ON SIMPLY TRANSITIVE GROUPS WITH
TRANSITIVE ABELIAN SUBGROUPS
OF THE SAME DEGREE*

BY

DOROTHY MANNING

Introduction. It was in 1900 that William Burnside† first proved that a simply transitive permutation group of prime degree p must contain an invariant subgroup of order p. He later showed‡ that a simply transitive group of degree p^m with p a prime and $m>1$ is imprimitive and compound if it contains a permutation of order p^m. In 1921 he§ published a short proof that a simply transitive group in which there is a transitive Abelian subgroup of the same degree is compound unless all the operations of the Abelian subgroup are of the same prime order. However, the proof is not sound, as we shall see in §15.

In 1933 Professor I. Schur‖ published a paper on those simply transitive groups of degree n in which there is a transitive cyclic subgroup of degree n. He found them to be imprimitive and compound when n is not a prime. He seems to have been unaware of Burnside's paper of 1921. It was this fact that led W. A. Manning to a critical study of the status of the problem, and to the conviction that an investigation of the remaining cases should be undertaken.

In this paper it will be proved that *if a simply transitive group of degree p^{a+b} (p a prime and $a \neq b$) contains a transitive Abelian subgroup of the same degree and of type (a, b), it is imprimitive and compound.* That no such theorem holds when $a=b$ is shown by the existence of exceptions. There is an infinite family of simply transitive primitive groups¶ of degree k^2 ($k>2$) and order $2(k!)^2$ which contain transitive Abelian subgroups of degree k^2 that are

---

† W. Burnside, *On the properties of groups of odd order*, Proceedings of the London Mathematical Society, vol. 33 (1900), p. 174; *On simply transitive groups of prime degree*, Quarterly Journal of Mathematics, vol. 37 (1906), p. 215; I. Schur, *Neuer Beweis eines Satzes von W. Burnside*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 17 (1908), p. 171; W. Burnside, *Theory of Groups of Finite Order*, 2d edition (1911), p. 341.

‡ W. Burnside, *Theory of Groups of Finite Order*, 2d edition (1911), p. 343.

§ W. Burnside, *On certain simply-transitive permutation-groups*, Proceedings of the Cambridge Philosophical Society, vol. 20 (1921), pp. 482–484.

‖ *Zur Theorie der einfach transitiven Permutationsgruppen*, Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-mathematische Klasse, 1933, pp. 598–623.

¶ W. A. Manning, *On the primitive groups of class ten*, American Journal of Mathematics, vol. 28 (1906), p. 235.

direct products of two Abelian subgroups of order k. The members of this family with $k = p^a > 2$ are exceptions to the proposed theorem.

There is a somewhat similar problem for solvable groups, first encountered by Professor J. F. Ritt.* He proved that a primitive solvable group in p^m letters with p prime and $m > 1$ cannot contain a substitution of order p^m except in the case $p = 2$, $m = 2$.

It should be noted that if an imprimitive group contains a transitive Abelian subgroup of the same degree, it is compound.† For if it were simple, the group according to which its systems of imprimitivity are permuted would contain a transitive Abelian subgroup of order n and degree less than n, an impossibility, since a transitive Abelian group is always regular.

1. In this section we reproduce without proof as much of the preliminary work of Burnside's paper of 1921‡ as we shall need.

Let a and b be natural numbers, p and q primes, the same or different. Any transitive Abelian permutation group of degree $n = p^a q^b$ generated by two permutations of orders p^a and q^b, may be written $\{P, Q\}$, where

$$\left.\begin{array}{ll} P: & x_{u,v} = x'_{u+1,v} \\ Q: & x_{u,v} = x'_{u,v+1} \end{array}\right\} (u = 0, 1, \cdots, p^a - 1; v = 0, 1, \cdots, q^b - 1),$$

the two symbols $x_{u,v}$ and $x_{y,z}$ representing the same letter if and only if $u \equiv y$ mod p^a and $v \equiv z$ mod q^b. (This rule is also to be applied to the $\xi_{u,v}$, the $\Gamma_{u,v}$, the $\Delta_{u,v}$, the $M_{u,v}$, the $m_{u,v}$, the $T_{i,j}$, and the $W_{i,j}$, which will be introduced later.)

Let $H = \{P, Q\}$ and let G be any simply transitive permutation group containing H as a proper subgroup.

If ϵ is a primitive p^ath and η a primitive q^bth root of unity,

$$T: \quad x_{u,v} = \frac{1}{n} \sum_{y=0}^{p^a-1} \sum_{z=0}^{q^b-1} \epsilon^{uy} \eta^{vz} \xi_{y,z} \quad (u = 0, 1, \cdots, p^a - 1; v = 0, 1, \cdots, q^b - 1)$$

completely reduces both G and H.

$$\begin{array}{lll} (1.1) & T^{-1}PT: & \xi_{y,z} = \epsilon^y \xi'_{y,z} \\ (1.2) & T^{-1}QT: & \xi_{y,z} = \eta^z \xi'_{y,z} \end{array} \right\} (y = 0, 1, \cdots, p^a - 1; z = 0, 1, \cdots, q^b - 1).$$

If we represent the variables of an irreducible constituent group Γ of $T^{-1}GT$: ξ_{α_v,β_v} ($v = 1, 2, \cdots, \mu$) (where μ is the degree of Γ), and the letters of a transitive constituent Δ of G_0 (the subgroup of G which fixes $x_{0,0}$): x_{a_u,b_u} ($u = 1, 2, \cdots, m$) (where m is the degree of Δ), and if $\chi_{P^{a_u}Q^{b_u}}$ represents the trace of the substitution of Γ which corresponds to $P^{a_u}Q^{b_u}$, then

$$(1.3) \qquad \chi_{P^{a_u}Q^{b_u}} = \sum_{v=1}^{\mu} \epsilon^{a_u\alpha_v}\eta^{b_u\beta_v} = \frac{\mu}{m}\sum_{u=1}^{m} \epsilon^{a_u\alpha_v}\eta^{b_u\beta_v},$$

provided Γ is not the identical constituent (on $\xi_{0,0}$ alone) and Δ is not the transitive constituent of G_0 on $x_{0,0}$.

2. We now establish a sufficient condition that the group G be imprimitive.

LEMMA I. *If any permutation S of G which is not also in G_0 corresponds to the identity of any irreducible constituent Γ of $T^{-1}GT$ except the identical constituent, G is imprimitive.*[*]

The correspondence between G and Γ is not one to one, for both S and the identity of G correspond to the identity of Γ. Let Γ' be the subgroup of Γ which corresponds to G_0. Let G' be the largest (proper or improper) subgroup of G which corresponds to Γ'. Then G_0 is a proper subgroup of G', for G' contains S. Since G is simply transitive, $\xi_{\alpha_1,\beta_1} + \cdots + \xi_{\alpha_\mu,\beta_\mu}$ is an absolute invariant of Γ',[†] while Γ, being irreducible, can have none. Hence Γ' is a proper subgroup of Γ, and G' is a proper subgroup of G. Therefore, G_0 is a non-maximal subgroup of G, and G is imprimitive.

