FINITE PROJECTIVE GEOMETRIES*

BY

OSWALD VEBLEN AND W. H. BUSSEY

By means of such a generalized conception of geometry as is inevitably suggested by the recent and wide-spread researches in the foundations of that science, there is given in § 1 a definition of a class of tactical configurations which includes many well known configurations as well as many new ones. In § 2 there is developed a method for the construction of these configurations which is proved to furnish all configurations that satisfy the definition. In §§ 4–8 the configurations are shown to have a geometrical theory identical in most of its general theorems with ordinary projective geometry and thus to afford a treatment of finite linear group theory analogous to the ordinary theory of collineations. In § 9 reference is made to other definitions of some of the configurations included in the class defined in § 1.

§ 1. *Synthetic definition.*

By a finite projective geometry is meant a set of elements which, for suggestiveness, are called points, subject to the following five conditions:

I. *The set contains a finite number* (> 2) *of points. It contains subsets called lines, each of which contains at least three points.*

II. *If A and B are distinct points, there is one and only one line that contains A and B.*

III. *If A, B, C are non-collinear points and if a line l contains a point D of the line AB and a point E of the line BC, but does not contain A, B, or C, then the line l contains a point F of the line CA* (Fig. 1).†

A plane ABC (A, B, C being non-collinear points) is defined as the set of all points collinear with a point A and any point of the line BC. It may be proved by III that a plane so defined has the usual projective properties. For example, a plane is uniquely determined by any three of its points which are non-collinear, and the line joining any two points of a plane is contained wholly in the plane.

A k-space is defined by the following inductive definition. *A point is a* 0-*space. If A_1, A_2, $\cdots$, A_{k+1} are points not all in the same* ($k-1$)-*space, the*

*Presented to the Society April 22, 1905. Received for publication November 20, 1905.

†The figures used in this paper are not to be considered as having the properties which they have in ordinary euclidean geometry, unless such properties follow from the explicitly stated hypotheses.

set of all points collinear with the point A_{k+1} *and any point of the* $(k-1)$-*space* $(A_1, A_2, \cdots, A_k)$ *is the k-space* $(A_1, A_2, \cdots, A_{k+1})$. Thus a line is a

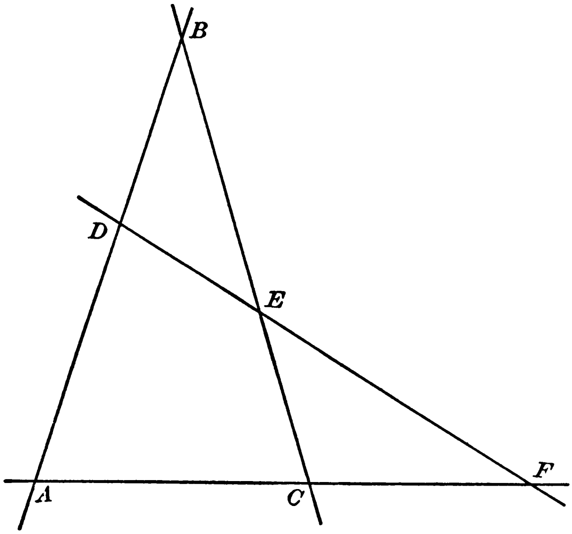
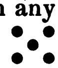


FIG. 1.

1-space, and a plane is a 2-space. From this definition it can be proved that spaces (if existent) satisfy the following well known theorem.

In a k-space, an l-space and an m-space have a point in common if $l + m \geqq k$. *They have in common at least an r-space if* $l + m - k = r$.

Remark: It is very convenient in practice to replace this theorem by a diagram consisting of $(k+1)$-points, of which any $l+1$ $(l \leqq k)$ represent an l-space. Thus in a 4-space, using the diagram , it is evident that any two 3-spaces (each being a set of 4 points) have in common a plane (three points). This scheme gives a finite geometry satisfying all the projective geometry axioms except those implying that a line contains more than two points.

The existence of the various spaces is postulated by the two conditions IV_k and V_k. (Axioms of extension and closure.)

IV_k. *If l is an integer less than k, not all of the points considered are contained in the same l-space.*

V_k. *If* IV_k *is satisfied, there exists in the set of points considered no* $(k+1)$-*space.*

The well known *principle of duality* follows from the axioms and definitions as given. Special cases of the principle are the following:

Any proposition (deducible from $I - V_k$*) about points and lines in a plane is valid if the words point and line be interchanged.*

Any proposition (deducible from $I - V_k$*) about points, lines, and planes in 3-space is valid if the words point and plane be interchanged.*

Let $s+1$ denote the number of points in a line. To obtain the number of points in a plane consider a line l and a point L not in l. L and each point of l determine a line in each of which there are s points in addition to the point L. Furthermore, every point of the plane is in one of these $s+1$ lines containing L. Therefore the number of points in the plane is s^2+s+1. By the principle of duality the number of lines in the plane is also s^2+s+1. In like manner the number of points in 3-space may be found to be s^3+s^2+s+1 and the number of points in k-space to be $s^k+s^{k-1}+\cdots+s+1$.

