The Finite, Discontinuous, Primitive Groups of Collineations in Three Variables.*)

By

H. F. Blichfeldt of Stanford University, California, U. S. A.

A complete enumeration of all finite, discontinuous groups of collineations in three variables was first attempted by C. Jordan in his well-known paper *Mémoire sur les équations différentielles linéaires à intégrale algebrique*, *Journal für die reine und angewandte Mathematik*, 84 (1878), p. 89. It appeared, however, shortly afterwards, that Jordan had overlooked two important groups, viz.: the G_{168}, discovered by Klein (*Mathematische Annalen*, 14 (1879), p. 428), and the G_{360}, discovered by Valentiner (Copenhagen, *Videnskabernes Selskabs Skrifter*, 6. *Raekke*, 1889). No other groups have since been added to Jordan's list. It seems therefore desirable to have a new and rigorous proof of the fact that Jordan's *groups together with the* G_{168} *and the* G_{360} *form indeed a complete set of the finite, discontinuous groups of collineations in three variables.* This is the theorem to be proved in the present paper.

1. We consider only finite groups of linear projective transformations of the plane $(x:y:z)$, and we call such groups *Collineation-groups* in three variables. We represent them by isomorphic groups of *linear homogeneous substitutions of determinants unity* in three variables (x, y, z), which groups we call *Linear Groups* (or *groups*, simply, where it cannot be misunderstood). The isomorphism will be $1:1$ or $1:3$, according as the linear group *does not* or *does* contain the group F of *similarity-substitutions* of order 3:

$$F:\begin{cases} x' = x, & y' = y, & z' = z; \\ x' = \omega x, & y' = \omega y, & z' = \omega z; \\ x' = \omega^2 x, & y' = \omega^2 y, & z' = \omega^2 z; & \qquad \omega^3 = 1,\ \omega \neq 1. \end{cases}$$

*) For a bibliography of this subject consult Wiman: *Endliche Gruppen linearer Substitutionen, Encyklopädie der Mathematischen Wissenschaften*, Bd. I, pp. 528—530. See also two papers by the author, *On the Order of Linear Homogeneous Groups, Transactions of the American Mathematical Society*, vol. 4 (1903), pp. 387—397, and vol 5 (1904), pp. 310—325.

Thus, to the three linear homogeneous substitutions

$$x' = \theta(a_1x + b_1y + c_1z), \qquad y' = \theta(a_2x + b_2y + c_2z),$$
$$z' = \theta(a_3x + b_3y + c_3z), \qquad \theta^3 = 1,$$

will correspond the one collineation

$$x' : y' : z' = (a_1x + b_1y + c_1z) : (a_2x + b_2y + c_2z) : (a_3x + b_3y + c_3z).$$

2. We say that the group is *primitive* if it does not leave invariant a *point* or a *triangle.* A finite group leaving invariant a point will also leave invariant a straight line not passing through the point and vice versa (the group is completely 'reducible'*). We call such a group *intransitive**). A group which leaves invariant the triangle of reference is said to be written in *monomial form***). Its substitutions merely permute among themselves the variables x, y, z, in addition to affecting them with certain constant factors. A substitution or a group which leaves invariant each of the vertices of the triangle of reference, is said to be written in *canonical form.* The variables x, y, z are merely multiplied by certain constants by the substitutions of such a group. A substitution S of finite period n

$$x' = a_1x + b_1y + c_1z, \quad y' = a_2x + b_2y + c_2z, \quad z' = a_3x + b_3y + c_3z$$

can always be transformed, by a proper choice of new variables x_1, y_1, z_1, into the canonical form:***)

$$x_1' = \theta_1x_1, \quad y_1' = \theta_2y_1, \quad z_1' = \theta_3z_1.$$

The quantities θ_1, θ_2, θ_3, called the *multipliers* of S, satisfy the equation $\theta^n = 1$. We have the equation

$$[S] = \theta_1 + \theta_2 + \theta_3 = a_1 + b_2 + c_3.$$

The quantity $[S]$, so defined, shall be called the *weight* of S.

3. The more fundamental phraseology and theory of abstract groups and permutation-groups will be supposed known.†) In particular, it may be mentioned that an *abelian group* consists of mutually commutative substitutions, and that a *simple group* contains no invariant subgroup. The only simple groups whose orders are $\leqq 504$ are the following: the alternating permutation-groups in 5 and 6 letters, of orders 60 and 360 respectively; a group of order 168 and one of order 504††). The

---

*) Maschke, *Mathematische Annalen* 52 (1899), p. 363.

**) Maschke, *American Journal of Mathematics* 17 (1895), p. 168.

***) See Moore, *Mathematische Annalen* 50 (1898), p. 215 for proof and references.

†) Consult Burnside, *Theory of Groups*, Cambridge University Press, 1897; and Weber, *Algebra*, Bd II, Braunschweig (Vieweg und Sohn), 2nd edition, 1899.

††) Burnside, *Theory of groups*, pp. 371—375.

usual way of executing a consecutive set of linear substitutions $ABC\cdots$ in the order from left to right will be adhered to here. For instance, if we restrict ourselves to two variables x, y, and A is the substitution $x'' = a_1 x' + b_1 y'$, $y'' = c_1 x' + d_1 y'$, B the substitution $x' = a_2 x + b_2 y$, $y' = c_2 x + d_2 y$, so that

$$x'' = (a_1 a_2 + b_1 c_2) x + (a_1 b_2 + b_1 d_2) y,$$
$$y'' = (c_1 a_2 + d_1 c_2) x + (c_1 b_2 + d_1 d_2) y,$$

we write instead but one accent in the two substitutions A, B (i. e. B as above, $A: x' = a_1 x + b_1 y$, $y' = c_1 x + d_1 y$), and then indicate the order in which the two substitutions are executed by the symbol AB.

By the order of a group (i. e. total number of substitutions of the group) *shall be understood the order of the corresponding collineation-group, unless otherwise stated.*

4. A list of the finite, non-abelian, groups of linear homogeneous substitutions, of determinants $= 1$, in two variables x, y, will be useful for later references and is therefore given here. Each group is represented by a set of substitutions that generate it.*)

1⁰. The *Dihedral* group of order $2n$:

$$\begin{cases} S: & x' = \alpha x, \quad y' = \alpha^{-1} y, \quad \alpha^n = 1; \\ T: & x' = y, \quad y' = -x. \end{cases}$$

2⁰. The *Tetrahedral* group of order 12 (as a collineation-group; of order 24 as a linear group. When written as a linear group, it contains the group of similarity-substitutions in two variables: $x' = x$, $y' = y$; $x' = -x$, $y' = -y$):

$$\begin{cases} S: & x' = y, \quad y' = -x; \\ T: & x' = ix, \quad y' = -iy, \quad i^2 = -1; \\ U: & x' = \frac{1}{2}(-1 - i)x + \frac{1}{2}(1 + i)y, \\ & y' = \frac{1}{2}(-1 + i)x + \frac{1}{2}(-1 + i)y. \end{cases}$$

3⁰. The *Octahedral* group of order 24 (as a collineation-group; of order 48 as a linear group):

$$\begin{cases} S,\ T \text{ and } U \text{ of } 2^0; \\ V: \quad x' = \frac{1}{\sqrt{2}}(1 + i)x, \quad y' = \frac{1}{\sqrt{2}}(1 - i)y. \end{cases}$$

*) See Klein, *Vorlesungen über das Ikosaeder* (Leipzig 1884), pp. 36—42; Weber, *Algebra*, Bd. II, pp. 269—287 (2nd edition, 1899).