3. Throughout this paper, i and j will represent positive integers relatively prime to p and q, respectively.

We introduce

$$T_{i,j}: \qquad x_{u,v} = \frac{1}{n}\sum_{y=0}^{p^a-1}\sum_{z=0}^{q^b-1}(\epsilon^i)^{uy}(\eta^j)^{vz}\xi_{y,z}$$

$$(u = 0, 1, \cdots, p^a - 1; v = 0, 1, \cdots, q^b - 1),$$

and let $\Gamma_{y,z}$ represent the irreducible constituent of $T^{-1}GT$ which affects, among others, the variable $\xi_{y,z}$, and let $\Gamma_{y,z}^{(i,j)}$ represent the irreducible constituent of $T_{i,j}^{-1}GT_{i,j}$ which affects $\xi_{y,z}$. If we replace ϵ by ϵ^i and η by η^j, we obtain from the substitution $T^{-1}AT$, the substitution $T_{i,j}^{-1}AT_{i,j}$.

Since we can write T in the form

* Cf. W. Burnside, *Theory of Groups of Finite Order*, 2d edition (1911), p. 342.

† W. Burnside, *On certain simply-transitive permutation-groups*, Proceedings of the Cambridge Philosophical Society, vol. 20 (1921), p. 483.

$$x_{u,v} = \frac{1}{n} \sum_{y=0}^{p^a-1} \sum_{z=0}^{q^b-1} \epsilon^{u(iy)} \eta^{v(jz)} \xi_{iy,jz}$$

$$(u = 0, 1, \cdots, p^a - 1; v = 0, 1, \cdots, q^b - 1),$$

$T = T_{i,j} W_{i,j}$, where $W_{i,j}$ is the permutation $\xi_{y,z} = \xi'_{iy,jz}$ $(y=0, 1, \cdots, p^a-1;$ $z=0, 1, \cdots, q^b-1)$. Hence $T^{-1}AT = W_{i,j}^{-1}(T_{i,j}^{-1}AT_{i,j})W_{i,j}$. This shows that $\Gamma_{y,z}^{(i,j)}$ and $\Gamma_{iy,jz}$ differ only in the names of their variables. That is, if we consider the corresponding matrix groups, the variables of $\Gamma_{y,z}^{(i,j)}$ being denoted $\xi_{\alpha_1,\beta_1}, \xi_{\alpha_2,\beta_2}, \cdots, \xi_{\alpha_\mu,\beta_\mu}$ and the rows and columns of the matrices of the first matrix group being made to correspond to the variables in that order, then the variables of $\Gamma_{iy,jz}$ are $\xi_{i\alpha_1,j\beta_1}, \xi_{i\alpha_2,j\beta_2}, \cdots, \xi_{i\alpha_\mu,j\beta_\mu}$ and if the rows and columns of the matrices of the second group are made to correspond to the variables in this order, then the two matrix groups consist of the same matrices and the two matrices which correspond to A are equal.* Combining the results of these two paragraphs, we have

LEMMA II. *If we replace ϵ by ϵ^i and η by η^j, we "replace $\Gamma_{y,z}$ by $\Gamma_{iy,jz}$," that is, from the matrix of $\Gamma_{y,z}$ which corresponds to any permutation of G, we obtain the matrix of $\Gamma_{iy,jz}$ which corresponds to the same permutation of G, provided that if the rows and columns of the matrices of $\Gamma_{y,z}$ correspond to the variables $\xi_{\alpha_1,\beta_1}, \xi_{\alpha_2,\beta_2}, \cdots, \xi_{\alpha_\mu,\beta_\mu}$ in that order, then the rows and columns of the matrices of $\Gamma_{iy,jz}$ (which necessarily correspond to the variables $\xi_{i\alpha_1,j\beta_1}, \xi_{i\alpha_2,j\beta_2}, \cdots, \xi_{i\alpha_\mu,j\beta_\mu}$) correspond to them in that order.*

This gives us

LEMMA III. *If we replace ϵ by ϵ^i and η by itself, we replace $\Gamma_{0,z}$ by itself. If we replace ϵ by itself and η by η^j, we replace $\Gamma_{y,0}$ by itself.*

4. The operation of replacing ϵ by ϵ^i and η by η^j, we may denote by

$$\begin{pmatrix} \epsilon, & \eta \\ \epsilon^i, & \eta^j \end{pmatrix}.$$

These operations form a group K which is simply isomorphic to the group K' whose letters are the $p^a q^b$ symbols $\Gamma_{y,z}$ and whose permutations are of the form

$$\begin{pmatrix} \Gamma_{y,z} \\ \Gamma_{iy,jz} \end{pmatrix} = \begin{pmatrix} \Gamma_{0,0} & \cdots & \Gamma_{p^a-1,q^b-1} \\ \Gamma_{0,0} & \cdots & \Gamma_{i(p^a-1),j(q^b-1)} \end{pmatrix}.$$

Its order is $\phi(p^a)\phi(q^b)$.†

---

* Two matrices are equal to one another if and only if corresponding elements are equal.

† Euler's ϕ-function.

Our system of notation for the irreducible constituents gives us as many different symbols for a given irreducible constituent as it has variables. The actual number γ of irreducible constituents is less than $p^a q^b$, for otherwise G would be Abelian and H would not be a proper subgroup of G. Let K'' represent the group according to which the irreducible constituents are permuted by the operations of K. Then K'' is of degree γ, its order lies between 1 and $\phi(p^a)\phi(q^b)$, inclusive, and the number of its transitive constituents (counting those on one letter) lies between 2 and $(a+1)(b+1)$, inclusive, and will be shown later to be greater than 2.

DEFINITION. *The $\phi(p^{a-u})\phi(q^{b-v})$ variables ξ_{ip^u, iq^v} for given values of u and v $(0 \leq u \leq a, 0 \leq v \leq b)$ will be said to belong to the (u, v) category.*

LEMMA IV. *The variables of the (u, v) category are affected by irreducible constituents all of which belong to the same transitive constituent of K''.*

For Γ_{ip^u, iq^v} is replaced by $\Gamma_{i'p^u, i'q^v}$ by the operation

$$\begin{pmatrix} \epsilon & , & \eta \\ \epsilon^i & , & \eta^j \end{pmatrix}^{-1} \cdot \begin{pmatrix} \epsilon & , & \eta \\ \epsilon^{i'} & , & \eta^{i'} \end{pmatrix}$$

of K.

We shall say that the (u, v) category belongs to this transitive constituent of K''.

It follows from Lemma II that all the irreducible constituents of a given transitive constituent of K'' have the same number of variables belonging to any given category. Hence Lemma IV gives us

LEMMA V. *If there are t irreducible constituents of $T^{-1}GT$ in a given transitive constituent of K'' and if one of these irreducible constituents affects a variable of the (u, v) category, then it must affect exactly $1/t$ of the variables of that category.*

5. We now prove

LEMMA VI. *If $\Gamma_{y,0}$ affects ξ_{ip^u, iq^v} $(v < b)$, it affects each of the variables ξ_{ip^u, q^v}, $\xi_{ip^u, 2q^v}$, $\cdots$, $\xi_{ip^u, (q-1)q^v}$, $\xi_{ip^u, (q+1)q^v}$, $\cdots$, $\xi_{ip^u, b-q^v}$. Whether $v < b$ or not, the number t of irreducible constituents in the transitive constituent of K'' to which $\Gamma_{y,0}$ belongs must divide $\phi(p^{a-u})$. Similarly for $\Gamma_{0,z}$. If $\Gamma_{y,0} = \Gamma_{0,z}$, $t = 1$ and this irreducible constituent affects all the variables of the (u, v) category.*

If $\Gamma_{y,0}$ affects ξ_{ip^u, iq^v}, $\Gamma_{y,0} = \Gamma_{ip^u, iq^v}$. By Lemma III, if we replace ϵ by itself and η by any primitive q^bth root of unity, $\eta^{i'}$ (say), we replace $\Gamma_{y,0}$ by itself. By Lemma II, if we do the same thing to Γ_{ip^u, iq^v}, we obtain $\Gamma_{ip^u, ij'q^v}$. If we let j' run through a reduced set of residues mod q^b, jj' will do the same, while if $v < b$, $jj'q^v$ will assume values congruent to q^v, $2q^v$, $\cdots$, $(q-1)q^v$,

$(q+1)q^v, \cdots, q^b-q^v \bmod q^b$, each $\phi(q^b)/\phi(q^{b-v})$ times. Hence the first statement.

