of (i) every other element in the same diagonal which is not adjacent to (u, v) must vanish, also the first equation of (ii) or the last equation of (iii) show that the adjacent ones vanish. Hence if $1+\sum_{u<v} a_{uv}e_{uv}$ belongs to a maximal abelian normal subgroup and has one nonzero element in the diagonal $v-u=1$, then all the other elements in this diagonal vanish.

Suppose now that the vth column is the first which is not composed entirely of zeros and a_{uv} the last nonvanishing element of it. In other words $a_{uv}\neq 0$ and $a_{ij}=0$ if $j<v$ and also if $j=v$, $i>u$. If $v=n$, $1+L\in A_{n-1}$ so we assume $v<n$.

There are two cases to consider: (a) $u>1$, (b) $u=1$.

(a) We may take $i=v$ in (i) and this gives $a_{uv}a_{j,j+1}=a_{uv}a_{j,j+2}=\cdots=0$ provided $j>v$. Thus $a_{rs}=0$ whenever $r>v$.

Take $j=u$ in (ii), then in the equation

$$a_{u,u+1}a_{u+1,m}+\cdots+a_{uv}a_{vm}+\cdots+a_{u,m-1}a_{m-1,m}=0$$

all the a_{rs} for which $s<v$ vanish by our choice of a_{uv}, and all the a_{rs} for which $r>v$ vanish by the result we have just proved. Thus $a_{vm}=0$ (all $m>v$).

Finally we have $a_{rs}=0$ whenever $r\geqq v$, and we now see that in this case $1+L\in A_{v-1}$.

(b) We may take $i=v$ in (i) and we find just as before that $a_{rs}=0$ whenever $r>v$.

The first equation of (iii) is

$$a_{12}a_{2i}+a_{13}a_{3i}+\cdots+a_{1v}a_{vi}+\cdots+a_{1,i-1}a_{i-1,i}=0.$$

Now $a_{12}=\cdots=a_{1,v-1}=0$ by our choice of a_{uv}, and $a_{rs}=0$ whenever $r>v$ by above, so that only one term remains in the equation. Thus $a_{vi}=0$ $(v<i<n)$.

Finally $a_{rs}=0$ whenever $r\geqq v$ except possibly a_{vn}. If $a_{vn}=0$, then just as before $1+L\in A_{v-1}$.

However in fact a_{vn} need not be zero and each of its possible $q-1$ nonzero values gives us a new maximal abelian normal subgroup. Any normal subgroup containing for example $x=1+e_{1v}+ce_{vn}$ must contain all the conjugates of x in G. Now $x^{-1}-1-e_{1v}-ce_{vn}+ce_{1n}$ and $(1-ae_{vw})x(1+ae_{vw})=x+ae_{1w}$. Hence any normal subgroup containing x must contain all $1+ae_{1w}$ for $w>v$, $a\in K$ and similarly must contain all $1+ae_{wn}$ for $w<v$, $a\in K$.

Suppose now that y belongs to an abelian normal subgroup containing x, and say $y=1+\sum_{i<j}a_{ij}e_{ij}$. Then y must commute with x and also with $1+e_{1w}$ (all $w>v$) and $1+e_{wn}$ (all $w<v$). This shows that $a_{rs}=0$ if $r\geqq v$, also if $s\leqq v$, except possibly $a_{1v}\neq 0$ or $a_{vn}\neq 0$ but in this case $ca_{1v}=a_{vn}$.

Thus $N_v(c)=Gp[1+ae_{1v}+cae_{vn},\ (a\in K)]\ N_{v-1,v+1}$ is the unique maximal abelian normal subgroup containing x.

The results of this section may be summarised in

THEOREM 6. *The maximal abelian normal subgroups of G_n fall into two distinct classes:*

$$A_i=N_{i,i+1}\qquad (i=1,2,\cdots,n-1),$$

$$N_v(c), \qquad \text{where} \quad c \neq 0, c \in K, (v = 2, \cdots, [n+1/2]).$$

7. **The characteristic subgroups.** We have the following fundamental

THEOREM 7. *The characteristic subgroups of G are precisely the normal partition subgroups whose partitions are symmetric about the second diagonal.*

PROOF. We consider the effect of an automorphism θ on the maximal abelian normal subgroups. Certainly it is clear that these must be permuted among themselves. All of the "exceptional" maximal abelian normal subgroups $N_v(c)$ except for $v=2$ are contained in H_2 and H_2 is characteristic in G. Also no A_i is contained in H_2 so we expect the A_i $(1<i<n-1)$ to be permuted by θ. These A_i divide naturally into pairs of groups with the same order, and for example we see that A_2 transforms under θ into itself or into A_{n-2}. Moreover θ leaves A_2 invariant if and only if θ leaves A_{n-2} invariant. Hence both A_2A_{n-2} and $N_{2,n-1}=A_2\cap A_{n-2}$ are characteristic subgroups of G_n.