4⁰. The *Icosahedral* group of order 60 (as a collineation-group; of order 120 as a linear group):

$$\begin{cases} S: & x' = y, \quad y' = -x; \\ T: & x' = \alpha x, \quad y' = \alpha^{-1} y, \quad \alpha^5 = 1, \quad \alpha \neq 1; \\ U: & x' = \frac{1}{\alpha - \alpha^{-1}}(x - (\alpha^2 + \alpha^{-2})y), \quad y' = \frac{1}{\alpha - \alpha^{-1}}(-(\alpha^2 + \alpha^{-2})x - y). \end{cases}$$

5. The arrangement of the analysis is as follows:

I. *Preliminary Theorems.*

II. *The Order is not Divisible by any Prime* > 7.

III. *The Order is a Factor of* $2^3 \cdot 3^3 \cdot 5^2 \cdot 7^2$. It is shown that, if the order is divisible by 2^4, or 3^4 etc., then will the group considered contain a certain invariant subgroup H, and will not be primitive unless the order of H is of the form 3^k. The primitive groups containing invariant subgroups of this order are the 'Hessian' group of order $216 = 2^3 \cdot 3^3$ and some of its subgroups (art. 23). The Theorem III is therefore established.

IV. *Auxiliary Theorems.* In any case where the order is divisible by $3^3 \cdot 5$, $3^3 \cdot 7$, 5^2, 7^2 or $5 \cdot 7$, the group has an invariant subgroup H and is therefore not primitive. Hence, the order is a factor of one of the numbers $2^3 \cdot 3^3$, $2^3 \cdot 3^2 \cdot 5$, or $2^3 \cdot 3^2 \cdot 7$.

V. *Classification of the Primitive Groups.* The results are as follows:

A. Primitive groups having invariant intransitive subgroups (none).

B. Primitive groups having invariant monomial subgroups:

1⁰. The *Hessian* group of order 216 as a collineation-group, of order 648 as a linear group:

$$\begin{cases} S: & x' = y, \quad y' = z, \quad z' = x; \\ T: & x' = x, \quad y' = \omega y, \quad z' = \omega^2 z, \quad \omega^3 = 1, \quad \omega \neq 1; \\ U: & x' = \varphi x, \quad y' = \varphi y, \quad z' = \varphi \omega z, \quad \varphi^3 = \omega^2; \\ V: & x' = \varrho(x + y + z), \quad y' = \varrho(x + \omega y + \omega^2 z), \quad z' = \varrho(x + \omega^2 y + \omega z), \\ & \varrho = \frac{1}{\omega - \omega^2}. \end{cases}$$

2⁰. A subgroup of the Hessian group, of order 72 as a collineation-group, and of order 216 as a linear group:

$$\begin{cases} S, T \text{ and } V \text{ of } 1^0; \\ UVU^{-1}: \quad x' = \varrho(x + y + \omega^2 z), \quad y' = \varrho(x + \omega y + \omega z), \\ \qquad\qquad z' = \varrho(\omega x + y + \omega z). \end{cases}$$

3⁰. A subgroup of the Hessian group, of order 36 as a collineation-group, and of order 108 as a linear group: S, T and V of 1⁰.

C. Primitive groups isomorphic with simple abstract groups:

4⁰. Group of order 60, both as a collineation- and as a linear group:

$$\begin{cases} E_1: & x' = y, \quad y' = z, \quad z' = x; \\ E_2: & x' = x, \quad y' = -y, \quad z' = -z; \\ E_3: & x' = \frac{1}{2}(-x + \mu_2 y + \mu_1 z), \quad y' = \frac{1}{2}(\mu_2 x + \mu_1 y - z), \\ & z' = \frac{1}{2}(\mu_1 x - y + \mu_2 z), \\ & \mu_1 = \alpha + \alpha^4 = \frac{1}{2}(-1 + \sqrt{5}), \quad \mu_2 = \alpha^2 + \alpha^3 = \frac{1}{2}(-1 - \sqrt{5}), \\ & \alpha^5 = 1. \end{cases}$$

5⁰. Group of order 360 as a collineation-group, of order 1080 as a linear group:

$$\begin{cases} E_1, E_2 \text{ and } E_3 \text{ of } 4^0; \\ E_4: \quad x' = -x, \quad y' = -\omega z, \quad z' = -\omega^2 y, \qquad \omega^2 + \omega + 1 = 0. \end{cases}$$

6⁰. Group of order 168, both as a collineation- and as a linear group:

$$\begin{cases} S: & x' = \varepsilon x, \quad y' = \varepsilon^2 y, \quad z' = \varepsilon^4 z, \qquad \varepsilon^7 = 1, \quad \varepsilon \neq 1; \\ T: & x' = z, \quad y' = x, \quad z' = y; \\ U: & x' = h(\alpha x + \beta y + \gamma z), \quad y' = h(\beta x + \gamma y + \alpha z), \quad z' = h(\gamma x + \alpha y + \beta z), \\ & \alpha = \varepsilon^4 - \varepsilon^{-4}, \quad \beta = \varepsilon^2 - \varepsilon^{-2}, \quad \gamma = \varepsilon - \varepsilon^{-1}, \\ & h = \frac{1}{7}(\varepsilon + \varepsilon^2 + \varepsilon^4 - \varepsilon^{-1} - \varepsilon^{-2} - \varepsilon^{-4}) = \frac{1}{\sqrt{-7}}. \end{cases}$$

6. For a detailed study of the subject of linear groups consult the following memoires, in addition to those mentioned in the footnotes and in the synopsis by Wiman, '*Endliche Gruppen linearer Substitutionen*', *Encyklopädie der Mathematischen Wissenschaften,* Bd. 1, pp. 522—554:

Weber: Algebra II, Lineare Gruppen.

Frobenius: a series of articles in the *Sitzungsberichte der Kgl. Preuß. Akademie der Wissenschaften,* beginning with '*Über Gruppencharaktere*', Sitzungsberichte 1896, p. 985.

I. Schur: '*Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*', *Journal für die reine und angewandte Mathematik,* Bd. 127 (1904), p. 20; also articles given in the *Sitzungsberichte der Kgl. Preuß. Akad. d. Wiss.,* beginning with '*Über eine Klasse von endlichen Gruppen linearer Substitutionen*', 1905, p. 77.

W. Burnside: a series of papers in the *Proceedings of the London Mathematical Society,* beginning with '*On group characteristics*', vol. 33 (1900), p. 146; also a paper '*On the reduction of a group of homogeneous linear substitutions of finite order*', *Acta Mathematica* 28 (1904), p. 369.

