ON THE ORDER OF LINEAR HOMOGENEOUS GROUPS *

(SUPPLEMENT)

BY

H. F. BLICHFELDT

§ 1. The author has given a superior limit to the value of a prime p which may divide the order of a finite, primitive group of linear homogeneous substitutions, of determinants unity, in n variables, namely $p \leq (n-1)(2n+1)$ (with reductions for the cases $n \leq 6$).† He has also proved that, if such a group G contains a substitution S of variety $m (\leq n)$ and of order $p^{a+c} \geq mp^c$, then will G contain an invariant subgroup H (or be itself such a group), which possesses the property that, if V be a substitution of G , and T one of H , then is $(V)_p \equiv (VT)_p \pmod{p}$.‡

The groups not containing H being by far the most difficult to determine, at least when n is small, the author proves, in the present paper, a theorem supplementing the one just stated, giving a lower general limit to the highest power of p which may divide the order of a group G not containing H , than flows from the theorem stated. The paper also gives further reductions to the general formula for the limit to p , as well as to the special cases when $n \leq 6$.

§ 2. THEOREM 14. *If a group G in n variables has an abelian subgroup K of order $p^a \geq p^n$, then will G have an invariant subgroup H containing a subgroup of K of order p^{a-n+1} . If S is any substitution of H , and V any of G , then is $(V)_p \equiv (VS)_p \pmod{p}$.*

Let K be written in canonical form, and let its substitutions be $I = S_0, S_i$ ($i = 1, 2, \dots, p^a - 1$), with the multipliers

$$(1, 1, 1, \dots, 1), (\theta_{1,i}, \theta_{1,i}\theta_{2,i}, \theta_{1,i}\theta_{3,i}, \dots, \theta_{1,i}\theta_{n,i}).$$

To the determinant (6) of $L-G$ II will correspond the following matrix of p^a rows and $1 + m$ columns, where m corresponds to "variety" of theorem 10:

* Presented to the Society (Chicago), April 14, 1906. Received for publication February 13, 1906.

† *On the Order of Linear Homogeneous Groups*, Transactions, vol. 4 (1903), pp. 387-397.

‡ *On the Order of Linear Homogeneous Groups* (second paper), *ibid.*, vol. 5 (1904), pp. 310-325. The theorem, stated on page 315 of the paper, is numbered 10. These two articles will be referred to by $L-G$ I and $L-G$ II, respectively.

$$(1) \quad \left\| \begin{array}{cccccc} (V) & 1 & 1 & \cdots & 1 \\ (VS_1)\theta_{1,1}^{-1} & 1 & \theta_{2,1} & \cdots & \theta_{m,1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (VS_i)\theta_{1,i}^{-1} & 1 & \theta_{2,i} & \cdots & \theta_{m,i} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{array} \right\| = 0.$$

Now, to this matrix* may be added p^{a-m+1} rows of the form

$$(2) \quad (VS_i) - (V) + (1 - \theta)X_i, 0, 0, \dots, 0,$$

where θ is a root of $p^a - 1 = 0$, and where X_i is a linear function of the quantities $(V), (VS_1), \dots$, with coefficients that are integral functions of θ , the numerical coefficients entering being integers or fractions whose denominators are prime to p . To prove this proposition we shall assume it true for all possible matrices of similar form, but containing fewer columns. Under this assumption, we may add to the matrix (1) $p^{a-m+2} - 1$ rows of the form

$$(VS_i) - (V) + (1 - \theta)X_i, 0, 0, \dots, 0, Y_i,$$

where the quantities Y_i are integral functions of θ with numerical coefficients which are integers or fractions whose denominators are prime to p . Let us suppose that i can take any one of the values $2, 3, \dots, p^{a-m+2}$.

