DETERMINATION OF THE ORDINARY AND MODULAR TERNARY LINEAR GROUPS*

BY

HOWARD H. MITCHELL

INTRODUCTION.

It is proposed in this paper to determine the finite groups of collineations in three homogeneous variables, a collineation being of the form

$$\rho x_i' = \sum_{j=1}^{3} a_{ij} x_j \qquad (i = 1, 2, 3).$$

The determination will be made both in the case where the coefficients a_{ij} are ordinary numbers and in the case where they are marks of a finite Galois field, $GF(p^n)$, p being an odd prime and n a positive integer. The variables x_i are therefore regarded as homogeneous coördinates of the points either of the ordinary plane or of a modular plane,† $PG(2, p^n)$.

The finite groups of collineations in the ordinary plane have been already determined.‡ The treatment of the problem in this paper is however different from any thus far given. It is based almost entirely on geometrical methods and it is hoped may prove of interest. The discussion for this case is contained in §§ 2–10.

Considerable work has been done on the ternary modular groups. For the case where the coefficients of the transformations are in the $GF(p)$, the question was considered by BURNSIDE.§ For the same case a complete determination of those groups which contain operators of period p was made by DICKSON.‖

* Presented to the Society, under different titles, December 30, 1909, April 30 and September 7, 1910.

† O. VEBLEN and W. H. BUSSEY, *Finite Projective Geometries*, these Transactions, vol. 7 (1906), pp. 241–259.

‡ For a bibliography of this subject consult WIMAN, *Endliche Gruppen linearer Substitutionen*, *Encykopädie der Mathematischen Wissenschaften*, Bd. I, pp. 528–530. The first accurate solution of the problem is due to BLICHFELDT, *On the Order of Linear Homogeneous Groups*, these Transactions, vol. 4 (1903), pp. 387–397, and vol. 5 (1904), pp. 310–325; also *The Finite, Discontinuous, Primitive Groups of Collineations in Three Variables*, Mathematische Annalen, vol. 63 (1907), pp. 552–572.

§ Proceedings of the London Mathematical Society, vol. 26 (1895), pp. 58–106.

‖ American Journal of Mathematics, vol. 27 (1905), pp. 189–202.

For the case where the coefficients are in the $GF(p^2)$, a discussion of those groups whose orders are divisible by p^6, p^5 and p^4 was given by R. L. BÖRGER.*

As a result of the determination of the ternary modular groups in this paper, the subgroups of the two systems of simple groups, $LF(3, p^k)$ and $HO(3, p^{2k})$, are found in the cases where p is an odd prime.† The $LF(3, p^k)$ is the group of all ternary transformations the coefficients of which lie in the $GF(p^k)$ and which have for determinant a cube in that field. It is identical with the group of all collineations of the modular plane, $PG(2, p^k)$, if $p^k - 1$ is not divisible by 3, and is a self-conjugate subgroup of that group of index 3 if $p^k - 1$ is divisible by 3. Its order is

$$\frac{1}{\mu}(p^{2k} + p^k + 1)(p^k + 1)p^{3k}(p^k - 1)^2,$$

where μ is the greatest common divisor of 3 and $p^k - 1$. The $HO(3, p^{2k})$ is a subgroup of the $LF(3, p^{2k})$ having an invariant of the form

$$x_1^{p^k+1} + x_2^{p^k+1} + x_3^{p^k+1} = 0.$$

Its order is

$$\frac{1}{\nu}(p^{2k} - p^k + 1)(p^k + 1)^2 p^{3k}(p^k - 1),$$

where ν is the greatest common divisor of 3 and $p^k + 1$.

The binary modular groups have been fully determined. For the case where the coefficients are in the $GF(p)$ the determination was made by GIERSTER.‡ In the general case the problem has been solved by E. H. MOORE§ and by WIMAN.‖ A treatment based on these two papers is given by DICKSON (*Linear Groups*, Chap. XII). A new treatment will be given in this paper.

The writer wishes to acknowledge his indebtedness to Professor O. VEBLEN of Princeton University for constant and valuable aid in the preparation of the paper.

§1. BINARY GROUPS.

We consider transformations in two homogeneous variables of the form

$$\rho x_i' = \sum_{j=1}^{2} a_{ij} x_j \qquad (i = 1, 2).$$

* *Ibid.*, vol. 32 (1910), pp. 289–298.

† See DICKSON, *Linear Groups*, pp. 75–78, 126–144.

‡ Mathematische Annalen, vol. 18 (1881).

§ *The Subgroups of the Generalized Finite Modular Group, Decennial Publications of the University of Chicago*, vol. 9 (1904), pp. 141–190.

‖ *Bestimmung aller Untergruppen einer doppelt unendlichen Reihe von einfachen Gruppen*, Bihang till K. Svenska Vet.-Akad. Handlingar, vol. 25, part 1, no. 2.

These transformations may be regarded as permuting the points $(x_1 x_2)$ of a line (either ordinary or modular). Any such transformation leaves invariant either one or two points on the line. In the case of the ordinary line any transformation of finite period leaves invariant two points. The groups containing such transformations only are well known. They are cyclic groups of order d, dihedral groups of order $2d$, tetrahedral groups of order 12, octahedral groups of order 24, and icosahedral groups of order 60. No further discussion will be given of these groups.

We therefore consider those groups on the modular line which contain transformations leaving invariant a single point. Any such transformation is additive and of period p.* Any group containing these additive transformations will contain at least one additive group, which leaves invariant a point and contains all the additive transformations which have that point for fixed point. The order of any such additive group is a power of p, say p^m. If the fixed point be (10), the additive group is represented by $[x_1 + \lambda x_2, x_2]$, where λ takes all the values in an additive field $\alpha_1\lambda_1 + \alpha_2\lambda_2 + \cdots + \alpha_m\lambda_m$, the α's being integers $0, 1, 2, \cdots, p-1$, and each λ_j a mark not included in the additive field $\alpha_1\lambda_1 + \cdots + \alpha_{j-1}\lambda_{j-1}$. There will be conjugate with it $1 + fp^m$ additive groups, f being 0 or a positive integer. All additive transformations must therefore lie in these conjugate additive groups.

The additive group will be self-conjugate under a maximum metacyclic group of order $d_1 p^m$, where d_1 is a factor of $p^m - 1$ (in special cases we may have $d_1 = 1$). Such a metacyclic group contains p^m conjugate cyclic groups, each of which leaves invariant two points and is of period d_1. If (01) be the other fixed point of one of these cyclic groups, the metacyclic group may be generated by the additive group together with $[\eta x_1, x_2]$, where η is of period d_1 and belongs to the multiplier field of the additive field. If Ω denotes the order of the whole group there will be $\Omega/d_1 p^m$ additive groups containing $(p^m - 1)\Omega/d_1 p^m$ additive transformations. There will also be in the group Ω/d_1 or $\Omega/2d_1$ cyclic groups of order d_1 containing $(d_1 - 1)\Omega/d_1$ or $(d_1 - 1)\Omega/2d_1$ transformations, according as one of those cyclic groups is self-conjugate under itself only or under a dihedral group interchanging its two fixed points. Any other maximal cyclic group of order d_i, which does not lie in a metacyclic group, will be self-conjugate either under itself only or under a dihedral group of order $2d_i$ interchanging its two fixed points. Conjugate with such a cyclic group there will be Ω/d_i or $\Omega/2d_i$ cyclic groups containing $(d_i - 1)\Omega/d_i$ or $(d_i - 1)\Omega/2d_i$ transformations.

The order of the group will be equal to the number of transformations which it contains. Hence Ω must satisfy a Diophantine equation of the following

*Throughout the paper p denotes the modulus. The discussion of the binary groups applies also to the case $p = 2$.

form:*

$$\Omega = 1 + (p^m - 1)\frac{\Omega}{d_1 p^m} + \sum_{i=1}^{r}(d_i - 1)\frac{\Omega}{f_i d_i} \qquad (f_i = 1, 2).$$

The coefficient of Ω on the right of the above equation must be less than unity. Also, since the group contains a subgroup of order $d_1 p^m$, the coefficient of Ω on the right must be equal to or greater than $(d_1 p^m - 1)/d_1 p^m$. If $d_1 = 1$, we find therefore that either the final sum is absent, or it contains but one term, in which case $f_2 = 2$. If $d_1 > 1$, either $r = 1$, $f_1 = 1$, or $r = 2$, $f_1 = f_2 = 2$.

If $d_1 = 1$ and the final sum is absent, we obtain $\Omega = p^m$, i. e., a single additive group.

If $d_1 = 1$ and there is one term in the final sum, we have either $p^m = 2$, $\Omega = 2d_2$, which represents a dihedral group, or $p^m = 3$, $d_2 = 2$, $\Omega = 12$, which represents a tetrahedral group.

If $d_1 > 1$, $r = 1$, $f_1 = 1$, we obtain $\Omega = d_1 p^m$, which represents a single metacyclic group.

If $d_1 > 1$, $r = 2$, $f_1 = f_2 = 2$, we shall show that d_1 and d_2 cannot contain any common factor except 2. The cyclic groups of order d_1, when transformed by one of their number, will be permuted in cycles of period d_1 or $d_1/2$. Hence the total number of conjugate groups of order d_1 must be of the form $1 + fd_1/2$. If we suppose the groups of order d_1 to be transformed by one of the groups of order d_2, it is evident that the number of the former must also be of the form $f'd_2/2$. Hence d_1 and d_2 can contain no common factor except 2.

The order, Ω, must be the least common multiple of p^m, $2d_1$, and $2d_2$. For it must be divisible by the least common multiple, since the group contains subgroups of those orders. Moreover if we collect the three terms on the right and write the equation

$$\Omega = 1 + \frac{I}{M}\Omega,$$

where M denotes the least common multiple and I is an integer, it is clear that Ω cannot be greater than M.

Hence, if p is odd, Ω must have one of the two values, $d_1 d_2 p^m$, and $2d_1 d_2 p^m$, according as d_1 and d_2 are both divisible by 2 or have no common factor. For $p = 2$, $\Omega = d_1 d_2 p^m$.

Putting $\Omega = d_1 d_2 p^m$ in the equation, we obtain

$$(d_2 - d_1)p^m - 2(d_2 - 1) = 0.$$

Hence

$$d_2 = fp^m + 1, \qquad d_1 = f(p^m - 2) + 1,$$

* This type of Diophantine equation originated in C. JORDAN's attempt to determine all finite collineation groups in the ordinary plane, Journal für die reine und angewandte Mathematik, vol. 84 (1878), p. 89.

where f denotes an integer. But d_1 is a divisor of $p^m - 1$. Hence

$$f = 1,\ d_1 = p^m - 1,\ d_2 = p^m + 1,\ \Omega = (p^m + 1)p^m(p^m - 1).$$

Putting $\Omega = 2d_1 d_2 p^m$ in the equation, we obtain

$$(d_2 - d_1)p^m - (2d_2 - 1) = 0.$$

Hence

$$d_2 = \tfrac{1}{2}(fp^m + 1), \qquad d_1 = \tfrac{1}{2}(fp^m + 1) - f,$$

where f denotes an odd integer. But d_1 is a divisor of $p^m - 1$. Hence

$$f = 1,\ d_1 = \frac{p^m - 1}{2},\ d_2 = \frac{p^m + 1}{2},\ \Omega = \tfrac{1}{2}(p^m + 1)p^m(p^m - 1);$$

or $f = 3,\ p^m = 3,\ d_1 = 2,\ d_2 = 5,\ \Omega = 60$.

We consider the possible group of order $(p^m + 1)p^m(p^m - 1)$. Each additive group of order p^m is self-conjugate under a metacyclic group of order $(p^m - 1)p^m$. Hence there are $p^m + 1$ such additive groups. The $p^m + 1$ fixed points of these additive groups must therefore be permuted among themselves. The two fixed points of each cyclic group of order $p^m - 1$ are interchanged by transformations of the group, i. e., they are among the $p^m + 1$ points. The additive group leaving fixed one of these points is transitive on the rest.

