FINITE GROUPS HAVING UNIQUE PROPER CHARACTERISTIC SUBGROUPS. I

By D. R. TAUNT

Received 12 April 1954

1. *Introduction.* It is well known that a characteristically-simple finite group, that is, a group having no characteristic subgroup other than itself and the identity subgroup, must be either simple or the direct product of a number of isomorphic simple groups. It was suggested to the author by Prof. Hall that finite groups possessing exactly one proper characteristic subgroup would repay attention. We shall call a finite group having a unique proper characteristic subgroup a 'UCS group'. In the present paper we first give some results on direct products of isomorphic UCS groups, and then we consider in more detail one of the types of UCS groups which can exist, that consisting of groups whose orders are divisible by exactly two distinct primes.

Let K be a proper characteristic subgroup of a group G. Then any characteristic subgroup of K is characteristic in G; and if $L \supset K$ and is such that L/K is characteristic in G/K, then L is characteristic in G. Hence a necessary condition for K to be the unique proper characteristic subgroup of G is that K and G/K should be characteristically-simple. If either K or G/K is the direct product of simple groups of composite order, then G is insoluble; on the other hand, if both K and G/K are elementary Abelian groups of prime-power order, then G is soluble (and in fact is Abelian or metabelian). In the former case, the order (G) of G is divisible by at least three distinct primes, and in the latter case by at most two. There are two main classes of soluble UCS groups, namely groups of prime-power order and groups in which the order of the characteristic subgroup is prime to its index.

A soluble UCS group of the second kind will be an A-group of order $p^r q^s$, where p, q are distinct primes, and its characteristic subgroup will be a Sylow subgroup N, of order p^r (say). There must be more than one Sylow subgroup of order q^s, for otherwise G would have two distinct proper characteristic subgroups. If M is any of the Sylow q-subgroups, then M is a complement of N in G and we may write‡

$$G = \mathrm{Gp}\{M, N, \vartheta\},$$

where ϑ is the homomorphism of M into $\mathfrak{A}(N)$ defined by

$$n^{\vartheta(m)} = m^{-1}nm \ (m \in M, \ n \in N). \tag{1·1}$$

The characteristic subgroup N is the derived subgroup of G, and the centre of G is the identity. (This is a simple example of a general property of A-groups (1, 2).) It follows that ϑ must be an isomorphism, for any element of its kernel permutes with every element of N and hence belongs to the centre of G. Since further N is characteristic and M belongs to a characteristic class of conjugate subgroups, we have precisely

‡ Here we use the notation of (3)—subsequently referred to as 'R'.

https://doi.org/10.1017/S0305004100029881 Published online by Cambridge University Press

the situation considered in R, § 3, and we shall apply results obtained there to groups of this kind.

The prime-power UCS groups can be further subdivided into two types, comprising groups all of whose elements other than the identity are of prime order, and groups having some elements of order the square of a prime. We hope to return to the consideration of such groups later.

2. *Direct products of UCS groups.* The direct product of a number of isomorphic characteristically-simple groups is itself characteristically-simple. The corresponding result for UCS groups is not true without reservation. In the following theorem we give conditions under which the result does hold; we shall show by examples that the removal of the conditions may invalidate the conclusion.

THEOREM 2·1. *Let G be a UCS group with proper characteristic subgroup N, satisfying the following conditions:*

(i) *no element of G other than 1 is invariant under every automorphism of G;*

(ii) *no element of G/N other than N/N is invariant under every automorphism of G/N induced by an automorphism of G.*

Then the direct product of a finite number of groups, each isomorphic to G, is itself a UCS group.

Proof. Let $G^{[k]}$ be the group whose elements are all the rows $\mathbf{x} = (x_1, x_2, \ldots, x_k)$ of k elements of G, with multiplication defined by $\mathbf{xy} = \mathbf{z}$, $z_i = x_i y_i$; this group has identity $\mathbf{1} = (1, 1, \ldots, 1)$, and $\mathbf{x}^{-1} = (x_1^{-1}, x_2^{-1}, \ldots, x_k^{-1})$. It suffices to prove that, for any k, $G^{[k]}$ is a UCS group, since any direct product of k groups, each isomorphic to G, is isomorphic to $G^{[k]}$.

If H is any subgroup of G, we denote by H_i $(1 \leqslant i \leqslant k)$ that subgroup of $G^{[k]}$ consisting of all elements $\mathbf{x}$ with $x_i \in H$ and $x_j = 1$ if $j \neq i$. Then $H_1 H_2 \ldots H_k = H^{[k]}$.

The automorphism group of $G^{[k]}$ contains elements of two special kinds (but is not, in general, generated by them). If π is any permutation of the set $1, 2, \ldots, k$, mapping i onto $\pi(i)$, then the (1, 1) mapping θ_π of $G^{[k]}$ onto itself defined by

$$\mathbf{x}^{\theta_\pi} = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(k)})$$

is an automorphism. Also, if $\phi \in \mathfrak{A}(G)$, then for each i satisfying $1 \leqslant i \leqslant k$ an automorphism ϕ_i of $G^{[k]}$ is defined by $\mathbf{x}^{\phi_i} = (x_1, \ldots, x_{i-1}, x_i^{\phi}, x_{i+1}, \ldots, x_k)$.

Now let K be a characteristic subgroup of $G^{[k]}$, $K \neq \{\mathbf{1}\}$, and let x_i be a non-identical component of an element $\mathbf{x} \in K$. If $\phi \in \mathfrak{A}(G)$, then $\mathbf{y} = \mathbf{x}^{\phi_i}\mathbf{x}^{-1} \in K$; we have $y_i = x_i^{\phi} x_i^{-1}$, $y_j = 1$ if $j \neq i$. If $x_i \notin N$, we can (by hypothesis (ii)) choose ϕ so that $Nx_i^{\phi} \neq Nx_i$, whence $y_i \notin N$; if $x_i \in N$, we can (by hypothesis (i)) choose ϕ so that $y_i \neq 1$. If the smallest characteristic subgroup of G containing y_i is H, then $H_i \subset K$; hence $H_j \subset K$ for each j and so $H^{[k]} \subset K$. Thus if $x_i \notin N$, we have $G^{[k]} = K$; if $x_i \in N$, then $N^{[k]} \subset K$. But if for every $\mathbf{x} \in K$ we have $x_i \in N$ for each i, then $K \subset N^{[k]}$ and we deduce $K = N^{[k]}$. Thus the only possible proper characteristic subgroup of $G^{[k]}$ is $N^{[k]}$; and the fact that this is indeed characteristic follows at once, because $G^{[k]}$ is certainly not characteristically-simple.

In considering which UCS groups satisfy the hypothesis of the above theorem we may ignore Abelian UCS groups, for which the direct-product theorem is trivially

https://doi.org/10.1017/S0305004100029881 Published online by Cambridge University Press

true. An Abelian p-group G has characteristic subgroups $G^{(r)}$ and $G_{(s)}$, consisting respectively of all p^rth powers of elements of G, and of all elements whose orders divide p^s. If G is to be a UCS group we must have $G^{(2)} = G_{(0)} = \{1\}$, $G^{(1)} = G_{(1)}$, $G^{(0)} = G_{(2)} = G$; G has all its invariants equal to p^2 and has proper characteristic subgroup $G^{(1)}$. Conversely, if G has invariants all equal to p^2 it is a UCS group, and any direct product of groups isomorphic to G has the same property. This incidentally shows that hypotheses (i) and (ii) are not necessary, since the cyclic group of order 4 satisfies neither of them.

