ON THE ORDER OF LINEAR HOMOGENEOUS GROUPS*

BY

H. F. BLICHFELDT

The different types of finite groups of linear homogeneous substitutions in two and three variables have been enumerated by KLEIN, GORDAN, C. JORDAN and VALENTINER. The different types of such groups in two variables were determined by KLEIN† through geometrical considerations; GORDAN‡ made the problem depend upon that of finding the different solutions of the equation $1 + \cos\phi_1 + \cos\phi_2 + \cos\phi_3 = 0$, ϕ_1, ϕ_2, ϕ_3 being rational angles. JORDAN§ and VALENTINER‖ constructed certain fundamental equations involving the orders of the different types of groups in three variables, which equations would furnish a finite number of groups only.

JORDAN then attempted to employ his method in enumerating all the groups in four variables,¶ but found the complete discussion of his fundamental equation well nigh impossible. Even in the case of three variables the work was a formidable one, as shown by the fact that two simple groups of orders 168 and 360 respectively escaped his notice.

It may, therefore, not be amiss to give some general theorems of a simple nature bearing on the order of the linear homogeneous groups in n variables. In particular, limits are found to the number of different primes dividing the order of the "primitive groups."

The following explanation of technical terms and phrases used will be necessary. Any substitution S of a linear homogeneous group H of finite order in n variables $x_1, x_2, \cdots, x_n$ will be of the form

$$x_i' = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \qquad (i = 1, 2, \cdots, n).$$

We shall say the group is of *degree* n.

* Presented to the Society (San Francisco), April 25, 1903, under a different title. Received for publication June 15, 1903.

† Mathematische Annalen, vol. 9 (1875), p. 183.

‡ Mathematische Annalen, vol. 12 (1877), p. 28.

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

‖ Kjóbenhavnske Skr. (6), vol. 5 (1889), p. 64.

¶ Atti della Reale Accademia di Napoli, vol. 8 (1879).

If it is possible to choose new variables $y_1, y_2, \cdots, y_n$, where

$$y_i = b_{i1}x_1 + b_{i2}x_2 + \cdots + b_{in}x_n \qquad (i=1, 2, \cdots, n),$$

such that all the substitutions of H are of the form

$$y_i' = \alpha_{i1}y_1 + \alpha_{i2}y_2 + \cdots + \alpha_{im}y_m \qquad (i=1, 2, \cdots, m;\ m<n),$$

$$y_j' = \beta_{j,m+1}y_{m+1} + \beta_{j,m+2}y_{m+2} + \cdots + \beta_{j,n}y_n \quad (j=m+1, m+2, \cdots, n),$$

we shall say that the group H is *intransitive*, otherwise the group is said to be *transitive.**

A transitive group is said to be *imprimitive*, if the variables of the group can be so selected that they fall in systems of m each, $m<n$, of such a nature that any substitution of the group will transform all the variables of any one system into linear functions of the variables of the same or another system. If the variables of a transitive group cannot be so selected, the group is said to be *primitive.*

It has been proved in several ways† that the variables may be so chosen that a substitution S of finite period can be thrown into *canonical form:*

$$x_i' = \alpha_i x_i \qquad (i=1, 2, \cdots, n),$$

in which case the constants α_i, called the *multipliers* of the substitution, are certain roots of unity. In fact, if k is the least integer for which the equation $\alpha^k = 1$ is satisfied by $\alpha_1, \alpha_2, \cdots, \alpha_n$, then is k the order of the above substitution. If $\alpha_1 = \alpha_2 = \cdots = \alpha_n$, the substitution is called a *similarity-substitution.*

Now, it may be possible so to choose the variables that all the substitutions of of a group H have the canonical form. In such an event we shall say that the group is written in *canonical form.* A group that can be written in canonical form is plainly *abelian*, i. e., its substitutions are permutable, and it is intransitive, if $n>1$.

Since every group considered is linear and homogeneous, we shall, as a rule, dispense with the adjectives "linear" and "homogeneous" with reference to a group.

§ 1.

THEOREM I. *Every abelian group can be written in canonical form.*‡

* MASCHKE has used the word "intransitive" with the meaning given here. See Mathematische Annalen, vol. 52 (1899), p. 363.