Since three points may be sent by a transformation into any other three, we may choose three of the $p^m + 1$ points as (01), (10), (11). The following three transformations will then be in the group: $[\eta x_1, x_2]$, $[x_1 + x_2, x_2]$, $[x_1, x_1 + x_2]$, where the period of η is $p^m - 1$. The powers of η together with 0 form the Galois field, $GF(p^m)$. The three transformations generate a group of order $(p^m + 1)p^m(p^m - 1)$, which is the group of all transformations with coefficients in the $GF(p^m)$.

We may construct the group of order

$$\tfrac{1}{2}(p^m + 1)p^m(p^m - 1)$$

by replacing η by η^2. It is the group of all transformations with coefficients in the $GF(p^m)$ and having for determinant a square in that field.

The group of order 60 is an icosahedral group. For it contains $\Omega/2 \cdot 2 = 15$ involutions, each of which lies in one four-group. Hence the fifteen involutions arrange themselves in five four-groups. Each involution leaves fixed the four-group in which it lies and permutes the other four in pairs. The group must then be a G^5_{60}, i. e., an icosahedral group. Such a group may be generated by the three operators, E_1: $[x_1 + x_2, x_2]$, E_2: $[ix_1, -x_1 - ix_2]$, E_3: $[-ix_1, ix_2]$ $(i^2 = -1)$, which satisfy the generational relations:*

$$E_1^3 = E_2^2 = E_3^2 = (E_1E_2)^3 = (E_1E_3)^2 = (E_2E_3)^3 = I.$$

*E. H. MOORE, Proceedings of the London Mathematical Society, vol. 27 (1897), pp. 357-366; DICKSON, *Linear Groups*, p. 289.

§ 2. Canonical Forms of Transformations in the Plane.*

The transformations in the plane† may be classified according to the five types of invariant figures. Those of type I leave fixed a triangle; those of type II leave fixed two points and two lines; those of type III leave fixed a lineal element; those of type IV leave fixed all the points of a line and all the lines through a point off that line; those of type V leave fixed all the points of a line and all the lines through a point on that line (Fig. 1).

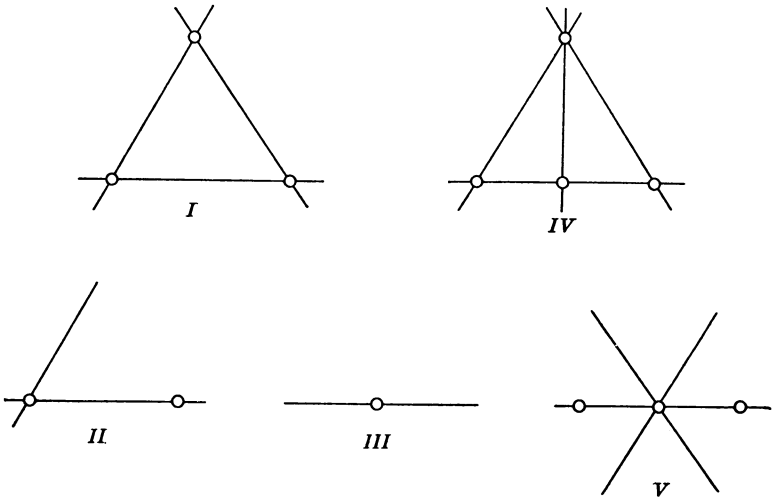

Fig. 1.

A transformation of type I may be written in canonical form $[\alpha x_1, \beta x_2, \gamma x_3]$. This transformation is of finite period in the ordinary plane provided the ratios of the three quantities, α, β, γ, are roots of unity (not unity itself).

A transformation of type II may be written $[\alpha x_1, x_2 + x_3, x_3]$, where $\alpha \neq 0, 1$. The period of this transformation is infinite in the ordinary plane and in the modular plane contains p as a factor.

A transformation of type III may be written $[x_1 + x_2, x_2 + x_3, x_3]$. The period is infinite in the ordinary plane and equal to p in the modular plane (since $p > 2$).

A transformation of type IV may be written $[\alpha x_1, x_2, x_3]$, where $\alpha \neq 0, 1$. In the ordinary plane it is of finite period if α is a root of unity. We will refer to a transformation of this type as an *homology*. In particular, if the period is 2, i. e., if $\alpha = -1$, we will refer to it as a *reflection*.

A transformation of type V may be written $[x_1, x_2 + x_3, x_3]$. In the ordinary plane it is of infinite period and in the modular plane of period p. We

* Cf. Veblen and Young, *Projective Geometry*; Dickson, *Linear Groups*, chaps. X, XI.

† For the modular plane the discussion will be limited to the case where p is an odd prime.

shall refer to a transformation of this type as an *elation*. Any power d of the transformation of type II such that $\alpha^d = 1$ is an elation.

§ 3. General Theorems.

Theorem 1. *A group leaving fixed a line and represented on the points of that line by a four-group contains a reflection with that line as axis; dually, a group leaving fixed a point and represented on the lines through the point by a four-group contains a reflection with that point as center.*

We shall prove the first half of this theorem. We choose the fixed line as $x_3 = 0$ and the fixed pair of points of one involution of the four-group as (100) and (010). If then we choose as (110) one of the fixed points of another of the three involutions, the other fixed point will be (1–10). Then any two transformations which are represented on the fixed line by these two involutions are of the form

$$[\alpha x_1 + \gamma_1 x_3,\ -\alpha x_2 + \gamma_2 x_3,\ x_3], \qquad [\beta x_2 + \delta_1 x_3,\ \beta x_1 + \delta_2 x_3,\ x_3].$$

Their product is $[\alpha\beta x_2 + \epsilon_1 x_3,\ -\alpha\beta x_1 + \epsilon_2 x_3,\ x_3]$. This is a transformation which is represented on the fixed line by the third involution of the four-group.

The square of any one of these three transformations will leave fixed all the points on $x_3 = 0$ and hence will be either an homology or an elation with that line as axis or else the identity. One at least of them, however, must be an homology of even period, since if the periods of α^2 and β^2 are both odd the period of $-\alpha^2\beta^2$ will be even. An homology of even period will contain as a power a reflection.

The dual theorem may be proved in a similar manner.

Theorem 2. *A group permuting cyclically the vertices of a triangle and represented on each side of the triangle by a cyclic group of order d is of order $3dd'$, where d' is a factor of d which is divisible by all the prime factors of d of the form $3f - 1$ and all the factors 3 with the exception of at most one.*

We choose the fixed triangle as the triangle of reference. A transformation which is of period d on $x_3 = 0$ may be written $[x_1, \omega x_2, \omega^e x_3]$, where ω is of period d, the coefficient of x_3 being a power of ω since the period of the transformation on $x_1 = 0$ and $x_2 = 0$ must be a factor of d. If we transform this transformation by a transformation permuting cyclically the vertices of the fixed triangle, we obtain $[x_1, \omega^{-e} x_2, \omega^{1-e} x_3]$. The eth power of the first transformation by the second is the homology $[x_1, x_2, \omega^{e^2-e+1} x_3]$.

From the theory of quadratic forms it follows that $e^2 - e + 1$ cannot be divisible by any primes of the form $3f - 1$ or by 3 to a higher power than the first. The period of the homology is then divisible by all the prime factors of the form $3f - 1$ and all the factors 3 with the exception of at most one.

Theorem 3. *A group making all six permutations on the vertices of a tri-*

angle and represented on each side of the triangle by a dihedral group of order $2d$ *is of order* $2d^2$ *or* $6d^2$ *if* d *is divisible by* 3 *and of order* $6d^2$ *if* d *is not divisible by* 3.

We choose the fixed triangle as the triangle of reference. The group will contain a transformation of period d on $x_3 = 0$ of the form, $[x_1, \omega x_2, \omega^e x_3]$, where ω is of period d. A transformation interchanging $x_1 = 0$ and $x_2 = 0$ and leaving $x_3 = 0$ fixed transforms this into $[x_1, \omega^{-1}x_2, \omega^{e-1}x_3]$. As a product we obtain the homology (or the identity), $[x_1, x_2, \omega^{2e-1}x_3]$. Similarly there is in the group the homology, $[x_1, x_2, \omega^{2-e}x_3]$. The product of the first homology by the square of the second gives $[x_1, x_2, \omega^3 x_3]$. This homology is of period $d/3$ or d according as d is or is not divisible by 3.

In particular if there are no homologies with centers at the vertices of the triangle and having for axes the opposite sides, we must have $d = 3$. If there are only reflections, we must have $d = 2, 6$.

§ 4. Multiplicative Groups containing only Homologies and Transformations of Type I; General Properties.

Since homologies and transformations of type I are called multiplicative, groups containing transformations of those types only will be referred to as *multiplicative* groups. Any group in the ordinary plane is thus multiplicative.

Theorem 4. *In a multiplicative group a transformation which leaves fixed the center of an homology must leave fixed its axis and vice-versa.*

The product of an homology and the transformed of its inverse by a transformation leaving fixed its center but not its axis is an elation.

Theorem 5. *No multiplicative group can contain two homologies such that the line joining their centers passes through the intersection of their axes.*

The product of two homologies such that the line joining the centers passes through the intersection of their axes is of type II or III.

§ 5. Multiplicative Groups containing Homologies of higher Period than 3.

Theorem 6. *No multiplicative group which does not leave invariant a point, line, or triangle can contain homologies of period greater than* 5.

A group which does not leave invariant a point, line, or triangle and which contains homologies of period greater than 5 will contain two such homologies which are not commutative. These two homologies will leave invariant the point of intersection of their axes and the line joining their centers. But they cannot generate on the line joining their centers a group which is cyclic, dihedral, tetrahedral, octahedral, or icosahedral. Hence no group can contain homologies of period greater than 5.

Theorem 7. *No multiplicative group which does not leave invariant a point, line, or triangle can contain homologies of period* 5.

Consider two homologies of period 5 which are not commutative. They must generate the icosahedral group on the line joining their centers. Since there are in the icosahedral group involutions interchanging the fixed points of the C_5 there will be two homologies of period 5 represented on the fixed line by the same C_5. As a product we may then obtain an homology of period 5 having the fixed line for axis. But there will also be a reflection having that line for axis, since the icosahedral group contains a four-group as a subgroup (Theorem 1). There must then be an homology of period 10 having that line for axis, which is impossible (Theorem 6).

Theorem 8. *No multiplicative group which does not leave fixed a point, line, or triangle can contain homologies of period* **4.**

Consider two homologies of period 4 which are not commutative. They must generate the octahedral group on the line joining their centers. The centers and axes of the two homologies must then harmonically separate each other. We choose them as (010) and $x_2 = 0$, (01–1) and $x_2 - x_3 = 0$. Since in a G_{24} there are involutions interchanging the two fixed points of a C_4 there is an homology with center (001) and axis $x_3 = 0$ and consequently an homology with center (100) and axis $x_1 = 0$. Hence there must be an axis joining any two centers. Consequently, since but six axes can pass through (100), there can be no homologies the centers of which do not lie on one of those six axes. Since we assume no line remains invariant under the group there must be other centers on each of the six axes. If a center on $x_2 = 0$ be chosen as (10–1), the corresponding axis must harmonically separate (100) and $x_1 = 0$, and will therefore be $x_1 - x_3 = 0$. But (10–1) and $x_1 - x_3 = 0$ do not harmonically separate (01–1) and $x_2 - x_3 = 0$. The two homologies having them for centers and axes cannot then generate an octahedral group on $x_1 + x_2 + x_3 = 0$. No group containing homologies of period 4 is therefore possible.

§6. Multiplicative Groups containing Homologies of Period 3.