The second statement then follows from Lemma V.

The irreducible constituent $\Gamma_{y,0}$ is invariant under the operation

$$\begin{pmatrix} \epsilon & , & \eta \\ \epsilon & , & \eta^j \end{pmatrix},$$

and $\Gamma_{0,z}$ is invariant under

$$\begin{pmatrix} \epsilon & , & \eta \\ \epsilon^i & , & \eta \end{pmatrix}.$$

Hence if $\Gamma_{y,0}=\Gamma_{0,z}$, it is invariant under their product

$$\begin{pmatrix} \epsilon & , & \eta \\ \epsilon^i & , & \eta^j \end{pmatrix},$$

and thus under the group K. Then $\Gamma_{y,0}$ alone forms one of the transitive constituents of K'' and, by Lemma V, it must affect all the variables of each category which belongs to it.

LEMMA VII. *The group K'' has at least two transitive constituents besides the one on $\Gamma_{0,0}$ alone.*

If K'' had only one transitive constituent besides the one on $\Gamma_{0,0}$ alone, all the variables except $\xi_{0,0}$ would belong to it. Then each of its irreducible constituents would contain at least one variable of an (a, v) category with $v<b$ and at least one variable of a (u, b) category with $u<a$. Hence, by Lemma VI, it would consist of just one irreducible constituent. Then $T^{-1}GT$ would consist of two irreducible constituents. But that is impossible, for G is, by hypothesis (§1), simply transitive.[*]

6. We now restrict our attention to the irreducible constituent $\Gamma_{p^{a-1},0}$ and the permutations P^vQ^z of the Abelian subgroup H. Let $\chi_{P^vQ^z}$ represent the trace of the substitution of $\Gamma_{p^{a-1},0}$ which corresponds to P^vQ^z and let μ represent the degree of $\Gamma_{p^{a-1},0}$.

It follows from Lemma VI that for the transitive constituent of K'' to which $\Gamma_{p^{a-1},0}$ belongs, t must divide $p-1$. Let

$$(6.1) \qquad\qquad c = (p-1)/t.$$

It also follows from Lemma VI (together with equations (1.1) and (1.2)) that we may write

---

[*] W. Burnside, *Theory of Groups of Finite Order*, 2d edition (1911), p. 339.

$$\chi_{PQ} = d_{a,b}(\epsilon^{A1} + \cdots + \epsilon^{A_c p^{a-1}})(\eta + \cdots + \eta^{q-1} + \eta^{q+1} + \cdots + \eta^{qb-1})$$

$$+ d_{a-1,b}(\epsilon^{pB1} + \cdots + \epsilon^{pB_c p^{a-2}})(\eta + \cdots + \eta^{q-1} + \eta^{q+1} + \cdots + \eta^{qb-1}) + \cdots$$

$$+ d_{1,b}(\epsilon^{p^{a-1}C1} + \cdots + \epsilon^{p^{a-1}C_c})(\eta + \cdots + \eta^{q-1} + \eta^{q+1} + \cdots + \eta^{qb-1})$$

$$+ d_{0,b}(\eta + \cdots + \eta^{q-1} + \eta^{q+1} + \cdots + \eta^{qb-1})$$

$$+ d_{a,b-1}(\epsilon^{D1} + \cdots + \epsilon^{D_c p^{a-1}})(\eta^q + \cdots + \eta^{(q-1)q} + \eta^{(q+1)q} + \cdots + \eta^{qb-q})$$

(6.2)
$$+ \cdots + d_{0,b-1}(\eta^q + \cdots + \eta^{(q-1)q} + \eta^{(q+1)q} + \cdots + \eta^{qb-q}) +$$

$$\cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots$$

$$+ d_{a,1}(\epsilon^{E1} + \cdots + \epsilon^{E_c p^{a-1}})(\eta^{qb-1} + \cdots + \eta^{qb-qb-1}) + \cdots$$

$$+ d_{0,1}(\eta^{qb-1} + \cdots + \eta^{qb-qb-1})$$

$$+ d_{a,0}(\epsilon^{F1} + \cdots + \epsilon^{F_c p^{a-1}}) + d_{a-1,0}(\epsilon^{pG1} + \cdots + \epsilon^{pG_c p^{a-2}}) + \cdots$$

$$+ d_{1,0}(\epsilon^{p^{a-1}H1} + \cdots + \epsilon^{p^{a-1}H_c}) + d_{0,0},$$

where $d_{k,l} = 1$ or 0 depending on whether the variables of the $(a-k, b-l)$ category do or do not belong to the transitive constituent of K'' which includes $\Gamma_{p^{a-1},0}$, and where each $A, B, \cdots, H$ is relatively prime to p and no two A's are equal, no two B's are equal, etc. Notice that $d_{1,0} = 1$ and $d_{0,0} = 0$.

Because of (1.1) and (1.2), we have

(6.3)
$$T^{-1}P^uQ^zT: \qquad \xi_{u,v} = \epsilon^{yu}\eta^{zv}\xi'_{u,v}$$

$$(u = 0, 1, \cdots, p^a - 1; v = 0, 1, \cdots, q^b - 1).$$

This shows that the substitution of $\Gamma_{p^{a-1},0}$ which corresponds to P^uQ^z is a multiplication and that it may be obtained from the substitution of $\Gamma_{p^{a-1},0}$ which corresponds to PQ by replacing ϵ by ϵ^y and η by η^z in each multiplier. We may obtain $\chi_{P^uQ^z}$ from χ_{PQ} by replacing ϵ by ϵ^y and η by η^z provided χ_{PQ} is written out in full as the sum of the μ multipliers just as they are taken from (6.3). (Any cancellation or substitution making use of any relation existing between powers of ϵ or powers of η, or between ϵ and η, etc., before replacing ϵ by ϵ^y and η by η^z will in general lead to incorrect results.) However, the expression in the right-hand member of (6.2) is such that we may obtain $\chi_{P^uQ^z}$ from it by replacing ϵ by ϵ^y and η by η^z.