† See MOORE, *An Universal Invariant for Finite Groups of Linear Substitutions, etc.*, Mathematische Annalen, vol. 50 (1898), p. 215, for proof and references.

‡ BURNSIDE, Proceedings London Mathematical Society (1898), p. 331; L. E. DICKSON, these Transactions (1902), pp. 292-293.

THEOREM II. *If a group H has a self-conjugate subgroup G which is abelian and whose substitutions are not all similarity-substitutions, the group H is intransitive or imprimitive.*

By a proper choice of the variables $x_1, x_2, \cdots, x_n$, the group G will be written in canonical form (Theorem I). Suppose, if G be so written, its substitutions have the form

$$x_1' = \alpha x_1,\ x_2' = \alpha x_2,\ x_3' = \beta x_3,\ x_4' = \beta x_4,\ x_5' = \gamma x_5,\ \cdots,\ x_n' = \kappa x_n,$$

where no two of the multipliers $\alpha, \beta, \gamma, \cdots, \kappa$ are equal for every substitution of G. Then are the expressions

$$a_1 x_1 + a_2 x_2,\ a_3 x_3 + a_4 x_4,\ a_5 x_5,\ \cdots,\ a_n x_n,$$

$a_1, a_2, \cdots$ being arbitrary constant, *relative invariants* of G.

Now, since G is self-conjugate in H, any substitution of H will transform the system of invariants just given into another such system, say

$$b_1 x_1 + b_2 x_2,\ b_3 x_3 + b_4 x_4,\ b_5 x_5,\ \cdots,\ b_n x_n.$$

This substitution will therefore transform the variables x_1, x_2 into linear functions of themselves or into linear functions of x_3, x_4 or any other set of two letters that constitute the variables of an invariant of G. It is readily seen that the group H is intransitive or imprimitive.

§ 2.

THEOREM III. *If the order h of a group H in n variables is $p^a q^b \cdots$, where $p, q, \cdots$ are primes each greater than n, then must H be abelian.*

The theorem is self-evident for $n = 1$. Assume the theorem true for all groups of the kind considered in less than n variables, to prove it true for any such group in n variables.

We may restrict ourselves to the case of groups whose substitutions have the determinant 1. For it is plain that if the group of substitutions of determinant 1 obtained from any group H in the manner indicated in WEBER'S *Algebra*, II, 2d edition, pp. 188–189, is abelian, the group H will be abelian.

Let us therefore consider a group G of linear substitutions of determinant 1. Let the order of G be $p^{a_1} q^{b_1} \cdots$; $p, q, \cdots$ being primes each greater than n, the degree of G. It is evident that this group can contain no similarity-substitutions except the identical substitution.

If G is non-abelian, all of its subgroups may be abelian, or it must contain at least one non-abelian subgroup all of whose subgroups are abelian. Let G' be such a non-abelian group, of order $p^{a_2} q^{b_2} \cdots$. Groups of this character have

been studied by G. A. MILLER and H. C. MORENO,* who proved that they are composite.

It follows (Theorem II) that G' is intransitive or imprimitive. In any event, it is plain that the group generated by the $n!$th powers of the substitutions of G' is intransitive. The group so generated is, however, the group G' itself, the order of this being prime to $n!$.

The groups obtained from G' by selecting its different systems of transitivity are, by assumption, abelian. This must, therefore, also be the case with G', contrary to the supposition as to the nature of G'. Thus G must be abelian, and therefore also H.

§ 3.

In the proof of the next theorem the following lemma is used:

LEMMA. *Let $E = 0$ be an equation, the left-hand member of which is the sum of certain roots of unity. If the factors of the indices of these roots are powers of primes $p, q, r, \cdots$, the exponents of these powers being less than $a+1, b+1, c+1, \cdots$, respectively, then we may write each of the roots considered in the form:*

$$\bar{\alpha}^A \bar{\beta}^B \bar{\gamma}^C \cdots \alpha_1^{A_1} \beta_1^{B_1} \gamma_1^{C_1} \cdots,$$

where $\alpha_1, \beta_1, \gamma_1, \cdots$ are, respectively, primitive roots of the equations

$$\theta^p - 1 = 0, \theta^q - 1 = 0, \theta^r - 1 = 0, \cdots,$$

and where $\bar{\alpha}, \bar{\beta}, \bar{\gamma}, \cdots$, are, respectively, primitive roots of the equations $\theta^{p^a} - 1 = 0, \theta^{q^b} - 1 = 0, \theta^{r^c} - 1 = 0, \cdots$. Moreover, the numbers

$$A, B, C, \cdots, A_1, B_1, C_1, \cdots$$

may be so chosen that $A < p^{a-1}$, $A_1 < p$; $B < q^{b-1}$, $B_1 < q$; etc.