The join of A_1, A_{n-1} and $N_2(c)$ is just A_1A_{n-1} and this again is characteristic in G_n.

If we write $r'=n+1-r$, then τ sends P_{rs} into $P_{s'r'}$. Any symmetric normal partition subgroup may be built up as a join of $N_{rs}N_{s'r'}$ $(r=1, 2, \cdots)$. But these may all be obtained as intersections of groups which we have shown to be characteristic. For example we intersect A_2A_{n-2} successively with A_3A_{n-3}, A_4A_{n-4}, $\cdots$ and then the square partition subgroups $N_{rr'}$ to obtain every $N_{2s}N_{s',n-1}$. Combining these results with the corollary to Theorem 5 we have the above theorem.

8. **The automorphisms of G_n.** Since the automorphisms of G have been completely determined by Palov[2] for the case of a ground field with p elements, we shall sketch the parts of this section which are merely generalizations of his work, and we shall also try as far as possible to use his notation.

The group $\mathfrak{I}$ of inner automorphisms is isomorphic to G_n/H_{n-1} and so has order $q^{(n^2-n-2)/2}$.

The diagonal automorphism induced by the diagonal matrix W is the identity if and only if W is a scalar matrx. Hence $\mathfrak{D}$ has order $(q-1)^{n-1}$.

The ground field K may be regarded as a vector space of dimension k over the field $GF(p)$ of integers mod p. Let $a_1, \cdots, a_k$ be a basis. The group $GL_k(p)$ of all nonsingular linear transformations of K induces a group $\mathfrak{L}$ of automorphisms of G: if $g\in GL_k(p)$ then γ is the induced automorphism which maps the generators $1+a_i e_{r,r+1}$ into $1+a_i^g e_{r,r+1}$ ($i=1, \cdots, k$; $r=1, \cdots, n-1$).

$\mathcal{L}\cap\mathcal{D}$ consists of the automorphisms induced by matrices of D of the form

$$\begin{pmatrix} a & & & & \\ & a^2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & a^n \end{pmatrix}, \qquad a \neq 0,\ a \in K.$$

For each $i=1, \cdots, k$; $r=1, \cdots, n-1$ there is a *central* automorphism τ_r^i which maps the one generator $1+a_i e_{r,r+1}$ into $1+a_i e_{r,r+1} + b_i e_{1n}$ (where b_i is an arbitrary element of K), and leaves the other generators invariant. For $r=1$ and $r=n-1$ these are already inner automorphisms. Let $\mathcal{Z}$ be the group generated by τ_r^i ($i=1, \cdots, k$; $r=2, \cdots, n-2$), then $\mathcal{Z}$ is elementary abelian of order $q^{k(n-3)}$.

There are two types of *extremal* automorphisms

$$\sigma_1(b): 1 + ae_{12} \to 1 + ae_{12} + abe_{2n} \qquad (b \in K),$$

and

$$\sigma_2(b): 1 + ae_{n-1,n} \to 1 + ae_{n-1,n} + abe_{1,n-1} \qquad (b \in K).$$

The group $\mathcal{U}$ generated by the extremal automorphisms is elementary abelian of order q^2. We write $\mathcal{P}=\mathcal{Z}\mathcal{U}$. (This is a direct product.)

THEOREM 8. *The group $\mathcal{A}$ of all automorphisms of G is generated by the subgroups* $[\tau]$, $\mathcal{L}$, $\mathcal{D}$, $\mathfrak{J}$, $\mathcal{P}$.

PROOF. If α is an automorphism which leaves H_2 elementwise invariant and which induces the identity automorphism on G/H_2, then α may be obtained by multiplying each element of G_n by an element in the centre (H_{n-2}) of H_2.[6] The central automorphisms are clearly of this type.

