ON THE ORDER OF LINEAR HOMOGENEOUS GROUPS*

(SECOND PAPER)

BY

H. F. BLICHFELDT

Introduction.

§ 1. In 1878 JORDAN proved a theorem concerning linear homogeneous groups which may be enunciated as follows: Every such group G in n variables has an abelian self-conjugate subgroup F of order f, and the order of G is λf, where λ is inferior to a fixed number which depends only upon n.† The proof of this theorem is quite remarkable, the more so since the limit of λ is not determined. The writer of the present article is not aware of any attempts that have been made since 1878 to find a limit to λ—aside from the cases $n = 2, 3, 4$—and he presents herewith some theorems which, in connection with some given by him in these Transactions, vol. 4 (1903), pp. 387–397, can be utilized to determine a number that λ must divide, at least in the case of "primitive" groups. However, the chief object of the present paper is not this, but rather the presentation of some methods and theorems that are useful in the construction of the groups considered. As an illustration, the primitive groups in three variables are enumerated at the end of the paper.

The technical terms and phrases defined in the paper *On the order of linear homogeneous groups*, these Transactions, vol. 4, already referred to, will be retained here. As the present article is considered a continuation of this earlier paper—to which we shall hereafter refer by *Linear groups* I—we shall begin with Theorem 8, meaning by the Theorems 1–7 those of *Linear groups* I. Unless otherwise stated, the substitutions used are linear and homogeneous in the variables concerned, and of determinant 1.

Primitive groups containing intransitive self-conjugate subgroups.

§ 2. Let H be an intransitive self-conjugate subgroup of a primitive group G in n variables. Its different systems of intransitivity may not contain the same number of variables, especially as H may possibly be exhibited as an

* Presented to the Society at the San Francisco meeting, December 25, 1903. Received for publication December 18, 1903.

† Journal für Mathematik, vol. 84 (1878), p. 89.

intransitive group in more than one way. Supposing the least number of variables that may occur in a system is a, let $x_1, x_2, \cdots, x_a$ be the variables of such a system or set, as we shall call it. Then must H be transitive in $x_1, x_2, \cdots, x_a$.

The substitutions of G cannot all leave the set $(x_1, \cdots, x_a)$ invariant (we shall say that a substitution or a group leaves a set of variables invariant if the given substitution or the substitutions of the given group transform each of the variables of the set into linear functions of the set), or G would be intransitive.* Hence, some one substitution of G must transform the set $(x_1, \cdots, x_a)$ into a new set $(y_1, \cdots, y_a)$, the variables of which are not all linear functions of $x_1, \cdots, x_a$ alone, which set must also be left invariant by H. If $y_1, \cdots, y_a$, which are evidently linearly independent of each other, were connected with $x_1, \cdots, x_a$ by b linear relations $(b < a)$, say $x_1 = y_1, x_2 = y_2, \cdots, x_b = y_b$, to which form such relations could always be brought by a proper transformation, then it is evident that H should leave invariant the set $(x_1, \cdots, x_b)$, i. e., H could not be transitive in the variables $x_1, \cdots, x_b, x_{b+1}, \cdots, x_a$.* Thus, the $2a$ variables $x_1, \cdots, x_a; y_1, \cdots, y_a$ are linearly independent.

If $2a < n$, G cannot leave the variables $(x_1, \cdots, x_a, y_1, \cdots, y_a)$ invariant. Hence, some one substitution of G must transform $(x_1, \cdots, x_a)$ into a new set $(z_1, \cdots, z_a)$, which must also be left invariant by H. If $3a < n$, we proceed in the same manner, and we get, finally, k sets of variables $(n = ka)$, linearly independent of each other,

$$(1) \qquad (x_1, \cdots, x_a), \quad (y_1, \cdots, y_a), \quad (z_1, \cdots, z_a), \quad \cdots,$$

forming the different systems of intransitivity of H.

§ 3. Now, G cannot merely permute among themselves the sets (1), or it would be imprimitive. Some one substitution of G must therefore transform the set $(x_1, \cdots, x_a)$ into a set containing variables from two or more of the sets (1), say from the second and third. Let the set obtained be

$$(2) \qquad \sum_{i=1}^{a} (\alpha_{ij} y_i + \beta_{ij} z_i) \qquad (j = 1, 2, \cdots, a),$$

which is also left invariant by H.

The expressions

$$\sum_{i=1}^{a} \alpha_{ij} y_i \qquad (j = 1, 2, \cdots, a)$$

must be linearly independent of each other, or H would be intransitive in the variables $y_1, \cdots, y_a$, by MASCHKE's theorem. Similarly, the expressions

$$\sum_{i=1}^{a} \beta_{ij} z_i \qquad (j = 1, 2, \cdots, a)$$

* MASCHKE, *Beweis des Satzes, dass diejenigen endlichen linearen Substitutionsgruppen, in welchen einige durchgehends verschwindende Coefficienten auftreten, intransitiv sind*, Mathematische Annalen, vol. 52 (1899), pp. 363–368.

must be linearly independent of each other. We may therefore, by a transformation affecting only the letters $y_1, \cdots, y_a$, write the set (2) in the form

$$y_1 + z_1,\ y_2 + z_2,\ \cdots,\ y_a + z_a.$$

It is readily seen that H will leave the invariant set

$$(3) \qquad s_1 y_1 + s_2 z_1,\ s_1 y_2 + s_2 z_2,\ \cdots,\ s_1 y_a + s_2 z_a,$$

s_1 and s_2 being arbitrary constants.