We now make use of the following procedure: Replace ϵ by ϵ^y and η by η^z in the right-hand member of (6.2) (obtaining $\chi_{P^uQ^z}$). The sums obtained from the sums of powers of η are equal to ordinary integers. Replace each by the corresponding integer and collect like powers of ϵ, reducing exponents mod p^a. The result is a polynomial in ϵ with integers as coefficients. We write it

$$\chi_{P^uQ^z} = \sigma_0 + \sigma_1\epsilon + \sigma_2\epsilon^2 + \cdots + \sigma_{p^a-1}\epsilon^{p^a-1}.$$

Using the first and third members of (1.3), we obtain

$$(6.4) \qquad \sum_{k=0}^{p^a-1} \sigma_k \epsilon^k = \frac{\mu}{m} \sum_{u=1}^{m} \epsilon^{a_u \cdot p^{a-1}} \eta^{b_u \cdot 0},$$

where m denotes the degree of $\Delta_{y,z}$, the transitive constituent of G_0 which includes $x_{y,z}$ and where $x_{a_1,b_1}, x_{a_2,b_2}, \cdots, x_{a_m,b_m}$ are the letters of $\Delta_{y,z}$. Equation (6.4) holds except when $y \equiv 0 \mod p^a$ and $z \equiv 0 \mod q^b$ at the same time. From (6.4) we obtain

$$\sum_{k=0}^{p^a-1} \sigma_k \epsilon^k = \frac{\mu}{m} \sum_{l=0}^{p-1} \pi_l \epsilon^{l p^{a-1}},$$

where π_l is the number of letters x_{a_u,b_u} of $\Delta_{y,z}$ whose first subscripts a_u are congruent to $l \mod p$. Hence ϵ is a root of the equation

$$(6.5) \qquad \sum_{k=0}^{p^a-1} \sigma_k x^k - \frac{\mu}{m} \sum_{l=0}^{p-1} \pi_l x^{l p^{a-1}} = 0,$$

whose coefficients are rational numbers. But ϵ is also a root of the equation

$$(6.6) \qquad 1 + x^{p^{a-1}} + x^{2 p^{a-1}} + \cdots + x^{(p-1) p^{a-1}} = 0,$$

which is irreducible in the field of rational numbers.* Hence if the left-hand member of (6.5) is not identically zero, it must be divisible by the left-hand member of (6.6). In either case we may write the left-hand member of (6.5) in the form

$$(\gamma_0 + \gamma_1 x + \cdots + \gamma_{p^{a-1}-1} x^{p^{a-1}-1})(1 + x^{p^{a-1}} + x^{2 p^{a-1}} + \cdots + x^{(p-1) p^{a-1}}).$$

Therefore,

$$\sigma_0 - \frac{\mu}{m} \pi_0 = \sigma_{p^{a-1}} - \frac{\mu}{m} \pi_1 = \sigma_{2 p^{a-1}} - \frac{\mu}{m} \pi_2 = \cdots = \sigma_{(p-1) p^{a-1}} - \frac{\mu}{m} \pi_{p-1},$$

and

$$m = \sum_{l=0}^{p-1} \pi_l = \sum_{l=0}^{p-1} \left\{ \pi_k + \frac{m}{\mu} (\sigma_{l p^{a-1}} - \sigma_{k p^{a-1}}) \right\}.$$

Hence

$$(6.7) \qquad m \left\{ \mu + p \sigma_{k p^{a-1}} - (\sigma_0 + \sigma_{p^{a-1}} + \cdots + \sigma_{(p-1) p^{a-1}}) \right\} = p \mu \pi_k$$
$$(k = 0, 1, \cdots, p-1).$$

Let

$$(6.8) \qquad M_{y,z} = (p-1)\sigma_0 - (\sigma_{p^{a-1}} + \sigma_{2 p^{a-1}} + \cdots + \sigma_{(p-1) p^{a-1}}),$$

---

* Weber, *Lehrbuch der Algebra*, 2d edition (1898), vol. 1, pp. 459 and 600.

for the permutation $P^v Q^z$, and write $m_{y,z}$ instead of m for the degree of $\Delta_{y,z}$. When $k=0$, (6.7) becomes

(6.9) $$m_{y,z}\{\mu + M_{y,z}\} = p\mu\pi_0.$$

Adding the $p-1$ equations for which $k=1, 2, \cdots, p-1$, we obtain

(6.10) $$m_{y,z}\{(p-1)\mu - M_{y,z}\} = p\mu(\pi_1 + \pi_2 + \cdots + \pi_{p-1}).$$

When using these formulas, we must remember that $\pi_0, \cdots, \pi_{p-1}$ depend on $\Delta_{y,z}$ and that these formulas do not apply to $\Delta_{0,0}$.

7. Since p and μ are constants and since $m_{y,z}$ and π_0 can each have but one value for a given transitive constituent of G_0, (6.9) gives us

LEMMA VIII. *If $\Delta_{y',z'}$ is the same transitive constituent of G_0 as $\Delta_{y,z}$, then $M_{y',z'} = M_{y,z}$.*

DEFINITION. *The $\phi(p^{a-u})\phi(q^{b-v})$ letters $x_{i_{p^u},j_{q^v}}$ (u and v fixed) will be said to belong to the (u, v) category of letters.*

From the meaning of the π_l it follows that $\Delta_{y,z}$ includes at least one letter of some $(0, v)$ category if and only if $\pi_1 + \pi_2 + \cdots + \pi_{p-1} > 0$. Since $m_{y,z}$, μ, and p are positive integers, (6.10) shows us that when $\Delta_{y,z}$ is not $\Delta_{0,0}$, $\pi_1 + \pi_2 + \cdots + \pi_{p-1} > 0$ if and only if $(p-1)\mu - M_{y,z} > 0$.

LEMMA IX. *If $(p-1)\mu - M_{y,z} > 0$ and $\Delta_{y,z}$ is not $\Delta_{0,0}$, $\Delta_{y,z}$ includes at least one $x_{i,v}$ and $M_{y,z}$ is equal to at least one of the $M_{i,v}$.*

8. We now develop two sufficient conditions for the imprimitivity of G.

LEMMA X. *If an irreducible constituent of $T^{-1}GT$ which is not $\Gamma_{0,0}$ affects no variable of any $(0, v)$ category (or if it affects no variable of any $(u, 0)$ category), G is imprimitive.*

For if Γ affects no variable of any $(0, v)$ category, (1.1) shows that $P^{p^{a-1}}$ corresponds to the identity of Γ, and then, by Lemma I, G is imprimitive. If Γ affects no variable of any $(u, 0)$ category, $Q^{q^{b-1}}$ corresponds to the identity of Γ and again G is imprimitive.

LEMMA XI. *If $d_{a,b} = d_{a-1,b} = \cdots = d_{0,b}$, or if $d_{a,b} = d_{a,b-1} = \cdots = d_{a,0}$, G is imprimitive.*

For if $d_{a,b} = d_{a-1,b} = \cdots = d_{0,b} = 0$, it follows from the meaning of the $d_{k,l}$ (§6) that $\Gamma_{p^{a-1},0}$ contains no variable of the $(0, 0)$, the $(1, 0)$, $\cdots$, or the $(a, 0)$ category, and then, by Lemma X, G is imprimitive. If $d_{a,b} = d_{a-1,b} = \cdots = d_{0,b} = 1$, all the variables of those categories belong to the transitive constituent of K'' which includes $\Gamma_{p^{a-1},0}$. By Lemma VII, there must then be at least one transitive constituent of K'' besides the one

on $\Gamma_{0,0}$ alone whose irreducible constituents affect none of the variables of those categories. We apply Lemma X to one of those irreducible constituents and see that G is imprimitive. Hence, if $d_{a,b}=d_{a-1,b}=\cdots=d_{0,b}$, G is imprimitive. The proof of the other half of the lemma is similar.