Now, let the terms of E be so written, and let us substitute the arbitrary letters $x, y, z, \cdots$ for $\bar{\alpha}, \bar{\beta}, \bar{\gamma}, \cdots$, and $x_1, y_1, z_1, \cdots$ for $\alpha_1, \beta_1, \gamma_1, \cdots$, calling the resulting expression E'. If then we replace the powers

$$y_1, y_1^2, \cdots, y_1^{q-1}; \; z_1, z_1^2, \cdots, z_1^{r-1}; \; \cdots$$

by the numbers $+1, 0, -1$ in any manner such that we get

$$1 + y_1 + y_1^2 + \cdots + y_1^{q-1} = 0, \; 1 + z_1 + z_1^2 + \cdots + z_1^{r-1} = 0, \cdots,$$

and if we replace $x_1, x, y, z, \cdots$ and their powers by $+1$, the resulting value of E' will be an integer $\equiv 0 \pmod{p}$.

* *Non-abelian Groups in which every Subgroup is Abelian*, these TRANSACTIONS, vol. 4 (1903), pp. 398–404.

The first part of this lemma is evident. To prove the second part we need the following theorem due to KRONECKER *: *if p is a prime and a any integer, the expression* $X \equiv 1 + x^{p^{a-1}} + x^{2p^{a-1}} + \cdots + x^{(p-1)p^{a-1}}$ *can not be decomposed into factors of lower degree in x, whose coefficients are rational functions of a primitive root of unity, unless the exponent of this root is divisible by p.*

It follows from this theorem that if the coefficients c_i in the function $f(x) \equiv \sum c_i x^i$ are sums of roots of unity, whose indices are prime to p, and if $f(\alpha) = 0$, where α is a primitive root of the equation $\theta^{p^a} - 1 = 0$, then is $f(x)$ divisible by X. Moreover, we readily see that if we write $f = f_1 + f_2 + f_3 + \cdots$, where f_k consists of all of the terms of $\sum c_i x^i$ for which the exponents i will give the same remainder $r_k \pmod{p^{a-1}}$, then must every expression f_k be divisible by X. †

It follows that if the coefficients $c_{i,j}$ of the function

$$f(x, x_1) \equiv \sum_{i=0}^{p^{a-1}-1} \sum_{j=0}^{p-1} c_{i,j} x^i x_1^j$$

are sums of roots of unity whose indices are prime to p, and if $f(\bar{\alpha}, \alpha_1) = 0$, where $\bar{\alpha}$ and α_1 are, respectively, primitive roots of $\theta^{p^a} - 1 = 0$, $\theta^p - 1 = 0$, then is $f(x, x_1)$ divisible by $1 + x_1 + x_1^2 + \cdots + x_1^{p-1}$, and the quotient is free from x_1. From this again it follows that we can write the expression E' of the lemma in the form

$$E' = (1 + x_1 + x_1^2 + \cdots + x_1^{p-1}) E_1 + (1 + y_1 + y_1^2 + \cdots + y_1^{q-1}) E_2 + (1 + z_1 + z_1^2 + \cdots + z_1^{r-1}) E_3 + \cdots,$$

where the expressions E_i are integral functions of $x, y, z, \cdots, x_1, y_1, z_1, \cdots$, with integral coefficients. In addition, E_1 is free from x_1, E_2 from y_1, E_3 from z_1, etc. The truth of the second part of the lemma is seen immediately.

§ 4.

THEOREM IV. *In any group H of degree n, all the substitutions whose orders are divisible by no prime less than $(n-1)(2n+1)+1$ form a subgroup.*

In any substitution T of finite period, say

$$(1) \qquad x_i' = a_{i1} x_1 + a_{i2} x_2 + \cdots + a_{in} x_n \qquad (i = 1, 2, \cdots, n),$$

the sum of the multipliers (which, as remarked above, are certain roots of unity),

* *Mémoire sur les facteurs irréductibles de l'expression* $x^n - 1$, Journal de Mathématiques pures et appliquées, t. 19 (1854), p. 178.