The simplest example of a finite geometry which satisfies the definition for $k=2$ is the well known triple system

0	1	2	3	4	5	6
1	2	3	4	5	6	0
3	4	5	6	0	1	2

which consists of 7 points arranged in 7 lines of 3 points each. A finite plane geometry of 13 points arranged in 13 lines of 4 points each is the following:

0	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	0
3	4	5	6	7	8	9	10	11	12	0	1	2
9	10	11	12	0	1	2	3	4	5	6	7	8

For some purposes it is convenient to have the finite geometry exhibited in a table as follows:

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	x				x						x		x
1	x	x				x						x	
2		x	x				x						x
3	x		x	x				x					
4		x		x	x				x				
5			x		x	x				x			
6				x		x	x				x		
7					x		x	x				x	
8						x		x	x				x
9	x						x		x	x			
10		x						x		x	x		
11			x						x		x	x	
12				x						x		x	x

In this table the incidence of a line h and a point k is indicated by a mark x in the column h and the row k. The table shows at a glance the 4 points of a line and the 4 lines containing a point.

An example of a finite plane geometry having 5 points in a line may be found on p. 305 of vol. 5 of these Transactions.

§ 2. *Analytic definition.*

If $x_1, x_2, \cdots, x_{k+1}$ are marks of a Galois field* of order $s = p^n$, there are $(s^{k+1}-1)/(s-1) = s^k + s^{k-1} + \cdots + s + 1$ elements of the form $(x_1, x_2, \cdots, x_{k+1})$, provided that the elements $(x_1, x_2, \cdots, x_{k+1})$ and $(lx_1, lx_2, \cdots, lx_{k+1})$ are thought of as the same element when l is any mark $\neq 0$, and provided that the element $(0, 0, \cdots, 0)$ is excluded from consideration. These elements constitute a finite projective geometry of k-dimensions when arranged according to the following scheme. The equation

$$u_1 x_1 + u_2 x_2 + \cdots + u_{k+1} x_{k+1} = 0 \tag{1}$$

(the domain for coefficients and variables being the $GF[s]$) is said to be the equation of a $(k-1)$-space except when $u_1 = u_2 = \cdots = u_{k+1} = 0$. It is denoted by the symbol $(u_1, u_2, \cdots, u_{k+1})$. The symbols $(u_1, u_2, \cdots, u_{k+1})$ and $(lu_1, lu_2, \cdots, lu_{k+1})$, l being any mark $\neq 0$, denote the same $(k-1)$-space. The points of the $(k-1)$-space are those points of the finite geometry which satisfy its equation. A $(k-2)$-space is represented by two equations of type (1) and a $(k-l)$-space by l equations of type (1). There are $s^l + s^{l-1} + \cdots + s + 1$ points in l-space and, in particular, $s+1$ points in a line.

The finite projective k-dimensional geometry, obtained in this way from the $GF[s]$, is denoted by the symbol $PG(k, s)$. Since there is a Galois field of order s for every s of the form $s = p^n$, it follows that there is a $PG(k, p^n)$ for every pair of integers k and n and for every prime p. It will be proved in § 4 that every finite projective k-dimensional geometry satisfying the definition of § 1 is a $PG(k, p^n)$ if $k > 2$.

§ 3. *The modulus* 2.

The method used in § 2 to obtain the $PG(k, s)$ from the $GF[s]$ may be described as *analytic geometry in a finite field.* It may be applied to any field of finite order $s = p^n$, but here as elsewhere the modulus 2 gives rise to an exceptional case. Let the symbols 1, 3, 4, 5 denote the four vertices of a complete quadrangle (Fig. 2) in the $PG(2, p^n)$. Let the three pairs of opposite sides

* For the definition and properties of a Galois field see E. H. Moore, *Mathematical Papers, Chicago Congress of* 1893, pp. 210–226 ; L. E. Dickson, *Linear Groups*, pp. 1–14. For Galois field tables for $p^n \leqq 169$, $n > 1$ see W. H. Bussey, Bulletin of the American Mathematical Society, vol. 12 (1905–06), pp. 22–38.