9. To simplify the formulas, we let

$$(9.1) \qquad d_{a+1,0} = \cdots = d_{a+1,b} = d_{0,b+1} = \cdots = d_{a,b+1} = d_{a+1,b+1} = 0,$$

and let $R_{u,v}$ represent the number of variables in the $(a-u, b-v)$ category affected by $\Gamma_{p^{a-1},0}$. Then

$$(9.2) \qquad R_{u,v} = d_{u,v}\phi(p^u)\phi(q^v)/t.$$

Equation (6.8) now gives us

$$
\begin{aligned}
(9.3) \qquad M_{ip^k,jq^l} = {} & d_{k+1,l+1}cp^kq^l - \sum_{v=0}^{l} R_{k+1,v} \\
& + (p-1)\left(-\sum_{u=1}^{k} d_{u,l+1}cp^{u-1}q^l - d_{0,l+1}q^l + \sum_{u=0}^{k}\sum_{v=0}^{l} R_{u,v}\right).
\end{aligned}
$$

(To obtain this expression, it is neither necessary nor desirable to calculate $\sigma_{p^{a-1}}$, $\sigma_{2p^{a-1}}$, $\cdots$, $\sigma_{(p-1)p^{a-1}}$ separately. It is easier to calculate their sum directly.)

To calculate $(p-1)\mu - M_{ip^k,jq^l}$, we make use of the fact that we may write

$$
\begin{aligned}
\mu = \sum_{u=0}^{a}\sum_{v=0}^{b} R_{u,v} = {} & \sum_{u=0}^{k}\sum_{v=0}^{l} R_{u,v} + \sum_{u=0}^{k}\sum_{v=l+1}^{l+1} R_{u,v} + \sum_{u=k+1}^{k+1}\sum_{v=0}^{l} R_{u,v} \\
& + \sum_{u=k+1}^{k+1}\sum_{v=l+1}^{l+1} R_{u,v} + \sum_{u=k+2}^{a}\sum_{v=0}^{l+1} R_{u,v} + \sum_{u=0}^{k+1}\sum_{v=l+2}^{b} R_{u,v} + \sum_{u=k+2}^{a}\sum_{v=l+2}^{b} R_{u,v},
\end{aligned}
$$

where any summation is to be considered equal to zero if one or both of its $\sum$'s starts with a number larger than the one with which it ends. Then

$$
\begin{aligned}
(9.4) \qquad (p-1)\mu - M_{ip^k,jq^l} = {} & (p-1)\left\{\sum_{u=k+2}^{a}\sum_{v=0}^{l+1} R_{u,v} + \sum_{u=0}^{k+1}\sum_{v=l+2}^{b} R_{u,v}\right. \\
& \left. + \sum_{u=k+2}^{a}\sum_{v=l+2}^{b} R_{u,v}\right\} + d_{k+1,l+1}cp^kq^l\{(p-1)(q-1)-1\} \\
& + \sum_{v=1}^{l} d_{k+1,v}cp^{k+1}(q-1)q^{v-1} + d_{k+1,0}cp^{k+1} \\
& + \sum_{u=1}^{k} d_{u,l+1}c(p-1)p^{u-1}q^{l+1} + d_{0,l+1}(p-1)q^{l+1}.
\end{aligned}
$$

10. Since we wish to prove whenever it may be possible that G is imprimitive, we need only consider the case when the conditions of Lemma XI are not satisfied. Then at least one of the $d_{u,b}=1$ and at least one of the $d_{a,v}=1$. We seek to show, when possible, that under these conditions $(p-1)\mu - M_{ip^k,jq^l} > 0$.

Notice first that each term of (9.4) is $\geqq 0$, and that each term is >0 if the corresponding $d_{u,v} \neq 0$ with the exception of the term $d_{k+1,l+1}cp^kq^l$ $\{(p-1)(q-1)-1\}$ when $p=q=2$.

If $k+2 \leqq a$, the terms which involve the $d_{a,v}$ $(v=0, 1, \cdots, b)$ occur within the first pair of brackets. Hence, since at least one of the $d_{a,v}=1$, $(p-1)\mu - M_{ip^k,jq^l} > 0$. Similarly if $l+2 \leqq b$.

If $k=a-1$ and $l=b-1$, the $d_{a,v}$ $(v=0, 1, \cdots, b)$ and $d_{u,b}$ $(u=0, 1, \cdots, a-1)$ occur in the last five terms (counting a summation as a term now) and $(p-1)\mu - M_{ip^k,jq^l} > 0$ except when $d_{a,0} = \cdots = d_{a,b-1} = d_{0,b} = \cdots = d_{a-1,b} = 0$ and $p=q=2$, and then it equals zero.

If $k=a-1$ and $l=b$, the $d_{a,v}$ $(v=0, 1, \cdots, b)$ occur in the terms $\sum_{v=1}^{l} d_{k+1,v}cp^{k+1}(q-1)q^{v-1}$ and $d_{k+1,0}cp^{k+1}$. Hence $(p-1)\mu - M_{ip^k,jq^l} > 0$. Similarly if $k=a$ and $l=b-1$.

The case $k=a$, $l=b$ corresponds to $\Delta_{0,0}$ and is of no interest since we cannot apply Lemma IX.

Combining these results, we find

LEMMA XII. *Unless one or more of the three conditions*

(1) $d_{a,b}=d_{a,b-1}= \cdots = d_{a,0}$,

(2) $d_{a,b}=d_{a-1,b}= \cdots = d_{0,b}$, *or*

(3) $p=q=2$

holds, $(p-1)\mu - M_{ip^k,jq^l} > 0$ *for each transitive constituent* Δ_{ip^k,jq^l} *not* $\Delta_{0,0}$.

When conditions (1) and (2) do not hold but condition (3) does, $(p-1)\mu - M_{ip^k,jq^l} = \mu - M_{2^k,2^l}$. Now $\mu - M_{2^k,2^l} > 0$ for all transitive constituents (not $\Delta_{0,0}$) except perhaps $\Delta_{2^{a-1},2^{b-1}}$. Lemma IX and its proof then tell us that when $\mu - M_{2^{a-1},2^{b-1}} = 0$, each transitive constituent of G_0 includes at least one letter of some $(0, v)$ category except $\Delta_{0,0}$ and $\Delta_{2^{a-1},2^{b-1}}$, and that they do not. Then $x_{2^{a-1},2^{b-1}}$ must be the only letter of $\Delta_{2^{a-1},2^{b-1}}$, and G_0 fixes at least two letters, $x_{0,0}$ and $x_{2^{a-1},2^{b-1}}$. Hence G is imprimitive.