A. Loewy: '*Über die Reducibilität der Gruppen linearer homogener Substitutionen*', *Transactions of the American Mathematical Society*, vol. 4 (1903), p. 44, and further papers in the same journal.

On the special problem of the collineation groups in four variables consult Bagnera, *Rendiconti del Circolo Matematico di Palermo*, 1901, p. 161, and 1905, p. 1; Autonne, *Journal de Mathématiques pures et appliquées*, 1901, p. 351; Blichfeldt, *Transactions of the Am. Math. Society*, 1905, p. 230 and *Mathematische Annalen*, 1905, p. 204.

I. Preliminary Theorems.

7. The Theorems 1—3 will be assumed true for all linear groups in two variables, as they may be verified either directly from the list of the binary groups given (art. 4), or by employing the methods used below in the case of three variables to the case of two variables.

Theorem 1. *An abelian group can be written in canonical form.*

An abelian group G which is not the group F (art. 1) merely (for which the theorem is evident), contains an invariant substitution A which is not a similarity-substitution. Let us choose the variables so that A is written in canonical form (art. 2), say

$$x' = \alpha x, \quad y' = \beta y, \quad z' = \gamma z.$$

If no two of the multipliers α, β, γ are equal, we prove the theorem simply by determining the general form of any other substitution B of G, which must satisfy the relation

$$AB = BA.$$

If $\alpha = \beta \neq \gamma$, we find the general form of B (i. e. of every substitution of G) to be the following:

$$x' = ax + by, \quad y' = cx + dy, \quad z' = ez.$$

The substitutions

$$x' = ax + by, \quad y' = cx + dy$$

form an abelian group in two variables, which can be written in canonical form. New variables x_1, y_1, certain linear functions of x, y, may therefore be choosen so that every substitution of G is of the form

$$x_1' = \theta_1 x_1, \quad y_1' = \theta_2 y_1, \quad z' = \theta_3 z.$$

Theorem 2. *A group G containing an invariant abelian subgroup $H \neq F$ is either intransitive or can be written in monomial form.*

We prove the theorem simply by writing H in canonical form, and then find the general form of a substitution B of G such that $BA_1 = A_2 B$, where A_1, A_2 belong to H.

Theorem 3. *A group G whose order is the power of a prime p can be written in monomial form.*

Consider a group G of order p^m. We can construct a series of groups

$$G, G_1, G_2, \cdots$$

of orders p^m, p^{m-1}, p^{m-2}, $\cdots$, each of which is contained in all that stand to the left of it and is invariant in G*). Now, if G is abelian, the theorem is true (Theo. 1). If G_1 is abelian, but G not, then can G_1 not be the group F, whose substitutions are commutative with every substitution of G**). Hence, G is intransitive or can be written in monomial form, by Theo. 2. If G is intransitive, say of the form

$$x' = ax + by, \quad y' = cx + dy, \quad z' = ez,$$

the group formed of the substitutions

$$x' = ax + by, \quad y' = cx + dy$$

will be of order p^n. The Theorem to be proved being true for two variables, it would be true for three.

If G_{i+1} is abelian, but G_i not, then is $G_{i+1} \neq F$. The group G, leaving G_{i+1} invariant, could be written in monomial form, and the Theorem is proved.

8. Lemma 1. *Let $\Sigma = 0$ be a true equation, the left-hand member of which is the sum of a finite number of roots of unity. A certain root of unity of order p^n (p being a prime), say θ, may be selected so that every term of Σ is the product of a power of θ and a root whose index***) is prime to p. Then, if θ be replaced by 1, the resulting equation may no longer be true, but the left-hand member will become $p \times$ (the sum of a finite number of roots of unity).*

This follows immediately from a Theorem by Kronecker†) which says that, θ being regarded a variable, the quantity Σ either is divisible by the expression

$$1 + \theta^{p^{n-1}} + \theta^{2p^{n-1}} + \cdots + \theta^{(p-1)p^{n-1}}$$

or vanishes for all values of θ. If θ_1 represents $\theta^{p^{n-1}}$, so that θ_1 is a primitive root of the equation $\theta_1{}^p - 1 = 0$, then we can write every power of θ occurring in Σ in the form $\theta^t \theta_1^{t_1}$, where $t < p$, $t_1 < p$. Then Kronecker's Theorem says that either will Σ vanish for every value of θ and θ_1, or must be divisible by $1 + \theta_1 + \theta_1{}^2 + \cdots + \theta_1{}^{p-1}$. In other

*) Burnside, *Theory of Groups*, p. 64.

**) Ibid. p. 63.

***) By the *index* of a root of unity φ we mean the least positive integer m for which $\varphi^m = 1$.

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

words, *if Σ be arranged according to powers of θ_1, then are the coefficients equal.*

9. Let $\theta, \alpha, \beta, \cdots$ represent a system of primitive roots of the equations

$$\theta^{p^n} - 1 = 0, \quad \alpha^{q^m} - 1 = 0, \quad \beta^{r^l} - 1 = 0, \cdots,$$

and $\theta_1, \alpha_1, \beta_1, \cdots$ primitive roots of the equations

$$\theta_1^p - 1 = 0, \quad \alpha_1^q - 1 = 0, \quad \beta_1^r - 1 = 0, \cdots,$$

$p, q, r, \cdots$ being different primes. We shall suppose the system $\theta, \alpha, \beta, \cdots$ chosen so that every term of Σ can be written in the form of a product of powers of roots of the system. Then a little consideration of Kronecker's Theorem will convince one that the terms of the quantity Σ can be arranged in the following form:

$$\Sigma = T(1 + \theta_1 + \theta_1^2 + \cdots + \theta_1^{p-1}) + A(1 + \alpha_1 + \alpha_1^2 + \cdots + \alpha_1^{q-1}) + B(1 + \beta_1 + \beta_1^2 + \cdots + \beta_1^{r-1}) + \cdots,$$

where the powers of θ contained in T are $< p$, those of α in A are $< q$, those of β in B are $< r$, etc. It is then apparent that the equation $\Sigma = 0$ is satisfied whatever finite values be given to the roots $\theta, \alpha, \beta, \cdots, \theta^2, \alpha^2, \beta^2, \cdots$, etc.; $\theta_1, \alpha_1, \beta_1, \cdots, \theta_1^2, \alpha_1^2, \beta_1^2, \cdots$, etc., regarded now as independent quantities, so long as

$$1 + \theta_1 + \theta_1^2 + \cdots + \theta_1^{p-1} = 0, \quad 1 + \alpha_1 + \alpha_1^2 + \cdots + \alpha_1^{q-1} = 0,$$
$$1 + \beta_1 + \beta_1^2 + \cdots + \beta_1^{r-1} = 0, \cdots.$$