meet as follows: 1 3 and 4 5 in a point 0, 1 4 and 3 5 in a point 2, and 1 5 and 3 4 in a point 6. Let the equations of the lines 1 5, 4 5, 3 4 be, respectively, $\alpha = 0$, $\beta = 0$, $\gamma = 0$ (abridged notation). As in SALMON's *Conic Sections* (10th edition), p. 57, Ex. 1, the equations of the lines 0 6 and 2 6 may be found to be, respectively, $l\alpha + n\gamma = 0$ and $l\alpha - n\gamma = 0$, l and n being marks of the

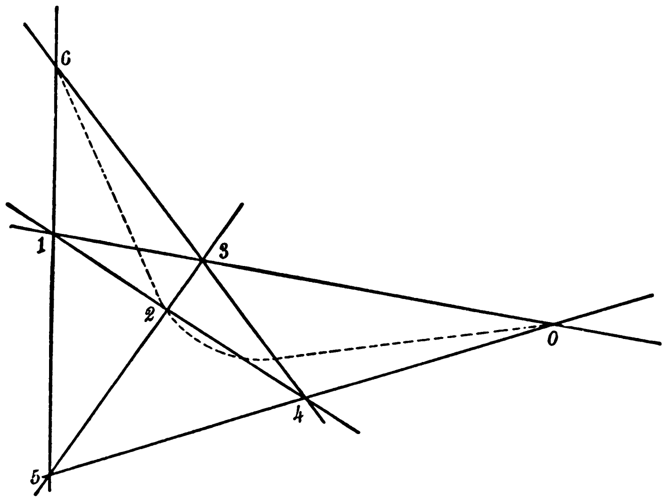


FIG. 2.

$GF[p^n]$. If the modulus of the field is 2, $n\gamma = -n\gamma$, and the lines 0 6 and 2 6 coincide, i. e., the diagonal points of the quadrangle are collinear. This does not happen if $p > 2$. It will be observed that the figure of the complete quadrangle in a geometry having the modulus 2 [i. e., in a $PG(k, 2^n)$] is thus proved to be identical with the triple system in 7 elements given in § 1.

To exclude from consideration the case of the modulus 2 it is therefore sufficient to add the following condition VI to those of the synthetic definition of § 1.

VI. *The diagonal points of a complete quadrangle are not collinear.*

In the following paragraphs, VI is not assumed unless it is so stated in the text.

§ 4. *General synthetic theory.*

The elementary part of the synthetic theory follows from conditions I–V quite independently of the hypothesis that the number of points is finite. If a certain further hypothesis is added, it is possible to develope * large parts of the theory

*The deduction from hypotheses I–VII of a portion of the usual projective geometry, corresponding in a general way to Part I of REYE's *Geometrie der Lage* was carried out in detail by O. VEBLEN in a course of lectures delivered at the University of Chicago during the winter quarter, 1905. Mimeographed reports (referred to below as *Notes*) of these lectures as worked out by Mr. N. J. LENNES and other members of the class are on file in the mathematical library of the University of Chicago.

of collineations, conic sections, quadric surfaces, and algebraic curves and surfaces in general, without deciding whether the number of points is finite or not. This further hypothesis may be stated in the form:

VII. *Let A, B, C be three collinear points, and let A', B', C' be three other collinear points not on the same line. If the pairs of lines AB' and $A'B$, BC' and $B'C$, CA' and $C'A$ intersect, the three points of intersection are collinear.**

This hypothesis VII is a consequence of the hypothesis that the number of points is finite whenever the geometry considered is of three or more dimensions. The proof of this statement is in outline as follows: From hypotheses I–IV follows the DESARGUES theorem about perspective triangles: *If two triangles*

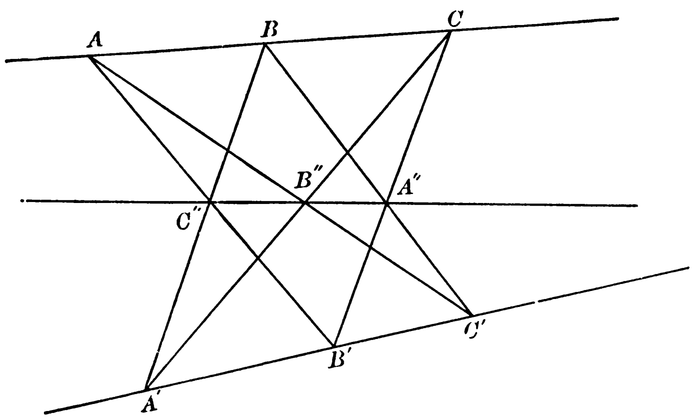


FIG. 3.