Noticing that H could not leave invariant the set (3), and also a set of the form

$$s_1 y_i + s_2 z_i' \qquad (i = 1, 2, \cdots, a),$$

$z_1', z_2', \cdots$ being linear functions of the variables $z_1, z_2, \cdots, z_a$, unless $z_1' = \rho z_1$, $z_2' = \rho z_2, \cdots$, we can carry out the process just started, proving finally that H must leave invariant a set of the form

$$(4) \qquad s_1 x_i + s_2 y_i + s_3 z_i + \cdots + s_k w_i \qquad (i = 1, 2, \cdots, a),$$

containing all the ka variables of G.

§ 4. Any substitution S of G will therefore transform the expression

$$\sum_{i=1}^{a} t_i (s_1 x_i + s_2 y_i + s_3 z_i + \cdots + s_k w_i),$$

$t_1, t_2, \cdots, t_a, s_1, s_2, \cdots, s_k$ being arbitrary constants, into the expression

$$\sum_{i=1}^{a} t_i' (s_1' x_i + s_2' y_i + s_3' z_i + \cdots + s_k' w_i),$$

where the different constants $t_1' s_1', t_2' s_1', \cdots, t_1' s_2', \cdots$, are obtained from the constants $t_1 s_1, t_2 s_1, \cdots, t_1 s_2, \cdots$, by a linear transformation, the matrix of which is the matrix transposed of the substitution S in the variables $x_1, x_2, \cdots, y_1, \cdots$. It can now be proved without difficulty that we may so choose $s_1', s_2', \cdots, t_1', t_2', \cdots$, that the letters $s_1, s_2, \cdots, s_k$ are transformed into $s_1', s_2', \cdots, s_k'$ by a linear substitution S' of determinant $\Delta' = 1$, the aggregate of which substitutions form a group G' isomorphic with G. Moreover, the letters $t_1, t_2, \cdots, t_a$ are transformed into $t_1', t_2', \cdots, t_a'$ by a linear substitution S'' of determinant Δ'', the aggregate of which form a group G'' isomorphic with G. If the matrices of S' and S'' are respectively

$$S': \begin{array}{c|cccc} & s_1 & s_2 & \cdots & s_k \\ \hline s_1 & \alpha_1 & \alpha_2 & \cdots & \alpha_k \\ s_2 & \beta_1 & \beta_2 & \cdots & \beta_k \\ \vdots & \cdot & \cdot & \cdot & \cdot \\ s_k & \kappa_1 & \kappa_2 & \cdots & \kappa_k \end{array}, \qquad S'': \begin{array}{c|cccc} & t_1 & t_2 & \cdots & t_a \\ \hline t_1 & \lambda_1 & \lambda_2 & \cdots & \lambda_a \\ t_2 & \mu_1 & \mu_2 & \cdots & \mu_a \\ \vdots & \cdot & \cdot & \cdot & \cdot \\ t_a & \rho_1 & \rho_2 & \cdots & \rho_a \end{array},$$

that of S is

$$S: \quad \begin{array}{c|cccccc} & x_1 & x_2 & \cdots & x_a & y_1 & \cdots \\ \hline x_1 & \alpha_1\lambda_1 & \alpha_1\mu_1 & \cdots & \alpha_1\rho_1 & \beta_1\lambda_1 & \cdots \\ x_2 & \alpha_1\lambda_2 & \alpha_1\mu_2 & \cdots & \alpha_1\rho_2 & \beta_1\lambda_2 & \cdots \\ \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x_a & \alpha_1\lambda_a & \alpha_1\mu_a & \cdots & \alpha_1\rho_a & \beta_1\lambda_a & \cdots \\ y_1 & \alpha_2\lambda_1 & \alpha_2\mu_1 & \cdots & \alpha_2\rho_1 & \beta_2\lambda_1 & \cdots \\ \vdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{array}.$$

To a similarity-substitution of G will correspond similarity-substitutions of G' and G''. The determinant of S being unity by assumption, we have $(\Delta')^a(\Delta'')^k = (\Delta'')^k = 1$. It follows that the groups G' and G'' are finite.

It will be found by an inspection of S, S' and S'', that if G is primitive, G' and G'' must be primitive.

We shall say that the group G is *produced* from the two groups G' and G''. Two primitive groups G' and G'' will not necessarily produce a primitive group G. On the other hand, primitive groups in four variables will result if for G' and G'' we take any two primitive groups in two variables, combining with every substitution S' of G' every substitution S'' of G'', in the manner shown.

We shall embody our results in the following

THEOREM 8. *If G, a primitive group in n variables, has an intransitive, non-abelian, self-conjugate subgroup H, then is $n = ka$, where k is the number of systems of intransitivity of H containing the least number of variables $a > 1$. By a proper choice of variables we can arrange these in k sets*

$$x_1, x_2, \cdots, x_a; \qquad y_1, y_2, \cdots, y_a; \qquad \cdots; \qquad w_1, \cdots, w_a;$$

so that H leaves invariant the system

$$s_1x_i + s_2y_i + \cdots + s_kw_i \qquad (i = 1, 2, \cdots, a),$$

$s_1, s_2, \cdots, s_k$ being arbitrary constants

Groups whose orders are powers of primes.

§ 5. DEFINITION. If the variables $x_1, x_2, \cdots, x_n$ of a group G may be so selected that the substitutions of G are all of the form

$$x_i' = \alpha_i x_{\lambda_i} \quad (i = 1, 2, \cdots, n;\ \lambda_1, \lambda_2, \cdots, \lambda_n = 1, 2, \cdots, n;\ \lambda_i \neq \lambda_j),$$

then we shall say that the group may be written in *semi-canonical* form.