Theorem 9. *The Hessian group G_{216} is the only multiplicative group containing homologies of period* 3, *which does not leave invariant a point, line, or triangle.*

A group which contains homologies of period 3 and which does not leave invariant a point, line, or triangle, will contain two such homologies which are not commutative. We choose the center and axis of the first as (100) and $x_1 = 0$, and the center of the second as (111). If the point of intersection of the two axes be chosen as (01–1), the axis of the second will be some line of the pencil, $Ax_1 + x_2 + x_3 = 0$. The group of the points on the line, $x_2 - x_3 = 0$, which joins the two centers, must be the tetrahedral group G_{12}. For if it were the octahedral or icosahedral group there would be an homology of period 3 having $x_2 - x_3 = 0$ for axis, since in either of these groups there are involutions

interchanging the fixed points of the C_3. But since there must be a reflection having that line for axis (Theorem 1), there would then be an homology of period 6 having that line for axis, which is impossible (Theorem 6). In order that the two homologies shall generate the tetrahedral group on $x_2 - x_3 = 0$, the axis of the second must be $x_1 + x_2 + x_3 = 0$. The two homologies are then

$$[\omega x_1,\ x_2,\ x_3],$$

$$x_1' = (\omega + 2)x_1 + (\omega - 1)x_2 + (\omega - 1)x_3,$$

$$x_2' = (\omega - 1)x_1 + (\omega + 2)x_2 + (\omega - 1)x_3, \quad (\omega^2 + \omega + 1 = 0).$$

$$x_3' = (\omega - 1)x_1 + (\omega - 1)x_2 + (\omega + 2)x_3$$

There are then on $x_2 - x_3 = 0$ the four centers (100), (111), (ω11), ($\omega^2$11), and there are four axes $x_1 = 0$, $x_1 + x_2 + x_3 = 0$, $\omega^2 x_1 + x_2 + x_3 = 0$, $\omega x_1 + x_2 + x_3 = 0$, passing through (01–1). The group is of order 24, having (2, 1) isomorphism with the tetrahedral group. The transformations which are represented by C_2 on $x_2 - x_3 = 0$ are C_4 in the plane. Together these three C_4 form the quaternion G_8.

In any group containing this group of order 24 every other homology of period 3 must be commutative with one of the above four. For consider one which is not. It cannot generate with the reflection with center (01–1) and axis

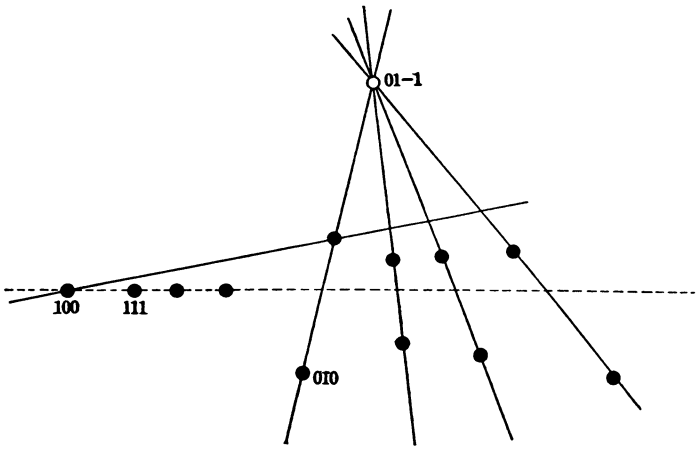

FIG. 2.

$x_2 - x_3 = 0$ a tetrahedral group on the line joining their centers, since we have seen that the transformations in the plane which are represented by C_2 in the tetrahedral group are C_4 in the plane. The group on the line joining the centers must then be dihedral. But this will involve an homology of period 3 having for axis the line joining the centers. But since the group of the lines through

(01–1) must be the tetrahedral group, there can be but four axes through it. There can be therefore no such homology.

There can be but two homologies of period 3 commutative with each of the four homologies in the group of order 24, since if the group of the points on one of the four axes is not dihedral, there will be a reflection having that line for axis (Theorem 1) and hence an homology of period 6 having that line for axis. If a center on $x_1 = 0$ be chosen as (010), the corresponding axis must pass through (100) and with the center harmonically separate (01–1) and $x_2 - x_3 = 0$, which are the center and axis of the reflection (Fig. 2). The homology is then $[x_1, \omega x_2, x_3]$.

There are then twelve homologies of period 3 in the group which form by threes four triangles. The group leaving one of the triangles point-wise invariant is of order 9, all six permutations are made on its vertices, and the group is transitive on the triangles. Its order is therefore $9 \cdot 6 \cdot 4 = 216$. It is the well-known Hessian group, permuting among themselves the nine inflexional points of a cubic curve. In this case they are (01–1), (01–ω), (01–ω^2), (10–1), (10–ω), (10–ω^2), (1–10), (1–ω0), (1–$\omega^2$0). It is the largest group which leaves invariant the Abelian G_9 generated by $[x_1, \omega x_2, \omega^2 x_3]$, $[x_2, x_3, x_1]$. From the unique choice of coördinates it follows that there is a single conjugate set of G_{216} under the whole collineation group of the plane.

§ 7. Multiplicative Groups which contain Reflections; General Properties.

Having made an exhaustive study of multiplicative groups which contain homologies of higher period than 2, we will assume in the remaining discussion of those groups that the only homologies which are present are reflections. We suppose the existence of a group which contains reflections and consider a particular reflection in the group. We denote its center and axis by A and a respectively. There will be a group commutative with it which is (2, 1) isomorphic with the group of the points on a. There will be points conjugate with A under the group, some of which will not lie on a, since we assume that no triangle is left invariant. The points conjugate with A will lie on lines through A which will form one or more conjugate sets. Such a line may be an axis of a reflection, in which case its center will lie on a (Theorem 5). There will then be a center at its intersection with a, which may or may not be conjugate with A.

Consider a line through A which contains centers of reflections and which is not itself an axis of a reflection. There cannot then be a reflection with center at its intersection with a. The group of the points on this line cannot contain a four-group as a subgroup and hence will be dihedral, containing a cyclic base of odd order. Since a dihedral group may be generated by two reflections, the axes of all the reflections, whose centers lie on the line, will pass through a point.

All the reflections with centers on the line will be conjugate. We shall refer to a line of this character as an o-line.

There will be a cyclic group of odd order, d, having the o-line for one of the sides of its fixed triangle. This cyclic group will be self-conjugate in general only under the dihedral group of order $2d$. If however $d = 3$, it may be self-conjugate under a group of order 18, under which all six permutations are made on the vertices of its fixed triangle (Theorem 3). If therefore $d \neq 3$, there will be conjugate with this cyclic group $\Omega/2d$ cyclic groups, where Ω denotes the order of the whole group. In these groups there will be $(d-1)\Omega/2d$ transformations excluding the identity. If $d = 3$, there will be conjugate with the cyclic group either $\Omega/2\cdot 3$ or $\Omega/6\cdot 3$ cyclic groups containing

$$(3-1)\frac{\Omega}{2\cdot 3} \quad \text{or} \quad (3-1)\frac{\Omega}{6\cdot 3}$$

transformations other than the identity. If two o-lines are not conjugate, the two cyclic groups which leave them fixed will not be conjugate. Corresponding then to each conjugate set of o-lines on which the group is dihedral there will be a conjugate set of cyclic groups of type I.

Any two o-lines through the center of a reflection which are conjugate under the whole group are conjugate also under the group commutative with that reflection. For if two o-lines, b and b', through A are conjugate, there are transformations which send b to b' and a center on b into any center on b'. In particular there are transformations which leave A fixed and send b to b'. Hence if the group commutative with a reflection be of order g, there will be $\frac{1}{2}g$ o-lines in each conjugate set through its center.

Theorem 10. *In a multiplicative group which does not contain homologies of period 3 but which contains a C_3 self-conjugate under a G_9 permuting cyclically the vertices of its fixed triangle, any two of the C_3 which are conjugate under the whole group are conjugate also under the subgroup leaving the G_9 invariant.*

We choose two of the C_3 in the G_9 as those generated by $[x_1, \omega x_2, \omega^2 x_3]$, $[x_2, x_3, x_1]$, where $\omega^2 + \omega + 1 = 0$. The four fixed triangles of the C_3 in the G_9 then form the Hessian configuration. All the G_9 in which one of these C_3 lies form a single conjugate set. For if the group leaving its fixed triangle point-wise invariant is of order d, it will lie in $d/3$ groups G_9. But the group leaving the triangle point-wise invariant which also leaves one of the G_9 invariant is of order 3, since we have assumed no homologies of period 3 to be present. Hence the $d/3$ groups G_9 are all conjugate.

If there are transformations in the group which transform one C_3 into another C_3 in the same G_9, there will then be transformations which transform the first C_3 into the second, and a G_9 in which the first lies into any G_9 in

which the second lies. In particular the two C_3 will be conjugate under the group which leaves invariant the G_9 in which both lie.

§ 8. Multiplicative Groups containing no Four-Groups.

Theorem 11. *The only multiplicative groups, which do not leave invariant a point, line, or triangle, and which contain reflections but no four-groups, are the two Hessian groups G_{36} and G_{72}.*

If a group contains reflections but no four-groups, all the centers of the reflections will lie on o-lines through one of them. Consequently all reflections in the group will be conjugate. Commutative with each reflection there will be a certain group, whose order we denote by g. No transformation except the identity can be commutative with more than one of the reflections. If Ω denotes the order of the whole group, there will then be Ω/g reflections and $(g-1)\Omega/g$ transformations other than the identity in the groups commutative with the reflections. We suppose there are r conjugate sets of o-lines on which the centers of the reflections lie. The order of the group will then be equal to the product of the order of the group commutative with a single reflection times the number of reflections. Hence

$$\Omega = g\left\{1 + \frac{g}{2}\sum_{i=1}^{r}(d_i - 1)\right\}.$$

The order of the group will also be equal to the number of transformations which it contains, as follows:

$$\Omega = 1 + (g-1)\frac{\Omega}{g} + \sum_{i=1}^{r}(d_i - 1)\frac{\Omega}{f_i d_i} + \cdots,$$

where, if $d_i \neq 3, f_i = 2$; if $d_i = 3, f_i = 2, 6$.

We find that there are the following four solutions:

$$g = 2,\ r = 1,\ f_1 = 2,\ \Omega = 2d.$$

$$g = 2,\ r = 4,\ d_i = 3,\ f_i = 6,\ \Omega = 18.$$

$$g = 4,\ r = 2,\ d_i = 3,\ f_i = 6,\ \Omega = 36.$$

$$g = 8,\ r = 1,\ d_1 = 3,\ f_1 = 6,\ \Omega = 72.$$

The first solution gives simply a single dihedral group. In each of the other three cases there are four C_3, each of which is invariant under a G_{18}. If two C_3 be $[x_1, \omega x_2, \omega^2 x_3]$, $[x_2, x_3, x_1]$, where $\omega^2 + \omega + 1 = 0$, the four C_3 are then determined. If these groups exist they must then be subgroups of the Hessian G_{216}. They do exist, since the G_{216} is readily shown to be isomorphic with a tetrahedral group permuting the four triangles.

§ 9. Multiplicative Groups containing Four-Groups.

Theorem 12. *If a multiplicative group contains four-groups, every dihedral group which it contains will be contained by a group leaving invariant a conic.*

We choose two reflections which generate the dihedral group as those with centers (001) and (011), and axes $x_3 = 0$ and $x_2 + \lambda x_3 = 0$ respectively. The invariant family of conics is then $Ax_1^2 + x_2^2 + \lambda x_3^2 = 0$, where A is the parameter (Fig. 3).