ABC and $A'B'C'$ are in the same plane and if the lines AA', BB', CC' are concurrent, the lines AB and $A'B'$, BC and $B'C'$, CA and $C'A'$ intersect in points which are collinear. This is proved on page 29 of the *Notes* referred to above, and by means of this theorem there is developed on pp. 73–84 a geometric algebra for the points of a line.† It is proved that this algebra satisfies all the conditions for a field except the commutative law of multiplication. In particular the algebra is such that for every element a there is a unique element a' such that $a'a = 1 = aa'$. For such an algebra it has been shown by J. H. MACLAGAN-WEDDERBURN ‡ that the commutative law holds whenever

* The configuration involved here is known as the configuration of PAPPUS (Fig. 3). It may be described as a simple hexagon $AB'CA'BC'$ inscribed in two lines. Hypothesis VII is to the effect that the three pairs of opposite sides intersect, if at all, in three collinear points A'', B'', C''. HILBERT speaks of VII as *Pascal's theorem*. It is, of course, a degenerate case of the well-known theorem of PASCAL on a hexagon inscribed in a conic.

† Other developments of a geometric algebra practically equivalent to this one are given by G. HESSENBERG, Acta Mathematica, vol. 29 (1905), pp. 1–24, and by K. TH. VAHLEN, *Abstrakte Geometrie*, p. 110.

‡ *A theorem on finite algebras*, Transactions of the American Mathematical Society, vol. 6 (1905), p. 349.

the number of points is finite. On the other hand, it has been shown by HILBERT* (and it is shown by another method in the *Notes* referred to) that the commutative law of multiplication is equivalent to hypothesis VII. Therefore, if the number of points is finite, condition VII is satisfied.

By means of the algebra of points there may be built in the finite geometry defined by hypotheses I–VI a homogeneous analytic geometry of k dimensions in every case in which $k > 2$ (see pp. 82–84 of the *Notes*), and, since the algebra of points is abstractly identical with a Galois field, the analytic geometry so obtained is identical with that described in § 2. This proves that for a given $k > 2$, p and n there is one and only one finite projective geometry as defined in § 1 and that it is the $PG(k, p^n)$. (Cf. end of § 2.)

The essential difference in the case $k = 2$, i. e., in the case of plane geometry, is due to the fact that there exist finite non-desarguesian plane geometries.† The Desargues theorem about perspective triangles in a plane implies that the plane may be thought of as immersed in a 3-space. From this it follows that for a given p^n there is one and only one finite plane desarguesian geometry, viz., the $PG(2, p^n)$.

§ 5. *The Möbius net.*

On the line $x_1 = 0$, any point except (010) may be represented by a single coördinate, the value of x_2 when $x_3 = 1$. The point (010) may be represented

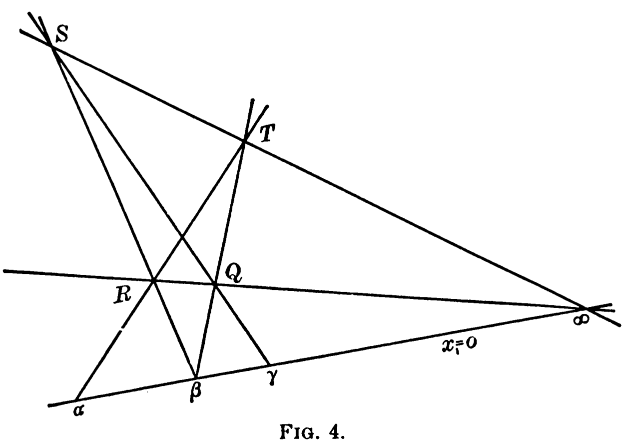


FIG. 4.

by the coördinate ∞. Let α and β be the coördinates of two points of the line. The harmonic conjugate of α with respect to β and ∞ may be constructed by the usual quadrangle construction as follows. Let S and T be any two points on a line through the point ∞. Let the lines $S\beta$ and $T\alpha$ meet in

* D. HILBERT, *Grundlagen der Geometrie*, chap. 6.

† Cf. *Non-desarguesian and non-pascalian geometries*, by J. H. MACLAGAN-WEDDERBURN and O. VEBLEN. This paper was read at the April (1905) meeting of the Chicago section but has not yet been published.

a point R. Let the lines $T\beta$ and $R\infty$ meet in a point Q. The line SQ meets the line $x_1 = 0$ in the required point γ (Fig. 4). If the line $ST\infty$ is chosen as the line $x_3 = 0$ and if S and T be chosen as the points $(\lambda 10)$ and (100) respectively, the equation of the line SQ may be proved to be $x_1 - \lambda x_2 + \lambda(2\beta - \alpha)x_3 = 0$. The point of intersection of the line SQ and the line $x_1 = 0$ is therefore $\gamma = 2\beta - \alpha$.