THEOREM 9. *A group whose order is a power of a prime can be written in semi-canonical form.*

We begin by proving that a group of degree $n > 1$ and of order p^a, p being a prime, is always intransitive or imprimitive.

For a group G of order p^a is either abelian or it must contain an abelian self-conjugate subgroup whose substitutions are not all similarity-substitutions. In both cases the theorem would be true (Theorem 2).

To show the existence of such a subgroup, if G is non-abelian, we may proceed as follows. We can form a series of groups G, G_1, G_2, $\cdots$ of orders p^a, p^{a-1}, p^{a-2}, $\cdots$, each of which is a self-conjugate subgroup of those that precede it.* The substitutions of G_1 cannot all be self-conjugate substitutions of G, the number of which is at most p^{a-2}.† Therefore if G_1 is abelian, the proposition is proved. If G_1 is non-abelian, consider G_2. Its substitutions cannot all be self-conjugate substitutions of G_1, etc. We finally arrive at an abelian self-conjugate subgroup of G of the required character.

We shall now prove Theorem 9 for a transitive group in n variables, assuming it true for any group of order p^m in less than n variables. Under this assumption the theorem follows for an intransitive group in n variables.

For a transitive and imprimitive group G of order p^a the variables must fall into p^b sets ($n = kp^b$) which are permuted according to a substitution-group in p^b letters. These may easily be shown to fall into p systems of imprimitivity. Hence, the variables of G may be separated into p sets of n/p variables each, and G is generated by an intransitive group G', which leaves each of these sets invariant, and a substitution T which permutes them according to a circular substitution of order p. We shall merely illustrate the remainder of the proof by the special case $p = 3$, $n = 6$. We may exhibit G' in the form

$$G' = \begin{bmatrix} G_1 & 0 & 0 \\ 0 & G_2 & 0 \\ 0 & 0 & G_3 \end{bmatrix},$$

G_1 being a group in two variables, x_1, x_2 of order 3^c, and can therefore, by assumption, be written in semi-canonical form. Without transforming the variables x_1 and x_2, we may write T in the form

$$x_1' = x_3, \quad x_2' = x_4, \quad x_3' = x_5, \quad x_4' = x_6,$$
$$x_5' = \alpha x_1 + \beta x_2, \quad x_6' = \gamma x_1 + \delta x_2.$$

As T^3 belongs to G', the matrix $\left[\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right]$ must be found among those of G_1, so that $\alpha\beta = \gamma\delta = 0$. Noting that, if S_1 and S_2 are written in semi-canonical forms, so is $S_3 = S_1 S_2$, we readily see the truth of Theorem 9.

On the orders of the substitutions of a primitive group.

§ 6. DEFINITIONS. Let E be the sum of a finite number of roots of unity. Each of these can be written as the product of one (θ) whose index is a power

* BURNSIDE, *Theory of Groups*, p. 64.

† Ibid., p. 63.

of p (a prime), and one of index m, a number prime to p. Then, if every root θ be replaced by 1, the resulting value of E shall be denoted by $(E)_p$. It follows from KRONECKER's Theorem (see § 3, *Linear groups* I) that if $E = 0$, then is $(E)_p = pF$, where F is the sum of a finite number of roots of unity. We shall write this equation in the form

$$(E)_p \equiv 0 \pmod{p}.$$

The multipliers of a substitution are roots of unity. The *number* of these roots that are different from one another shall be called the *variety* of the substitution. Thus, a similarity-substitution is of variety 1.

THEOREM 10. *If a group G in n variables has a substitution S of variety m and of order $p^{a+c} \geqq mp^c$, then will G contain a self-conjugate sub-group H containing $S^{p^a} = T$ and all further substitutions of G which possess the property*

$$(V)_p \equiv (VT)_p^* \pmod{p}, \tag{5}$$

V being any substitution of G. In particular, $n \equiv (T)_p \pmod{p}$.

§ 7. We begin by proving that (5) holds if $T = S^{p^a}$. Supposing ϕ to be a primitive root of the equation $\phi^{p^{a+c}} - 1 = 0$, let $(S) = \phi + \phi^\alpha + \phi^\beta + \cdots$. Form the equation corresponding to the equation (3) of *Linear groups* I,

$$(6) \quad \begin{vmatrix} (V) & 1 & 1 & 1 & \cdots \\ (VT) & \phi^{p^a} & \phi^{\alpha p^a} & \phi^{\beta p^a} & \cdots \\ (VS) & \phi & \phi^\alpha & \phi^\beta & \cdots \\ (VS^2) & \phi^2 & \phi^{2\alpha} & \phi^{2\beta} & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (VS^{m-1}) & \phi^{m-1} & \phi^{\alpha(m-1)} & \phi^{\beta(m-1)} & \cdots \end{vmatrix} = (V)A_0' - (VT)A_1' + \cdots = 0.$$

Each of the determinants A_i' may be divided by A_1', and in the quotients, as well as in the weights $(V), \cdots$, unity may be substituted for ϕ. There results the congruence

$$(V)_p \left(\frac{A_0'}{A_1'}\right)_p - (VT)_p + \cdots \equiv 0 \pmod{p}.$$

By the method of § 5, *Linear groups* I, we get

$$\left(\frac{A_0'}{A_1'}\right)_p \equiv 1 \pmod{p}; \quad \left(\frac{A_i'}{A_1'}\right)_p \equiv 0 \pmod{p} \qquad (i > 1),$$

so that (5) follows.