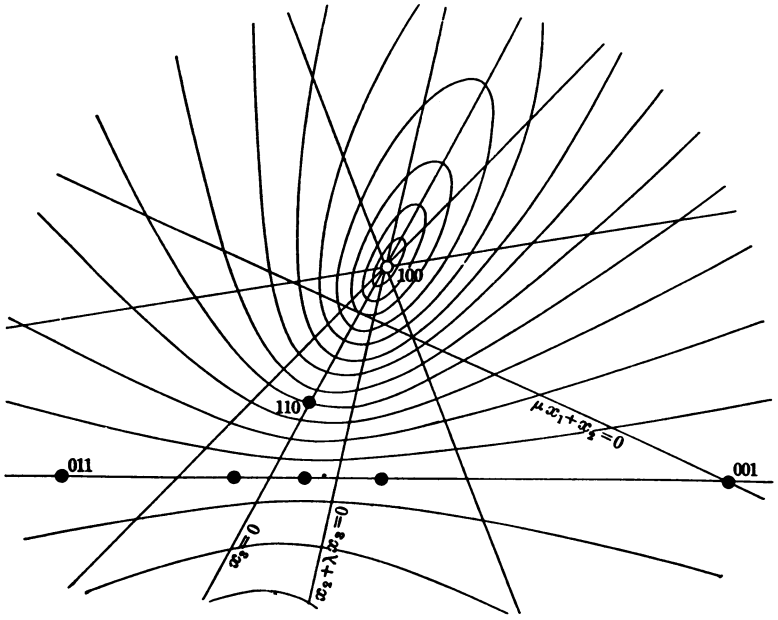

Fig. 3.

If there is a single reflection which does not lie in a four-group, the centers of all the other reflections will lie on o-lines through its center. Hence all reflections will be conjugate and no reflection can lie in a four-group. If four-groups do appear therefore, every reflection must lie in a four-group. Consider for example the reflection with center (001) and axis $x_3 = 0$, and suppose that the only reflections with which it is commutative have centers at (100) and (010). Since no triangle is supposed left invariant, (100) will be conjugate with points not on $x_1 = 0$ or $x_2 = 0$. These points must then lie on o-lines through (001), and hence must be conjugate with (001). But if (100) is a center of a reflection, more than two reflections will be commutative with that reflection. Hence more than two reflections in such a case must be commutative with the reflection with center (001).

There will be then in any case reflections commutative with that with center (001), whose centers are not (100) or (010). If the center of such a reflection

is (110) and its axis is $\mu x_1 + x_2 = 0$, the reflection will leave invariant in common with the dihedral group the conic $\mu x_1^2 + x_2^2 + \lambda x_3^2 = 0$.

Theorem 13. *A group which does not leave invariant a point, line, or triangle, and which contains four-groups, will contain either an octahedral group G_{24} or an icosahedral group G_{60}.*

Any group which does not leave invariant a point, line, or triangle, and which contains reflections, will contain two reflections which are not commutative and hence a dihedral group. It will then contain a group leaving invariant a conic (Theorem 12). The groups which leave a conic invariant are the regular solid groups. The only two which contain dihedral groups as subgroups are the octahedral group G_{24}, and the icosahedral group G_{60}.

Theorem 14. *The G_{168}^{7} is the only multiplicative group which contains an octahedral group G_{24}, but not an icosahedral group G_{60}.*

If we choose the four points which are permuted by the octahedral group as (111), (-111), (1-11), (11-1) (Fig. 4), it may be generated by the following transformations:

$$S\colon\ [-x_1, x_3, x_2],$$

$$T\colon\ [x_2, x_1, x_3],$$

$$U\colon\ [x_1, x_3, x_2].$$

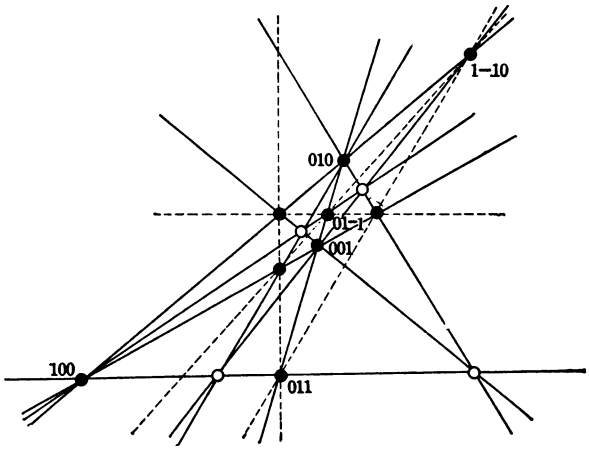

FIG. 4.

These generators satisfy the relations:

$$S^2 = T^2 = U^2 = (ST)^3 = (SU)^2 = (TU)^3 = I.$$

The G_{24} contains two sets of reflections, three in one set conjugate with SU and six in the other set conjugate with U. Any group which contains the G_{24} must contain reflections not in the G_{24}, since the latter can be invariant under

no larger group. Every reflection not commutative with one of the three reflections conjugate with SU must generate with the four-group containing those three reflections an octahedral group, since it will leave invariant a conic common to that four-group. There can be no dihedral group of order greater than 8 (Theorem 12). Hence each of the reflections conjugate with SU can be commutative with but four reflections. The invariant four-group of the G_{24} generated by S, T, and U, i. e., the four-group with fixed triangle (100)(010)(001), can therefore lie in but three other octahedral groups, i. e., groups having for fixed triangles (100)(011)(01–1), (010)(101)(10–1), (001)(110)(1–10). Hence every reflection in the group containing the G_{24} must be commutative with a reflection of the G_{24}. No more reflections can be commutative with a reflection which is conjugate under the G_{24} with SU, and but two more reflections can be commutative with each of the six reflections which are conjugate with U under that group. The only group which may contain the G_{24} is therefore a group containing $3 + 6 + 6 \cdot 2 = 21$ reflections. The centers of these twenty-one reflections must lie on the four axes and on four o-lines through a center of one of them. They will all be conjugate, and the order of the group will be $8 \cdot 21 = 168$.

A reflection commutative with U must generate with S a dihedral group of order 8 (Theorem 12). Such a reflection is

$$V: \begin{aligned} x_1' &= -\lambda^2 x_2 - \lambda^2 x_3, \\ x_2' &= -2x_1 + \lambda x_2 - \lambda x_3, \\ x_3' &= -2x_1 - \lambda x_2 + \lambda x_3. \end{aligned}$$

This reflection must generate a G_{24} with the dihedral G_6 generated by T and U, and hence either its product by T must be of period 3 or the product of VU by T must be of period 3. Without loss of generality we may take $(TV)^3 = I$. The condition for this is $\lambda^2 - \lambda + 2 = 0$, $\lambda = \frac{1}{2} \pm \frac{1}{2}\sqrt{-7}$. In this case we have the generational relations:

$$V^2 = (VU)^2 = (VT)^3 = I, \qquad VSVS = U.$$

A group of order 168 is then generated by S, T, U, and V. We suppose the operators of the G_{24} written down in a horizontal row, and form a multiplication table (multiplying on the left) of seven rows, of which the multipliers are I, V, TV, UTV, STV, $SUTV$, $TSUTV$. If these seven rows be numbered from 1 to 7 in the order in which their multipliers are written, they are permuted as follows by the four generators when applied as left-hand multipliers:

$$\begin{aligned} S&: (1)(2)(35)(46)(7), \\ T&: (1)(23)(4)(5)(67), \\ U&: (1)(2)(34)(56)(7), \\ V&: (12)(3)(4)(56)(7). \end{aligned}$$

The 168 operators are thus permuted among themselves. The rows must all be distinct, for if two coincide, all must coincide. This is impossible, since V does not lie in the octahedral group. Hence a group of order 168 is generated. It is representable on seven letters, e. g., on the seven rows, and is simple.

Theorem 15. *The G^{6}_{360} is the only multiplicative group containing an icosahedral group G_{60}.*

We choose (100), (010), (001) as the three centers of one of the four-groups of a G_{60}. Since a four-group in a G_{60} is self-conjugate under a tetrahedral group, there will be four C_3 permuting cyclically these three centers. Each of the C_3 must be self-conjugate under a G_6. We choose as (111) the fixed point of a C_3 through which pass the three axes of reflections. Two of the transformations of the tetrahedral group are then

$$E_1\colon\ [x_2, x_3, x_1], \qquad E_2\colon\ [x_1, -x_2, -x_3].$$

A reflection generating with E_1 a dihedral G_6 takes the form

$$E_3\colon \begin{aligned} x_1' &= (\alpha^2+\alpha)x_1 - \alpha x_2 + (\alpha+1)x_3,\\ x_2' &= -\alpha x_1 + (\alpha+1)x_2 + (\alpha^2+\alpha)x_3,\\ x_3' &= (\alpha+1)x_1 + (\alpha^2+\alpha)x_2 - \alpha x_3. \end{aligned}$$

The centers of the fifteen reflections in the group with the exception of (010) and (001) must lie on o-lines through (100) which contain three or five centers (Fig. 5). At least one of the three reflections in the dihedral group containing

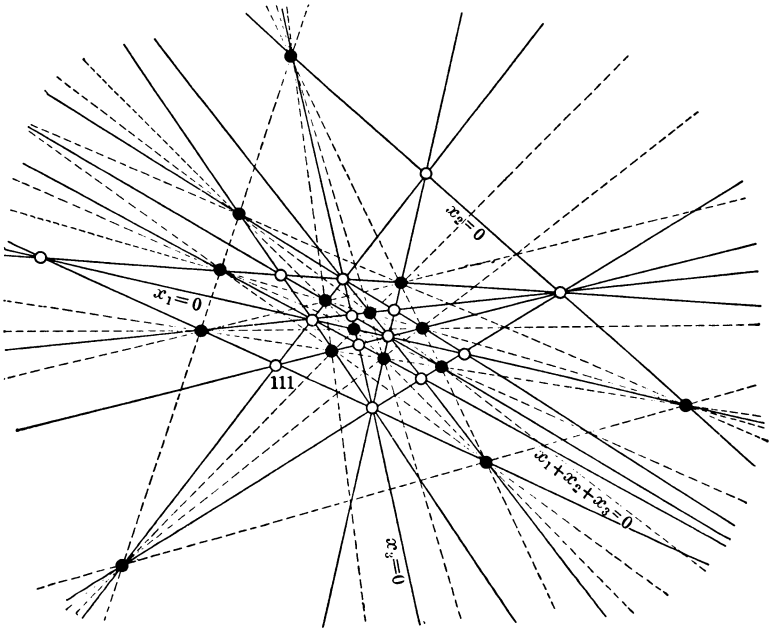

FIG. 5.

E_1 must be such that its product by E_2 is of period 3. In order that $(E_2E_3)^3 = I$, we must have $\alpha^2 + \alpha - 1 = 0$, $\alpha = (-1 \pm \sqrt{5})/2$. In this case the three transformations satisfy the following relations:

$$E_1^3 = E_2^2 = E_3^2 = (E_1E_2)^3 = (E_1E_3)^2 = (E_2E_3)^3 = I.$$

They therefore generate the icosahedral group G_{60}.*

There is a single conjugate set of G_{60} under the whole collineation group, since the two G_{60} which correspond to the two values of α are conjugate under the transformation $[x_1, x_3, x_2]$.

We inquire first whether any group can contain the G_{60} and have only two reflections commutative with each reflection. The reflections in such a group must arrange themselves by threes in four-groups, the vertices of the fixed triangles of these four-groups being permuted cyclically. Every reflection not in the four-group with fixed triangle (100)(010)(001) must generate with that four-group a G_{60}. Corresponding then to each pair of o-lines through one center which contain 3 centers there will be a pair of o-lines which contain 5 centers. Since there is no C_4 commutative with a reflection, the group cannot contain as a subgroup either the Hessian G_{36} or the G_{72}. Consequently since there can be but one conjugate set of o-lines containing 3 centers, the vertices of the fixed triangles of the C_3 cannot be permuted cyclically (Theorem 10).

If we denote by Ω the order of the whole group and by g the order of the group commutative with a four-group, Ω must then satisfy a Diophantine equation of the form:

$$\Omega = 1 + (g-1)\frac{\Omega}{3g} + (5-1)\frac{\Omega}{2\cdot 5} + (3-1)\frac{\Omega}{2\cdot 3} + \cdots.$$

In order that the coefficient of Ω on the right shall be less than unity, we must have $g = 4$, $\Omega = 60$. Hence no group can contain the G_{60} if only two reflections are commutative with a reflection.