It is readily proved that Y_i may be written in the form

$$Y_i = a_i(1 - \theta)^{\alpha_i} + b_i(1 - \theta)^{\beta_i} + c_i(1 - \theta)^{\gamma_i} + \dots \quad (\alpha_i < \beta_i < \gamma_i < \dots),$$

where α_i is one of the numbers $1, 2, \dots, p - 1$, while $b_i, c_i, \dots$ are integers or fractions whose denominators are prime to p . We shall suppose the rows arranged in such a way that

$$\alpha_2 = \alpha_3 = \dots = \alpha_{k+1} < \alpha_j \quad (j = k + 2, k + 3, \dots, p^{a-m+2}).$$

First, if $k \leq (p - 1)p^{a-m+1}$, we obtain $p^{a-m+2} - (k + 1) \geq p^{a-m+1} - 1$ rows of the form

$$(VS_j) - (V) + (1 - \theta)X_j - \frac{Y_j}{Y_2}[(VS_2) - (V) + (1 - \theta)X_2], 0, 0, \dots, 0;$$

i. e., of the form

$$(VS_j) - (V) + (1 - \theta)X'_j, 0, 0, \dots, 0.$$

Here the quantities X'_j are easily proved to be of the same general form as the quantities X_i , and hence the proposition assumed true for a matrix with m columns, is proved true for one of $m + 1$ columns.

Next, if $k > (p - 1)p^{a-m+1}$, we proceed thus: The numbers $\alpha_2, \alpha_3, \dots, \alpha_{k+1}$, taking the values $1, 2, \dots, p - 1$ only, may be separated into lots, among

* It is to be noticed that no two of the last m columns are identical.

which there must be one of $l \geq k/(p-1) \geq p^{a-m+1}$ numbers (say $a_2, a_3, \dots, a_{l+1}$), having one and the same value a_2 . Then we derive $l-1 \geq p^{a-m+1}-1$ rows of the form

$$(VS_i) - (V) + (1-\theta)X_i - \frac{Y_1}{Y_2} [(VS_2) - (V) + (1-\theta)X_2], 0, 0, \dots, 0;$$

i. e., of the form

$$(VS_i) - (VS_2) + (1-\theta)X'_i, 0, 0, \dots, 0.$$

But, if $l-1$ such rows result, it is readily proved that we could obtain $l-1$ rows of the form

$$(VS_2^{-1}S_i) - (V) + (1-\theta)X''_i, 0, 0, \dots, 0,$$

and the proposition is fully proved.

§ 3. Let us now consider the matrix (1). We may add the $p^{a-m+1}-1$ rows (2) to the p^a rows in (1). Provided that at least one of the determinants of m^2 elements, contained in the matrix obtained by erasing the first column of (1), does not vanish, we get, then, p^{a-m+1} equations of the form (including the identity when $S_i = I$):

$$(VS_i) - (V) + (1-\theta)X_i = 0.$$

The quantities X_i being integral functions of certain roots of unity, and containing no numerical coefficients whose denominators are multiples of p , the equations obtained may be written

$$(VS_i)_p - (V)_p \equiv 0 \pmod{p}.$$

From these it follows that the group G considered has an invariant subgroup H containing a subgroup of K of order p^{a-m+1} , and theorem 14 is proved (cf. the arguments in the proof of theorem 10 in *L-G II*).

§ 4. There remains to prove that there is at least one non-vanishing determinant of m^2 elements in the matrix

$$(3) \quad \begin{vmatrix} 1 & 1 & \dots & 1 \\ 1 & \theta_{2,1} & \dots & \theta_{m,1} \\ \cdot & \cdot & \cdot & \cdot \\ 1 & \theta_{2,i} & \dots & \theta_{m,i} \\ \cdot & \cdot & \cdot & \cdot \end{vmatrix}$$

Since no two of the columns are identical, there must be at least one root $\phi \neq 1$ in the r th column, $r \neq 1$, and, therefore, also one $\phi^{p^b} = \rho \neq 1$, $\rho^p = 1$, ρ being one of the multipliers of the substitution $S_k \theta_{1,k}^{-1}$, say. If we exhibit the abelian group K in the form

$$K \equiv A(1 + S_k + S_k^2 + \dots + S_k^{p-1}) + B(1 + S_k + S_k^2 + \dots + S_k^{p-1}) + \dots,$$