*The sum of the multipliers of a substitution S was in *Linear groups I* designated by (S) and called the *weight* of S. In a paper by BURNSIDE, Proceedings, London Mathematical Society, November, 1903, pp. 117–123, it is called the *characteristic* of S, and the different characteristics contained in a group G are proved to satisfy the conditions for a set of *Gruppencharaktere* in the theory of FROBENIUS. The term *weight* shall be used in the present paper, for the sake of uniformity of terminology with the paper *Linear groups I*.

We prove next that all the substitutions of G possessing this property form a group (H). Let T_1 and T_2 be any two such, then

$$(V)_p \equiv (VT_1)_p \text{ (mod. } p), \qquad \text{and} \qquad (VT_1)_p \equiv (VT_1T_2)_p \text{ (mod. } p).$$

Hence

$$(V)_p \equiv (VT_1T_2)_p \text{ (mod. } p).$$

Finally, to prove that H is self-conjugate in G, we note that, for any two substitutions A and B, $(A) = (BAB^{-1})$. Hence, if T belongs to H, and V and W to G, we have by (5),

$$(V)_p \equiv (W^{-1}VW)_p \equiv (W^{-1}VWT)_p \equiv (VWTW^{-1})_p \text{ (mod. } p).$$

§ 8. We might remark that in order to have

$$(T^i)_p \equiv n \text{ (mod. } p) \qquad (i = 1, 2, \cdots),$$

it is necessary that the number of times in which a given root, whose index is prime to p, occurs among the multipliers of T must be a multiple of p. For, let all the roots of $(T)_p$ be expressed in terms of a single root θ of index k, prime to p, so that

$$(T)_p = a + b\theta + c\theta^2 + \cdots + m\theta^{k-1}, \qquad a + b + c + \cdots + m = n.$$

Then since $(T^i)_p \equiv n$ (mod. p), and $\theta^l + \theta^{2l} + \theta^{3l} + \cdots + \theta^{kl} = 0$, where l is any integer not divisible by k, we have

$$\sum_{i=1}^{k} \theta^{-i}\{(T^i)_p - n\} = kb \equiv 0 \text{ (mod. } p).$$

Evidently b is a multiple of p. In the same way $c, \cdots, m$ are multiples of p.

It follows that if $p > n/2$, then is $(T)_p = n$, so that the order of T is a power of p. Hence, if G contains a substitution T of order $p^{a+c} \geqq np^c$, where $p > n/2$, then will G contain a self-conjugate subgroup H whose order is a power of p. This subgroup will contain the substitution T^{p^a}. If $p > n$, H is abelian (Theorem 3), and by referring to Theorem 2 we deduce the

COROLLARY 1. *A primitive group in n variables cannot contain a substitution of order p^2, if p is a prime $> n$.*

If $p = n$, H may be imprimitive. In any event, the group H' generated by the pth powers of the substitutions of H is abelian, but may, in this case, reduce to the group of similarity-substitutions of order n. We have therefore the

COROLLARY 2. *If a primitive group G in n variables (n being a prime) contains a substitution T of order n^a, then will G contain an imprimitive or abelian self-conjugate subgroup of order n^k, containing the substitution T^n. The substitution T^{n^2} must be a similarity-substitution or identity. In any event, $a < 4$.*

If $n/2 < p < n$, H must be intransitive, and at least one of its systems of intransitivity contains only one variable (Theorem 9). A primitive group could, therefore, not contain such a group self-conjugately (Theorem 8). We readily derive the

COROLLARY 3. *A primitive group in n variables cannot contain a substitution of order p^3, p being a prime, and $n/2 < p < n$.*

§ 9. THEOREM 11. *Let G contain two permutable substitutions S and T, which can therefore be written simultaneously in canonical form. Let it be given that to equal multipliers of S correspond equal multipliers of T, so that the variety of T is not greater than that of S. Furthermore, let it be given that the order (k) of S is greater than its variety (m), and that the order of T is a prime (p), not dividing k. Then will G contain a self-conjugate subgroup H, containing T, of the same characteristic property as the group H of the Theorem* 10.

Starting with the equation corresponding to (6), we deduce the equation

$$(V)_p(A'_0)_p - (VT)_p(A'_1)_p + (VS)_p(A'_2)_p \cdots \equiv 0 \pmod{p}.$$

We find $(A'_i)_p \equiv 0 \pmod{p}, i > 1$; and

$$(A'_0)_p \equiv (A'_1)_p \equiv (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) \cdots \equiv q \pmod{p},$$

say, $\alpha, \beta, \gamma, \cdots$ being the different multipliers of S. Hence,

$$q\{(V)_p - (VT)_p\} \equiv 0 \pmod{p}. \tag{7}$$

Let β/α be a primitive rth root of unity, r being a factor of k and therefore prime to p. Then is $\alpha - \beta$ a factor of

$$(\alpha - \beta)(\alpha^2 - \beta^2) \cdots (\alpha^{r-1} - \beta^{r-1}) = r\alpha^{r(r-1)/2}.$$

The congruence (7) may therefore be changed into the congruence (5) by multiplying both sides of (7) by a certain expression which is the sum of a finite number of roots of unity.