In particular, we may put 0 for every $\theta, \theta^2, \cdots, \theta^{p-1}$, $\alpha, \alpha^2, \cdots, \alpha^{q-1}$ $\beta, \beta^2, \cdots, \beta^{r-1}, \cdots$, occurring in $T, A, B, \cdots$, and replace $\theta_1, \theta_1^2, \cdots, \theta_1^{p-1}$, $\alpha_1, \alpha_1^2, \cdots, \alpha_1^{q-1}$, $\beta_1, \beta_1^2, \cdots, \beta_1^{r-1}, \cdots$ in such a manner by the numbers $0, 1, -1$ that we have $1 + \theta_1 + \theta_1^2 + \cdots + \theta_1^{p-1} = 0$, etc. If, however, this scheme be carried out only with reference to the roots $\theta, \theta^2, \cdots, \theta^{p-1}$, $\alpha, \alpha^2, \cdots, \alpha^{q-1}$, $\beta_1, \alpha_1^2, \cdots, \beta_1, \cdots$, at the same time replacing each of the roots $\theta_1, \theta_1^2, \cdots, \theta_1^{p-1}$ by 1, the quantity Σ will not necessarily be $= 0$, but will certainly be $\equiv 0 \pmod{p}$. We shall state this result in the following form:

Lemma 2. *Let every term of Σ be written in the form*

$$(\theta^t \alpha^a \beta^b \cdots)(\theta_1^{t_1} \alpha_1^{a_1} \beta_1^{b_1} \cdots), \qquad t, t_1 < p; \; a, a_1 < q; \; b, b_1 < r, \cdots.$$

Then if every factor $(\theta^t \alpha^a \beta^b \cdots)$ which is not already $= 1$ be replaced by 0, every factor $\theta_1^{t_1}$ by 1, and the powers $\alpha_1, \alpha_1^2, \cdots, \alpha_1^{q-1}, \beta_1, \beta_1^2, \cdots, \beta_1^{r-1}, \cdots$, regarded now as so many independent quantities, be replaced by 0, 1 or -1 in such a manner that the equations

$$1 + \alpha_1 + \alpha_1^2 + \cdots + \alpha_1^{q-1} = 0, \quad 1 + \beta_1 + \beta_1^2 + \cdots + \beta_1^{r-1} = 0, \cdots$$

are satisfied, then will the resulting value of Σ be an integer $\equiv 0 \pmod{p}$.

II. The Order is not Divisible by any Prime > 7.

10. Let G be a group whose order is divisible by a prime $p > 7$. Then it contains a substitution S of order p, which we may write in canonical form:

$$S: \quad x' = \theta_1 x, \quad y' = \theta_2 y, \quad z' = \theta_3 z, \qquad \theta_1{}^p = \theta_2{}^p = \theta_3{}^p = 1.$$

Two cases may arise: the multipliers are all different, or $\theta_1 = \theta_2 \neq \theta_3$. We shall consider only the first possibility, remarking that there will be hardly any difference in the manner of procedure in the two cases.

Let T be any other substitution of order p in G:

$$T: \quad x' = a_1 x + b_1 y + c_1 z, \quad y' = a_2 x + b_2 y + c_2 z, \quad z' = a_3 x + b_3 y + c_3 z.$$

Let us form the substitutions TS, TS^2, TS^λ. We have (art. 2)

$$\begin{aligned}[][T] &= a_1 + b_2 + c_3, \\ [TS] &= a_1\theta_1 + b_2\theta_2 + c_3\theta_3, \\ [TS^2] &= a_1\theta_1{}^2 + b_2\theta_2{}^2 + c_3\theta_3{}^2, \\ [TS^\lambda] &= a_1\theta_1{}^\lambda + b_2\theta_1{}^\lambda + c_3\theta_3{}^\lambda.\end{aligned}$$

Eliminating the quantities a_1, b_2, c_3 we get the equation

$$\text{(1)} \qquad \begin{vmatrix} [T] & 1 & 1 & 1 \\ [TS] & \theta_1 & \theta_2 & \theta_3 \\ [TS^2] & \theta_1{}^2 & \theta_2{}^2 & \theta_3{}^2 \\ [TS^\lambda] & \theta_1{}^\lambda & \theta_2{}^\lambda & \theta_3{}^\lambda \end{vmatrix} = 0.$$

Dividing by $(\theta_1 - \theta_2)(\theta_2 - \theta_3)(\theta_3 - \theta_1)$ we get

$$[TS^\lambda] + [T]\,\Sigma_1 + [TS]\,\Sigma_2 + [TS^2]\,\Sigma_3 = 0,$$

the coefficients Σ_1, Σ_2, Σ_3 being certain integral functions of θ_1, θ_2, θ_3. The weights $[TS^\lambda]$, $[T]$, $\cdots$ being each the sum of three roots of unity (art. 2), we have an equation $\Sigma = 0$ of the type considered in articles 8—9.

We shall apply the Lemma 2, and put 1 for every root whose index is p. To such roots belong θ_1, θ_2 and θ_3, and the quantities Σ_1, Σ_2 and Σ_3 take the values

$$-\frac{(\lambda-1)(\lambda-2)}{2}, \quad \lambda(\lambda-2), \quad -\frac{\lambda(\lambda-1)}{2}$$

respectively, as may be proved readily. To clear of fractions we multiply throughout by $p+1$. The weights $[TS^\lambda]$, $[T]$, etc., being each the sum of three roots of unity, will take integral values lying between -3 and $+3$, inclusive, by the process of article 9. Indicating the resulting value of the indeterminate quantity $[TS^\lambda]$ by $[TS^\lambda]'$, we obtain, finally, a congruence of the form

$$[TS^\lambda]' \equiv a\lambda^2 + b\lambda + c \pmod{p}, \qquad \lambda = 0, 1, 2, \cdots, p-1;$$

a, b, c being certain integers independent of λ.

Bearing in mind that $[TS^\lambda]'$ can have only 7 different values, namely ± 3, ± 2, ± 1, 0, we find without much trouble that the congruence is possible only if $a \equiv b \equiv 0 \pmod{p}$ when $p > 7$. It follows that

$$[TS^\lambda]' \equiv [T]' \equiv 3 \pmod{p},$$

since T was, by assumption, a substitution of order p.

Now, the weight $[TS^\lambda]$, for any given value of λ, could contain no roots not satisfying the equation $\theta^p - 1 = 0$. For if it did, we could at the outset have made one such root 0 by the scheme laid down in article 9, in which case the quantity $[TS^\lambda]$ (for the value of λ given) would have had one of the values ± 2, ± 1, 0 only. No one of these numbers is, however, $\equiv 3 \pmod{p}$, if $p > 7$.

11. The product of any two substitutions of G each of order p, as TS, must therefore be the identical substitution (whose weight is $1+1+1$) or be a substitution of order p. It follows that all the substitutions of order p contained in G, together with the identical substitution, form a group by themselves. This group, H say, is transformed into itself by the substitutions of G, as a substitution of order p is transformed into one of the same order. The order of H is evidently a power of p. It can therefore be written in monomial form (Theorem 3). A monomial group will, however, contain substitutions of order 2 or 3, unless the monomial form is the canonical merely, in which case the group is evidently abelian. Accordingly, H is an abelian group, and G can not be primitive (Theorem 2). Hence, finally, a primitive group can contain no substitution of prime order $p > 7$.