We suppose next that a reflection is commutative with more than two reflections. Since the group cannot contain a dihedral group of order greater than 10 (Theorem 12), the centers and axes of two reflections which are commutative with the same reflection, but not with each other, must separate each other harmonically. There can then be but four reflections commutative with any reflection. A four-group can then be commutative only with itself. A reflection commutative with E_2 must then generate a G_{24} with the G_{12} generated by E_1 and E_2. Such a G_{24} is an octahedral group and will leave invariant a conic. This conic cannot be $x_1^2 + x_2^2 + x_3^2 = 0$, since that is left invariant by a G_{60}. It must then be $x_1^2 + \omega x_2^2 + \omega^2 x_3^2 = 0$, where ω is a cube root of unity. There must be at least 45 reflections in the group, since a reflection not in the G_{60}

*E. H. MOORE, Proceedings of the London Mathematical Society, vol. 28 (1897), pp. 357-366; DICKSON, *Linear Groups*, p. 289.

must be conjugate with at least 30 reflections under that group. We may show that the maximum number must be 45. There are three reflections in the invariant four-group of the G_{12} generated by E_1 and E_2, and two more reflections commutative with each of those three. Every reflection not commutative with any one of the three reflections of the four-group will leave a conic invariant in common with the four-group, and hence must generate with the four-group either a G_{24} or a G_{60}. The four-group can lie in but three octahedral groups other than the one under which it remains invariant, i. e., octahedral groups whose invariant four-groups contain a reflection in common with the above four-group. Each of the three G_{24} will contain four reflections not commutative with any one of three reflections of that four-group. Since the four-group can be commutative only with itself, every G_{60} in which it lies must contain the G_{12} generated by E_1 and E_2. Since the conic $x_1^2 + \omega x_2^2 + \omega^2 x_3^2 = 0$ is left invariant by a G_{24}, there can be but two such G_{60}, i. e., those having for fixed conics $x_1^2 + x_2^2 + x_3^2 = 0$, $x_1^2 + \omega^2 x_2^2 + \omega x_3^2 = 0$. There can then be but $3 + 3\cdot 2 + 3\cdot 4 + 2\cdot 12 = 45$ reflections. There will be four o-lines through the center of a reflection, on which lie 5 centers. Hence the group commutative with a reflection must be of order 8 and the whole group of order $8\cdot 45 = 360$. One of the reflections commutative with E_2 is

$$E_4: \ [x_1, \ \omega^2 x_3, \ \omega x_2].$$

This reflection satisfies with the three generators of the G_{60} the following relations:

$$E_4^2 = (E_1 E_4)^2 = (E_2 E_4)^2 = (E_3 E_4)^3 = I.$$

It therefore generates with the G_{60} a G_{360}^6.* Two G_{360}^6 corresponding to the choice of ω contain the G_{60}. The G_{360} however contains two sets of G_{60} and a transformation carrying a G_{60} not conjugate with the G_{60} generated by E_1, E_2, E_3 into the latter transforms one G_{360} into the other. There is therefore a single conjugate set of G_{360} in the plane.

§ 10. Groups containing only Transformations of Type I.

A complete discussion of multiplicative groups which contain homologies has been given. Any group which contains only transformations of type I must be of odd order, since a transformation of period 2 is a reflection. Any cyclic group contained by such a group can then be self-conjugate only under itself or under a group permuting cyclically the vertices of its fixed triangle. If Ω denotes the order of the whole group, it must then satisfy a Diophantine equation of the form

$$\Omega = 1 + \sum_{i=1}^{r} (d_i - 1) \frac{\Omega}{f_i d_i} \qquad (f_i = 1, 3).$$

* Moore, loc. cit., Dickson, loc. cit.

If the order of the group is divisible by 3, we may take d_1 to be divisible by 3. If then $f_1 = 3$, there must be four conjugate sets of C_3 (Theorem 10). Hence $r \geqq 4$, and each of the first four d's is divisible by 3. This can happen only if $r = 4$, $d_2 = d_3 = d_4 = 3$, $\Omega = 3d_1$. If on the other hand $f_1 = 1$, we find $r = 1$, $\Omega = d_1$, or $r = 2$, $d_1 = 3$, $\Omega = 3d_2$.

If the order of the group is not divisible by 3, we have $r = 1$, $\Omega = d_1$. We have therefore

Theorem 16. *No multiplicative group which does not leave invariant a point, line or triangle can contain only transformations of type I.*

The discussion of the groups in the ordinary plane is therefore complete.

§ 11. Groups containing Transformations of Type III, but not Elations.

We now consider the possibility of groups containing transformations of type III, but not elations, and consequently no transformations of type II. There can be no homologies present which have a common center but different axes, or vice-versa, so that Theorem 4 holds. Theorem 5 does not hold, but instead we have

Theorem 17. *A group containing transformations of type III but not elations cannot contain two homologies such that the line joining their centers passes through the intersection of their axes unless they are both of period 2.*

The product of two homologies such that the line joining their centers passes through the intersection of their axes will leave invariant two points on that line unless one transformation on that line is conjugate with the inverse of the other. Unless the homologies are both of period 2 we may choose their powers so that this is not the case. The product is therefore of type II in the plane.

Theorems 6, 7, 8, 9 are proved independently of the assumption of the non-existence of transformations of type III in the group. The Hessian group G_{216} however contains no transformations of type III. Hence we have

Theorem 18. *There is no group which contains transformations of type III but not elations, which does not leave invariant a point, line, or triangle, and which contains homologies of higher period than 2.*

If transformations of type III appear, there may be a new kind of o-lines through the center of a reflection, i. e., o-lines on which the group of the points is metacyclic, containing an additive base. There cannot be more than a single conjugate set of such o-lines, since their number must be of the form $1 + fp^m$, where p^m denotes the order of the additive group on the line. If the order of the group commutative with a reflection is g, and the order of the subgroup of that group which leaves fixed an o-line of this sort is h, the number of such o-lines through the center of the reflection will be g/h.

Theorem 10 holds in this case also. In the proof of Theorem 11 however it

is necessary to consider the additional case where o-lines of the sort described above appear.

If there are no reflections commutative with a reflection, and if there is a set of o-lines, each of which is left invariant by a metacyclic group of order hp^m, any group which exists (of order Ω) will contain $(g-1)\Omega/g$ transformations in the groups commutative with the reflections and $(p^m-1)\Omega/hp^m$ transformations of type III. Hence Ω must satisfy an equation of the form:

$$\Omega = 1 + (g-1)\frac{\Omega}{g} + (p^m-1)\frac{\Omega}{hp^m} + \cdots.$$

In order that the coefficient of Ω on the right shall be less than unity, no more terms representing transformations can appear, and also $h = g$. We then have $\Omega = gp^m$, which represents the single metacyclic group.

If we combine this result with Theorem 11, and observe that the G_{36} and G_{72} contain no transformations of type III, we have

Theorem 19. *No group exists which contains transformations of type III but not elations, which does not leave invariant a point, line, or triangle, and which contains reflections but no four-groups.*

Theorem 12 holds in this case without modification. We prove also

Theorem 20. *If a group containing four-groups contains a metacyclic group of order $2p^m$ (the operators of period p being of type III), that metacyclic group will be contained by a group leaving invariant a conic.*

A metacyclic group of order $2p^m$ will leave invariant a one-parameter family of conics. For consider a single transformation of type III, such as

$$[x_1 + x_2 + x_3,\ x_2 + 2x_3,\ x_3].$$

This leaves invariant the family $x_2^2 + Ax_3^2 - 4x_1x_3 = 0$ (Fig. 6). The above

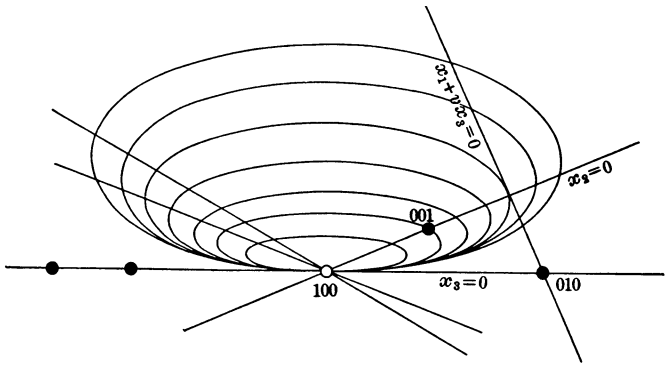

FIG. 6.

transformation is invariant under any transformation of type III leaving fixed (100) and $x_3 = 0$ and the same family of conics. Hence we may choose the

center of a reflection in the metacyclic group arbitrarily as (010). The axis will be a line, $x_2 + \mu x_3 = 0$, passing through (100). This reflection will transform the above transformation into a transformation which is its inverse on $x_3 = 0$. The transformed transformation is

$$[x_1 - x_2 + (1 - 2\mu)x_3,\ x_2 - 2x_3,\ x_3].$$

The product of the two is an elation unless $\mu = 0$. The reflection must therefore leave fixed the conics. Hence every reflection in the metacyclic group leaves fixed the conics. Since the metacyclic group of order $2p^m$ may be generated by the p^m reflections which it contains, it leaves fixed the conics.

Since we have assumed the existence of four-groups, the reflection with center (010) and axis $x_2 = 0$ will lie in a four-group. Since the metacyclic group is invariant under any elation with center (100) and axis $x_3 = 0$, we may choose the center of a reflection in that four-group arbitrarily as (001). Its axis will be a line, $x_1 + \nu x_3 = 0$, passing through (010). This reflection leaves invariant in common with the metacyclic group the conic $x_2^2 - 2\nu x_3^2 - 4x_1x_3 = 0$.

Theorem 21. *If a group containing four-groups contains transformations of type III, it will contain a group leaving invariant a conic, which is either an octahedral group G_{24}, an icosahedral group G_{60}, a group of order $(p^m + 1)p^m(p^m - 1)/2$, or a group of order $(p^m + 1)p^m(p^m - 1)$.*

Any group which contains reflections will contain two reflections which are not commutative, provided no point, line or triangle is left invariant. Hence it will contain either a dihedral group or a metacyclic group and therefore (either by Theorem 12 or by Theorem 20) a group leaving invariant a conic. The group leaving a conic invariant is simply isomorphic with the group of the points on a line.* Hence this group must be either an octahedral group G_{24}, an icosahedral group G_{60}, a group of order $(p^m + 1)p^m(p^m - 1)/2$, or a group of order $(p^m + 1)p^m(p^m - 1)$. (See § 1.)

Theorem 22. *A $G^7_{168}(p = 3)$ is the only group containing transformations of type III such that its largest subgroup leaving invariant a conic is a G_{24}.*

The proof of this theorem is the same as that of Theorem 14; except that, having obtained the group of order 168, we have yet to determine when it contains transformations of type III. This will be the case only if $p = 3, 7$. For $p = 7$ the G_{168} leaves invariant a single conic. Hence the theorem is as stated.

Theorem 23. *A $G^6_{360}(p = 5)$ and a $G_{720}(p = 5)$ are the only groups containing transformations of type III such that their largest subgroup leaving invariant a conic is a G_{60}.*

The proof is the same as that of Theorem 15 with slight modifications. We make use of Theorem 20 as well as of Theorem 12 in showing that the only

* VEBLEN and YOUNG, *Projective Geometry*, Chapter VIII, Theorem 15.

o-lines which exist contain 3 or 5 centers. We show in the same way that there can be but 45 reflections in the group. It was shown under Theorem 15 that the group commutative with a reflection was of order 8, since there must be through its center four o-lines containing 5 centers each. For $p = 5$ however it is possible that there may also be a group of order 16 permuting these four o-lines. A transformation of period 8 transforming the $G_{360}(p = 5)$ into itself is given by

$$[x_1,\ (2\omega + 1)x_2 + (\omega - 1)x_3,\ -(\omega + 2)x_2 + (2\omega + 1)x_3].$$

A group of order 720 therefore exists.

The G_{360} also contains transformations of type III if $p = 3$. In this case however it leaves invariant a single conic. Hence the theorem is as stated.