§ 10. Let the multipliers of the substitution T be denoted by $\alpha_1, \alpha_2, \cdots, \alpha_n$, so that

$$(T) = \sum_{i=1}^{n} \alpha_i.$$

Let us form the quantities

$$(T)' = \sum \alpha_i \alpha_j, \ (T)'' = \sum \alpha_i \alpha_j \alpha_k, \cdots \quad (i, j, k, \cdots = 1, 2, \cdots, n; \ i \neq j \neq k \neq \cdots).$$

Let the number of roots in (T) that are different from one another be m_1 (the variety of T), the number of the $\frac{1}{2}n(n-1)$ products of $(T)'$ that are distinct be m_2, etc. Then we shall, for the present, call the greatest of the numbers

$m_1, m_2, \cdots$ the *rank* of T, and denote it by M. Evidently $M \leqq {}_nC_{n/2}$ if n is even, and $M \leqq {}_nC_{(n+1)/2}$ if n is odd.

THEOREM 12. *If a group G of degree n contains a substitution T of rank M and of order $p^{a+c} \geqq M\rho^c$, p being a prime, then will G contain a self-conjugate sub-group of order p^k which will contain a substitution of order p^c, namely T^{p^a}.*

Let S be T^{p^a}. We shall first prove that if V be any substitution of G, then will the order of VS contain no other prime factors than p and those contained in the order of V. Let the variables of G be so chosen that T is written in canonical form. By theorem 10 we have

$$(V)_p \equiv (VS)_p \pmod{p}.$$

Moreover, the method employed to prove this theorem may be used in exactly the same manner to prove that we have

$$(8) \qquad \begin{cases} (V)' \equiv (VS)'_p \pmod{p}, \\ (V)'' \equiv (VS)''_p \pmod{p}, \\ \cdots\cdots\cdots\cdots \end{cases}$$

As the two sets of quantities $(V), (V)', \cdots; (VS), (VS)', \cdots$ are, respectively, the elementary symmetric functions of the multipliers of V and VS, which multipliers shall be designated by $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$; $\zeta_1, \zeta_2, \cdots, \zeta_n$, we must have

$$\{(\rho-\epsilon_1)(\rho-\epsilon_2)\cdots(\rho-\epsilon_n)\}_p \equiv \{(\rho-\zeta_1)(\rho-\zeta_2)\cdots(\rho-\zeta_n)\}_p \pmod{p},$$

for every value of ρ. Hence

$$\{(\zeta_i-\epsilon_1)(\zeta_i-\epsilon_2)\cdots(\zeta_i-\epsilon_n)\}_p \equiv 0 \pmod{p},$$

and therefore also

$$(9) \qquad \{(\zeta_i^k-\epsilon_1^k)(\zeta_i^k-\epsilon_2^k)\cdots(\zeta_i^k-\epsilon_n^k)\}_p \equiv 0 \pmod{p}.$$

Suppose it possible that the order of VS contain a prime factor $q \neq p$ and not contained in the order of V. Then we may choose k such that the congruence (9) becomes

$$(\eta-1)^n \equiv 0 \pmod{p},$$

the index of η being q. But this congruence is an impossibility, $\eta - 1$ being a factor of q.

Now, as in the case of the Theorem 10, all the substitutions possessing the properties of the substitution S, indicated by the congruences (8), form a group H, self-conjugate in G. All the substitutions of this group whose orders are powers of p must, by what has just been proved, form a group whose order is a power of p, and this group is plainly contained in G self-gonjugately. But

among the substitutions of this group is T^a (called S in the proof), a substitution of order p^c. Hence the theorem.

§ 11. THEOREM 13. *If the group G contains two substitutions S and T, of orders p and q (different prime numbers > 2) respectively, whose weights do not contain all the primitive pth and qth roots of unity, then will G contain a substitution of order pq.*

Consider the system of equations (2) of *Linear groups* I, under the condition $v = 1$. Assuming that the list $\alpha, \beta, \cdots, \kappa$ does not include all the roots of $(\theta^p - 1)/(\theta - 1) = 0$, let ρ be one such different from $\alpha, \beta, \cdots, \kappa$. Then is evidently

$$(T) + \rho^{-1}(ST) + \rho^{-2}(S^2T) + \cdots + \rho^{-p+1}(S^{p-1}T) = 0.$$

The assumption that none of the weights $(ST), (S^2T), \cdots$ contain both pth and qth roots of unity is untenable, which can be seen as follows. Under the assumption, suppose at least one of these weights, (S^iT), contains pth roots. We will transpose all the corresponding terms $\rho^{-i}(S^iT)$, and by means of the relation $1 + \rho + \rho^2 + \cdots + \rho^{p-1} = 0$ we can change the right-hand member of the resulting equation into such a form that this becomes an identity in ρ. Then (T) = sum of roots of unity, the indices of which are prime to q. But this is impossible, since (T) contains only qth roots and is not equal to an integer, as at least one qth root is absent by assumption. Thus, none of the weights of the equation considered can contain pth roots. In this event the equation can be true only if $(T) = (ST) = \cdots = (S^{p-1}T)$. Similarly we find $(S) = (ST) = \cdots = (ST^{q-1})$. Hence $(T) = (S)$, an impossibility. Accordingly, at least one of the weights considered must contain both pth and qth roots of unity, and the theorem is proved.