If $(1+e_{r,r+1})^\alpha = 1+e_{r,r+1}+be_{2n}$ and $r>1$, by commuting with $1+e_{12}$ we find an element in H_2 which is not invariant unless $b=0$.

If $(1+e_{12})^\alpha = 1+e_{12}+be_{2n}$, then since $1+e_{12}$, $1+ae_{12}$ commute we must have $(1+ae_{12})^\alpha = 1+ae_{12}+abe_{2n}$. There is a similar argument involving $1+ae_{n-1,n}$. It is now clear that $\alpha \in \mathcal{P}$.

It remains to be shown that if α is any automorphism of G then we may (simultaneously) copy the effect of α on H_2 and on G/H_2 using only the automorphisms of $[\tau]$, $\mathcal{L}$, $\mathcal{D}$ and $\mathfrak{J}$.

Under an automorphism α the subgroups A_i are either all left in-

[6] H. Zassenhaus, *The theory of groups*, Chap. 2, Exercise 6, p. 78.

variant or are all reflected in the second diagonal. By multiplying by τ if necessary we may assume that α leaves each A_i invariant.

If $(1+ae_{12})^\alpha = 1+\bar{a}e_{12}+\cdots$ (where the extra terms are in N_{13}) then $\{1+(ra+sb)e_{12}\}^\alpha = 1+(r\bar{a}+s\bar{b})e_{12}+\cdots$ where r, s are integers mod p. Hence α induces a linear transformation $a \to \bar{a}$ of the vector space K.

The set $\{1+a_ie_{r,r+1};\ (i=1,\cdots,k;\ r=1,\cdots,n-1)\}$ is a minimal system of generators of G_n. Hence $\{(1+a_ie_{12})^\alpha;\ (i=1,\cdots,k)\}$ is part of a minimal system of generators of G_n and $\bar{a}_1,\cdots,\bar{a}_k$ is again a basis of the vector space K. The linear transformation $a\to\bar{a}$ is thus nonsingular.

If $(1+ae_{23})^\alpha = 1+a'e_{23}+\cdots$, $a\to a'$ is again a linear transformation of K. Now the commutator $(1+ae_{12},\ 1+be_{23}) = 1+abe_{13}$ has the same value if we interchange a and b, and so $1+\bar{a}b'e_{13}+\cdots = 1+a'\bar{b}e_{13}+\cdots$. If $b\neq 0$, since N_{12} cannot map into N_{13} and N_{23} cannot map into N'_{23} neither $\bar{b}$ nor b' vanishes and $\bar{a}/\bar{b}=a'/b'$. The effect of α on P_{12} is thus the same as the effect on P_{23} apart from a constant factor. Since we may use a diagonal automorphism to give the required constant factors in $P_{23}, P_{34},\cdots, P_{n-1,n}$ there is an element β of $\mathcal{LD}$ which has the same effect as α on G_n mod H_2. Let us divide through by β and assume that α induces the identity on G/H_2.

We now look for an inner automorphism which has the same effect as α on H_2.

If, under α, $1+e_{23}\to 1+e_{23}+fe_{13}+ae_{24}$ (mod H_3) then by commuting with $1+de_{12}$ we see that $1+de_{13}\to 1+de_{13}+dae_{14}$ (mod H_4) (all $d\in K$). We transform by $1+ae_{34}$. This transformation also sends $1+e_{46}\to 1+e_{46}-ae_{36}$ (mod H_4) and $1+e_{47}\to 1+e_{47}-ae_{37}$ (mod H_5) but this is a necessary contribution since $1+e_{13}$, $1+e_{46}$ commute and $1+e_{67}\to 1+e_{67}$ (mod H_2).

If, under α, $1+e_{24}\to 1+e_{24}+be_{25}+ce_{14}$ (mod H_4) we transform by $1+be_{45}-ce_{12}$. This transformation also affects $1+e_{57}$ and $1+e_{58}$ but here again there is a necessary contribution.

By such inner automorphisms using elements in P_{ij}, $j-i=1$, we copy the effect of α on P_{ij} $(j-i=2)$ mod H_4 and P_{ij} $(j-i=3)$ mod H_5. Since H_2 is generated by the P_{ij} for which $j-i=2$, 3 we finally obtain an inner automorphism which has the same effect as α on H_2 by transforming successively by elements in P_{ij}, $j-i=1, 2, 3,\cdots$. This completes the proof of Theorem 8.

CAMBRIDGE UNIVERSITY