§ 12. Groups containing Transformations of Type III which contain larger Subgroups leaving a Conic Invariant.

Theorem 24. *There exists no group which does not contain elations or homologies of higher period than* 2, *and which contains a set of reflections each of which is commutative with a group* (2, 1) *isomorphic with either the tetrahedral, octahedral, or icosahedral group.*

If a group commutative with a reflection is (2, 1) isomorphic with either the tetrahedral or icosahedral group, it can contain no four-group. For all the involutions in either a G_{12} or a G_{60} lie in four-groups (on the axis), in any one of which all three involutions are conjugate. If two of the involutions are performed by reflections, the third will be performed by a C_4. But this is impossible, since the three involutions are conjugate. Hence no one of the involutions on the line can be performed by a reflection.

If the group commutative with a reflection is (2, 1) isomorphic with an octahedral group, none of the involutions of the included tetrahedral group can be performed by reflections. The six involutions not in the tetrahedral group however may be performed by reflections. In this case there will be twelve reflections commutative with the given reflection. The group commutative with the given reflection will contain four conjugate dihedral groups of order 12 and three conjugate dihedral groups of order 8.

Each of these dihedral groups will be contained by a group leaving invariant a conic (Theorem 12). Hence some of the twelve reflections commutative with the given reflection will be conjugate with that reflection, and hence all will be. There will then be twelve reflections commutative with every reflection. A dihedral group of order 8 will therefore lie in a group leaving invariant a conic which contains two conjugate sets of reflections. Such a group will be of order $(p^m + 1)p^m(p^m - 1)$, where $2(p^m - 1) = 8$, $p^m = 5$. No group is then possible unless $p = 5$.

Consider now a dihedral G_{12}. Each reflection commutative with one of the six reflections of this G_{12} (other than the invariant reflection) must generate a G_{120} with the G_{12}. Since a G_{120} contains 25 reflections and the G_{12} contains 7, the reflections commutative with these six reflections which are not in the dihedral group must be grouped in sets of 18. But there are 60 such reflections and hence this is impossible. No group can then exist for $p = 5$.

Theorem 25. *A G^7_{2520} is the only group such that its largest subgroup leaving invariant a conic is a G_{120} $(p = 5)$, provided that no elations are present.*

A G_{120} $(p = 5)$ is generated by

$$E_1\colon [x_2, x_3, x_1], \qquad E_2\colon [x_1, -x_2, -x_3], \qquad E_5\colon [x_1, x_3, x_2],$$

$$E_3\colon x_1' = x_1 - 2x_2 - 2x_3, \qquad x_2' = -2x_1 - 2x_2 + x_3, \qquad x_3' = -2x_1 + x_2 - 2x_3.$$

The invariant conic is $x_1^2 + x_2^2 + x_3^2 = 0$. The G_{120} contains two conjugate sets of reflections. Each reflection conjugate with E_2 is commutative with a dihedral group of order 8; each reflection conjugate with E_5 is commutative with a dihedral group of order 12. (Fig. 7.)

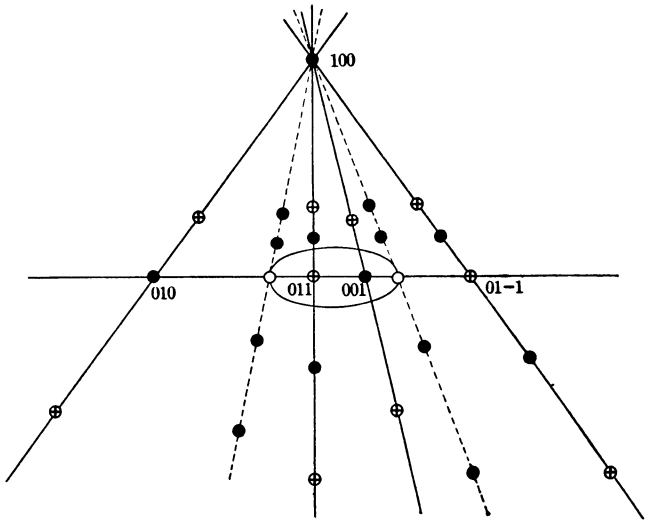

FIG. 7.

A group which contains the G_{120} will contain reflections not in the G_{120}. Since the G_{120} is supposed the largest subgroup leaving invariant a conic, no dihedral group of order greater than 12 can appear (Theorem 12). It may be shown readily that under any group containing the G_{120} E_2 must be invariant under a larger group. The only possible larger group which will not introduce a dihedral group of order greater than 12 and which will allow the group of the

points on $x_1 = 0$ and $x_1 - x_3 = 0$ to be dihedral is a G_{24} having for fixed triangle the fixed triangle of the G_{12} generated by E_1 and E_2. This G_{24} contains the C_3:

$$[x_1,\ \omega x_2,\ \omega^2 x_3] \qquad (\omega^2+\omega+1=0).$$

The fixed triangles of all the C_3 in the group will then be invariant under a G_9. The four-group which is invariant under the G_{12} generated by E_1 and E_2 will then lie in three G_{120}. Each of those G_{120} will contain 22 reflections not in that four-group. The four-group will also lie in nine G_{24} under which it is not invariant, i. e., G_{24} whose invariant four-groups have each a reflection in common with the above four-group. Each of these nine G_{24} will contain 4 reflections not in any one of the three G_{120}. There will then be $3+3\cdot 22+9\cdot 4=105$ reflections. These will all be conjugate and the order of the group must be $24\cdot 105 = 2520$.

As a product of the above C_3 and E_5 we obtain

$$E_4\colon\ [x_1,\ \omega^2 x_3,\ \omega x_2].$$

The five generators are found to satisfy the relations:

$$E_1^3 = E_2^2 = E_3^2 = E_4^2 = E_5^2 = I, \qquad (E_i E_{i+1})^3 = I, \qquad (E_i E_j)^2 = I \quad (j > i+1).$$

A G_{2520}^7 is then generated.*

Theorem 26. *No group which does not contain elations can contain a group of order* $(p^m+1)p^m(p^m-1)/2$ *or* $(p^m+1)p^m(p^m-1)$ *leaving a conic invariant, provided* $p^m > 5$, *and provided it contains no larger group leaving a conic invariant.*

The group commutative with a reflection in a group of order

$$\tfrac{1}{2}(p^m+1)p^m(p^m-1) \quad \text{or} \quad (p^m+1)p^m(p^m-1)$$

leaving a conic invariant is dihedral and hence the group of the points on the axis of the reflection is dihedral. There is but one pair of points on the axis which are interchanged provided the group of the points on the axis is larger than the four-group, i. e., provided the group commutative with the reflection is of order greater than 8. For the group of order $(p^m+1)p^m(p^m-1)/2$ this will be true if $p^m \pm 1 > 8$, $p^m > 9$; for the group of order $(p^m+1)p^m(p^m-1)$ it will be true if $2(p^m \pm 1) > 8$, $p^m > 5$. If then $p^m > 5$ and if the group is not the $G_{168}(p^m = 7)$ or the $G_{360}(p^m = 3^2)$, there will be but one pair of points on the axis which are interchanged by the group.

Excluding for the moment these two cases, we may show that there can be no more reflections commutative with a reflection. For there certainly cannot

* MOORE, l. c.; DICKSON, l. c.

be more than two such reflections, i. e., the two leaving the two points pointwise invariant. (If a reflection interchanges the points, it will leave fixed the conic.) But if we add two reflections we must add more than two, since any such reflection must generate together with a dihedral group containing the reflection with which it is commutative (other than the dihedral group which leaves the latter reflection invariant) a group of order $(p^m+1)p^m(p^m-1)/2$ or $(p^m+1)p^m(p^m-1)$ leaving invariant a conic. This group can have in common with the other group which leaves fixed a conic only the reflections of the dihedral group. Hence there will be more than two reflections added which are commutative with the latter reflection.

If the group is the $G_{168}(p^m=7)$ or the $G_{360}(p^m=3^2)$, there can be no more reflections commutative with a reflection. For since the group is supposed the largest group present which leaves invariant a conic, there can be no dihedral group present of order greater than 10 (Theorem 12). Hence there can be only four reflections commutative with any reflection in the group.

Suppose now that there is a reflection not commutative with any reflection in the group. It will leave invariant in common with any four-group of that group a conic. It must generate with that four-group some group leaving invariant a conic which can contain no reflections commutative with any of the three reflections of the four-group except those three reflections themselves. Such a group must be an icosahedral group G_{60}. Every reflection not in the original group leaving fixed a conic must then generate with this four-group a G_{60}. But there cannot be any transformations commutative with the four-group other than those of the four-group itself without involving more reflections commutative with the reflections of the four-group. Hence there cannot be more than four C_3 permuting cyclically the vertices of the fixed triangle of the four-group, i. e., all the G_{60} must contain the same tetrahedral group. A tetrahedral group however leaves fixed but three conics, one of which is the original conic. There can then be but two such G_{60}, each of which contains twelve reflections other than those of the four-group. There cannot then be more than 24 more reflections, which is impossible.

§ 13. Groups containing only Transformations of Types III and I.

Theorem 27. *There exists no group which contains only transformations of types* III *and* I *and which does not leave invariant a point, line, or triangle.*

Any group which contains only transformations of types III and I must be of odd order, since a transformation of period 2 is a reflection.

An additive group of order p^m containing transformations of type III will be self-conjugate under a metacyclic group of order d_1p^m, containing p^m conjugate cyclic groups of order d_1 which contain transformations of type I. (In partic-

ular d_1 may be unity.) Any cyclic group of order d_i containing transformations of type I will be self-conjugate either under itself only or under a group of order $3d_i$ permuting cyclically the vertices of its fixed triangle.

If we denote the order of the whole group by Ω, and enumerate the transformations which the group must contain, we are led to the following Diophantine equation:

$$\Omega = 1 + (p^m - 1)\frac{\Omega}{d_1 p^m} + \sum_{i=1}^{r}(d_i - 1)\frac{\Omega}{f_i d_i} \qquad (f_i = 1, 3).$$

If $f_1 = 3$, we may show that $d_1 = 3$. Let the fixed point and line of an additive group be (100) and $x_3 = 0$ and let the vertices of the fixed triangle of a cyclic group of order d_1 in the metacyclic group, under which the additive group is self-conjugate, be (100), (010), (001). A transformation of period d_1 in that cyclic group will be given by

$$[x_1, \omega x_2, \omega^e x_3], \tag{1}$$

where the period of ω is d_1. A transformation of type III in the additive group will be given by

$$\begin{aligned} x_1' &= x_1 + \alpha x_2 + \beta x_3, \\ x_2' &= \quad x_2 + \gamma x_3, \\ x_3' &= \quad\quad x_3 \end{aligned} \qquad (\alpha \neq 0, \gamma \neq 0). \tag{2}$$

If we transform (2) by (1), we obtain

$$\begin{aligned} x_1' &= x_1 + \alpha\omega x_2 + \beta\omega^e x_3, \\ x_2' &= \quad x_2 + \gamma\omega^{e-1} x_3, \\ x_3' &= \quad\quad x_3. \end{aligned} \tag{3}$$

If we transform (2) by (3), we obtain

$$\begin{aligned} x_1' &= x_1 + \alpha x_2 + (\beta + \alpha\gamma\omega^{e-1} - \alpha\gamma\omega) x_3, \\ x_2' &= \quad x_2 \quad + \quad \gamma x_3, \\ x_3' &= \quad\quad\quad x_3. \end{aligned} \tag{4}$$

The transformation (4) is the same as (2) on the line $x_3 = 0$. Hence (4) must be identical with (2). Hence $\omega^{e-1} = \omega$, $e \equiv 2 \pmod{d_1}$. But if the vertices of the fixed triangle of (1) are permuted cyclically, we must have $e^2 - e + 1 \equiv 0 \pmod{d_1}$. [See the discussion under Theorem 2.] Hence $2^2 - 2 + 1 \equiv 0 \pmod{d_1}$; $d_1 = 3$.