COROLLARY. *A group G of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} N$, where $p_1, p_2, \cdots, p_m$ are primes each greater than $n + 1$, contains an abelian subgroup of order $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$.*

To prove this corollary, we may assume it true for all groups in less than n variables. It follows immediately for all intransitive groups in n variables. Let us therefore consider a transitive group G of the order given. A substitution S of order $p > n + 1$ will fulfill the condition of the Theorem 13. Hence, the group G contains a substitution of order $p_1 p_2$, which can evidently be written as the product of two substitutions A and B, of orders p_1 and p_2 respectively. The subgroup of G of order p_1^α to which A belongs being abelian, this group and the substitution B will generate an intransitive group, containing the substitution A self-conjugately. The order of this group is divisible by $p_1^\alpha p_2$. For such a group the corollary has been proved true. There results that we have an abelian subgroup of G of order $p_1^\alpha p_2$, the product of a group G_1 of order $p_1^{\alpha_1}$ and a substitution C of order p_2. But this substitution is

contained in an abelian subgroup G_2 of G of order $p_2^{\alpha_2}$. The groups G_1 and G_2 will therefore generate an intransitive group, whose order is divisible by $p_1^{\alpha_1} p_2^{\alpha_2}$. This has an abelian subgroup H_2 of order $p_1^{\alpha_1} p_2^{\alpha_2}$. In the same way we find that G contains an abelian subgroup H_3 of order $p_1^{\alpha_1} p_3^{\alpha_3}$. We may, obviously, assume that H_2 and H_3 have in common a group of order $p_1^{\alpha_1}$. Then will H_2 and H_3 generate an intransitive group, etc.

§ 12. We have now the means in hand whereby to determine a limit to the order of the primitive groups in n variables. It was shown in *Linear groups* I how we can obtain the limit to the highest prime which may divide the order g of such a group G. We shall now proceed to find a superior limit to the power of a prime p contained in the order of the group. We shall by p^{n_p} denote the highest power of p which divides $n!$.

Let p^N be the highest power of p which divides g. Then G contains a subgroup of order p^N, and this again an abelian subgroup G' of order $g' \geqq p^{N-n_p}$, if $N > n_p$ (Theorem 9). Let G' be written in canonical form. Then it is plain that we can have no more than $p^{n-1} - 1$ substitutions of order p contained in G'; no more than $p^{2(n-1)} - 1$ substitutions of orders p^2 and p, and so on. Therefore, if $p^a \geqq n > p^{a-1}$, and $N - np > (n-1)(a+c-1)$, G will contain a self-conjugate subgroup H containing a substitution of order p^c, this subgroup being of the kind considered in the Theorem 10. Again, if

$$p^a \geqq \frac{n!}{(n/2!)^2} > p^{a-1} \qquad \text{when } n \text{ is even,}$$

or

$$p^a \geqq \frac{n!}{(n-1)/2!\,(n+1)/2!} > p^{a-1} \quad \text{“} \quad \text{“} \quad \text{“ odd,}$$

and if

$$N - n_p > (a+c-1)(n-1),$$

then will G, according to the Theorem 12, contain a self-conjugate subgroup K of order p^k, containing a substitution of order p^c.

Suppose $n = n_1 p^a$, where $n_1 = 1$ or is prime to p. Then will the p^ath powers of the substitutions of K generate an intransitive group L which will contain a substitution of order p^{c-a}, if $c > a$. Now, at least one of the systems of intransitivity of L contains only one variable. Accordingly, since L is a self-conjugate subgroup of G, this could not be primitive unless the substitutions of L are all similarity-substitutions (Theorem 8). This could not be the case, however, if $c - a > a$.

Therefore, if G is primitive, and its order is divisible by p^N, then must

$$N \leqq n_p + (a + 2\alpha)(n-1).$$

But,

$$n_p < \frac{n}{p-1}, \qquad \alpha \leqq \frac{\log n}{\log p}, \qquad \text{and} \qquad a < 1 + \frac{\log A}{\log p},$$

A being the highest term in the expansion of $(1+1)^n$. Hence,

$$N < \frac{n}{p-1} + \left(1 + \frac{\log n^2 A}{\log p}\right)(n-1).$$

This number is evidently a great deal higher than necessary. In any given case it may be reduced by a closer inspection of the subgroups of order p^N. We have assumed that the substitutions considered are of variety n, whereas this may be much less in special cases. Theorems 10, 11 and 13 and their corollaries may be used to advantage, especially in the case of simple groups.

In any event, a number can now be found which the order of a primitive group of substitutions of determinant 1 must divide. If the determinants of the substitutions of a group G are not all $= 1$, we may write each of these in the form SA, where A is a substitution of determinant 1 and S a similarity-substitution. The substitutions A will form a group G' whose order λ is a factor of the order of G, and we can tabulate the substitutions of G in such a manner as to show that the order of G is λf, where f is the order of a group F of similarity-substitutions, contained self-conjugately in G. If G is primitive, so is G', and we have, accordingly, proved JORDAN'S Theorem (Introduction) for primitive groups and are, moreover, able to give in any special case a number that λ must divide.

The primitive groups in three variables.