† This argument is given by GORDAN: *Ueber endliche Gruppen*, etc., Mathematische Annalen, vol. 12 (1877), pp. 29-30.

is equal to $a_{11} + a_{22} + \cdots + a_{nn}$, as they are the roots of the *characteristic equation* of T.* We shall call this sum the *weight* of the substitution T.

Now, let S and T be any two substitutions of a group H in n variables, and let the orders of S and T be p^v and $p^a q^b \cdots$ respectively, $p, q, \cdots$ being primes each greater than $(n-1)(2n+1)$.

Let the variables be chosen in such a manner that S has the canonical form. Suppose this to be

$$x_1' = \alpha x_1,\ x_2' = \alpha x_2,\ x_3' = \beta x_3,\ x_4' = \beta x_4,\ x_5' = \gamma x_5,\ \cdots,\ x_n' = \kappa x_n,$$

where $\alpha \neq \beta \neq \gamma \neq \cdots \neq \kappa$. Let T be of the form (1).

Then if the substitutions

$$T,\ ST,\ S^2T,\ \cdots,\ S^{p^v-1}T,$$

be formed, we will find certain linear relations among their weights.* Indicating these by $(T), (ST), \cdots, (S^{p^v-1}T)$, we have namely,

$$(2)\qquad \begin{cases} (T) = a_{11} + a_{22} + a_{33} + \cdots + a_{nn}, \\ (ST) = \alpha a_{11} + \alpha a_{22} + \beta a_{33} + \cdots + \kappa a_{nn}, \\ (S^2T) = \alpha^2 a_{11} + \alpha^2 a_{22} + \beta^2 a_{33} + \cdots + \kappa^2 a_{nn}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ (S^{p^v-1}T) = \alpha^{p^v-1} a_{11} + \alpha^{p^v-1} a_{22} + \beta^{p^v-1} a_{33} + \cdots + \kappa^{p^v-1} a_{nn}. \end{cases}$$

Supposing there are just m different multipliers, $\alpha, \beta, \gamma, \kappa$, in S, we can eliminate the quantities $a_{11} + a_{22}, a_{33} + a_{44}, \cdots, a_{nn}$ between $m+1$ of the equations (2), say the first m and the $r+1$th, $m \leqq r \leqq p^v - 1$.

The equation thus obtained will be of the form

$$(3)\qquad \begin{vmatrix} (T) & 1 & 1 & 1 & \cdots & 1 \\ (ST) & \alpha & \beta & \gamma & \cdots & \kappa \\ (S^2T) & \alpha^2 & \beta^2 & \gamma^2 & \cdots & \kappa^2 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ (S^{m-1}T) & \alpha^{m-1} & \beta^{m-1} & \gamma^{m-1} & \cdots & \kappa^{m-1} \\ (S^rT) & \alpha^r & \beta^r & \gamma^r & \cdots & \kappa^r \end{vmatrix} \equiv (T)A_0' - (ST)A_1' + \cdots + (-1)^m (S^rT)A_m' = 0,$$

say, which equation, it may be noticed, is true for all values of r.

*JORDAN, Journal für Mathematik, vol. 84 (1878), p. 112.

†Compare GORDAN, Mathematische Annalen, vol. 12 (1877), pp. 23-25; MASCHKE, ibid., vol. 50 (1898), p. 492.

As $\alpha, \beta, \gamma, \cdots$ are all different and are p^vth roots of unity, the alternant $\sum \pm \alpha\beta^2 \cdots \kappa^{m-1}$ is not zero and is plainly a factor of each of the coefficients $A_0', A_1', \cdots$. Dividing this factor out, we obtain a typical form of the desired linear relations

$$E = (T)A_0 - (ST)A_1 + \cdots + (-1)^{m-1}(S^{m-1}T)A_{m-1} + (-1)^m(S^rT) = 0. \tag{4}$$

§ 5.