Suppose now that G is a non-Abelian UCS group, with proper characteristic subgroup N. If hypothesis (i) is not satisfied, there exists $x \in G$ invariant under every automorphism of G. Then $\{x\}$ is characteristic and can only be N; we deduce that *N is the centre of G and is of prime order.* Similarly, if hypothesis (ii) does not hold there exists $x \notin N$ such that $Nx^\phi = Nx$ for all $\phi \in \mathfrak{A}(G)$. Then $\{N, x\}$ is characteristic and must be G, showing that G/N is cyclic and hence that *N is of prime index in G.* Although neither of these conditions is sufficient for the corresponding hypothesis to be false, each enables us to establish the truth of the hypothesis in important cases. For example, if G is a non-Abelian p-group, N must be the centre and hence of index at least p^2, showing that (ii) is true.

One of the hypotheses fails immediately if either N or G/N is of order 2. Examples of UCS groups in which this occurs are the quaternion group Q of order 8, and the symmetric group S_m of degree m, where $m = 3$ or $m \geqslant 5$. We shall show that in neither case is the direct product of two isomorphic groups itself a UCS group.

If G is any non-Abelian UCS group, its centre Z is contained in its commutator subgroup G'. The groups Q, S_m have the further property that each has a unique minimal proper normal subgroup. If a group G has these two properties it is easy to find all the automorphisms of $G^{[2]}$. If $\theta \in \mathfrak{A}(G^{[2]})$, endomorphisms θ_i $(i = 1, 2, 3, 4)$ of G are defined by $(x, y)^\theta = (x, 1)^\theta (1, y)^\theta = (x^{\theta_1}, x^{\theta_2})(y^{\theta_3}, y^{\theta_4})$. Since θ is homomorphic, $(x'x, yy')^\theta = (x', y)^\theta (x, y')^\theta$, implying that $x^{\theta_1} y^{\theta_3} = y^{\theta_1} x^{\theta_3}$ and $x^{\theta_2} y^{\theta_4} = y^{\theta_4} x^{\theta_2}$ for all $x, y \in G$. Conversely, if (for $1 \leqslant i \leqslant 4$) θ_i is an endomorphism of G with kernel K_i and image H_i, then the mapping θ of $G^{[2]}$ into itself defined by $(x, y)^\theta = (x^{\theta_1} y^{\theta_3}, x^{\theta_2} y^{\theta_4})$ is an endomorphism of $G^{[2]}$ if $[H_1, H_3] = [H_2, H_4] = \{1\}$ (where square brackets denote commutators). Further, θ is $(1, 1)$ if $x^{\theta_1} y^{\theta_3} = x^{\theta_2} y^{\theta_4} = 1$ implies $x = y = 1$. Necessary conditions for this, obtained by setting $y = 1$ and $x = 1$ in turn, are

$$K_1 \cap K_2 = K_3 \cap K_4 = \{1\}.$$

In the special case we are considering, these conditions are also sufficient. For now $K_1 \cap K_2 = \{1\}$ implies that $K_1 = \{1\}$ or $K_2 = \{1\}$. If $K_1 = \{1\}$, then $H_1 = G$, $H_3 \subset Z$, $K_3 \neq \{1\}$, $K_4 = \{1\}$, $H_4 = G$, $H_2 \subset Z$. Also $H_3 \subset Z$ implies that $K_3 \supset G' \supset Z$, and similarly $K_2 \supset Z$. But if $x^{\theta_1} y^{\theta_3} = x^{\theta_2} y^{\theta_4} = 1$, we have, since $y^{\theta_3} \in Z$, that $x^{\theta_1} \in Z$, $x \in Z$, $x^{\theta_2} = 1$, $y^{\theta_4} = 1, y = 1, x^{\theta_1} = 1, x = 1$; so θ is an automorphism. Similarly, θ is an automorphism if θ_2, $\theta_3 \in \mathfrak{A}(G)$ and H_1, H_4 are contained in Z; and these two types exhaust the automorphisms of $G^{[2]}$.

Suppose now that G is the quaternion group Q, consisting of the 8 elements ± 1, $\pm i$, $\pm j$, $\pm k$ with the rules of calculation $i^2 = j^2 = k^2 = -1$, $jk = -kj = i$, etc. Then $N = G' = Z = \{-1\}$, and $N^{[2]}$ is characteristic in $G^{[2]}$, being both its centre and com-

https://doi.org/10.1017/S0305004100029881 Published online by Cambridge University Press

mutator subgroup. But also, if $\theta \in \mathfrak{A}(G^{[2]})$, $(-1,-1)^\theta = ((-1)^{\theta_1}(-1)^{\theta_3}, (-1)^{\theta_2}(-1)^{\theta_4}) = (-1,-1)$, since $(-1)^{\theta_i}$ has value -1 or 1 according as θ_i is an automorphism or a proper endomorphism of G. Thus $G^{[2]}$ has a characteristic subgroup of order 2 as well as $N^{[2]}$ of order 4, and is therefore not a UCS group.

In our other example $G = S_m$, with $m = 3$ or $m \geqslant 5$, $N = G' = A_m$, the alternating group of degree m, and $Z = \{1\}$. Then $N^{[2]}$ is the commutator subgroup of $G^{[2]}$ and is therefore characteristic, of index 4. The only automorphisms of $G^{[2]}$ are of form $(x,y)^\theta = (x^{\theta_1}, y^{\theta_4})$ or $(x,y)^\theta = (y^{\theta_3}, x^{\theta_2})$, where $\theta_i \in \mathfrak{A}(G)$. If we regard $G^{[2]}$ as an intransitive permutation group of degree $2m$, we see that it has a subgroup K of index 2, consisting of all the even permutations. But (x,y) is even if either *both* or *neither* of x, y is even, and this property is evidently preserved under any of the automorphisms of $G^{[2]}$. It follows that K is characteristic but distinct from $N^{[2]}$, and again G is not a UCS group. We remark that (G) has two distinct prime factors, or more than two, according as $m = 3$ or $m \geqslant 5$, so that we have counter-examples from two of our main types of group.

Another simple example of this phenomenon (with N of index 3 in G) is afforded by the group $G = \{x, y\}$, where $x^7 = y^3 = 1$, $y^{-1}xy = x^2$. If $\theta \in \mathfrak{A}(G)$, then it is easily seen that $x^\theta = x^r$, $y^\theta = x^s y$, where r, s are integers and r is not a multiple of 7. The subgroup of $G^{[2]}$ consisting of all elements of form $(x^a y^c, x^b y^c)$ is characteristic and of index 3, while $N^{[2]}$ is characteristic and of index 9.

3. *Criterion for A-group to have unique characteristic subgroup.* Let p, q be distinct primes. Then any UCS group G of order $p^r q^s$, having characteristic subgroup of order p^r, is expressible as $\mathrm{Gp}\{M, N, \vartheta\}$, where M, N are elementary Abelian groups of orders q^s, p^r respectively, and ϑ is an isomorphism of M onto a subgroup $\mathfrak{M}$ of $\mathfrak{A}(N)$. Conversely, for any such isomorphism ϑ, $\mathrm{Gp}\{M, N, \vartheta\}$ is an A-group in which N is the characteristic Sylow p-subgroup and M belongs to the transitive characteristic class of Sylow q-subgroups. We have seen (R, (3·4), special case (a)), that, for given M, N, two groups constructed thus‡ are isomorphic if and only if the corresponding images of M are conjugate subgroups of $\mathfrak{A}(N)$. The isomorphism problem which arises whenever groups are constructed is therefore solved in this case; we are left with the problem of finding necessary and sufficient conditions on ϑ for $G = \mathrm{Gp}\{M, N, \vartheta\}$ to be a UCS group. Since the group is known if the conjugacy class of $\mathfrak{M}$ in $\mathfrak{A}(N)$ is known, the conditions can be given in terms of $\mathfrak{M}$.