$A, B, \dots$ being substitutions of K not identical with powers of S_λ , it becomes evident that the sum of all the roots in the column considered can be written so as to have $1 + \rho + \rho^2 + \dots + \rho^{p-1}$ as a factor and is therefore zero. Accordingly, by adding all the rows of (3) together, we get a row of the form

$$p^a, 0, 0, \dots, 0.$$

Moreover, it is clear that we can multiply the rows by such roots of unity that their sum is

$$0, p^a, 0, \dots, 0;$$

etc. There results a determinant whose value is p^{na} , and theorem 14 is fully proved.

§ 5. It now follows that, if the order of a collineation group G in n variables is divisible by p^{n+n_p} , when p is a prime, and n_p denotes the highest power of p that divides $n!$, then will G contain a self-conjugate subgroup H , or be itself such a group. For, a group of order p^k can be written in monomial form (theorem 9, *L-G* II). The group of order p^{n+n_p} contained in G will accordingly have an abelian subgroup of order p^n at least, which subgroup, when written as a linear homogeneous group, will be of order p^{n+l} , if it contains a group of similarity-substitutions of order p^l .

COROLLARY. *The factor of the order of a collineation group G (not containing H), which is the product of primes each $\leq n$, must divide $n! (2 \cdot 3 \cdots p)^{n-1}$, where $2, 3, \dots, p$ denote all the different primes $\leq n$.*

§ 6. For the purpose of lowering the limit of p ($p > n$), we shall consider the case of a group G containing a substitution S of order p and of variety m , but no substitution of order pk ($k > 1$) unless such a substitution is the product of one of order p and a similarity substitution. Let V be any substitution of G . In the series of weights,

$$(V), (VS), \dots, (VS^{p-1}),$$

write $+1, 0$ or -1 for every root of unity of an index prime to p , according to the scheme explained in § 3 of *L-G* I. We shall, however, leave unchanged the roots of index p . The resulting expressions will be indicated by $[V], [VS], \dots$. Then every $[VS^a]$ will be an integer lying between $-n$ and $+n$, inclusive, if the order of VS^a is prime to p ; otherwise $[VS^a]$ will be the sum of n p th roots of unity,* the negative of such a sum, or 0, depending on the value ($1, -1$ or 0) allotted to the multipliers of the similarity substitution $\{VS^a\}^p$. Let w denote the number of weights $[VS^a]$ which are

* No primitive group in n variables can have a substitution of order p^2 , if $p > n$. See Cor. 1, page 316, of *L-G* II.

therefore $\beta = \gamma = \dots = 0$, an absurdity. Hence the proposition:

$$w \equiv p + 1 - m - m'.$$

Now, according to §§ 4-5 of *L-G I*, we have the congruence

$$A_r^0 \equiv ar^{m-1} + br^{m-2} + \dots = f(r) \pmod{p},$$

where $a, b, \dots$ are certain integers. The numbers A_r^0 are integers all lying between $-n$ and $+n$ inclusive, and, by the proposition just proved, at least $p + 1 - m - m'$ of them are either $+n$ or $-n$. However, at most $2(m-1)$ of the remainders of $f(r) \pmod{p}$ can be $+n$ or $-n$, unless $f(r)$ is merely a constant. This it could not be in all cases, as then, for every V of G , we would have $(V)_p \equiv (VS)_p \pmod{p}$, and G would have an invariant subgroup H , which would be of order p' and would therefore be abelian. In such a case G could not be primitive (theorems II and III, *L-G I*). Thus,

$$2(m-1) \geq p + 1 - m - m' \quad \text{or} \quad p \leq 3m + m' - 3 \leq 3m + n - 3.$$

We have now proved

THEOREM 15. *If a primitive collineation-group G in n variables has a substitution of order p ($p > n$) and of variety m ($m \leq n$), but none of order pk , then is $p \leq 3m + n - 3$.*

If, in such a group, there is a substitution of order pk , which is the product of one (S) of order p and one of order k , then can the variety of S be $n-1$ at most, unless there is an invariant subgroup H (theorem 11, *L-G II*). The number p can then not exceed $(n-2)(2n+1)$.