We can apply the lemma of § 3 to the equation (4). To begin with, let 1 be substituted for every root of the equation $(\theta^{p^v} - 1)(\theta^{p^a} - 1) = 0$ that may occur in (4), and let $y, z, \cdots, y_1, z_1, \cdots$ be written for all other roots, according to the rule laid down in the lemma. If then we substitute 1 for $y, z, \cdots$ and their powers, and assign to the powers $y_1, y_1^2, \cdots, y_1^{q-1}, z_1, z_1^2 \cdots$, etc., the values -1, 0 or $+1$ in any manner such that we get

$$1 + y_1 + y_1^2 + \cdots + y_1^{q-1} = 0, \quad \text{etc.},$$

the left-hand member of (4) becomes an integer $\equiv 0 \pmod{p}$. Let the result be written in the form

$$E'' \equiv [T]B_0 - [ST]B_1 + \cdots + (-1)^{m-1}[S^{m-1}T]B_{m-1} + (-1)^m[S^rT] \equiv 0 \pmod{p}, \tag{5}$$

where B_k is the resulting value of A_k, which contained no other root than those of $\theta^{p^v} - 1 = 0$ and $\theta^2 - 1 = 0$; and $[S^kT]$ that of (S^kT).

As each of the weights (S^kT) is the sum of n roots of unity, it is easily seen that the expressions $[S^kT]$ must be integers lying between $-n$ and $+n$ inclusive.

It remains for us to find the number B_k, the resulting value of the coefficient A_k, which is the ratio of two minors of the determinant (3). In the quotient, 1 is to be substituted for the quantities $\alpha, \beta, \cdots, \kappa$, which are roots of the equation $\theta^{p^v} - 1 = 0$.

JACOBI has given the value of the determinant of m^2 elements

$$\begin{vmatrix} \alpha^a & \beta^a & \cdots & \kappa^a \\ \alpha^b & \beta^b & \cdots & \kappa^b \\ \alpha^c & \beta^c & \cdots & \kappa^c \\ \cdots & \cdots & \cdots & \cdots \end{vmatrix}$$

in the form

$$\begin{vmatrix} {}_mH_a & {}_mH_{a-1} & \cdots & {}_mH_{a-m+1} \\ {}_mH_b & {}_mH_{b-1} & \cdots & {}_mH_{b-m+1} \\ {}_mH_c & {}_mH_{c-1} & \cdots & {}_mH_{c-m+1} \\ \cdots & \cdots & \cdots & \cdots \end{vmatrix} \times \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha & \beta & \cdots & \kappa \\ \alpha^2 & \beta^2 & \cdots & \kappa^2 \\ \cdots & \cdots & \cdots & \cdots \end{vmatrix},$$

where ${}_mH_t = 0$, if $t < 0$; ${}_mH_0 = 1$; and where ${}_mH_t$, $t \geqq 1$, represents the sum of all products of degree t in the m letters $\alpha, \beta, \cdots, \kappa$. Substituting 1 for each of these letters in ${}_mH_t$, $t \geqq 1$, this becomes

$$\frac{(m+t-1)!}{(m-1)!\,t!} = {}_mH'_t,$$

say.

Now we easily find

$$\begin{vmatrix} {}_mH'_a & {}_mH'_{a-1} & \cdots & {}_mH'_{a-m+1} \\ {}_mH'_b & {}_mH'_{b-1} & \cdots & {}_mH'_{b-m+1} \\ {}_mH'_c & {}_mH'_{c-1} & \cdots & {}_mH'_{c-m+1} \\ \cdots & \cdots & \cdots & \cdots \end{vmatrix} = \begin{vmatrix} {}_1H'_a & {}_2H'_{a-1} & \cdots & {}_mH'_{a-m+1} \\ {}_1H'_b & {}_2H'_{b-1} & \cdots & {}_mH'_{b-m+1} \\ {}_1H'_c & {}_2H'_{c-1} & \cdots & {}_mH'_{c-m+1} \\ \cdots & \cdots & \cdots & \cdots \end{vmatrix}$$

$$= \begin{vmatrix} 1 & a & a^2 & \cdots & a^{m-1} \\ 1 & b & b^2 & \cdots & b^{m-1} \\ 1 & c & c^2 & \cdots & c^{m-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{vmatrix} \div \{2!\,3! \cdots (m-1)!\}.$$