Let the group of automorphisms of G be denoted by $\mathfrak{A}(G)$, and the subgroup of those automorphisms which map M onto itself by $\mathfrak{H}$. If $\theta \in \mathfrak{A}(G)$, then by Sylow's Theorem M^θ is conjugate in G to M, and we can therefore find an element $k \in N$ such that $M^\theta = M^\phi$, where ϕ is the inner automorphism of G defined by $g^\phi = k^{-1}gk$. Then $\psi = \theta\phi^{-1} \in \mathfrak{H}$, $\theta = \psi\phi$, and ϕ leaves every element of N unchanged. The effect of θ on a subgroup of N is therefore identical with the effect of ψ. Again, if $K \supset N$ then K is normal in G (since G/N is Abelian), whence $K^\theta = K$ if and only if $K^\psi = K$. It follows that a subgroup of G which is contained in or contains N is characteristic in G if and only if it is invariant under every $\psi \in \mathfrak{H}$.

‡ If we identify M with $\mathfrak{M}$ we may regard G as a subgroup of the holomorph of N. The results we quote could of course be readily established from this point of view.

https://doi.org/10.1017/S0305004100029881 Published online by Cambridge University Press

Suppose now that it is known that the only proper characteristic subgroup of G contained in or containing N is N itself. If K is characteristic, so also are $K \cap N$ and KN. If $K \cap N = N$, then $K \supset N$; if $KN = N$, then $K \subset N$; if neither occurs, then $K \cap N = \{1\}$ and $KN = G$. But in this last case we should have $(K) = q^s$ and G would be Abelian, a contradiction of the definition of G. Hence if K is any proper characteristic subgroup, $K = N$. Combining this result with that of the previous paragraph shows that G is a UCS group if and only if the only proper subgroup contained in or containing N which is invariant under every $\psi \in \mathfrak{H}$ is N itself.

Any $\psi \in \mathfrak{H}$ induces automorphisms χ, ω of M, N respectively, which together define ψ. The necessary and sufficient condition that given $\chi \in \mathfrak{A}(M)$ and $\omega \in \mathfrak{A}(N)$ should be induced by some element of $\mathfrak{H}$ is

$$\vartheta(m^\chi) = \omega^{-1}\vartheta(m)\,\omega \quad \text{for all } m \in M, \tag{3·1}$$

as we see by writing $\vartheta_1 = \vartheta_2 = \vartheta$ in equation (3·2) of R. We may interpret (3·1) thus: an automorphism ω of N can be extended to an automorphism of G (which can be taken to belong to $\mathfrak{H}$ if desired) if and only if it lies in the normalizer $\mathfrak{N}$ of $\mathfrak{M}$ in $\mathfrak{A}(N)$; an automorphism χ of M is extensible to an automorphism of G (which must lie in $\mathfrak{H}$) if and only if the corresponding automorphism $\overline{\chi} = \vartheta^{-1}\chi\vartheta$ of $\mathfrak{M}$ is of form $\tau(\omega)$, i.e. can be obtained by transformation by an element ω of $\mathfrak{N}$. (We note that, for any automorphism $\tau(\omega)$ of $\mathfrak{M}$ defined by an $\omega \in \mathfrak{N}$, $\chi = \vartheta\tau(\omega)\,\vartheta^{-1} \in \mathfrak{A}(M)$ and satisfies (3·1).)

A subgroup of N is characteristic in G, therefore, if and only if it is invariant under every element of $\mathfrak{N}$. Hence $\{1\}$ and N are the only subgroups with this property if and only if $\mathfrak{N}$ is an irreducible subgroup of $\mathfrak{A}(N)$.

Any subgroup $K \supset N$ is expressible in the form LN, where $L = K \cap M \subset M$; K is characteristic in G if and only if $L^\psi = L$ for every $\psi \in \mathfrak{H}$, i.e. if and only if $L^\chi = L$ for every $\chi \in \mathfrak{A}(M)$ which satisfies (3·1) for some $\omega \in \mathfrak{N}$. Let $L^\vartheta = \mathfrak{L} \subset \mathfrak{M}$; then $L = L^\chi$ if and only if $\mathfrak{L} = \mathfrak{L}^{\overline{\chi}} = \omega^{-1}\mathfrak{L}\omega$. Thus K is characteristic if and only if $\mathfrak{L}$ is normal in $\mathfrak{N}$. Hence no subgroup of G lying strictly between N and G can be characteristic if and only if $\mathfrak{M}$ is a minimal normal subgroup of $\mathfrak{N}$. We sum up in the following criterion:

THEOREM 3·2. *Let M, N be elementary Abelian groups of orders q^s, p^r respectively, p, q being different primes, and let ϑ be an isomorphism of M onto the subgroup $\mathfrak{M}$ of $\mathfrak{A}(N)$. Then $G = \mathrm{Gp}\{M, N, \vartheta\}$ is a UCS group if and only if* (i) *the normalizer $\mathfrak{N}$ of $\mathfrak{M}$ in $\mathfrak{A}(N)$ is irreducible, and* (ii) *$\mathfrak{M}$ is a minimal normal subgroup of $\mathfrak{N}$.*

4. *Irreducible subgroups of* $\mathfrak{A}(N)$. Let $x_1, x_2, \ldots, x_r$ be an arbitrary but fixed basis of N, an elementary Abelian group of order p^r. The general element x of N has a unique expression in the form $x_1^{\xi_1}, x_2^{\xi_2}, \ldots, x_r^{\xi_r}$, where $\xi_i \in GF(p)$ for each i, and x may therefore be specified by the $(1 \times r)$ matrix (or row-vector) $X = (\xi_1, \xi_2, \ldots, \xi_r)$. The set of all vectors X forms a vector space V of dimension r over $GF(p)$, and $x \leftrightarrow X$ is an isomorphism between N and the additive group of V. A (1, 1) correspondence between linear transformations θ of V and $(r \times r)$ matrices Θ over $GF(p)$ is defined by $X^\theta = X\Theta$; and θ is an automorphism of V if and only if Θ is non-singular, in which case $\Theta \in \mathfrak{L} = GL_r(p)$. From the natural isomorphism between the automorphism groups $\mathfrak{A}(N)$ and $\mathfrak{A}(V)$ we deduce an isomorphism between $\mathfrak{A}(N)$ and $\mathfrak{L}$, in which the auto-

https://doi.org/10.1017/S0305004100029881 Published online by Cambridge University Press

morphism θ of N defined by $x_i^\theta = \prod_{j=1}^{r} x_j^{\theta_{ij}}$ corresponds to the matrix $\Theta = (\theta_{ij})$ of $\mathfrak{A}$. It is convenient to identify N with V and $\mathfrak{A}(N)$ with $\mathfrak{A}$; then a subgroup $\mathfrak{M}$ of $\mathfrak{A}(N)$ may be regarded as a subgroup of $\mathfrak{A}$, and irreducibility has its usual matrix sense—the non-existence of any proper subspace of V invariant under all the matrices of $\mathfrak{M}$. This identification of $\mathfrak{M}$ with a subgroup of matrices depends on the particular choice of basis $x_1, x_2, \ldots, x_r$, but no specialization is introduced since we are concerned only with the conjugacy class of $\mathfrak{M}$ in $\mathfrak{A}(N)$.