But if $f_1 = 3$, $d_1 = 3$, there must be four conjugate sets of C_3 (Theorem 10).

Hence $r \geqq 4$. The coefficient of Ω on the right is then greater than unity, and hence there can be no solution.

If $f_1 = 1$, $r = 1$, $\Omega = d_1 p^m$. This represents a single metacyclic group.

If $d_1 = 1$, either $r = 2$, $f_2 = 3$, $p^m = 3$, $\Omega = 3d_2$, or else $r = 1$, $\Omega = p^m$. The first represents a group permuting cyclically the vertices of a triangle, and the second a single additive group.

§ 14. Groups containing Elations.

Theorem 28. *The only groups which do not leave invariant a point or a line and which contain elations are: the HO* $(3, p^{2k})$*; groups containing the HO* $(3, p^{2k})$ *as self-conjugate subgroups of index* 3, *if* $p^k + 1$ *is divisible by* 3*; the LF* $(3, p^k)$*; groups containing the LF*$(3, p^k)$ *as self-conjugate subgroups of index* 3, *if* $p^k - 1$ *is divisible by* 3.

Any group which contains elations will contain a group of largest order consisting wholly of elations with a common axis and center. We denote the order of such a group by p^k. We choose the center and axis of one such group as (010) and $x_3 = 0$. Since we assume that no point or line remains invariant under the group, there will be groups of elations whose centers do not lie on $x_3 = 0$ and whose axes do not pass through (010). We choose the center and axis of such a group as (001) and $x_2 = 0$. By hypothesis then the order of the group consisting of all the elations with center (001) and axis $x_2 = 0$ will be less than or equal to p^k. The group generated by these two groups of elations will leave invariant (100) and $x_1 = 0$. The group of the points on $x_1 = 0$ cannot contain an additive group of higher order than p^k, and hence (by § 1) must be of order $(p^k + 1)p^k(p^k - 1)/2$ or $60(p^k = 3)$. (The group of order $(p^k + 1)p^k(p^k - 1)$ on the line cannot be generated by additive transformations only.)

Under either of these two groups, (010) and $x_3 = 0$ will be conjugate with (001) and $x_2 = 0$. Hence (010) and $x_3 = 0$ will be conjugate with the center and axis of any group of elations, since in any conjugate set of such groups there will be groups whose centers do not lie on $x_3 = 0$ and whose axes do not pass through (010).

If the group of the points on $x_1 = 0$ is of order $(p^k + 1)p^k(p^k - 1)/2$, we may choose it as the group generated by the two groups of elations

$$(E): [x_1, x_2 + \lambda x_3, x_3], \qquad [x_1, x_2, \lambda x_2 + x_3],$$

where λ takes all values in the $GF(p^k)$. This group contains an invariant reflection with center (100) and axis $x_1 = 0$ (Theorem 1). The group contains a set of cyclic groups of period $(p^k - 1)/2$ on $x_1 = 0$. One such group is generated by $[x_1, \eta x_2, \eta^{-1} x_3]$, where η is of period $p^k - 1$. This cyclic group is of

period $p^k - 1$ on $x_2 = 0$ and $x_3 = 0$. The group generated by the two groups of elations (E) also contains a set of cyclic groups of period $(p^k + 1)/2$ on $x_1 = 0$. Such a cyclic group which leaves fixed $(01I)$ and $(01{-}I)$, where I is a square-root of a not-square in the $GF(p^k)$, may be generated by a transformation of the form

$$x_1' = x_1, \qquad Ix_2' + x_3' = J(Ix_2 + x_3), \qquad Ix_2' - x_3' = J^{-1}(Ix_2 - x_3),$$

where J is a mark of period $p^k + 1$. This cyclic group is of period $p^k + 1$ on $Ix_2 + x_3 = 0$ and $Ix_2 - x_3 = 0$.

A group of order $60\,(p^k = 3)$ on $x_1 = 0$ is generated by the two groups of elations:

$$[x_1,\ x_2 + x_3,\ x_3], \qquad [x_1,\ x_2,\ ix_2 + x_3],$$

where $i^2 = -1$. The group contains a set of cyclic groups of period 2 on $x_1 = 0$. One such group is generated by $[x_1, -ix_2, ix_3]$. It is of period 4 on $x_2 = 0$ and $x_3 = 0$. The group in the plane is of order 120, as it contains the invariant reflection $[x_1, -x_2, -x_3]$ (Theorem 1).

Since we assume that no point or line remains invariant, there will be groups of elations whose centers do not lie on $x_1 = 0$ and whose axes do not pass through (100). We consider one such group. It must generate together with the reflection with center (100) and axis $x_1 = 0$ a group on the line joining their centers which does not contain an additive group of higher order than p^k. If $p^k > 3$, this group on the line must be of order $(p^k + 1)p^k(p^k - 1)/2$ or $(p^k + 1)p^k(p^k - 1)$. If $p^k = 3$, it must be of order 12, 24, or 60. In any case there will be a reflection having this line for axis, and having for center the point of intersection of the axis of the generating group of elations with $x_1 = 0$ (Theorem 1). The involution on $x_1 = 0$ performed by this reflection must leave invariant the group of the points on $x_1 = 0$.

In the special case where the group of the points on $x_1 = 0$ is of order $60\,(p^k = 3)$, the involution performed by this reflection on $x_1 = 0$ must belong to the group of order 60. Suppose for example that the center of the reflection is (010) and its axis $x_2 = 0$. The group of the points on $x_2 = 0$ contains a C_4 generated by $[x_1, -ix_2, ix_3]$. It must then be of order 24. But the fixed points of this C_4 will be interchanged by the group. The transformed transformation is $[ix_1, -ix_2, x_3]$. This is of period 4 on $x_1 = 0$. The group of the points on $x_1 = 0$ is now no longer of order 60 and hence it must contain an additive group of higher order than 3. We therefore exclude this case from the discussion entirely.

In the general case, in order that the reflection whose center lies on $x_1 = 0$ and whose axis passes through (100) shall permute among themselves the $p^k + 1$ centers of elations on $x_1 = 0$, either (i) its center must lie at some point conju-

gate with $(01I)$ and its axis pass through the conjugate point with respect to the $GF(p^k)$, or (ii) its center will coincide with one of the centers of elations and its axis will pass through one of the other centers.

We consider the case (i). Consider in particular the reflection with center $(01I)$ and axis $Ix_2 + x_3 = 0$. The axes of the elations with centers on $Ix_2 + x_3 = 0$ must all pass through $(01I)$. The group of the points on $Ix_2 + x_3 = 0$ contains a cyclic group of order $p^k + 1$ with fixed points (100) and $(01{-}I)$. It must then be of order $(p^k + 1)p^k(p^k - 1)$. Since there must be transformations leaving fixed $(01I)$ and interchanging (100) and $(01{-}I)$, the group of the points on $x_1 = 0$ must be of the same order. The axes of all elations whose centers lie on $x_1 = 0$ must then pass through (100). Hence a unique correspondence must be established between the centers and axes of elations and between the centers and axes of reflections. There can then be no centers of elations on any of the $p^k + 1$ axes of elations through (100) except those on $x_1 = 0$.

All the centers of elations except those on $x_1 = 0$ must then lie on the $p^k(p^k - 1)$ lines through (100) whose coördinates are in the $GF(p^{2k})$, but not in the $GF(p^k)$. Since there will be $p^k + 1$ on each of these lines, the total number of centers of elations will be

$$p^k + 1 + (p^k + 1)p^k(p^k - 1) = p^{3k} + 1.$$

All the centers not on $x_1 = 0$ will be conjugate under the group generated by the two groups of elations (E). We choose a center on $Ix_2 + x_3 = 0$ arbritrarily as $(-11{-}I)$. The $p^{3k} + 1$ centers will then be the points $(\epsilon, \alpha I + \beta, \gamma I + \delta)$, where $\epsilon, \alpha, \beta, \gamma, \delta$ are in the $GF(p^k)$ and $\alpha\delta - \beta\gamma = \epsilon^2$. (Fig. 8

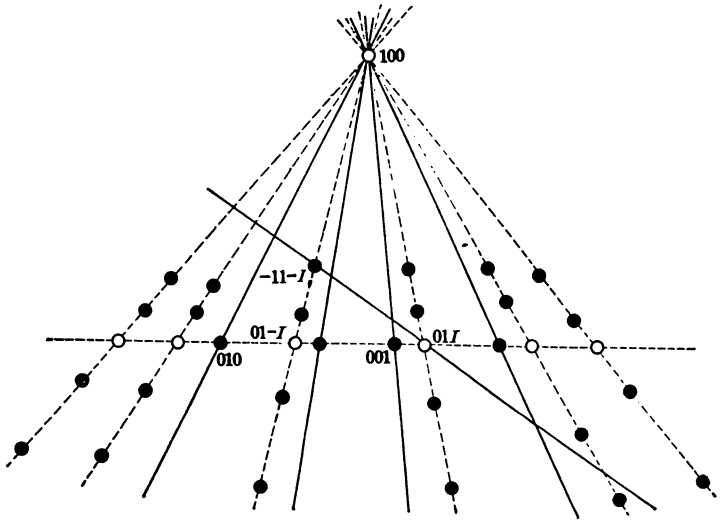

FIG. 8.

represents the configuration for $p^k = 3$.) The coefficients of the transformations permuting these points will lie in the $GF(p^{2k})$. We first seek to determine those groups which contain only transformations having for determinant a cube in the $GF(p^{2k})$.

The group will be transitive on the $p^{2k}(p^{2k} - p^k + 1)$ points whose coördinates lie in the $GF(p^{2k})$, but which are not centers of elations. The group of the points on any one of the axes of elations is metacyclic, containing p^{2k} involutions with a common fixed point. (The p^{3k} other axes of elations must meet that axis in p^{2k} points in sets of p^k each.) Hence (100) is conjugate with all the points on the axes of elations through it whose coördinates lie in the $GF(p^{2k})$ with the exception of the $p^k + 1$ centers of elations on $x_1 = 0$. It is also conjugate with all the points on the axes of reflections through it whose coördinates lie in the $GF(p^{2k})$, but which are not centers of elations.

Since all six permutations are made on the vertices of the triangle $(100)(01I)(01{-}I)$, there will be an homology of period $p^k + 1$ or $(p^k + 1)/2$ with center at each vertex (Theorem 3). But if $p^k + 1$ is divisible by 3, the determinant of an homology of period $p^k + 1$ will not be a cube in the $GF(p^{2k})$. Hence the period of the homology will be $(p^k + 1)/\nu$. (See Introduction.) The group leaving invariant (100) and $x_1 = 0$ is then of order

$$\frac{1}{\nu}(p^k+1)^2 p^k(p^k-1).$$

The whole group is of order

$$\frac{1}{\nu}(p^{2k} - p^k + 1)(p^k + 1)^2 p^{3k}(p^k - 1).$$

In order that the group of elations with center $(-11{-}I)$ shall permute among themselves the $p^{3k} + 1$ centers, we find that it must be given by

$$x_1' = \tfrac{1}{2}(2 + I\lambda)x_1 + \tfrac{1}{4}I\lambda x_2 - \tfrac{1}{4}\lambda x_3,$$

$$x_2' = -\tfrac{1}{2}I\lambda x_1 + \tfrac{1}{4}(4 - I\lambda)x_2 + \tfrac{1}{4}\lambda x_3,$$

$$x_3' = \tfrac{1}{2}I^2\lambda x_1 + \tfrac{1}{4}I^2\lambda x_2 + \tfrac{1}{4}(4 - I\lambda)x_3,$$

where λ takes all values in the $GF(p^k)$.

We may identify the group determined with the hyperorthogonal group,* $HO(3, p^{2k})$, by observing that it leaves invariant the function

$$x_1^{p^k+1} + \tfrac{1}{4}\left(x_2 + \frac{1}{I}x_3\right)^{p^k+1} - \tfrac{1}{4}\left(x_2 - \frac{1}{I}x_3\right)^{p^k+1}$$

*Cf. L. E. DICKSON, Mathematische Annalen, vol. 52 (1899), pp. 561–581; also *Linear Groups*, Chap. V.