Hence,

$$B_0 = \begin{vmatrix} 1 & 1 & 1 & \cdots \\ 1 & 2 & 2^2 & \cdots \\ 1 & 3 & 3^2 & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ 1 & m-1 & (m-1)^2 & \cdots \\ 1 & r & r^2 & \cdots \end{vmatrix}$$

$$\div \{2!\,3! \cdots (m-1)!\} = \frac{(r-1)(r-2)\cdots(r-m+1)}{(m-1)!};$$

$$B_1 = \frac{r(r-2)(r-3)\cdots(r-m+1)}{(m-2)!}, \cdots,$$

$$B_k = \frac{r(r-1)(r-2)\cdots(r-m+1)}{(r-k)(m-k-1)!\,k!} \qquad (k \leqq m-1).$$

Substituting in (4) and multiplying by $(p-1)!$ $(p > m-1)$ we have

$$(6) \quad P_r = \{[T]B_0 - [ST]B_1 + \cdots + (-1)^{m-1}[S^{m-1}T]\}(p-1)!$$
$$\equiv (-1)^m [S^r T] \pmod{p},$$

the expression P_r being an integral function of r with integral coefficients and of degree $m-1$ or less. If the coefficients of $r, r^2, \cdots, r^{m-1}$ are $\equiv 0 \pmod{p}$, we must have $P_0 \equiv P_1 \equiv \cdots \equiv P_{m-1} \pmod{p}$, or

$$(-1)^{m-1}[T] \equiv (-1)^{m-1}[ST] \equiv \cdots \equiv (-1)^{m-1}[S^{m-1}T] \pmod{p}.$$

Accordingly, if $[T] \not\equiv [ST] \pmod{p}$, P_r must be an integral function of r of the first degree at least. Assuming this to be the case, let us substitute in P_r of (6) the values $0, 1, 2, \cdots, p-1$ for r. This takes a number of different values, the remainders of which should all lie between the limits $-n$ and $+n$ inclusive, in order that the congruences (6) may be satisfied. Now, by a well known theorem, the number of different values (mod. p) of r which, when substituted in P_r, will give a definite remainder (mod. p), can not exceed the degree of P_r in r. Accordingly, the total number of different values (mod. p) of r that could satisfy the congruence (6) can not exceed $(m-1)(2n+1)$. Therefore, as $p > (n-1)(2n+1) \geqq (m-1)(2n+1)$, the congruences (6) can not be satisfied for all values r under the assumption $[T] \not\equiv [ST] \pmod{p}$. Thus $[T] \equiv [ST] \pmod{p}$, and as $|[T]| + |[ST]| \leqq 2n < p$, we must have $[T] = [ST]$. Hence, if p *be any prime greater than* $(n-1)(2n+1)$, *the congruences* (6) *require* $[T] = [ST]$.

It follows from this that (ST) can not contain roots of unity having prime indices different from those of the roots in (T) and (S). For, since the prime indices $p, q, \cdots$ of the roots contained in (T) and (S) are each greater than $2n+1$, we could otherwise distribute the numbers $-1, 0, +1$ in such a manner among the roots designated above by $y_1, z_1, \cdots, y_1^2, z_1^2, \cdots$, etc., that the value of $[T]$ becomes n, and so that the value of $[ST]$ becomes less than n numerically.

Accordingly, if the order of T is the product of powers of primes each greater than $(n-1)(2n+1)$, and the order of S is a power of a prime p greater than $(n-1)(2n+1)$, the order of ST must be a product of powers of primes each greater than $(n-1)(2n+1)$. Then, by a well-known theorem concerning the resolution of any substitution into a product of substitutions of the form S, we see the truth of Theorem IV.

It may be remarked that the limit considered in this theorem, $(n-1)(2n+1)$, is, in general, higher than necessary (see §6). The analysis just given leads to this question: what is the smallest number $\tau_n \leqq (n-1)(2n+1)$ such that no function exists of the form $P_r = ar^{n-1} + br^{n-2} + \cdots + k$ of degree not less than 1 and with integral coefficients, whose remainders (mod. p), p being any given prime greater than τ_n, will not all lie between $-n$ and $+n$ inclusive? The answer given above, $\tau_n = (n-1)(2n+1)$ is that most readily found, but is, as remarked, unnecessarily high in general.