An imprimitive matrix Γ of $GL_r(p)$ is defined thus: there is an integer $l > 1$ such that $r = kl$, and Γ may be divided up into l^2 blocks, each $(k \times k)$, in such a way that there is precisely one non-zero matrix in each row and in each column of blocks. The non-singularity of Γ implies that each non-zero block is itself non-singular, and hence is an element of $GL_k(p)$. We shall call the $(l \times l)$ permutation matrix, obtained from Γ by replacing each zero block by 0 and each non-zero block by 1, the *skeleton* of Γ.

LEMMA 4·1. *Let $r = kl$, and let $\mathfrak{R}$ be a subgroup of $GL_k(p)$ with the property that no non-zero k-vector is left invariant by every element of $\mathfrak{R}$. Let $\mathfrak{R}$ be a subgroup of $\mathfrak{A} = GL_r(p)$ with the following properties:*

(i) *each element of $\mathfrak{R}$ is imprimitive, and the skeletons of elements of $\mathfrak{R}$ form a transitive group $\mathfrak{T}$ of $(l \times l)$ permutation matrices;*

(ii) *$\mathfrak{R}$ contains every matrix of form $\operatorname{diag}\{\Delta_1, \Delta_2, \ldots, \Delta_l\}$ with $\Delta_i \in \mathfrak{R}$ for each i;*

(iii) *for each i, the matrices occurring as non-zero blocks in the i-th diagonal position of elements of $\mathfrak{R}$ form an irreducible group.*

Then $\mathfrak{R}$ is irreducible.

Proof. The r-dimensional vector space V over $GF(p)$ which is the substratum of $\mathfrak{A}$ may be expressed as a direct sum $V = U_1 \oplus U_2 \oplus \ldots \oplus U_l$, where U_j is the k-dimensional subspace of all vectors $X = (\xi_i)$ such that $\xi_i = 0$ unless $k(j-1) < i \leqslant kj$. Each U_j has a basis naturally derived from that of V, and may be regarded as a substratum for $GL_k(p)$. The set $U_1, U_2, \ldots, U_l$ exhibits the imprimitivity of $\mathfrak{R}$ and acts as a carrier for $\mathfrak{T}$. Suppose that U is a non-zero subspace of V invariant under $\mathfrak{R}$, and let X be a non-zero vector of U. We may write $X = X_1 + X_2 + \ldots + X_l$, where $X_j \in U_j$, and we may assume $X_i \neq 0$. By hypothesis, there is an element $\Delta \in \mathfrak{R}$ such that $X_i\Delta \neq X_i$; then, by (ii), $\Gamma = \operatorname{diag}\{\Delta_1, \Delta_2, \ldots, \Delta_l\} \in \mathfrak{R}$, where $\Delta_i = \Delta$, $\Delta_j = 1_k$ if $j \neq i$. Then $X\Gamma - X = X_i\Delta - X_i \in U$, so that U contains a non-zero element of U_i. By (iii), U contains the whole of U_i, and since (by (i)) $\mathfrak{T}$ is transitive, U contains each U_j. Hence $U = V$ and $\mathfrak{R}$ is irreducible.

COROLLARY 4·2. *Suppose that $\mathfrak{R}$ is normal in the irreducible subgroup $\mathfrak{L}$ of $GL_k(p)$, and $(\mathfrak{R}) > 1$. Let $\mathfrak{R} \subset GL_r(p)$ consist of every imprimitive matrix whose skeleton lies in a certain transitive group $\mathfrak{T}$ of $(l \times l)$ permutation matrices, and whose non-zero blocks all belong to the same coset of $\mathfrak{R}$ in $\mathfrak{L}$. Then $\mathfrak{R}$ is irreducible.*

Proof. The conditions (i), (ii) and (iii) of the lemma are clearly satisfied, the irreducible group of (iii) being $\mathfrak{L}$. It remains to be shown that $\mathfrak{R}$ satisfies the hypothesis on invariant vectors. Let U be the subspace of all k-vectors X such that $X\Delta = X$ for every $\Delta \in \mathfrak{R}$. Then U is invariant under $\mathfrak{L}$. For if $\Theta \in \mathfrak{L}$, $\Delta \in \mathfrak{R}$, $X \in U$, $\Theta\Delta = \Delta'\Theta$ for some

https://doi.org/10.1017/S0305004100029881 Published online by Cambridge University Press

$\Delta' \in \mathfrak{R}$ and we have $(X\Theta)\Delta = (X\Delta')\Theta = X\Theta$, $X\Theta \in U$. Since $\mathfrak{L}$ is irreducible, $U = 0$ or U contains every k-vector X. In the latter case we should have $\mathfrak{R} = \{1_k\}$, precluded by hypothesis. Hence $U = 0$ and $\mathfrak{R}$ is irreducible by Lemma 4·1.

COROLLARY 4·3. *If $\mathfrak{R}$ is irreducible and $(\mathfrak{R}) > 1$, and if $\mathfrak{R}$ consists of all imprimitive matrices with skeletons in the transitive group $\mathfrak{T}$ and with non-zero blocks in $\mathfrak{R}$, then $\mathfrak{R}$ is irreducible.*

This is the special case of Corollary 4·2 in which $\mathfrak{R} = \mathfrak{L}$. We mention that, for given groups $\mathfrak{R}$ and $\mathfrak{T}$, the conditions $\mathfrak{R}$ irreducible, $(\mathfrak{R}) > 1$, $\mathfrak{T}$ transitive are necessary for the irreducibility of $\mathfrak{R}$ defined thus (assuming that $l > 1$).

5. *Elementary Abelian subgroups of $GL_r(p)$.* We wish to find conjugacy classes in $\mathfrak{A} = GL_r(p)$ of elementary Abelian subgroups $\mathfrak{M}$ of order q^s, q being a prime distinct from p. Any such class may be regarded as a class of equivalent faithful representations, of degree r over $GF(p)$, of an abstract group M which is elementary Abelian of order q^s. We use two well-known results from representation theory which are valid whenever the order of the finite group G represented is not a multiple of the characteristic of the underlying field K: every representation of G by matrices with elements in K is completely reducible, and every irreducible representation occurs as a component of the regular representation. Algebraic closure of K is not necessary, so we may apply these results in the case $K = GF(p)$, $G = M$.