The locus of the points which are such that their coördinates satisfy this function equated to zero are the $p^{3k}+1$ centers of elations.

If p^k+1 is divisible by 3, a group exists containing the $HO(3, p^{2k})$ as a self-conjugate subgroup of index 3. It may be generated by the $HO(3, p^{2k})$ together with an homology of period p^k+1.

As follows from the unique choice of coördinates, there is a single conjugate set of $HO(3, p^{2k})$ under the whole collineation group.

We turn our attention again to the two groups of elations (E), and consider case (ii). If there is a group of elations with center on one of the axes through (100), and axis passing through the intersection of another one of those axes with $x_1=0$, the group on that axis must be of order $(p^k+1)p^k(p^k-1)$, since it contains a cyclic group of order p^k-1. Hence (100) will be conjugate with each of the p^k+1 centers of elations on $x_1=0$, since the fixed points of this cyclic group will be interchanged. Hence there will be at least p^k+1 axes of elations passing through each center. There can then be no centers not on any one of the p^k+1 axes through (100), since in that case we found that a polar configuration was determined. There will be p^k+1 centers on each of

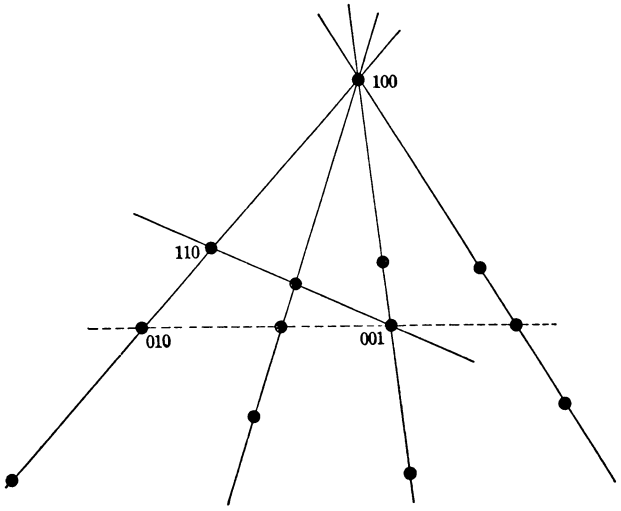

FIG. 9.

those p^k+1 axes, i. e., $p^{2k}+p^k+1$ in all. (Fig. 9 represents the configuration for $p^k=3$.)

If one of the centers on $x_3=0$ be (110), the $p^{2k}+p^k+1$ centers will be the points $(\alpha\beta\gamma)$, where α, β, γ lie in the $GF(p^k)$. The coefficients of the transformations in the group will then lie in the $GF(p^k)$. We consider first the groups containing only transformations the determinants of which are cubes in the $GF(p^k)$.

A group of elations with center (110) and axis passing through (001) will be given by

$$[(1+\lambda)x_1 - \lambda x_2,\ \lambda x_1 + (1-\lambda)x_2,\ x_3],$$

where λ takes all values in the $GF(p^k)$. Under the group generated by this group of elations together with the reflection with center (100) and axis $x_1 = 0$, (001) will remain invariant and there will be transformations interchanging (100) and (010). All six permutations will then be made on the vertices of the triangle (100)(010)(001). Hence there will be an homology of period $p^k - 1$ or $(p^k - 1)/2$ with center at each of the vertices (Theorem 3). But since if $p^k - 1$ is divisible by 3 the determinant of an homology of that period will not be a cube in the $GF(p^k)$, the period of the homology will be $(p^k - 1)/\mu$. (See Introduction.) The group of the points on any axis will be of order $(p^k + 1)p^k(p^k - 1)$, and consequently the group leaving (100) and $x_1 = 0$ fixed will be of order $(p^k + 1)p^k(p^k - 1)^2/\mu$. The group leaving fixed only (100) will be of order $(p^k + 1)p^{3k}(p^k - 1)^2/\mu$, and the whole group of order $(p^{2k} + p^k + 1)(p^k + 1)p^{3k}(p^k - 1)^2/\mu$. This is the $LF(3, p^k)$.*

If $p^k - 1$ is divisible by 3, a group exists containing the $LF(3, p^k)$ as a self-conjugate subgroup of index 3. It may be generated by the $LF(3, p^k)$ together with an homology of period $p^k - 1$.

§ 15. Subgroups of the Simple Groups $LF(3, p^k)$.

The subgroups of the $LF(3, p^k)$ are those groups which have been determined in this paper such that the coefficients of the transformations which they contain are in the $GF(p^k)$, and the determinant of any one of those transformations is a cube in that field, together with those subgroups which leave invariant a point, line, or triangle. There is a single conjugate set of each one of the groups under the whole collineation group of the plane. We suppose that the plane in which we are working is the $PG(2, p^k)$. If then the $LF(3, p^k)$ is the whole collineation group of the $PG(2, p^k)$, i. e., if $p^k - 1$ is not divisible by 3, there will be a single conjugate set of each subgroup; if $p^k - 1$ is divisible by 3, but a subgroup is invariant under a group of three times its order which is not a subgroup of the $LF(3, p^k)$, there will be also a single conjugate set of those subgroups; if however $p^k - 1$ is divisible by 3 and a subgroup is not invariant under a group which is not a subgroup of the $LF(3, p^k)$, then there will be three conjugate sets of those subgroups.

The subgroups are as follows:

1. Groups of order $(p^k + 1)p^{3k}(p^k - 1)^2/\mu$. Each of these groups leaves invariant a point and is isomorphic with a group of order $(p^k + 1)p^k(p^k - 1)$, permuting the lines through that point.

* Cf. L. E. Dickson, *Linear Groups*, pp. 75–78.

2. Groups of order $(p^k+1)p^{3k}(p^k-1)^2/\mu$. Each of these groups leaves invariant a line and is isomorphic with a group of order $(p^k+1)p^k(p^k-1)$, permuting the points on that line.

3. Groups of order $6(p^k-1)^2/\mu$. Each of these groups leaves invariant a triangle with coördinates in the $GF(p^k)$, and makes all six permutations on its vertices.

4. Groups of order $3(p^{2k}+p^k+1)/\mu$. Each of these groups leaves invariant a triangle with coördinates in the $GF(p^{3k})$, but not in the $GF(p^k)$, and permutes its vertices cyclically.

5. Groups of order $(p^k+1)p^k(p^k-1)$. Each such group leaves invariant a conic.

6. Groups of the same structure as that of the $LF(3, p^k)$ itself, i. e., the $LF(3, p^m)$, where m is a factor of k.

7. Groups containing the $LF(3, p^m)$ as self-conjugate subgroups of index 3 if p^m-1 is divisible by 3, and k/m is divisible by 3.

8. The hyperorthogonal groups, $HO(3, p^{2m})$, where $2m$ is a factor of k.

9. Groups containing the $HO(3, p^{2m})$ as self-conjugate subgroups of index 3 if p^m+1 is divisible by 3, and $k/2m$ is divisible by 3.

10. The Hessian groups of order 216 (if p^k-1 is divisible by 9), 72 and 36 (if p^k-1 is divisible by 3).

11. Groups of order 168, which exist if $\sqrt{-7}$ exists in the $GF(p^k)$, i. e., if k is even, or (by the law of quadratic reciprocity) if k is odd and $p=7$, $7f+1$, $7f+2$, or $7f+4$. For $p=7$ any one of these groups leaves invariant a conic.

12. Groups of order 360, which exist if both $\sqrt{5}$ and a cube root of unity exist in the $GF(p^k)$; i. e., if k is even, or if k is odd, provided $p=15f+1$ or $15f+4$. For $p=3$ any one of these groups leaves invariant a conic.

13. Groups of order 720 containing the groups of order 360 as self-conjugate subgroups. These exist only for $p=5$ and k even.

14. Groups of order 2520, each isomorphic with the alternating group on seven letters. These exist only for $p=5$ and k even.

Since the largest subgroup is of order $(p^k+1)p^{3k}(p^k-1)^2/\mu$, we have

Theorem 29. *The smallest number of letters on which the group, $LF(3, p^k)$, may be represented as a permutation group is $p^{2k}+p^k+1$.*

§ 16. Subgroups of the Simple Groups $HO(3, p^{2k})$.

The subgroups of the $HO(3, p^{2k})$ are those groups determined above which have an invariant conjugate with

$$x_1^{p^k+1}+x_2^{p^k+1}+x_3^{p^k+1}=0,$$

together with the subgroups which leave invariant a point, line, or triangle. Each set of subgroups forms a single conjugate set provided the $HO(3, p^{2k})$ is invariant under no larger group under the whole collineation group of the plane, i. e., if $p^k + 1$ is not divisible by 3. If $p^k + 1$ is divisible by 3, each set of subgroups will form a single conjugate set if any one of them is invariant under a group of three times its order which is a subgroup of the group under which the $HO(3, p^{2k})$ is invariant but not of the $HO(3, p^{2k})$ itself; otherwise there will be three conjugate sets.

The subgroups are as follows:

1. Groups of order $(p^k + 1)p^{3k}(p^k - 1)/\nu$. Any such group leaves invariant the center and axis of a group of elations and is isomorphic with a metacyclic group on the axis of order $(p^{2k} - 1)p^{2k}/\nu$.

2. Groups of order $(p^k + 1)^2 p^k (p^k - 1)/\nu$. Any such group leaves invariant the center and axis of an homology and is isomorphic with the group of the points on the axis, which is of order $(p^k + 1)p^k(p^k - 1)$.

3. Groups of order $6(p^k + 1)^2/\nu$. Any such group leaves invariant a triangle whose coördinates are in the $GF(p^{2k})$ and makes all six permutations on its vertices.

4. Groups of order $3(p^{2k} - p^k + 1)/\nu$. Any such group leaves invariant a triangle whose coördinates lie in the $GF(p^{6k})$, but not in the $GF(p^{2k})$, and permutes its vertices cyclically.

5. Groups of order $(p^k + 1)p^k(p^k - 1)$. Any such group leaves invariant a conic.

6. The hyperorthogonal groups, $HO(3, p^{2m})$, where m is a factor of k and k/m is odd.

7. Groups containing the $HO(3, p^{2m})$ as self-conjugate subgroups of index 3 if $p^m + 1$ is divisible by 3 and k/m is odd and is divisible by 3.

8. The Hessian groups of order 216 (if $p^k + 1$ is divisible by 9), 72 and 36 (if $p^k + 1$ is divisible by 3).

9. Groups of order 168, which exist if $\sqrt{-7}$ does not exist in $GF(p^k)$, i. e., if k is odd and $p = 7f + 3$, $7f + 5$, or $7f + 6$. For $p = 7$ these groups also appear, but each leaves invariant a conic.

10. Groups of order 360, which exist if $\sqrt{5}$ exists and a cube root of unity does not exist in the $GF(p^k)$, i. e., if k is odd and $p = 5$, $15f - 1$, or $15f - 4$. If k is even and $p = 3$ these groups also appear, but in that case each leaves invariant a conic.

11. Groups of order 720, which exist if $p = 5$ and k is odd.

12. Groups of order 2520, which exist if $p = 5$ and k is odd.

The largest subgroup of the $HO(3, p^{2k})$ is of order $(p^k + 1)p^{3k}(p^k - 1)/\nu$, except for $p^k = 5$, in which case the largest subgroup is of order 2520. Hence we have

Theorem 30. *The smallest number of letters on which the group* $HO(3, p^{2k})$ *may be represented as a permutation group is* $p^{3k}+1$, *except for* $p^k = 5$, *in which case the smallest number is* 50.

That the $HO(3, p^{2k})$ can be represented as a permutation group on $p^{3k}+1$ letters has been shown by Dickson (Mathematische Annalen, vol. 55, p. 532). Similar results are obtained by him in that paper for the general hyperorthogonal group in m variables.

NEW HAVEN, CONN.,
September, 1910.