The well-known Möbius net * is determined by any three points of a line. If the three points be chosen as the points A_1, A_2, ∞ of the line $x_1 = 0$ (Fig. 5), the fourth point A_3 is determined as the harmonic conjugate of A_1 with respect to A_2 and ∞; A_4 is the harmonic conjugate of A_2 with respect to A_3 and ∞;

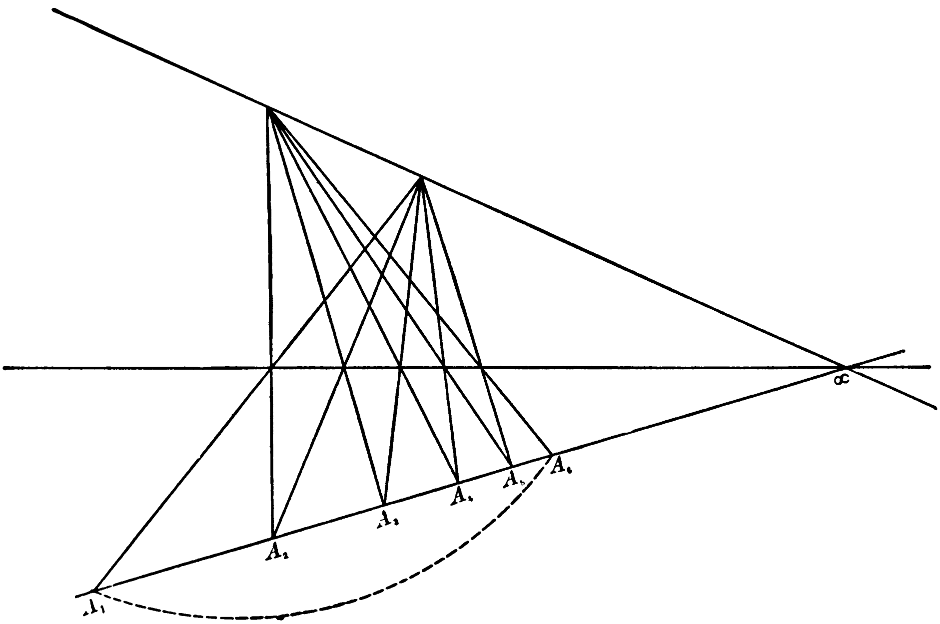


FIG. 5.

A_k is the harmonic conjugate of A_{k-2} with respect to A_{k-1} and ∞. The word net is used to denote the set of points A_1, A_2, $A_3 \cdots \infty$ and not to denote the whole figure.

Let the coördinate of the point A_1 be α and that of A_2 be $\alpha + 1$. Since the harmonic conjugate of a point α with respect to the points β and ∞ is the point $2\beta - \alpha$, the points of the net are α, $\alpha + 1$, $\alpha + 2$, $\cdots$, ∞. Since the modulus of the field is p, the series α, $\alpha + 1$, $\alpha + 2$, $\cdots$ consists of the p marks $\alpha, \alpha + 1, \alpha + 2, \cdots, \alpha + p - 1$. The $(p + 1)$-st mark is again α, i. e., the series repeats itself periodically. Fig. 5 is drawn for the case $p = 5$. The

* KLEIN, *Nicht-Euclidishe Geometrie*, vol. 1, p. 338 ff. MÖBIUS, *Gesammelte Werke*, vol. 1, p. 237 ff.

point A_6 is to be thought of as coincident with the point A_1. This proves that a finite projective geometry cannot be represented by a figure in ordinary geometry in which a line of the finite geometry consists of a finite set of points on a line of ordinary geometry.

As in ordinary projective geometry it can be proved that any set of three collinear points may be projected into any other set of three collinear points. Therefore any two Möbius nets are projective and the number of points in any net in any line is $p+1$. A net is determined by any three of its points. The p^n+1 points of a line may be arranged in p^{n-1} nets of $p+1$ points each, all of the nets having a point in common.