Theorem 4. *The order of a primitive group is not divisible by any prime* $p > 7$.

III. The Order is a Factor of $2^3 \cdot 3^3 \cdot 5^2 \cdot 7^2$.

12. We may study a group whose order is the power of a prime very easily by writing it in monomial form (Theorem 3). We shall not enter into the details of this simple problem, but merely state the following results:

α. A group of order 2^4 must contain a substitution of order 8, or a substitution of order 4 whose weight has the form $(-1 + i + i)$, $i^2 = -1$.

β. A group of order 3^4 (of order 3^5 as a linear group containing F) must contain a substitution whose 3^{rd} power is neither the identical substitution nor a similarity-substitution.

γ. A group of order p^3, $p > 3$, must contain a substitution of order p^2.

We shall proceed to show that a group G containing any of the special substitutions just mentioned must leave invariant a certain subgroup H, defined below, and that as a consequence it cannot be primitive. Now, by a well known theorem, a group whose order is divisible by p^n (p being a prime) contains a subgroup of order p^n.*) It follows, from Theorem 4 and from the results stated under α, β, γ, that the order of a primitive group must be a factor of $2^3 \cdot 3^3 \cdot 5^2 \cdot 7^2$.

13. Consider a group G containing a substitution S of order 8, whose multipliers are φ_1, φ_2, φ_3. At least one of these must be a primitive 8$^{\text{th}}$ root of unity, and we shall, for the present, assume that they are different one from the other. We choose the variables of G so that S is written in canonical form.

Let T be any other substitution of G. We can form an equation in the same manner as we formed (1) of article 10, by eliminating certain quantities a_1, b_2, c_3 from the weights of the substitutions T, TS^4, TS and TS^2, namely the equation:

$$\begin{vmatrix} [TS] & 1 & 1 & 1 \\ [TS^4] & \varphi_1{}^4 & \varphi_2{}^4 & \varphi_3{}^4 \\ [TS] & \varphi_1 & \varphi_2 & \varphi_3 \\ [TS^2] & \varphi_1{}^2 & \varphi_2{}^2 & \varphi_3{}^2 \end{vmatrix} = 0.$$

After multiplying out we divide by $(\varphi_1 - \varphi_2)(\varphi_2 - \varphi_3)(\varphi_3 - \varphi_1)$. The weights $[T]$, etc., being each the sum of three roots of unity, we obtain an equation $\Sigma = 0$ of the type considered in articles 8—9. We shall apply the Lemma 1, and put 1 for every root whose index is a power of 2. Indicating the modified weights by the symbols $[T]_2$, $[TS^4]_2, \cdots$, the resulting equation will be found to be of the form

$$3[T]_2 - [TS^4]_2 - 8[TS]_2 - 6[TS^2]_2 \equiv 0 \pmod{2},$$

or

$$[T]_2 \equiv [TS^4]_2 \pmod{2}.$$

14. The group G considered may contain other substitutions $S_1, S_2, \cdots$, besides S^4, enjoying the same property, viz:

$$(2) \qquad [T]_2 \equiv [TS_1]_2, \quad [T]_2 \equiv [TS_2]_2, \cdots \pmod{2},$$

T being any substitution of G. We shall prove *firstly*, that all such substitutions form a group H, and *secondly*, that this group is invariant in G.

Firstly, to show that, if S_1 and S_2 satisfy the congruences (2), so will $S_1 S_2$; i. e. to show that

$$[T]_2 \equiv [T(S_1 S_2)]_2 \pmod{2}.$$

---

*) Sylow's Theorem; see Burnside, *Theory of Groups*, p. 90.

Now, as T represents in turn all the substitutions of G, so does TS_1. Substituting TS_1 for T in the second of the congruences (2), we have

$$[(TS_1)]_2 \equiv [(TS_1)S_2]_2 \pmod{2},$$

i. e.

$$[TS_1]_2 \equiv [T(S_1 S_2)]_2$$
$$\equiv [T]_2 \pmod{2}$$

by the first of the congruences (2), proving the proposition.

Secondly, to show that, if T and V be any two substitutions of G, and if S_1 be a substitution of H, then is also VS_1V^{-1} a substitution of H. We have

(3) $$[V^{-1}TV]_2 \equiv [(V^{-1}TV)S_1]_2 \pmod{2}$$

by (2). But, we may readily prove that

$$[B] = [ABA^{-1}],$$

whatever be the substitutions (of finite orders) A and B. Hence,

$$[V^{-1}TV] = [T],$$
$$[(V^{-1}TV)S_1] = [V(V^{-1}TVS_1)V^{-1}] = [T(VS_1V^{-1})].$$

Substituting in (3) we get

$$[T]_2 \equiv [T(VS_1V^{-1})]_2 \pmod{2},$$

proving that VS_1V^{-1} belongs to H. That is, H is an invariant subgroup of G. The group H can neither be the group F nor the identical substitution, since H contains a substitution of order 2, namely S^4 (art. 13).

15. We have so far studied the effect of the presence in G of a substitution S of order 8, with three distinct multipliers. In like manner we may deal with the cases where G contains a substitution S' of order 8, two of whose multipliers are equal; or a substitution S'' of order 4, whose multipliers are $-1, i, i$; $i^2 = -1$. We begin with a determinant differing from the one of article 13 simply by lacking its last row and column in the former case, and its second row and last column in the latter. We show the presence of an invariant subgroup H in both cases, containing a known substitution of order 2, namely $(S')^4$ in the former case and $(S'')^2$ in the latter.

It remains for us to study the group H. It cannot contain a substitution whose order is a prime number $q \neq 2$. To prove this, let T in the congruences (2) be the identical substitution. Then we have

$$[T]_2 \equiv 3 \equiv [S^j]_2 \pmod{2},$$

S being a tentative substitution of H of order q, and S^j any power of S. If the multipliers of S are α, β, γ, we have

$$3 \equiv [S^j]_2 = \alpha^j + \beta^j + \gamma^j \pmod{2},$$

and therefore

$$3 \sum_{j=1}^{q} \eta^j \equiv \sum_{j=1}^{q} \eta^j (\alpha^j + \beta^j + \gamma^j) \pmod{2},$$

η being a root of the equation $\theta^q - 1 = 0$, which equation is also satisfied by α, β and γ. Now, if none of the latter roots are $= 1$, we get, by putting $\eta = 1$, the impossibility

$$3q \equiv 0 \pmod{2}.$$

In all other cases we get similar impossibilities by choosing a suitable value for η.

It follows that the order of H is a power of 2. We can therefore write this invariant subgroup of G in monomial form. When so written, we find it to be either

a) abelian, in which case G is not primitive (Theorem 2), or

b) intransitive, having a single invariant straight line. This line should evidently also be invariant under G, in which case G is intransitive, not primitive (art. 2).