Therefore, regardless of whether $p=q=2$ or not, we have, with the aid of Lemmas XI and IX,

LEMMA XIII. *If G is primitive, each transitive constituent of G_0 except $\Delta_{0,0}$ includes at least one letter of some $(0, v)$ category, and M_{p^k,q^l} is equal to at least one of the M_{i,jq^h} when $k+l < a+b$. Also each transitive constituent includes at least one letter of some $(u, 0)$ category, and M_{p^k,q^l} is equal to at least one of the $M_{ip^f,j}$.*

11. We can obtain an expression for M_{ip^k,jq^l} which is more convenient than (9.3) for comparing the M's as indicated in Lemma XIII. To this end, we observe that $(p-1)d_{0,v} = cd_{0,v}$, for if $d_{0,v} = 0$, it is obviously true and if $d_{0,v} = 1$, $\Gamma_{p^{a-1},0} = \Gamma_{0,jq^{b-v}}$, $t = 1$ (Lemma VI), and (6.1) gives us $c = p-1$. Starting from (9.3), we replace each $R_{u,v}$ by its value in terms of $d_{u,v}$, c, p, q, u, and v, making use of (9.2) and (6.1). The coefficient of each $d_{0,v}$ contains $p-1$ as a factor and we replace $(p-1)d_{0,v}$ by $cd_{0,v}$. On simplifying, we find

(11.1)
$$M_{ip^k,jq^l} = c \sum_{u=0}^{k} \sum_{v=0}^{l} D_{u,v} p^u q^v,$$

where

(11.2)
$$D_{u,v} = d_{u,v} - d_{u,v+1} - d_{u+1,v} + d_{u+1,v+1}.$$

LEMMA XIV. $D_{u,v}$ is an integer and $\left| D_{u,v} \right| \leqq 2$. Furthermore, $\left| D_{a,v} \right| \leqq 1$ and $\left| D_{u,b} \right| \leqq 1$.

For each $d_{u,v}$ is equal to one or zero (§6) and each $d_{a+1,v}$ and $d_{u,b+1}$ is zero (§9).

LEMMA XV. If $M_{p^k,q^l} = M_{i,jq^h}$ with $h < l$,

$$\sum_{u=1}^{k} \sum_{v=0}^{l} D_{u,v} p^u q^v = - \sum_{v=h+1}^{l} D_{0,v} q^v;$$

with $h = l$,

$$\sum_{u=1}^{k} \sum_{v=0}^{l} D_{u,v} p^u q^v = 0;$$

with $h > l$,

$$\sum_{u=1}^{k} \sum_{v=0}^{l} D_{u,v} p^u q^v = \sum_{v=l+1}^{h} D_{0,v} q^v.$$

If $M_{p^k,q^l} = M_{ip^f,j}$ with $f < k$,

$$\sum_{u=0}^{k} \sum_{v=1}^{l} D_{u,v} p^u q^v = - \sum_{u=f+1}^{k} D_{u,0} p^u;$$

with $f = k$,

$$\sum_{u=0}^{k} \sum_{v=1}^{l} D_{u,v} p^u q^v = 0;$$

with $f > k$,

$$\sum_{u=0}^{k} \sum_{v=1}^{l} D_{u,v} p^u q^v = \sum_{u=k+1}^{f} D_{u,0} p^u.$$

These may be obtained from (11.1).

LEMMA XVI. *If* $D_{a,0}=D_{a,1}=\cdots=D_{a,b-1}=0$, *or if* $D_{0,b}=D_{1,b}=\cdots$ $=D_{a-1,b}=0$, *G is imprimitive.*

For if $D_{a,0}=D_{a,1}=\cdots=D_{a,b-1}=0$, $d_{a,0}=d_{a,1}=\cdots=d_{a,b-1}=d_{a,b}$ and if $D_{0,b}=D_{1,b}=\cdots=D_{a-1,b}=0$, $d_{0,b}=d_{1,b}=\cdots=d_{a-1,b}=d_{a,b}$. In either case G is imprimitive, by Lemma XI.

For future convenience we introduce the function $F(h, l)$ defined in this way:

$$F(h, l) = -\sum_{v=h+1}^{l} D_{0,v}q^v \quad \text{when } 0 \leqq h < l \leqq b;$$

$$F(h, l) = 0 \qquad\qquad \text{when } 0 \leqq h = l \leqq b;$$

$$F(h, l) = \sum_{v=l+1}^{h} D_{0,v}q^v \quad \text{when } 0 \leqq l < h \leqq b.$$

12. We are now ready to prove the theorem stated in the introduction. For this purpose we take $p=q$ and $a>b$ and suppose that G is primitive. Let s be an integer satisfying $0 \leqq s \leqq b-1$ and consider M_{p^{a-1},p^s}. Because of Lemma XIII, it is equal to at least one of the M_{i,jp^h} ($h=0, 1, \cdots$, or b). Then because of Lemma XV, we have

$$(12.1) \qquad\qquad \sum_{u=1}^{a-1}\sum_{v=0}^{s} D_{u,v}p^{u+v} = F(h, s).$$

Since $a+s \leqq a+b-1 < a+b$, we also know that, M_{p^a,p^s} must be equal to at least one of the M_{i,jp^h}, to $M_{i',j'p^{h'}}$, say. Then

$$(12.2) \qquad\qquad \sum_{u=1}^{a}\sum_{v=0}^{s} D_{u,v}p^{u+v} = F(h', s).$$

(The values of h and h' are determined by the group G, but are unknown to us.) Subtracting (12.1) from (12.2), we find

$$(12.3) \qquad\qquad \sum_{v=0}^{s} D_{a,v}p^{a+v} = F(h', s) - F(h, s).$$

Notice that for a fixed value of s the coefficient of $D_{0,v}$ in $F(h, s)$ if not zero is independent of h. Hence, if the values of h and h' are such that the coefficient of $D_{0,v}$ in neither $F(h, s)$ nor $F(h', s)$ is zero, the corresponding terms cancel in $F(h', s) - F(h, s)$.

We now take $s=0$ and try to show that $D_{a,0}=0$. For that purpose, it is sufficient to show that $|D_{a,0}p^a| < p^a$, for then $|D_{a,0}| < 1$, and since $D_{a,0}$ is an integer (Lemma XIV), it must be zero.

Since $p=q$,

$$F(0, 0) = 0,$$
$$F(1, 0) = D_{0,1}p,$$
$$F(2, 0) = D_{0,1}p + D_{0,2}p^2,$$

$$\cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot \ \cdot$$

$$F(b, 0) = D_{0,1}p + D_{0,2}p^2 + \cdots + D_{0,b}p^b.$$

If $b=1$, (12.3), Lemma XIV, and the condition $b<a$ used in turn give us

$$|D_{a,0}p^a| \leq |D_{0,1}p| \leq p < p^a.$$

There remains for consideration the case $b>1$.
If $h<b$ and $h'<b$,

$$|D_{a,0}p^a| \leq |D_{0,1}p| + |D_{0,2}p^2| + \cdots + |D_{0,b-1}p^{b-1}|$$
$$\leq 2p + 2p^2 + \cdots + 2p^{b-1} = 2(p^b - p)/(p - 1)$$
$$\leq 2p^b - 2p < p^{b+1} \leq p^a.$$

If $h=h'=b$,

$$D_{a,0}p^a = 0, \qquad D_{a,0} = 0.$$

The remaining possibility is that $h=b$ and $h'<b$ or that $h'=b$ and $h<b$. Then if $D_{0,b}=0$,

$$|D_{a,0}p^a| \leq |D_{0,1}p| + |D_{0,2}p^2| + \cdots + |D_{0,b-1}p^{b-1}| + 0$$
$$\leq 2p + 2p^2 + \cdots + 2p^{b-1} < p^a.$$

If $D_{0,b}\neq 0$, $D_{0,b}=\pm 1$, by Lemma XIV. Then, since $D_{0,b-1}$ is an integer and $|D_{0,b-1}| \leq 2$, $D_{0,b-1}$ is equal to $D_{0,b}$, $2D_{0,b}$, $-D_{0,b}$, $-2D_{0,b}$, or 0.
If $D_{0,b-1}=D_{0,b}$,

$$d_{0,b-1} - d_{0,b} - d_{1,b-1} + d_{1,b} = d_{0,b} - d_{1,b},$$
$$d_{0,b-1} - d_{1,b-1} = 2(d_{0,b} - d_{1,b}),$$
$$d_{0,b-1} - d_{1,b-1} \equiv 0 \bmod 2.$$

But

$$|d_{0,b-1} - d_{1,b-1}| \leq 1.$$

Therefore $d_{0,b-1}-d_{1,b-1}=0$, $d_{0,b}-d_{1,b}=0$, and $D_{0,b}=0$, contrary to our hypothesis.