A collineation is defined as a point transformation by which lines are transformed into lines. A collineation transforms four harmonic points into four harmonic points because it transforms a complete quadrangle into a complete quadrangle. Therefore, if a collineation leaves three points of a net fixed, it leaves the whole net fixed point by point. In the $PG(k, p)$ there are but $p+1$ points in a line, i. e., the points of a line constitute a single net. Therefore a collineation which leaves three points of a line fixed leaves the whole line fixed point by point. Therefore any collineation, other than the identity, has at most two fixed points in a line; in a plane it has at most three non-collinear fixed points; and in a k-space it has at most $k+1$ fixed points if no k of them are in the same $(k-1)$-space. In the $PG(k, p^2)$ a collineation may have more than three fixed points in a line, because when three points of the line are fixed only one net of the line is necessarily fixed point by point. The number of fixed points in this case is discussed below. The situation here is analogous to that in ordinary complex projective geometry. The nets correspond in their definition and properties to VON STAUDT's* chains, i. e., to circles if the chains be represented in the complex plane. Any three points of a line in the $PG(k, p^2)$ determine a net or, as it is now to be called, a chain. Let α be a chain, and let P be a point of the line but not of the chain α. Let A be a point of the chain α. If X be any other point of α, the three points P, X, A determine one and only one chain. Since X may be chosen as any one of the $p+1$ points of α other than the point A, there are at least p chains containing P and A. The total number of points in these p chains is equal to $p(p-1)+2=p^2-p+2$. The number of points of the line which are not contained in any of these chains is therefore $(p^2+1)-(p^2+p+2)=p-1$. Let β be the chain determined by P, A, and any one of these $p-1$ points. Since β cannot contain any other point of any of the p chains through P and A, it must contain all of the above mentioned $p-1$ points. The chains α and β, therefore, have one and only one point in common and are said to be tangent to each other. We have thus proved that through a given point P of the line

* v. STAUDT, *Beiträge zur Geometrie der Lage*, p. 137.

there is one and only one chain tangent to a given chain α. The system of all chains having in common a given point of the line affords, if the given point be excluded, a system of sets of p points each such that no two sets have more than one point in common and such that any two points of the line determine one of the sets. Moreover, containing a given point of the line, there is one and only one set β which has no point in common with a given set α. Thus there is defined a set of points and subsets of it entirely analogous in their intersectional properties to the lines of the ordinary euclidean plane. It is also analogous to the system of circles through a fixed point of the ordinary complex plane. The system of all chains of a line is of course analogous to the system of all circles and straight lines in a plane.*

If a collineation leaves fixed, point by point, a chain α and a point P not in α, it must be the identity because through every other point of the line there passes at least one chain which contains P and two points of α, i. e., every other point of the line is contained in at least one chain of which three points are fixed. Therefore a collineation in the $PG(k, p^2)$ may have more than two fixed points on a line but not so many as four unless they are contained in the same chain.

In the $PG(k, p^n)$, the chains of a line constitute a configuration analogous to the set of all circles in n-dimensional space. Any four points of the line, if they are not all contained in the same chain, determine a 2-chain, a configuration analogous to a sphere. Any five points, if they are not all contained in the same 2-chain, determine a 3-chain, a configuration analogous to a hypersphere;† and any $(l+1)$ points $(l \leqq n)$, if they are not contained in the same $(l-2)$-chain, determine an $(l-1)$-chain, a configuration analogous to an $(l-1)$-sphere. A collineation can have as fixed points at most $n+1$ points not all contained in the same $(n-1)$-chain. If $n+2$ points, no $n+1$ of which are in the same $(n-1)$-chain, are fixed, the collineation is the identity.

§ 6. *Collineation groups in the* $PG(k, p^n)$.

The collineation group of the $PG(k, p^n)$ is defined as the group of all collineations in the $PG(k, p^n)$. In § 5, it has been proved for the $PG(k, p)$ that a collineation of a line may have at most two fixed points. As in ordinary projective geometry, it can be proved for the $PG(k, p)$ that there is a collineation determined by any three points of the line, i. e., there is one and only one collineation that transforms a given set of three points into another given set of three points. In like manner it can be proved that there is one and only one collineation of a plane determined by any four points no three of which are in the same line, and that one and only one collineation of an l-space is determined by any $l+2$ points no $l+1$ of which are in the same $(l-1)$-space.

* Cf. another definition of such a configuration in § 9.

† A circle is a 1-sphere, a sphere is a 2-sphere, etc.

Let A, B, C be three points of a line. By a collineation, A may be transformed into any point A' of the line (A' may be chosen in $p+1$ ways); B may then be transformed into any point B' other than A' (B' may be chosen in p ways); and C may be transformed into any point C' other than A' and B' (C' may chosen in $p-1$ ways). The collineation is then completely determined, and the order of the collineation group of the line is seen to be $(p+1)p(p-1)=p(p^2-1)$.

Let A and B be two points of a plane. Let σ_2 denote the number of points in the plane and let σ_1 denote the number of points on a line. By a collineation, A may be transformed into any point A' of the plane (A' need not be different from A and may therefore be chosen in σ_2 ways); B may be then transformed into any point B' other than A' (B' may be chosen in σ_2-1 ways); any other point C of the line AB may then be transformed into a point C' of the line $A'B'$(C' may be chosen in $p-1$ ways because $\sigma_1=p+1$); any point D not on the line AB may then be transformed into any point D' not on the line $A'B'$(D' may be chosen in $\sigma_2-\sigma_1$ ways), and finally any point E, other than A and D of the line AD, may be transformed into any point E', other than A' and D', of the line $A'D'$(E' may be chosen in $p-1$ ways). The collineation is then completely determined, and the order of the collineation group of the plane is the product of the factors which represent the number of choices at the successive stages of the determination of the collineation, i. e., the order is $\sigma_2(\sigma_2-1)(p-1)\cdot(\sigma_2-\sigma_1)(p-1)$.