From Theorems III and IV it follows that all the substitutions whose orders are products of powers of primes each greater than $(n-1)(2n+1)$ form an abelian subgroup of the group H, which is evidently self-conjugate in H.

§ 6.

We shall now consider more particularly the groups of degrees 3, 4, 5 and 6. We shall restrict ourselves to groups whose substitutions are of determinant 1, in which case none of the substitutions except identity considered in Theorem IV can be similarity-substitutions. We can therefore employ Theorem II directly.

Concerning the groups in three variables.

As remarked above, the limit $(n-1)(2n+1)$ can, in general be reduced. For $n=3$ the reduction depends upon the solution of the following problem: what is the least number τ_3 such that for any prime $p > \tau_3$ no function exists of the form $ar^2+br+c \not\equiv c \pmod{p}$, a, b, c being integers, all of whose remainders $(\mathrm{mod.}\ p)$ lie between -3 and $+3$ inclusive? By trying in turn all the primes less than 14 $[=(n-1)(2n+1)]$ we find that τ_3 must be 7 at least, but need not be higher. Accordingly, we have the

THEOREM V. *The order of a primitive group in three variables has the prime factors* 2, 3, 5 *and* 7 *only.*

Concerning the groups in four and five variables.

Here we have to find if functions

$$ar^3+br^2+cr+d \not\equiv d,\ ar^4+br^3+cr^2+dr+e \not\equiv e \pmod{p},$$

exist, all of whose remainders lie between -4 and $+4$, -5 and $+5$ (limits included), respectively. In the first case, no such function exists if p is a prime greater than 13, and no function of the second form exists for a prime p greater than 19. Hence

THEOREM IV. *The order of a primitive group in four variables is divisible by no prime greater than* 13. *The order of a primitive group in five variables is divisible by no prime greater than* 19.

Concerning groups in six variables.

The limit is here found to be 23.* An exception occurs in the case of $p=31$. The function r^5 has the remainders (mod. 31) $0, \pm 1, \pm 5, \pm 6$. By a more detailed study of the possible forms of the quantities $[S^kT]$ (§ 5)

* The limit may be 19 for $n=6$. The author has not considered whether functions may exist of the form $ar^5+br^4+cr^3+dr^2+er+f$ all of whose remainders (mod. 23) lie between -6 and $+6$ inclusive.

it is found, however, that if one of these numbers can be $+5$, another may be put equal to 4 or 3 by a proper distribution of the numbers $-1, 0, +1$ among the roots indicated in § 5 by $y_1, z_1, \cdots, y_1^2, z_1^2, \cdots$, etc. As the remainders of r^5 ought to be the numbers $[S^k T]$, we may exclude the prime $p = 31$.

THEOREM VII. *The order of a primitive group in six variables is divisible by no prime greater than* 23.

The orders of imprimitive and intransitive groups do not, of course, obey these laws. But such groups are, in general, of a simpler type. Thus, the imprimitive groups in three variables are of the type

$$x_1' = ax_i, \quad x_2' = bx_j, \quad x_3' = cx_k, \qquad (i, j, k = 1, 2, 3);$$

the constants a, b, c being certain roots of unity and different for the different substitutions.

Again, either an imprimitive group in four variables has the type

$$x_1' = ax_i, \; x_2' = bx_j, \; x_3' = cx_k, \; x_4' = dx_l, \quad (i, j, k, l = 1, 2, 3, 4);$$

or else its substitutions can be divided into two sets of the following types:

$$x_1' = ax_3 + bx_4, \quad x_2' = cx_3 + dx_4, \quad x_3' = \alpha x_1 + \beta x_2, \quad x_4' = \gamma x_1 + \delta x_2;$$

$$x_1' = a'x_1 + b'x_2, \quad x_2' = c'x_1 + d'x_2, \quad x_3' - \alpha' x_3 + \beta' x_4, \quad x_4' = \gamma' x_3 + \delta' x_4.$$

The construction of such a group would depend upon the construction of the primitive groups in two variables.

In the same way the construction of the imprimitive groups in six variables would depend upon the construction of the primitive groups in two and three variables.

STANFORD UNIVERSITY,
June, 1903.