To resume, if the order of G is divisible by 2^4, then will G contain a substitution of order 8, or one of order 4 whose multipliers are $-1, i, i$. The group G will, in both cases, contain an invariant subgroup H and is not primitive. Accordingly, *the order of a primitive group is not divisible by* 2^4.

16. In exactly the same way we prove that if G has a substitution of order p^2, $p > 3$, then it has an invariant subgroup H of order p^m. Such a group being abelian (cf. art. 11), it follows that G is not primitive (Theorem 2). Hence, *the order of a primitive group is not divisible by p^3, p being a prime > 3.*

In the case $p = 3$ we find that *a linear group can have no substitution of order 3^m, whose 3^{rd} power is not the identical or a similarity-substitution, unless it has an invariant subgroup H of order 3^n.* It will be shown later (art. 23) that there are three primitive groups which contain invariant subgroups whose orders are powers of 3. A cursory examination of these groups reveals the fact, however, that they contain no substitution whose 3^{rd} power is not the identical or a similarity-substitution. It follows that *the order of no primitive collineation group is divisible by* 3^4 (cf. articles 12 and 16). Hence, finally, we have the

Theorem 5. *The order of a primitive group is a factor of $2^3 \cdot 3^3 \cdot 5^2 \cdot 7^2$.*

IV. Auxiliary Theorems.

17. Theorem 6. *If the group G contains a substitution S of order* 5 *and one T of order* 7; *i. e. if the order of G is divisible by* $5 \cdot 7$, *then will G contain a substitution of order* $5 \cdot 7$.

Let $[S] = \alpha_1 + \alpha_2 + \alpha_3$. Choose the variables so that T is written in canonical form. Then if a_1, b_2, c_3 be the coefficients in the principal diagonal of the matrix of S, we have

$$[ST^i] = a_1\beta_1^i + b_2\beta_2^i + c_3\beta_3^i, \quad i = 0, 1, 2, \cdots, 6.$$

Hence, if β be a primitive 7^{th} root of unity different from β_1^{-1}, β_2^{-1}, β_3^{-1}, then

(4) $[S] + \beta[ST] + \beta^2[ST^2] + \beta^3[ST^3] + \beta^4[ST^4] + \beta^5[ST^5] + \beta^6[ST^6] = 0$

Assume the theorem not true, so that none of the weights $[ST^i]$ contains both 7^{th} and 5^{th} roots at the same time. Let us arrange according to powers of β. Then must the coefficients of the different powers be equal (art. 8). Now,

a) if none of the weights $[ST^i]$ contains 7^{th} roots of unity, the equation considered is already arranged, and we have

$$[S] = [ST];$$

b) if some of the weights contain 7^{th} roots, say $[ST]$, $[ST^3]$, $\cdots$ then we will write the sum of the corresponding terms in the form

$$\beta[ST] + \beta^3[ST^3] + \cdots = k_0 + \beta k_1 + \beta^2 k_2 + \cdots + \beta^6 k_6,$$

and (4) becomes

$$\{[S] + k_0\} + \beta k_1 + \beta^2\{k_2 + [ST^2]\} + \beta^3 k_3 + \cdots = 0,$$

from which follows:

(5) $$[S] + k_0 = k_1, \quad \text{or} \quad \alpha_1 + \alpha_2 + \alpha_3 + k_0 - k_1 = 0.$$

Arranging this equation according to the five different powers of α, the coefficients should be equal (art. 8). But, $k_0 - k_1$ being free from 5^{th} roots, the equation (5) has at most four different powers of α, so that the coefficients should all be $= 0$, which is absurd. Hence, only (a) is tenable.

By writing S in canonical form instead of T, still assuming the theorem to be proved not true, we get in the same way

$$[T] + \alpha[ST] + \alpha^2[S^2T] + \alpha^3[S^3T] + \alpha^4[S^4T] = 0,$$

and

$$[T] = [ST].$$

Hence,

$$[S] = [T], \quad \text{or} \quad \alpha_1 + \alpha_2 + \alpha_3 = \beta_1 + \beta_2 + \beta_3,$$

which, like (5), is an impossibility. Accordingly, at least one of the weights $[ST^i]$ must contain both 5^{th} and 7^{th} roots of unity, and the theorem is proved.

18. Theorem 7. *If a linear group G has a substitution S of order* 5 (*or* 7) *and a substitution T whose multipliers are* $\varphi, \varphi, \varphi\omega^2$, *where* $\varphi^3 = \omega$, $\omega^2 + \omega + 1 = 0$, *then it has one of order* $9 \cdot 5$ (*or* $9 \cdot 7$).

Proceeding as in article 17, we obtain an equation of the form

$$[S] + \varphi^2\omega[ST] + \varphi[ST^2] = 0. \tag{6}$$

Now, it follows from Kronecker's Theorem (art. 8) that the equation

$$A + \varphi B + \varphi^2 C = 0,$$

(A, B, C being sums of roots of unity none of which can be written in the form $\varepsilon\varphi\omega^a$ or $\varepsilon\varphi^2\omega^a$, where ε is a root whose index is prime to 3) can be satisfied only if $A = B = C = 0$. Then the assumption that none of the weights $[ST]$ and $[ST^3]$ can contain both 9^{th} roots and 5^{th} (or 7^{th}) roots at the same time is readily proved untenable.

19. The two preceeding theorems state that G contains a substitution V of order $p^n q$, p and q being prime to each other, under certain conditions. This is the same as saying that, when these conditions are fulfilled, G contains two commutative substitutions $S\left(=V^{p^n}\right)$ and $T(=V^q)$ whose orders are prime to each other. In such cases G will have an invariant subgroup H, as we shall proceed to show, unless the weights of S and T are of certain types.

Theorem 8. *Let S and T be two commutative substitutions of a group G, of orders q and p^n respectively; p and q being different prime numbers. Then if two of the multipliers of S be not equal, G has an invariant subgroup H.*

The substitutions S and T generate an abelian group, which we will write in canonical form. We suppose

$$S : x' = \alpha_1 x, \quad y' = \alpha_2 y, \quad z' = \alpha_3 z;$$
$$T : x' = \beta_1 x, \quad y' = \beta_2 y, \quad z' = \beta_3 z$$

and assume that α_1, α_2 and α_3 are all different. Let A be any substitution of G, and let the coefficients in the principal diagonal of the matrix of A be a_1, b_2 and c_3. Then if we eliminate the three last quantities between the four equations obtained by writing down the weights

$$[A] = a_1 + b_2 + c_3, \ [AT] = a_1\beta_1 + b_2\beta_2 + c_3\beta_3, \ [AS] = \text{etc.}, \ [AS^2] = \text{etc.},$$

as in article 10, we get the equation

$$\begin{vmatrix} [A] & 1 & 1 & 1 \\ [AT] & \beta_1 & \beta_2 & \beta_3 \\ [AS] & \alpha_1 & \alpha_2 & \alpha_3 \\ [AS^2] & \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{vmatrix} = 0.$$

We shall apply the Lemma 1, and write 1 for every root whose index is a power of p. Then we have

$$\{[A]_p - [AT]_p\}(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \equiv 0 \pmod{p}.$$

This congruence can be changed into the following

$$[A]_p - [AT]_p \equiv 0 \pmod{p},$$

by multiplying both sides by a suitable factor. Now, A being any substitution of G, this last congruence indicates an invariant subgroup H of the kind defined in article 14 for $p = 2$.