§ 13. We shall consider in order the three cases:

A. Primitive groups having imprimitive self-conjugate subgroups.

B. Primitive groups which are simple.

C. Primitive groups which have intransitive self-conjugate subgroups.

D. Primitive groups having primitive self-conjugate subgroups.

A. Let G be a primitive group having an imprimitive self-conjugate subgroup H. By studying the different possible cases of imprimitive groups, which are all of the type

$$x_1' = \alpha x_i, \qquad x_2' = \beta x_j, \qquad x_3' = \gamma x_k \qquad (i, j, k = 1, 2, 3;\ i \neq j \neq k),$$

and by taking for H the group generated by the 2nd powers of the substitutions of such a group, we find readily that either the 3rd powers of the substitutions of H will generate an abelian group which is not merely the group of similarity-substitutions, or H will contain substitutions of order 3, and possibly of order 9 and variety 2. In the first case, G could not be primitive, since the abelian group obtained from H in the manner indicated is contained self-conjugately in G. In the second case, H will contain self-conjugately the group H' generated by the substitutions

$$P: \quad x_1' = x_2,\ x_2' = x_3,\ x_3' = x_1;$$

$$Q: \quad x_1' = x_1,\ x_2' = \omega x_2,\ x_3' = \omega^2 x_3 \qquad (\omega^3 = 1,\ \omega \neq 1);$$

and is itself generated by this group and the substitution

$$R: \qquad x_1' = \phi x_1,\ x_2' = \phi x_2,\ x_3' = \phi\omega^2 x_3 \qquad (\phi^3 = \omega),$$

if it does not coincide with H'.

The group H possesses the relative invariant $x_1x_2x_3$, and this is the only one of the third order if the substitution R be present in H, whereas the group H' possesses a set of four that can each be resolved into linear factors, namely

$$(10) \qquad x_1x_2x_3;\ x_1^3 + x_2^3 + x_3^3 - 3\theta x_1x_2x_3 \qquad (\theta = 1, \omega, \omega^2).$$

If H contains R, G is evidently imprimitive, as it should then leave invariant, to a constant factor, the function $x_1x_2x_3$. Hence, G must contain H' self-conjugately, and must permute among themselves the invariants (10). Imposing upon the substitutions of G this condition, it is easily found that the generating substitutions of G, aside from P and Q, are

$$S: \quad \rho x_1' = x_1 + x_2 + x_3,\ \rho x_2' = x_1 + \omega x_2 + \omega^2 x_3,\ \rho x_3' = x_1 + \omega^2 x_2 + \omega x_3, \qquad \rho = \omega - \omega^2;$$

$$T: \quad \rho x_1' = x_1 + \omega x_2 + \omega x_3,\ \rho x_2' = \omega^2 x_1 + \omega x_2 + \omega^2 x_5, \qquad \rho x_3' = \omega^2 x_1 + \omega^2 x_2 + \omega x_3,\ \rho = \omega - \omega^2$$

$$U: \quad \phi\rho x_1' = \omega^2 x_1 + \omega^2 x_2 + \omega^2 x_3,\ \phi\rho x_2' = \omega x_1 + \omega^2 x_2 + x_3, \qquad \phi\rho x_3' = \omega x_1 + x_2 + \omega^2 x_3,\ \rho = \omega - \omega^2;$$

where $\phi^3 = \omega$.

The substitutions S, S and T, S and U, and the group H' generate, respectively, primitive groups of orders 108, 216 and 648. They all contain the group F of similarity-substitutions (contained in H'), and their quotient-groups (abstract groups) $G' = G/F$, of orders 36, 72 and 216, are the *Hessian group* and some of its subgroups, discussed by Jordan in his determination of the linear groups in three variables.*

§ 14. *B.* By Theorem 5, the order of a primitive group G in 3 variables is of the form $2^a3^b5^c7^d$. By Theorem 10, Corollaries 1–3, we can have no substitutions of orders 8, 81, 25 or 49. If there is a substitution of order 27, G contains a self-conjugate subgroup H of order 3^k containing a substitution of order 9, which is not a similarity-substitution. The group H is abelian or imprimitive, and G would be imprimitive or intransitive in either case (cf. case *A*). In the same way we find that G cannot contain a substitution of order 9, the 3d power of which is not a similarity-substitution.

We now find, by studying the groups of orders 2^a, 3^b, 5^c, 7^d in detail, that

1°. $a \leqq 3$; 2°. $b \leqq 4$; 3°. c (and d) $\leqq 2$;

4°. If $b \geqq 3$, there is a similarity-substitution;

* Journal für Mathematik, vol. 84 (1878), p. 89.

5°. If $b = 4$, there is a substitution of order 9 and variety 2;

6°. If c (or d) $= 2$, there is a substitution of order 5 (or 7) and of variety 2. We shall prove that we can have no substitution of order 5 and of variety 2. Let, if possible, S be such a substitution. Its weight may be written $a + a + a^3$, where $a^5 = 1$. Then, if A be any substitution of G, we have

$$(A)\frac{\alpha^{3r+1} - \alpha^{r+3}}{\alpha^3 - \alpha} - (AS)\frac{\alpha^{3r} - \alpha^r}{\alpha^3 - \alpha} + (AS^r) = 0,$$

an equation obtained in the same manner as equation (6). Hence,

$$(11) \qquad (A)_5(r-1) - (AS)_5 r + (AS^r)_5 \equiv 0 \pmod 5.$$

Let A be of order 5. Then $(A)_5 = 3$. It is plain that $(AS)_5$ cannot contain 7th roots of unity. In fact, we find without much trouble that the order of AS must be a factor of 30. The weight of this substitution is therefore of the form $\epsilon_1 + \epsilon_2 + \epsilon_3 = 1$, where $\epsilon_1^{30} = \epsilon_2^{30} = \epsilon_3^{30} = 1$. It follows that $(AS)_5$ must have one or other of the values

$$(12) \qquad 0, -1, \pm 2, -\omega, -\omega^2, \pm 2\omega, \pm 2\omega^2, \pmod 5.$$

Moreover, the value of $(AS^r)_5$ is found in the same way to be one of the quantities (12). Substituting, therefore, the different quantities (12) in (11), taking different values for r, we find that the only value possible for $(AS)_5$ is -2 (mod. 5), i. e., the substitution AS must be of order 5 or 1.