In like manner it may be seen that the order of the collineation group of k-space is

$$N=\sigma_k(\sigma_k-1)(p-1)\cdot(\sigma_k-\sigma_1)(p-1)\cdot(\sigma_k-\sigma_2)(p-1)\cdots(\sigma_k-\sigma_{k-1})(p-1),$$

where $\sigma_k=p^k+p^{k-1}+\cdots+p+1=(p^{k+1}-1)/(p-1)$, the number of points in k-space ($\sigma_0=1$). The expression for N may be written

$$N=(p-1)^k\sigma_k\prod_{j=0}^{k-1}(\sigma_k-\sigma_j).$$

Substitute the values for σ_k and σ_j, as indicated above, and the expression becomes

$$N=(p-1)^k\left(\frac{p^{k+1}-1}{p-1}\right)\prod_{j=0}^{k-1}\left[\frac{p^{k+1}-p^{j+1}}{p-1}\right]$$

$$=\frac{(p^{k+1}-1)\prod_{i=1}^{k}(p^{k+1}-p^i)}{p-1}=\frac{1}{p-1}\prod_{i=0}^{k}(p^{k+1}-p^i).$$

But this is exactly the order * of the group $LF(k+1,p)$ of all linear fractional transformations on k variables having coefficients in the $GF[p]$, and having determinant not zero.

* L. E. DICKSON, *Linear Groups*, p. 87.

Therefore, by observing that every transformation of the group is a collineation, it is proved that the group $LF(k+1, p)$ is the collineation group of the $PG(k, p)$.

The collineation group of the $PG(k, p^n)$, $n > 1$, is not linear.* It will be sufficient to show this in detail for the case of the plane. The equation of a line in the $PG(2, p^n)$ is

$$(0) \qquad a_1x_1 + a_2x_2 + a_3x_3 = 0\,.$$

The result of raising this equation to the power p^k is

$$(k) \qquad a_1^{p^k}x_1^{p^k} + a_2^{p^k}x_2^{p^k} + a_3^{p^k}x_3^{p^k} = 0\,.$$

This equation contains only three terms because every other term in the expansion has a coefficient which is a multiple of p and is therefore congruent to zero modulo p. Conversely, the result of raising equation (k) to the power p^{n-k} is equation (0) because $\rho^{p^n} = \rho$ if ρ is any mark of the $GF[p^n]$. Therefore equations (0) and (k) represent the same line or, in other words, any line may be represented by any one of the n equations (k), $(k = 0, 1, \cdots, n-1)$, $n-1$ of which are not linear. Moreover, any equation of the form

$$(1) \qquad a_1x_1^{p^k} + a_2x_2^{p^k} + a_3x_3^{p^k} = 0$$

represents a line since it becomes linear upon being raised to the power p^{n-k}. The transformation

$$(A_k): \qquad \begin{cases} \dfrac{x_1'}{x_3'} = \dfrac{a_1x_1^{p^k} + b_1x_2^{p^k} + c_1x_3^{p^k}}{a_3x_1^{p^k} + b_3x_2^{p^k} + c_3x_3^{p^k}}, \\[2ex] \dfrac{x_2'}{x_3'} = \dfrac{a_2x_1^{p^k} + b_2x_2^{p^k} + c_2x_3^{p^k}}{a_3x_1^{p^k} + b_3x_2^{p^k} + c_3x_3^{p^k}}, \end{cases}$$

is a collineation because it transforms any equation of type (1) into another of type (1). It is therefore evident that the group of all collineations in the $PG(k, p^n)$, $n > 1$, is not the linear fractional group. The group of all collineations is not further considered in this paper.

§ 7. *Linear groups.*

To define synthetically, in the $PG(k, p^n)$, the group $LF(k+1, p^n)$,† $n>1$, it is necessary to make use of the fact that condition VII, which is a valid proposition in the $PG(k, p^n)$, is equivalent to the following form of the fun-

* This is analogous to the fact that the collineation group is not linear in ordinary complex projective geometry.