Let p belong to exponent $e \bmod q$; this means that e is the smallest positive integer such that $p^e \equiv 1 \pmod q$. Then $q \mid p^e - 1$ and $e \mid q - 1$. Any primitive qth root of unity $\mu \pmod p$ lies in $GF(p^e)$ but in no Galois field of smaller order. Thus μ is a root of a polynomial $P(x) \equiv x^e + \lambda_{e-1}x^{e-1} + \ldots + \lambda_1 x + \lambda_0$, which is irreducible relative to the field $GF(p)$ in which all the coefficients lie; the other roots of $P(x)$ are $\mu^p, \mu^{p^2}, \ldots, \mu^{p^{e-1}}$. The matrix

$$\Lambda = \begin{pmatrix} 0 & 0 & \ldots & 0 & -\lambda_0 \\ 1 & 0 & \ldots & 0 & -\lambda_1 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -\lambda_{e-1} \end{pmatrix} \tag{5·1}$$

lies in $GL_e(p)$ (since $\lambda_0 \neq 0$) and has characteristic equation $P(x) = 0$, and every matrix with this characteristic equation is conjugate in $GL_e(p)$ to Λ. (See, for example, (4), § 111.) Since $P(x)$ is irreducible, so is Λ; since each characteristic root is a qth root of unity, Λ is of order q.

Now p is a primitive eth root of unity $(\bmod q)$, and $q - 1 = ef$ for some integer f. Let us write $\pi \in GF(q)$ for the congruence class of $p \pmod q$; then we can find a primitive $(q-1)$th root of unity in $GF(q)$, say β, such that $\pi = \beta^f$, and every non-zero element α of $GF(q)$ is of form β^h, with $0 \leqslant h \leqslant q - 2$. Since Λ, Λ^π, Λ^{π^2}, ..., $\Lambda^{\pi^{e-1}}$ are conjugate in $GL_e(p)$, the matrices Λ^{β^h} and Λ^{β^j} are conjugate if and only if $h \equiv j \pmod f$. The powers of Λ (other than $\Lambda^0 = 1_e$) may thus be classified into f conjugacy classes, each containing e distinct powers, and we may take as representatives of the several classes the matrices Λ, Λ^β, ..., $\Lambda^{\beta^{f-1}}$.

If $H = \{x\}$ is a cyclic group of order q, the mapping $x \to \Lambda^\alpha$ gives an irreducible representation of H, of degree e over $GF(p)$, for each non-zero $\alpha \in GF(q)$. We get f

https://doi.org/10.1017/S0305004100029881 Published online by Cambridge University Press

inequivalent representations by taking for α the values $1, \beta, \beta^2, \ldots, \beta^{f-1}$. Together with the identical representation these must exhaust the irreducible representations of H, since the total of their degrees is $ef+1 = q$, the order of H. Each of these representations must occur once only in the regular representation of H.

A representation of an elementary Abelian group M of order q^s can be obtained as the product of a homomorphism of M onto a cyclic group H of order q, and a representation of H. There are $(q^s-1)/(q-1) = m$ distinct subgroups of M of order q^{s-1} to serve as kernel of the homomorphism, and so we get in this way fm irreducible and inequivalent representations, each of degree e. If we include the identical representation we have accounted for distinct irreducible representations of total degree $1+efm = q^s$, so every irreducible representation is equivalent to one of these. Using the property of complete reducibility, we may summarize our conclusions in the following form, adapted to the problem under consideration:

LEMMA 5·2. *Any elementary Abelian subgroup $\mathfrak{M}$ of $\mathfrak{A} = GL_r(p)$, of order a power of q, is conjugate in $\mathfrak{A}$ to a subgroup each of whose elements is of form*

$$\operatorname{diag}\{\Lambda^{\alpha_1}, \Lambda^{\alpha_2}, \ldots, \Lambda^{\alpha_c}, 1_t\}, \tag{5·3}$$

where each $\alpha_i \in GF(q)$, Λ is given by (5·1), *and $r = ce+t$.* (Here t is the same for all elements of the group. We may suppose that, for each i, α_i is non-zero for some matrix of the group, since otherwise we could expunge the ith block and change t to $t+e$.)

COROLLARY 5·4. *If $e > 1$ and $\mathfrak{M}$ is cyclic of order q, then the normalizer $\mathfrak{N}$ of $\mathfrak{M}$ in $\mathfrak{A}$ contains the centralizer of $\mathfrak{M}$ properly.*

Proof. We may assume that $\mathfrak{M} = \{\Theta\}$, where Θ is of form (5·3). Since Λ is conjugate in $GL_e(p)$ to Λ^p, there is an element Σ of $GL_e(p)$ such that $\Sigma^{-1}\Lambda\Sigma = \Lambda^p$. Then, if $\Psi = \operatorname{diag}\{\Sigma, \Sigma, \ldots, \Sigma, 1_t\}$, $\Psi^{-1}\Theta\Psi = \Theta^p$, $\Psi \in \mathfrak{N}$. But $\Theta = \Theta^p$ would imply $p \equiv 1 \pmod q$, that is, $e = 1$; hence if $e > 1$, Ψ does not belong to the centralizer of $\mathfrak{M}$.

6. *General results on UCS groups of order $p^r q^s$.*

THEOREM 6·1. *Let G be a UCS group of order $p^r q^s$, having characteristic subgroup N of order p^r. Then the direct product of a number of groups each isomorphic to G is itself a UCS group, except possibly if $s = 1$ and $q \mid p-1$.*

Proof. Since the centre of G is the identity, the hypothesis (i) of Theorem 2·1 certainly holds, and our result follows from that theorem if (ii) also holds. We may assume $s = 1$, since if $s \geqslant 2$ (ii) certainly holds. Then if the exponent e of $p \pmod q$ exceeds 1, Corollary 5·4 shows that there are elements of $\mathfrak{N}$ which transform $\mathfrak{M}$ non-identically. Hence there are non-identical automorphisms of M, and so also of G/N, which can be extended to automorphisms of G. Since G/N is of prime order, no element other than N/N can be invariant under any such automorphism, and so (ii) is satisfied if $s = 1$, $e > 1$. We shall see in § 8 that the conclusion is certainly false if $r = s = 1$ and $q \mid p-1$; the examples at the end of § 2 are special cases illustrating this phenomenon.

For given p, q, the simplest example of a UCS group with order of form $p^r q^s$ is a certain group G_1 of order $p^e q$. This is the group defined by the elementary Abelian group N_1 of order p^e, and the cyclic subgroup $\mathfrak{M}_1 = \{\Lambda\}$ of $\mathfrak{A}_1 = GL_e(p)$, of order q (where Λ is given by (5·1)). The normalizer $\mathfrak{N}_1$ of $\mathfrak{M}_1$ in $\mathfrak{A}_1$ is irreducible, since $\mathfrak{M}_1$

https://doi.org/10.1017/S0305004100029881 Published online by Cambridge University Press

itself is so; and $\mathfrak{M}_1$ is a minimal normal subgroup of $\mathfrak{N}_1$, being of prime order. Hence G_1 is a UCS group. We may specify G_1 explicitly as $\{x_1, x_2, \ldots, x_e, y\}$, where the generators satisfy the relations

$$\left.\begin{aligned} x_1^p = x_2^p = \ldots = x_e^p = y^q = 1, \\ y^{-1}x_1 y = x_e^{-\lambda_0}, \\ y^{-1}x_i y = x_{i-1}x_e^{-\lambda_{i-1}} \quad (2 \leqslant i \leqslant e). \end{aligned}\right\} \tag{6·2}$$

The fundamental rôle played by this group is shown by the next theorem.