20. It is thus shown that, if G contains a substitution V of order $p^n q$, p and q being different primes > 2, and is to be primitive, then must the substitution V^{p^n}, when written in canonical form, be of the type:

(7) $$V^{p^n}: x' = \alpha_1 x, \quad y' = \alpha_1 y, \quad z' = \alpha_2 z; \quad \alpha_1^q = \alpha_2^q = 1.$$

Again, if the order of G is divisible by 5^2 (or by 7^2), then G has an abelian subgroup of order 5^2 (or 7^2) (cf. art. 11) and must necessarily have a substitution of order 5 (or 7) of type (7). This we prove readily by constructing the different possible types of canonical groups of order 5^2 (or 7^2), omitting the cases where such groups contain substitutions of order 5^2 (or 7^2) (cf. art. 16).

Let us now consider a group G having a substitution S_1 of type (7). This substitution leaves invariant a point ($x = 0$, $y = 0$) and *every* straight line through it. Let S_2 be another substitution into which S_1 is transformed by a substitution of G; S_2 will also leave invariant a certain point (say $\bar{x} = 0$, $\bar{y} = 0$) and every straight line through that point. Therefore, the straight line joining the two points, ($x = 0$, $y = 0$) and ($\bar{x} = 0$, $\bar{y} = 0$), must be left invariant by both S_1 and S_2. Accordingly, S_1 and S_2 will generate an intransitive group (art. 2) say of type

(8) $$x' = ax + by, \quad y' = cx + dy, \quad z' = ez.$$

The substitutions

(9) $$x' = ax + by, \quad y' = cx + dy$$

will form a finite group in two variables.

21. Let S_1 be of order 7. A substitution of order 7, contained in a group of type (9), must be commutative with every substitution of the group (cf. art. 4). Hence, the substitutions S_1 and S_2 must be commutative with each other, as far as they are looked upon as transforming the variables x, y. But then it is readily seen from the form of (8) that they are completely commutative. Accordingly, all the substitutions $S_1, S_2, \cdots$, which are transformed one into the other by the substitutions of G, are mutually commutative, and will therefore generate an abelian group, evidently contained invariantly in G. In this event G is not primitive (Theorem 2).

22. Let S_1 be of order 5. If S_1 and S_2 are not commutative, the group (9) generated by them must be the Icosahedral group 4^0, article (4). Among its substitutions are found the two, A, of order 3, written in canonical form, and B, a similarity-substitution of order 2:

$$A: x' = \omega x, \quad y' = \omega^2 y; \quad \omega^2 + \omega + 1 = 0;$$
$$B: x' = -x, \quad y' = -y.$$

The group (8) will then contain the substitutions

$$A_1: x' = \omega x, \quad y' = \omega^2 y, \quad z' = e_1 z;$$
$$B_1: x' = -x, \quad y' = -y, \quad z' = e_2 z.$$

The quantities e_1 and e_2 are 1 or are 5^{th} roots of unity, (8) being generated by substitutions of order 5. It is therefore allowed to put $e_1 = e_2 = 1$, which is equivalent to replacing A_1 and B_1 by their 5^{th} powers. But, A_1 and B_1 being commutative, we may call them S and T respectively and employ the reasoning of art. 19 to show that G has an invariant subgroup H. Hence, if G is to be primitive, S_1 and S_2 must be commutative. However, by following the reasoning of the latter half of article 21, we find that G cannot be primitive in this case either. Hence, finally, *a primitive group G can have no substitution of order* 5 *or* 7 *and of type* (7).

Constructing the different possible types of collineation-groups of order 3^3 allowed in a primitive group after article 16, we find that all such groups have a substitution T of the kind mentioned in Theorem 7. Now, by referring to the theorems 6, 7 and 8, we verify the following:

Theorem 9. *The order of a primitive group G is not divisible by* $3^3 \cdot 5$, $3^3 \cdot 7$, 5^2, 7^2 *nor by* $5 \cdot 7$. *The order is therefore a factor of one of the numbers* $2^3 \cdot 3^3$, $2^3 \cdot 3^2 \cdot 5$ or $2^3 \cdot 3^2 \cdot 7$.

V. Classification of the Primitive Groups.

A Primitive groups having invariant intransitive subgroups.

23. No such subgroup could be abelian (Theorem 2). If an intransitive group is not abelian, it has a single invariant point. This point must evidently be transformed into itself by any group G containing the given intransitive group invariantly, and such a group G could not be primitive (art. 2).

B. Primitive groups having invariant monomial subgroups.

Let G contain an invariant monomial subgroup K. This subgroup leaves invariant the triangle whose sides are $x=0$, $y=0$ and $z=0$. If this is the only triangle left invariant by K, then must G evidently leave that triangle invariant also. We therefore seek the form of a monomial group K leaving more than one triangle invariant, and yet not being intransitive. We readily find but one type for K, namely that generated by the substitutions:

$$\begin{cases} S: x'=y, \quad y'=z, \quad z'=x; \\ T: x'=x, \quad y'=\omega y, \quad z'=\omega^2 z, \qquad \omega^2+\omega+1=0. \end{cases}$$

This group is of order 9 (as a collineation-group) and leaves invariant each of the four triangles:

$$t_1=(x=0,\ y=0,\ z=0),$$
$$t_2,\ t_3,\ t_4=(x+y+\theta z=0,\ x+\omega y+\theta\omega^2 z=0,\ x+\omega^2 y+\theta\omega z=0);$$
$$\theta=1,\ \omega,\ \omega^2.$$

The primitive groups permuting among themselves these four triangles are generated by the substitutions

$$U=(t_2 t_3 t_4): x'=\varphi x, \quad y'=\varphi y, \quad z'=\varphi\omega z, \quad \varphi^3=\omega^2;$$
$$V=(t_1 t_2)(t_3 t_4): x'=\varrho(x+y+z), \quad y'=\varrho(x+\omega y+\omega^2 z),$$
$$z'=\varrho(x+\omega^2 y+\omega z), \quad \varrho=\frac{1}{\omega-\omega^2};$$
$$UVU^{-1}=(t_1 t_4)(t_2 t_3): x'=\varrho(x+y+\omega^2 z), \quad y'=\varrho(x+\omega y+\omega z),$$
$$z'=\varrho(\omega x+y+\omega z);$$

as follows:

1⁰. The Hessian group of order 216*):

S and T of K, U and V.

2⁰. An invariant subgroup of the Hessian group, of order 72:

S, T, V and UVU^{-1}.

3⁰. An invariant subgroup of 2⁰, of order 36:

S, T and V.

These groups, when written as linear groups, all contain the group F of similarity-substitutions, and their orders as linear groups are therefore 648, 216 and 108 respectively.