From this it follows that all the substitutions of G of order 5 form a group, in which case G could not be primitive (Theorems 2, 3). For, from what has just been proved, the product of any substitution of order 5 and one of order 5 and variety 2 is a substitution of order 5. Now, if we have *one* substitution of order 5 and variety 2, any substitution of order 5 can be written as the product of two substitutions, each of order 5 and variety 2, which we see when we write any subgroup of G of order 5^k in canonical form, bearing in mind that conjugate substitutions have the same multipliers.

In the same way we can prove that G cannot contain a substitution of order 7 and variety 2. It follows that the order of G is not divisible by 25 or by 49. Nor is it divisible by 5.7, for we have in such a case a substitution of order 5.7 (Theorem 13), which we could write as the product of two of orders 5 and 7 respectively, permutable with each other. Since neither of these could be of variety 2, we could employ Theorem 11 to prove that G would contain a self-conjugate subgroup of order 7; an impossibility.

If the order of G is divisible by 5 or by 7, G cannot contain a substitution of order 9 and variety 2. For, let S be of order 5, and T of order 9 and variety 2, and let $(T) = \phi + \phi + \phi\omega^2$, where $\phi^3 = \omega$, $\omega^3 = 1$, $\omega \neq 1$. The equation corresponding to (6) is here

$$(S) + \omega\phi^2(ST) + \phi(ST^2) = 0.$$

We see at once that either (ST) or (ST^2) must contain both 5th and 9th roots of 1. There would result a substitution of order 5.9. The group G would contain a self-conjugate subgroup of order 3^k (Theorem 11), containing a substitution of order 9, and could not be primitive (Cf. case A). Similarly, G cannot contain a substitution of order 7 and one of order 9 and variety 2.

Referring now to the list of conditions 1°–6°, we find that the order of G is a factor of one of the following numbers.

I. G does not contain similarity-substitutions:

$$2^3 3^3, \qquad 2^3 3^2 5, \qquad 2^3 3^2 7;$$

II. G contains the group of similarity-substitutions:

$$2^3 3^4, \qquad 2^3 3^3 5, \qquad 2^3 3^3 7.$$

§ 15. The orders of the simple groups desired are factors of the numbers of the series I, the greatest of which is 504. As is well known, there are only four types of abstract simple groups whose orders are less than 505, namely, groups of orders 60, 168, 360 and 504. This last group contains an abelian subgroup of order 8, all of whose substitutions are of order 2.* Such an abelian group cannot, however, be constructed as a linear group in 3 variables, which is apparent when we attempt to write it in canonical form. The abstract simple group of order 360 contains a subgroup of order 9. When we attempt to construct linear homogeneous groups in 3 variables of order 9, we find that they will contain either a similarity-substitution or a substitution of order 9 and of variety 2. The latter substitution is excluded from a primitive group containing a substitution of order 5, and the former could not be contained in a simple group. Thus, only the cases of orders 60 and 168 could furnish us primitive groups in 3 variables. That two such groups , one type of each, do exist is well known.†

§ 16. *C.* We come now to primitive groups having self-conjugate intransitive subgroups. By theorem 8 it appears that no primitive group G in 3 variables can have such a subgroup unless this is the group F of similarity-substitutions. The quotient-group (existing as an abstract group) $G' = G/F$ must be simple, or G would contain a self-conjugate subgroup different from the group F. The order of G being a factor of one of the numbers of the series II., that of G' must be a factor of one of the numbers of the series I. We obtain, for the order of G', one of the numbers 60, 168, 360 or 504.

As shown above, the case 504 may be dismissed. The case 360 can not be thrown out by the reasons given in § 15. In fact, a group of order 3.360 iso-

* BURNSIDE, *Theory of Groups*, p. 373; COLE, American Journal of Mathematics, vol. 15 (1893), pp. 303-315.

† See WIMAN, Mathematische Annalen, vol. 47 (1896), pp. 532–533, and Encyclopädie der Mathematischen Wissenschaften, Bd. 1, Heft 5 (1900), pp. 528–530, for references. See also MASCHKE, Mathematische Annalen, vol. 51 (1899), pp. 259–269.

morphic with the abstract simple group of order 360 and containing the group of similarity-substitutions can be represented as a linear homogeneous group in 3 variables.* Groups of orders 3.60 and 3.168, isomorphic with the abstract simple groups of orders 60 and 168 respectively, and containing the group F, can also be constructed as linear homogeneous groups in 3 variables. We need only construct the groups $\{G_{60}, F\}$, $\{G_{168}, F\}$; G_{60} and G_{168} denoting the primitive groups of orders 60 and 168 mentioned in § 15.

§ 17. *D.* We come, finally, to primitive groups having primitive self-conjugate subgroups. — With each of the primitive groups already obtained is associated a system of invariants.* An examination of these invariants and of the conditions given in § 14 will disclose the fact that any one of the primitive groups given is contained self-conjugately only in itself or in the group generated by a similarity-substitution and the group itself, excepting the case of the G_{108}, which is contained self-conjugately in the G_{216}, and this again in the G_{648}.

The primitive groups in three variables, linear and homogeneous, have now been enumerated. We have found the orders 648, 216, 108, 1080, 60, 168, (180, 504). The groups of orders 180, 504 are isomorphic with the groups of order 60 and 168 respectively.*

* Cf. WIMAN, Mathematische Annalen, vol. 47 (1896), pp. 532–533.