THEOREM 6·3. *Suppose that G is a UCS group of order $p^r q^s$, having characteristic subgroup of order p^r. Then, if the exponent of p (mod q) is e,*

(i) *$r = ce$ for some integer c, and $s \leqslant c$;*

(ii) *G is isomorphic to a subgroup of the direct product $G_1^{[c]}$, where G_1 is the UCS group defined by* (6·2)*;*

(iii) *if $e > 1$, this direct product is itself a UCS group.*

Proof. For given p^r, G is determined by the conjugacy class to which the subgroup $\mathfrak{M}$ of $\mathfrak{A} = GL_r(p)$ belongs. By Lemma 5·2, we may assume that $\mathfrak{M}$ consists of elements of form (5·3). The integer t is the dimension of the subspace U, of the underlying r-dimensional space V, consisting of all vectors X such that $X\Theta = X$ for every $\Theta \in \mathfrak{M}$, and we see (as in the proof of Corollary 4·2) that U is an invariant subspace for $\mathfrak{N}$. Hence if $1 \leqslant t \leqslant r-1$, $\mathfrak{N}$ is reducible; the case $t = r$ merely yields $\mathfrak{M} = \{1_r\}$. For non-trivial $\mathfrak{M}$ with irreducible normalizer $\mathfrak{N}$ we therefore have $t = 0$, $r = ce$. Thus $\mathfrak{M}$ is a subgroup of the group $\mathfrak{M}_c = \mathfrak{M}_1^{[c]}$, of order q^c, consisting of all matrices of form $\mathrm{diag}\{\Lambda^{\alpha_1}, \Lambda^{\alpha_2}, \ldots, \Lambda^{\alpha_c}\}$, with $\alpha_i \in GF(q)$. The group G constructed from $\mathfrak{M}$ is therefore isomorphic to a subgroup of that constructed from $\mathfrak{M}_c$, and this is clearly $G_1^{[c]}$. The final clause of the theorem is immediate from Theorem 6·1.

THEOREM 6·4. *Let G be a UCS group of order $p^r q^s$, defined by the subgroup $\mathfrak{M}$ (elementary Abelian of order q^s) of $GL_r(p)$; and let k be an integer exceeding* 1. *Let $\mathfrak{M}^*$ be that subgroup of $GL_{kr}(p)$ which consists of the q^s elements* $\mathrm{diag}\{\Theta, \Theta, \ldots, \Theta\}$, *where $\Theta \in \mathfrak{M}$. Then the group G^* of order $p^{kr}q^s$ defined by $\mathfrak{M}^*$ is a UCS group.*

Proof. The hypothesis implies that $\mathfrak{M}$ is a minimal normal subgroup of its normalizer $\mathfrak{N}$, which is irreducible. We show that the same is true of $\mathfrak{M}^*$ and its normalizer $\mathfrak{N}^*$. Let the centralizer of $\mathfrak{M}$ be the normal subgroup $\mathfrak{C}$ of $\mathfrak{N}$. The effect on any element of $\mathfrak{M}$ of transformation by an element Γ of $\mathfrak{N}$ is determined by the coset of $\mathfrak{C}$ to which Γ belongs. Hence $\mathfrak{N}^*$ certainly contains the group $\mathfrak{N}^*$ consisting of every imprimitive matrix all k of whose non-zero blocks belong to the same coset of $\mathfrak{C}$. Since $\mathfrak{C} \supset \mathfrak{M}$ we have $(\mathfrak{C}) > 1$, so all the hypotheses of Corollary 4·2 are satisfied. Therefore $\mathfrak{N}^*$ is irreducible, and hence $\mathfrak{N}^*$ is irreducible. A subgroup $\mathfrak{H}^*$ of $\mathfrak{M}^*$ must consist of all elements $\mathrm{diag}\{\Theta, \Theta, \ldots, \Theta\}$ with Θ in some subgroup $\mathfrak{H}$ of $\mathfrak{M}$; $\mathfrak{N}^*$ contains every matrix $\mathrm{diag}\{\Gamma, \Gamma, \ldots, \Gamma\}$ with $\Gamma \in \mathfrak{N}$, so that $\mathfrak{H}^*$ normal in $\mathfrak{N}^*$ would imply $\mathfrak{H}$ normal in $\mathfrak{N}$, and so $\mathfrak{H} = \{1_r\}$ or $\mathfrak{H} = \mathfrak{M}$. Thus $\mathfrak{M}^*$ is a minimal normal subgroup of the irreducible $\mathfrak{N}^*$, and G^* is a UCS group.

7. *UCS groups of order $p^r q$.* For given p, q, a complete account of the UCS groups of orders $p^r q^s$, with $r = ce$ and $s \leqslant c$, would require knowledge of which subgroups of $\mathfrak{M}_c$ had irreducible normalizers in which they were minimal normal subgroups. In this section we give the answer in the case $s = 1$; here the minimal property of $\mathfrak{M}$ is auto-

https://doi.org/10.1017/S0305004100029881 Published online by Cambridge University Press

matic and we have to consider only the irreducibility of $\mathfrak{N}$. If $\mathfrak{M} = \{\Theta\}$, where $\Theta = \operatorname{diag}\{\Lambda^{\alpha_1}, \Lambda^{\alpha_2}, \ldots, \Lambda^{\alpha_c}\}$, a necessary condition for this is that, for each i, α_i is a non-zero element of $GF(q)$. Using the notation of § 5 we may therefore write $\alpha_i = \beta^{h_i}$, where $0 \leqslant h_i \leqslant q-2$, and Θ is specified by the c-row $(h_1, h_2, \ldots, h_c)$. Then Θ^{β^u} is similarly specified by $(h_1+u, h_2+u, \ldots, h_c+u)$. The element Φ of $\mathfrak{M}_c$ determined by $(j_1, j_2, \ldots, j_c)$ is conjugate in $\mathfrak{A}$ to Θ if and only if the j_i's can be reordered to form a row $(j_1', j_2', \ldots, j_c')$ such that $j_i' \equiv h_i \pmod f$ for each i, where $ef = q-1$. We may therefore assume that Θ satisfies $0 = h_1 \leqslant h_2 \leqslant \ldots \leqslant h_c \leqslant f-1$, since in any case some power Θ^{β^u} is conjugate to an element with this property which generates a cyclic subgroup conjugate to $\mathfrak{M}$.

LEMMA 7·1. *Let $f = lt$. Then the cyclic subgroup $\{\Delta\}$ of $\mathfrak{M}_l$, where*

$$\Delta = \operatorname{diag}\{\Lambda, \Lambda^{\beta^t}, \ldots, \Lambda^{\beta^{(l-1)t}}\},$$

has irreducible normalizer in $GL_{le}(p)$.

Proof. Let $1 \leqslant v \leqslant l-1$, and let $\Gamma \in GL_e(p)$ be any matrix such that $\Gamma^{-1}\Lambda\Gamma = \Lambda^p = \Lambda^{\beta^{lt}}$; then $\Gamma^{-1}\Lambda^{\beta^{it}}\Gamma = \Lambda^{\beta^{(l+i)t}}$. Define

$$\Sigma_v = \begin{pmatrix} 0 & \ldots & 0 & \Gamma & \ldots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & 0 & \ldots & \Gamma \\ 1_e & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \ldots & 1_e & 0 & \ldots & 0 \end{pmatrix} \in GL_{le}(p),$$

where Γ occurs v times and $1_e(l-v)$ times. We see that

$$\Sigma_v^{-1}\Delta\Sigma_v = \operatorname{diag}\{\Lambda^{\beta^{vt}}, \ldots, \Lambda^{\beta^{(l-1)t}}, \Gamma^{-1}\Lambda\Gamma, \ldots, \Gamma^{-1}\Lambda^{\beta^{(v-1)t}}\Gamma\} = \Delta^{\beta^{vt}}.$$

Hence Σ_v lies in the normalizer of $\{\Delta\}$, which also contains $\mathfrak{M}_l$ and hence the group $\mathfrak{R}$ generated by $\mathfrak{M}_l$ and the Σ_v's (for each v). But the conditions of Lemma 4·1 are satisfied by $\mathfrak{R}$ (with $k = e$ and $\mathfrak{K} = \mathfrak{M}_1 = \{\Lambda\}$), and therefore the normalizer of $\{\Delta\}$ is irreducible.