---

*) Cf. Jordan, *Mémoire sur les équations différentielles linéaires à intégrale algébrique,* Journal für die reine und angewandte Mathematik, 84 (1878), p. 209.

C. Primitive groups isomorphic with abstract simple groups.

24. We found that the order of a primitive collineation-group was a factor of one of the numbers: $2^3 \cdot 3^3$, $2^3 \cdot 3^2 \cdot 5$ and $2^3 \cdot 3^2 \cdot 7$ (art. 22). The greatest of these numbers being 504, the question is therefore to determine all the primitive groups isomorphic with the four simple groups whose orders are not greater than this number; viz. the well known simple groups of orders 60, 168, 360 and 504 (art. 3).

There can be no group in three variables isomorphic with the simple group of order 504. For, this has an abelian subgroup of order 8, formed of 7 distinct substitutions of order 2 and the identical substitution.*) Attempting to write this subgroup in canonical form, we find it impossible as a group in three variables.

There is one, and only one, type of a primitive group isomorphic with each of the simple groups of orders 60 and 360 respectively, as shown by Maschke in Mathematische Annalen, Bd. 51 (1899), pp. 264—267. He derives the following types:

4^0. A simple group of order 60, generated by the substitutions

$$E_1 : x' = y,\quad y' = z,\quad z' = x;$$

$$E_2 : x' = x,\quad y' = -y,\quad z' = -z;$$

$$E_3 : x' = \frac{1}{2}(-x + \mu_2 y + \mu_1 z),\quad y' = \frac{1}{2}(\mu_2 x + \mu_1 y - z),$$
$$z' = \frac{1}{2}(\mu_1 x - y + \mu_2 z),$$

$$\mu_1 = \alpha + \alpha^4 = \frac{1}{2}(-1 + \sqrt{5}),\quad \mu_2 = \alpha^2 + \alpha^3 = \frac{1}{2}(-1 - \sqrt{5}),\quad \alpha^5 = 1.$$

This group does not contain the group F of similarity-substitutions and is therefore of order 60 as a linear group. It is simply isomorphic with the alternating permutation-group in five letters a, b, c, d, e, and its generating substitutions can be identified with the following permutations:

$$E_1 = (abc),\quad E_2 = (ab)(cd),\quad E_3 = (ab)(de).$$

5^0. A simple group of order 360 generated by**)

$$E_1,\ E_2 \text{ and } E_3 \text{ of } 4^0;$$

$$E_4 : x' = -x,\quad y' = -\omega z,\quad z' = -\omega^2 y,\quad \omega^2 + \omega + 1 = 0.$$

This group contains F and is therefore of order 1080 as a linear

---

*) See Burnside, *Theory of Groups*, p. 373.

**) See also Valentiner, *De endelige Transformations-Gruppers Theori*, Copenhagen, Videnskabernes Selkabs Skrifter, 6. Rekke (1889), p. 192.

group.*) It is simply isomorphic with the alternating group in six letters a, b, c, d, e, f:

$$E_1 = (abc), \quad E_2 = (ab)(cd), \quad E_3 = (ab)(de), \quad E_4 = (ab)(ef).$$

There is one, and only one type of a collineation-group simply isomorphic with the simple group of order 168, as shown by Weber in his Algebra, Bd. II, pp. (497—502) 2nd edition, 1899).**) This group is generated by the substitutions:

$$6^0.\ S: x' = \varepsilon x, \quad y' = \varepsilon^2 y, \quad z' = \varepsilon^4 x, \quad \varepsilon^7 = 1, \quad \varepsilon \neq 1;$$

$$T: x' = z, \quad y' = x, \quad z' = y;$$

$$U: x' = h(\alpha x + \beta y + \gamma z), \quad y' = h(\beta x + \gamma y + \alpha z), \quad z' = h(\gamma x + \alpha y + \beta z),$$

$$\alpha = \varepsilon^4 - \varepsilon^{-4}, \quad \beta = \varepsilon^2 - \varepsilon^{-2}, \quad \gamma = \varepsilon - \varepsilon^{-1},$$

$$h = \frac{1}{7}(\varepsilon + \varepsilon^2 + \varepsilon^4 - \varepsilon^{-1} - \varepsilon^{-2} - \varepsilon^{-4}) = \frac{1}{\sqrt{-7}}.$$

This group does not contain F and is therefore of order 168 as a linear group. We can represent the group as a permutation group in 7 letters a, b, c, d, e, f, g, in which case the generating substitutions given will appear in the forms

$$S_1 = (abcdefg), \quad T_1 = (abd)(cfe), \quad U_1 = (ab)(ce).$$

D. Primitive groups having primitive invariant subgroups.

We saw (art. 22) that the order of a primitive collineation group should be a factor of one of the numbers $2^3 \cdot 3^3$, $2^3 \cdot 3^2 \cdot 5$ or $2^3 \cdot 3^2 \cdot 7$. The groups 1^0 and 5^0 can therefore not be contained as subgroups in larger groups. The groups 2^0 and 3^0 have each a single invariant subgroup of order 9, namely the group K (art. 23). A group containing either 2^0 or 3^0 invariantly should therefore also leave K invariant, and could be none other than either 1^0 or 2^0. We find that 1^0 contains 2^0 invariantly, and 2^0 contains 3^0 invariantly.

Consider the group 4^0, of order $2^2 \cdot 3 \cdot 5$. A group G containing 4^0 invariantly must be of order $2^{2+a} \cdot 3^{1+b} \cdot 5$. Now, 4^0 has 10 subgroups of order 3, which must be permuted among themselves by the substitutions of G. Accordingly, there is in G a subgroup of order $2^{2+a} \cdot 3^{1+b} \cdot 5 : 10 = 2^{1+a} \cdot 3^{1+b}$, which transforms a given subgroup of 4^0 of order 3 into itself. Therefore, if $a > 0$, G contains a substitution of

*) That the linear group cannot be written without similarity-substitutions, is seen in the following manner. The simple G_{360} has an abelian subgroup of order 9, containing 8 substitutions of order 3. No such subgroup can be written in three variables directly as a linear group.

**) Cf. Klein, Mathematische Annalen, 14 (1878), p. 444.

order 2 commutative with a substitution of 4^0 of order 3. This is impossible, by Theorem 8. Hence, $a = 0$. Again, 4^0 has 6 subgroups of order 5. If $b > 0$, we would find in G a substitution of order 3 commutative with a substitution of order 5, which is likewise impossible by Theorem 8. Thus, the order of G is $2^2 \cdot 3 \cdot 5$, and $G = 4^0$.

Consider the group 6^0 of order $2^3 \cdot 3 \cdot 7$. A group G leaving this invariant should be of order $2^3 \cdot 3^{1+b} \cdot 7$. Now, 6^0 has 8 subgroups of order 7, and a substitution of order 3 which transforms a given substitution of order 7 into its 2nd or 4th power. If $b > 0$, G must contain a substitution of order 3 which is commutative with a substitution in 6^0 of order 7. But this is impossible by Theorem 8.