The case $D_{0,b-1}=2D_{0,b}$ can also be shown to be impossible when $D_{0,b}\neq 0$, and in much the same way.

If $D_{0,b-1}=-D_{0,b}$, we consider separately the two possibilities $|h-h'|=1$

and $|h-h'|>1$. ($|h-h'|=0$ is impossible since, by hypothesis, one of the numbers h or h' is equal to b and the other is not.)

When $|h-h'|=1$, one of the two numbers h and h' is equal to b and the other to $b-1$. Then

$$|D_{a,0}p^a| = |D_{0,b}p^b| = p^b < p^a.$$

When $|h-h'|>1$, if $b=2$,

$$\begin{aligned}|D_{a,0}p^a| &= |D_{0,1}p + D_{0,2}p^2| \\ &= |D_{0,2}(-p+p^2)| \\ &= p^2 - p < p^2 < p^a.\end{aligned}$$

If $b>2$,

$$\begin{aligned}|D_{a,0}p^a| &\leqq |D_{0,1}p| + \cdots + |D_{0,b-2}p^{b-2}| + |D_{0,b-1}p^{b-1} + D_{0,b}p^b| \\ &\leqq 2p + \cdots + 2p^{b-2} + p^b - p^{b-1} \\ &= 2(p^{b-1}-p)/(p-1) + p^b - p^{b-1} \\ &\leqq 2p^{b-1} - 2p + p^b - p^{b-1} \\ &< p^b + p^{b-1} < 2p^b \leqq p^a.\end{aligned}$$

So that if $D_{0,b-1}=-D_{0,b}$, $|D_{a,0}p^a|<p^a$.

The case $D_{0,b-1}=-2D_{0,b}$ may be handled in much the same way. Again $|D_{a,0}p^a|<p^a$.

The fifth and last possibility was $D_{0,b-1}=0$. Then, if $b=2$,

$$|D_{a,0}p^a| \leqq 0 + |D_{0,2}p^2| = p^2 < p^a.$$

If $b>2$,

$$\begin{aligned}|D_{a,0}p^a| &\leqq |D_{0,1}p| + \cdots + |D_{0,b-2}p^{b-2}| + 0 + |D_{0,b}p^b| \\ &\leqq 2p + \cdots + 2p^{b-2} + p^b \\ &= 2(p^{b-1}-p)/(p-1) + p^b \\ &\leqq 2p^{b-1} - 2p + p^b < 2p^b \leqq p^a.\end{aligned}$$

So that in all cases $D_{a,0}=0$.

We now make use of this fact and (12.3) to calculate $D_{a,s}$ when $0<s<b$. We may write (12.3):

$$D_{a,s}p^{a+s} = F(h', s) - F(h, s) - \sum_{v=0}^{s-1} D_{a,v}p^{a+v},$$

so that

$$\left| D_{a,s}p^{a+s} \right| \leqq \left| D_{0,1}p \right| + \cdots + \left| D_{0,b-1}p^{b-1} \right| + \left| D_{0,b}p^b \right|$$
$$+ \left| D_{a,0}p^a \right| + \left| D_{a,1}p^{a+1} \right| + \cdots + \left| D_{a,s-1}p^{a+s-1} \right|$$
$$\leqq 2p + \cdots + 2p^{b-1} + p^b + 0 + p^{a+1} + \cdots + p^{a+s-1}$$
$$= 2(p^b - p)/(p - 1) + p^b + (p^{a+s} - p^{a+1})/(p - 1)$$
$$\leqq 2p^b - 2p + p^b + p^{a+s} - p^{a+1}$$
$$= p^{a+s} + (3p^b - p^{a+1}) - 2p < p^{a+s},$$
$$D_{a,s} = 0.$$

Hence we have $D_{a,0} = D_{a,1} = \cdots = D_{a,b-1} = 0$. But, by Lemma XVI, that is impossible when G is primitive. Therefore G is imprimitive when $p = q$ and $a \neq b$. That it is also compound follows from the last paragraph of the introduction.

13. The corresponding theorem when $p \neq q$ is covered by Schur's paper.[*] However, we are now in a position to prove it quite easily. And a proof based on the properties of group characters is not without interest, for the question of the relative advantages of using the theory of group characters (and the roots of unity which it involves) or of avoiding all irrational quantities as Schur did, is of importance to future investigations in the field. We therefore include the proof.

We may without loss of generality suppose that $p < q$. Assume that G is primitive. Then, by Lemma XIII, $M_{p,1}$ is equal to some M_{i,jq^h} with $h = 0, 1, \cdots,$ or b.

If $h = 0$, Lemma XV gives us

$$\sum_{u=1}^{1} \sum_{v=0}^{0} D_{u,v}p^u q^v = 0,$$

$$D_{1,0} = 0.$$

If $h > 0$,

$$\sum_{u=1}^{1} \sum_{v=0}^{0} D_{u,v}p^u q^v = \sum_{v=1}^{h} D_{0,v}q^v,$$

$$D_{1,0}p = D_{0,1}q + D_{0,2}q^2 + \cdots + D_{0,h}q^h,$$

$$D_{1,0} \equiv 0 \bmod q.$$

Since p and q are both primes and $p < q$, $q \geqq 3$. Now $\left| D_{1,0} \right| \leqq 2$ (by Lemma XIV). Therefore $D_{1,0} = 0$.

Hence, regardless of h, $D_{1,0} = 0$.

Suppose $D_{1,0} = D_{2,0} = \cdots = D_{k-1,0} = 0$ and consider $M_{p^k,1}$ ($1 < k \leqq a$). By Lemma XIII, it is equal to some M_{i,jq^h} with $h = 0, 1, \cdots,$ or b.

* *Zur Theorie der einfach transitiven Permutationsgruppen*, Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-mathematische Klasse, 1933, pp. 598–623.

If $h=0$, by Lemma XV,

$$\sum_{u=1}^{k} \sum_{v=0}^{0} D_{u,v} p^u q^v = 0,$$

$$D_{1,0} p + D_{2,0} p^2 + \cdots + D_{k-1,0} p^{k-1} + D_{k,0} p^k = 0,$$

$$D_{k,0} p^k = 0,$$

$$D_{k,0} = 0.$$

If $h>0$,

$$\sum_{u=1}^{k} \sum_{v=0}^{0} D_{u,v} p^u q^v = \sum_{v=1}^{h} D_{0,v} q^v,$$

$$D_{k,0} p^k = D_{0,1} q + D_{0,2} q^2 + \cdots + D_{0,h} q^h,$$

$$D_{k,0} \equiv 0 \bmod q,$$

$$D_{k,0} = 0.$$

So that, regardless of h, $D_{k,0}=0$.