THEOREM 7·2. *Let p, q be distinct primes and let the exponent of $p \pmod q$ be e. Then the number of distinct UCS groups of order $p^r q$, with characteristic subgroup of order p^r, is equal to the number of factors of $(r, q-1)$ which are multiples of e, and each of the groups‡ is isomorphic to a group defined thus:*

Let $q-1 = ef$, $r = ce$, and suppose $l \mid (c, f)$; then write $c = kl$, $f = lt$. Define

$$\Theta_l = \operatorname{diag}\{\Lambda, \ldots, \Lambda, \Lambda^{\beta^t}, \ldots, \Lambda^{\beta^t}, \Lambda^{\beta^{2t}}, \ldots, \Lambda^{\beta^{(l-1)t}}\},$$

where Λ is the irreducible $(e \times e)$ matrix given by (5·1), each term $\Lambda^{\beta^{it}}$ occurs k times, and β is a primitive $(q-1)$th root of unity in $GF(q)$ such that $\beta^f = \pi$, the residue class of $p \pmod q$. Define a group of order $p^r q$ by taking $\mathfrak{M} = \{\Theta_l\}$ as subgroup of $\mathfrak{A}$.

Proof. The fact that, for any $l \mid (c, f)$, the group constructed from $\{\Theta_l\}$ is a UCS group follows at once from Lemma 7·1 and Theorem 6·4. Also $\{\Theta_l\}$ is not conjugate to $\{\Theta_{l'}\}$ if $l \neq l'$, so that there are as many distinct groups constructed in this way as there are factors of (c, f) (or factors of $(r, q-1)$ which are multiples of e). It remains to be shown that any cyclic subgroup of $\mathfrak{M}_c$ with irreducible normalizer is conjugate in $\mathfrak{A}$ to $\{\Theta_l\}$ for some factor l of (c, f).

‡ If r is not a multiple of e, there are no such groups (Theorem 6·3).

https://doi.org/10.1017/S0305004100029881 Published online by Cambridge University Press

Suppose that Θ is specified by the c-row $(h_1, h_2, \ldots, h_c)$; as we have seen, we may assume that $0 = h_1 \leqslant h_2 \leqslant \ldots \leqslant h_c \leqslant f-1$. The elements α of $GF(q)$ such that Θ^α is conjugate to Θ form a subgroup (necessarily cyclic) of the multiplicative group of $GF(q)$, which certainly contains β^f since $\Theta^{\beta^f} = \Theta^p$ is conjugate to Θ. The group is therefore of form $\{\beta^u\}$ where $u \mid f$; say $f = mu$. Then the elements of $\mathfrak{M}_c$ specified by $(h_1, h_2, \ldots, h_c)$ and $(h_1+ju, h_2+ju, \ldots, h_c+ju)$ are conjugate for each j satisfying $0 \leqslant j \leqslant m-1$. It follows that each of the numbers ju, $0 \leqslant j \leqslant m-1$, must occur equally often in the row $(h_1, h_2, \ldots, h_c)$; and if $h_1 = h_2 = \ldots = h_k = 0$, $h_{k+1} > 0$, then each occurs k times. Thus km of the c numbers are accounted for, and if $km = c$ we have $\Theta = \Theta_m$, $m \mid (c, f)$. We complete the proof by showing that, if $km < c$, then the normalizer of $\{\Theta\}$ is reducible.

If $km < c$, Θ is conjugate to an element $\Phi \in \mathfrak{M}_c$, where $\Phi = \operatorname{diag}\{\Lambda^{\alpha_1}, \Lambda^{\alpha_2}, \ldots, \Lambda^{\alpha_c}\}$ with $\alpha_i = \beta^{g_i}$, the g_i's satisfying $g_i \equiv 0 \pmod u$ if $1 \leqslant i \leqslant km$, $g_i \not\equiv 0 \pmod u$ if $km < i \leqslant c$. If Γ is any element of the normalizer of $\{\Phi\}$, then $\Gamma\Phi = \Phi^\alpha\Gamma$, where $\alpha = \beta^{nu}$ for some n. Let Γ be divided into c^2 blocks Γ_{ij}, each $(e \times e)$; our equation gives $\Gamma_{ij}\Lambda^{\alpha_j} = \Lambda^{\alpha\alpha_i}\Gamma_{ij}$ for all i, j. Now $\alpha_j = \beta^{g_j}$, $\alpha\alpha_i = \beta^{nu+g_i}$, and so Λ^{α_j}, $\Lambda^{\alpha\alpha_i}$ are conjugate if and only if $g_j \equiv nu + g_i \pmod f$, which demands $g_j \equiv g_i \pmod u$. But if $j \leqslant km$, $i > km$, or $j > km$, $i \leqslant km$, $g_j \not\equiv g_i \pmod u$ and Λ^{α_j}, $\Lambda^{\alpha\alpha_i}$ are not conjugate. But this implies by Schur's Lemma (in the form given in (5), Lemma (3·1·D), p. 83) that $\Gamma_{ij} = 0$, and we thus have a direct demonstration of the reducibility of the normalizer of $\{\Phi\}$ and hence of $\{\Theta\}$.

8. *The special case* $q \mid p-1$. The results we have obtained may be extended slightly if $q \mid p-1$, i.e. if $e = 1$. This implies that $p \geqslant 3$, which we assume throughout this section. In place of the matrix Λ we now merely have an element $\lambda \in GF(p)$ with $\lambda^q = 1$, $\lambda \neq 1$. Also $c = r$, $f = q-1$, and the group $\mathfrak{M}_r \subset \mathfrak{A} = GL_r(p)$ consists of the q^r diagonal matrices whose non-zero elements are all of form λ^{α_i} with $\alpha_i \in GF(q)$. We may rule out the trivial case $r = 1$, for then $\mathfrak{A}$ is cyclic of order $p-1$ and has a unique subgroup of order q; there is a single UCS group of order pq. So we suppose that $r \geqslant 2$.

The group $\mathfrak{A}$ has two important normal subgroups. Its centre $\mathfrak{Z}$ is cyclic of order $p-1$, and consists of all scalar matrices $\mu 1_r$. The matrices of $\mathfrak{A}$ having determinant 1 form a normal subgroup $\mathfrak{U}$ of index $(p-1)$ with cyclic quotient group. If the normalizer of $\mathfrak{M}$ in $\mathfrak{A}$ is $\mathfrak{N}$, then $\mathfrak{M} \cap \mathfrak{Z}$ and $\mathfrak{M} \cap \mathfrak{U}$ are also normal in $\mathfrak{N}$; if $\mathfrak{M}$ is a minimal normal subgroup of $\mathfrak{N}$, then each coincides either with $\mathfrak{M}$ or with $\{1_r\}$. The case $\mathfrak{M} \cap \mathfrak{Z} = \mathfrak{M}$ yields $\mathfrak{M} \subset \mathfrak{Z}$; $\mathfrak{M}$ is the unique subgroup of $\mathfrak{Z}$ of order q, $\mathfrak{N} = \mathfrak{A}$, and we always get a UCS group of order $p^r q$. (It is in fact the group obtained from that of order pq by the process described in Theorem 6·4.) So we shall assume $\mathfrak{M} \cap \mathfrak{Z} = \{1_r\}$.