§ 7. If $n = 4$, the theorem VI of *L-G I* states that $p \leq 13$. For $p = 13$ we can, however, find no function $ar^3 + br^2 + cr + d \not\equiv d$, all of whose remainders $\pmod{13}$ lie between -4 and $+4$ inclusive, and $13 + 1 - 8 = 6$ of which have the values $+4$ or -4 . Accordingly, by what precedes, a primitive group in 4 variables can have no substitution S of order 13 unless it has one of order $13k$, expressible as a product SR ($S^{13} = 1$, $R^k = 1$; R and S permutable; R not a similarity-substitution), whose weight is $\alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3 + \alpha_4\beta_4$, where $\alpha_i^{13} = 1$, $\beta_i^k = 1$. In this case we form the determinant corresponding to (3) of *L-G I*, with (T) , (R^aST) , (R^bS^2T) , (R^cS^3T) , (R^dS^4T) for the elements of the first column. We will choose a, b, c such that the resulting equation can be solved for (R^dS^4T) , and then replace all the 13th roots of unity by 1. Now, a primitive group G in 4 variables could not have an invariant subgroup H of such a nature that, if V and S be any substitutions of G and H respectively, $(V)_{13} \equiv (VS)_{13} \pmod{13}$. It follows that (R^dS^4T) is not expressible in the form $Ar + B$ (A and B being independent of r), since in that event there would be just such a subgroup H . Excluding, therefore,

this possibility, we find readily that three of the roots β_i are equal to each other, say $\beta_2 = \beta_3 = \beta_4$, and then that

$$(R^s S^r T)_{13} \equiv \beta_1^s A + \beta_2^s (Br^2 + Cr + D) \pmod{13},$$

the quantities A, B, C, D being independent of r and s .

If $A \equiv 0$, then is $(R^s S^r T)_{13} \equiv (S^r T)_{13} \beta_2^s \pmod{13}$; or, putting $T = S^{-r}$, $(R^s)_{13} \equiv 4\beta_2^s \pmod{13}$. But this is an impossible congruence for $s = 1$. Hence, $A \not\equiv 0$, and we have

$$(R^s S^r T)_{13} \beta_2^{-s} \equiv \left(\frac{\beta_1}{\beta_2} \right)^s A + Br^2 + Cr + D \pmod{13}.$$

The values $-1, 0, 1$ may now be assigned to the roots of unity involved, in accordance with the scheme of § 3, *L-G I*; and, as $\beta_1 \neq \beta_2$, we have a function

$$B_1 r^2 + C_1 r + D_1 + A' \neq D_1 + A' \pmod{13},$$

B_1, C_1, D_1 and A' being integers, the last of which is capable of taking, at our will, at least two different values. All the remainders $\pmod{13}$ of this function should lie between -4 and $+4$ inclusive. But such a function does not exist.*

In a similar manner we may deal with the cases $n = 5, p = 17$ or 19 ; $n = 6, p = 23$.† The results are expressed in the following

THEOREM 16. *The primes which may divide the orders of the primitive collineation-groups in 4, 5 and 6 variables are, respectively, not greater than 11, 12 and 19.*

BERLIN,

January, 1906.

* In the article written by the author on quaternary groups, *Mathematische Annalen*, vol. 60 (1905), pp. 204-231, it is proved, in a different manner, that the primitive collineation-groups in 4 variables can have no substitutions of order 11 or 13.

† The cases $n = 6, p = 17$ or 19 have not been examined by the author. It is very likely that we may, by the process given above, throw out at least 19.