Hence, by induction, $D_{1,0}=D_{2,0}=\cdots=D_{a,0}=0$.

Lemma XIII tells us that M_{p^k,q^l} is equal to at least one of the $M_{i,p^f,j}$. Then since $D_{1,0}=D_{2,0}=\cdots=D_{a,0}=0$, the second part of Lemma XV shows us that, regardless of the value of f,

$$\sum_{u=0}^{k} \sum_{v=1}^{l} D_{u,v} p^u q^v = 0.$$

By applying this equation using in turn the following sets of values for k and l:

$$(0, 1), \qquad (0, 2), \qquad \cdots, (0, b),$$
$$(1, 1), \qquad (1, 2), \qquad \cdots, (1, b),$$
$$\cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots,$$
$$(a - 1, 1), (a - 1, 2), \cdots, (a - 1, b),$$

we find $D_{u,v}=0$ ($u=0, 1, \cdots, a-1$; $v=1, 2, \cdots, b$). But $D_{0,b}=D_{1,b}=\cdots=D_{a-1,b}=0$ is impossible when G is primitive (Lemma XVI). Hence G is imprimitive when $p \neq q$.

14. Combining the results of §§12 and 13 with the remarks made in the introduction about imprimitive groups with transitive Abelian subgroups, we have the

THEOREM. *If p and q represent prime numbers, which may or may not be equal, and a and b positive integers, a simply transitive permutation group G of degree $n = p^a q^b$ which contains a transitive Abelian subgroup of degree n generated by two permutations, one of order p^a and one of order q^b, is imprimitive and has an invariant proper subgroup unless $p^a = q^b$.*

15. We are now ready to discuss Burnside's paper of 1921, which we mentioned in the introduction. It gives his proof of the theorem stated there when the Abelian subgroup can have two independent generators. The preliminary work is essentially that given in §1 of the present paper, the principal difference being that Burnside did not restrict the orders of the generators of the Abelian subgroup to powers of primes as has been done in this paper. The proof itself consists of two parts corresponding to the two cases in which (1) the order of at least one of the two generators is composite, and (2) the orders of both generators are primes.

In the first case, it will be sufficient to show that the work is incorrect when the orders of the generators are powers of primes. If, for example, p^a is composite, the statement from which Burnside concluded that G is compound says that P^p is represented by the identity of $\Gamma_{p^{a-1},0}$. However, that cannot in general be true, for Lemma I shows us that if it were true, G would be imprimitive. This is contradicted by the existence of exceptions, for example, the simply transitive primitive groups of degree k^2 and order $2(k!)^2$ mentioned in the introduction when $k = p^a$ with $a > 1$. So that the first and most important part of the proof must contain a serious mistake.

The other case which Burnside takes up is that in which the two generators are of different prime orders. To quote from this paper (changing the notation to conform with that which we have been using): "If p and q are different primes, and Γ is that irreducible representation to which $\xi_{1,0}$ beongs, so that $\chi_{P^a u Q^b u} = (\mu/m) \sum_{u=1}^{m} \epsilon^{au}$, then

$$(15.1) \qquad \frac{\mu}{m} \sum_{u=1}^{m} \epsilon^{au} = \sum_{v=1}^{\mu} \epsilon^{au} \alpha_v \eta^{b_u} \beta_v.$$

Unless each β_v is zero, in which case the group has a self-conjugate subgroup containing Q, this equation actually contains powers of η on the right. Hence when the indices of the powers of η are reduced (mod q) each power must occur with the same coefficient. This shews that μ must be a multiple of q, and $\cdots$." We cannot deny that μ is a multiple of q when at least one of the β_v is not equal to zero,[*] but we do deny that that conclusion can be drawn

---

[*] For the material of §§10–13 may be used to show that if the first two conditions of Lemma XII are not satisfied, either each transitive constituent of G_0 except $\Delta_{0,0}$ affects at least one $x_{i,z}$ $(i, p) = 1$, or G is imprimitive and $p = q = 2$. In the former case, we found that unless $p^a = q^b$, $D_{a,0} = \cdots = D_{a,b-1} = 0$ or $D_{0,b} = \cdots = D_{a-1,b} = 0$, both of which contradict the assumption that the first two conditions of Lemma XII are not satisfied. Therefore, except perhaps when $p = q = 2$ or $p^a = q^b$, at least one of the first two conditions of Lemma XII is satisfied. We apply this fact and Lemma VII to $\Gamma_{p^{a-1},0}$ when $n = pq$ $(p \neq q)$. Either $d_{1,1} = d_{1,0} \neq d_{0,1}$ or $d_{1,1} = d_{0,1} \neq d_{1,0}$. But $d_{1,0}$ always equals one. Therefore if $d_{1,1} = d_{0,1}$, both equal zero, and each β_v equals zero. Hence if at least one of the β_v is not zero, $d_{1,1} = d_{1,0} = 1$, $d_{0,1} = 0$, and $\mu = c(q-1) + c = cq$.

directly from (15.1). For if we use the permutation PQ, (15.1) becomes

(15.2) $$\frac{\mu}{m} \sum_{u=1}^{m} \epsilon^{\alpha u} = \sum_{v=1}^{\mu} \epsilon^{\alpha_v} \eta^{\beta_v}.$$

It is possible to set up letters for the transitive constituent of G_0 which involves $x_{1,1}$ and variables for $\Gamma_{1,0}$ which satisfy the requirements imposed by (15.2) and for which μ is not a multiple of q. For example, if $p=3$ and $q=5$, we might propose $x_{1,1}$, $x_{2,1}$, $x_{0,1}$, $x_{1,2}$, $x_{2,2}$, $x_{1,3}$, $x_{2,3}$, $x_{1,4}$, $x_{2,4}$ as the letters of $\Delta_{1,1}$, and $\xi_{1,0}$, $\xi_{2,0}$, $\xi_{0,1}$, $\xi_{0,2}$, $\xi_{0,3}$, $\xi_{0,4}$ as the variables of $\Gamma_{1,0}$. Then $\mu=6$, $m=9$, and (15.2) becomes

$$\frac{6}{9}(\epsilon + \epsilon^2 + 1 + \epsilon + \epsilon^2 + \epsilon + \epsilon^2 + \epsilon + \epsilon^2) = \epsilon + \epsilon^2 + \eta + \eta^2 + \eta^3 + \eta^4,$$

and since ϵ now denotes a primitive cube root of unity and η a primitive fifth root of unity, this reduces to

$$- 2 = - 2.$$

So that the proof of the second case is also incorrect.

The cases in which the Abelian subgroup cannot be generated by two generators Burnside dismisses with the statement, "It is clear that the same method of proof will apply, when the transitive Abelian subgroup has three or more independent generators." So the failure of his proof when the Abelian subgroup has two generators leaves the theorem unproved except in the cases dealt with elsewhere.

STANFORD UNIVERSITY,
    PALO ALTO, CALIFORNIA