Suppose now that we also have $\mathfrak{M} \cap \mathfrak{U} = \{1_r\}$. Then $\mathfrak{M}$ is cyclic, and no two elements of $\mathfrak{M}$ have the same determinant; so $\mathfrak{N}$ is the centralizer of $\mathfrak{M}$. But if $\mathfrak{M} = \{\Theta\}$, Θ is diagonal and its diagonal elements are not all equal; it is easily seen that its centralizer is reducible, whence $\mathfrak{N}$ is reducible. We must therefore have the other alternative, $\mathfrak{M} \subset \mathfrak{U}$. Thus $\mathfrak{M}\dagger \subset \mathfrak{M} = \mathfrak{M}_r \cap \mathfrak{U}$, the subgroup of all matrices $\operatorname{diag}\{\lambda^{\alpha_1}, \lambda^{\alpha_2}, \ldots, \lambda^{\alpha_r}\}$ with $\alpha_1 + \alpha_2 + \ldots + \alpha_r = 0$; $\mathfrak{M}\dagger$ is of order q^{r-1}. Thus every $\mathfrak{M}$ not lying in $\mathfrak{Z}$ which gives a UCS group is conjugate to a subgroup of $\mathfrak{M}\dagger$, and every UCS group constructed from such $\mathfrak{M}$ is isomorphic to a subgroup of $G\dagger$, of order $p^r q^{r-1}$, constructed from $\mathfrak{M}\dagger$.

The effect on a diagonal matrix of transformation by a monomial matrix is that of

https://doi.org/10.1017/S0305004100029881 Published online by Cambridge University Press

a permutation of its diagonal elements. The normalizer $\mathfrak{N}\dagger$ of $\mathfrak{M}\dagger$ therefore contains every monomial matrix of $\mathfrak{A}$, and so must be irreducible. (Apply Corollary 4·3 with $\mathfrak{K} = GL_1(p)$; $(\mathfrak{K}) > 1$ since $p \geqslant 3$.) For $\mathfrak{M}\dagger$ to be minimal normal in $\mathfrak{N}\dagger$ it is necessary that $q = r = 2$ or $q \nmid r$; for if $q \mid r$, $\mathfrak{M}\dagger \cap \mathfrak{Z}$ contains $\mathrm{diag}\{\lambda^\alpha, \lambda^\alpha, \ldots, \lambda^\alpha\}$ for each $\alpha \in GF(q)$ and is a proper subgroup of $\mathfrak{M}\dagger$ unless $r = 2$, $q = 2$. In this trivial case $G\dagger$ is the UCS group of order $2p^2$; otherwise $q \mid r$ implies that $G\dagger$ is not a UCS group. We finally show that if $q \nmid r$, then $G\dagger$ *is* a UCS group: $\mathfrak{M}\dagger$ is minimal normal in $\mathfrak{N}\dagger$.

We may take as generators of $\mathfrak{M}\dagger$ the $(r-1)$ matrices

$$\mathrm{diag}\{\lambda, 1, \ldots, 1, \lambda^{-1}\}, \quad \mathrm{diag}\{1, \lambda, \ldots, 1, \lambda^{-1}\}, \quad \ldots, \quad \mathrm{diag}\{1, \ldots, 1, \lambda, \lambda^{-1}\}.$$

By what we have shown about $\mathfrak{N}\dagger$ it is clear that any normal subgroup of $\mathfrak{N}\dagger$ containing any one of the generators contains them all. Let $\mathfrak{L}$ be a normal subgroup of $\mathfrak{N}\dagger$, $\mathfrak{L} \subset \mathfrak{M}\dagger$, and let $\mathrm{diag}\{\lambda^{\alpha_1}, \lambda^{\alpha_2}, \ldots, \lambda^{\alpha_r}\}$ be an element of $\mathfrak{L}$ distinct from the identity. If $q \nmid r$ the α_i's cannot be all equal, and we may assume $\alpha_1 \neq \alpha_r$, since any element obtained by permuting the α_i's also belongs to $\mathfrak{L}$. Then also

$$\mathrm{diag}\{\lambda^{\alpha_r}, \lambda^{\alpha_2}, \ldots, \lambda^{\alpha_{r-1}}, \lambda^{\alpha_1}\} \in \mathfrak{L},$$

and on division we have $\mathrm{diag}\{\lambda^{\alpha_1 - \alpha_r}, 1, \ldots, 1, \lambda^{\alpha_r - \alpha_1}\} \in \mathfrak{L}$. Since $\alpha_1 \neq \alpha_r$, this shows that $\mathrm{diag}\{\lambda, 1, \ldots, 1, \lambda^{-1}\} \in \mathfrak{L}$, $\mathfrak{L} = \mathfrak{M}\dagger$, $\mathfrak{M}\dagger$ is a minimal normal subgroup of $\mathfrak{N}\dagger$; $G\dagger$ is a UCS group if $q \nmid r$. We sum up our conclusions in the following theorem, which in the case $e = 1$ supersedes Theorem 6·3.

THEOREM 8·1. *Suppose that $q \mid p-1$, that $\lambda \in GF(p)$ is a primitive q-th root of unity, and that G is a UCS group of order $p^r q^s$, having characteristic subgroup of order p^r. Then either* (i) *$s = 1$ and G is defined by the generating relations*

$$x_1^p = x_2^p = \ldots = x_r^p = y^q = 1, \quad y^{-1} x_i y = x_i^\lambda \quad (i = 1, 2, \ldots, r);$$

or (ii) *$s \leqslant r-1$ and G is isomorphic to a subgroup of the group $G\dagger$, of order $p^r q^{r-1}$, defined by the relations*

$$x_1^p = x_2^p = \ldots = x_r^p = y_1^q = \ldots = y_{r-1}^q = 1,$$

$$y_j^{-1} x_i y_j = \begin{cases} x_i^\lambda & \text{if } i = j, \\ x_i & \text{if } i \neq j \text{ and } i < r, \\ x_i^{\lambda^{-1}} & \text{if } i = r. \end{cases}$$

The group $G\dagger$ is a UCS group if $q \nmid r$ or if $q = r = 2$, but otherwise is not.

I should like to express my gratitude to Prof. Hall for stimulating my interest in these problems, and for his most helpful comments on a preliminary draft of this paper.

REFERENCES

(1) HALL, P. The construction of soluble groups. *J. reine angew. Math.* 182 (1940), 206–14.
(2) TAUNT, D. R. On A-groups. *Proc. Camb. phil. Soc.* 45 (1949), 24–42.
(3) TAUNT, D. R. Remarks on the isomorphism problem in theories of construction of finite groups. *Proc. Camb. phil. Soc.* 51 (1955), 16–24.
(4) VAN DER WAERDEN, B. L. *Moderne Algebra*, II, 2nd ed. (Berlin, 1940).
(5) WEYL, H. *The classical groups*, 2nd ed. (Princeton, 1946).

JESUS COLLEGE
CAMBRIDGE

https://doi.org/10.1017/S0305004100029881 Published online by Cambridge University Press