† This symbol is used in this paper to denote the group of linear fractional transformations having determinant $\neq 0$ although DICKSON, in his *Linear Groups*, uses it for the group of linear fractional transformations of determinant unity.

damental theorem of projective geometry.* *If four collinear points* A, B, C, D *are transformed by a finite number of projections and sections into four points* A_1, B_1, C_1, D_1, *then, if by any finite number of projections and sections* A, B, C, D *are transformed into* A_1, B_1, C_1, D_1', D_1' *cannot be different from* D_1. This proposition should be carefully distinguished from the stronger form of the fundamental theorem which holds in the $PG(k, p)$ and in ordinary real projective geometry, namely, *Any transformation of points into points and lines into lines which transforms any set of four harmonic points into four harmonic points leaves a line* l *invariant point by point if three points of* l *are fixed.* The weak form is the one which holds in ordinary complex projective geometry.

A projective collineation is defined as a collineation such that, if four collinear points are transformed into four collinear points, the transformation can be effected by a finite number of projections and sections. The group of all such transformations is called the projective group of the $PG(k, p^n)$. The order of this group may be counted by the method used in § 6 for the collineation group of the $PG(k, p)$. The result is the same except that in the present case p^n replaces p. The order is $[1/(s-1)]\prod_{i=0}^{k}(s^{k+1}-s^i)$, where $s=p^n$. This is exactly the order of the group $LF(k+1, p^n)$† of all linear fractional transformations on k variables having coefficients in the $GF[p^n]$ and having determinant not zero.

To prove that the group $LF(k+1, p^n)$ is the projective group of the $PG(k, p^n)$ it is now sufficient to prove that every such linear fractional transformation is projective. Let A, B, C, D be four collinear points and let A, B', C', D' be four collinear points on another line through A. It is to be proved that the linear fractional transformation which transforms A, B, C, D into A, B', C', D' is a projective transformation, i. e., that the lines BB' and CC' meet on the line DD'. To prove this, the points A, D, D' (Fig. 6) are taken as the points (001), (010), (100), i. e., the triangle ADD' is taken as the fundamental triangle of the coördinate system. B and C are taken as $(01b)$ and $(01c)$, any two points of the line $x_1=0$. B' and C' are taken as $(10b')$ and $(10c')$ of the line $x_2=0$. The most general transformation of the group $LF(3, p^n)$ which transforms the line AD into the line AD' leaving the point A fixed and transforming B into B' and D into D' is easily determined to be

$$\frac{x_1'}{x_3'}=\frac{lx_1+bx_2}{nx_1+b'x_3}, \qquad \frac{x_2'}{x_3'}=\frac{mx_1}{nx_1+b'x_3},$$

l, m, n being arbitrary marks of the field. This transformation converts the

* F. Schur, Mathematische Annalen, vol. 51 (1898), p. 401. Also cf. *Notes*, p. 71.

† L. E. Dickson, *Linear Groups*, p. 87.

point $(01c)$ into the point $(1, 0, b'c/b)$, i. e., c' is determined to be $c' = b'c/b$. The equations of the lines BB' and CC' are now found to be, respectively, $b'x_1 + bx_2 - x_3 = 0$ and $b'cx_1 + bcx_2 - bx_3 = 0$. The point of intersection of

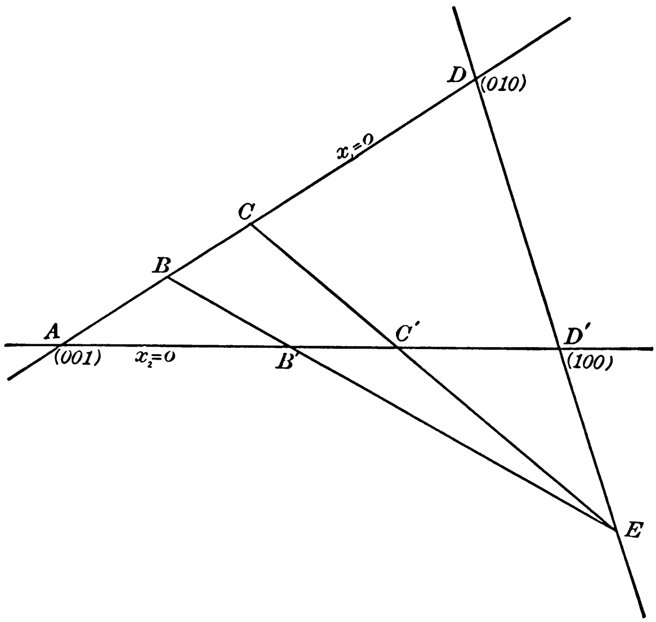


FIG. 6.

these two lines is the point E whose coördinates are $(b - b', 0)$. E is a point of the line $x_3 = 0$, i. e., of the line DD'. Since the points $ABCD$ are projective with the points A, B', C', D' from the center of projection E, the linear fractional transformation of A, B, C, D into A, B', C', D' is a projective transformation.

Having proved that the linear fractional transformation of four collinear points A, B, C, D into the four collinear points A, B', C', D' ($B'C'D'$ being any three points on any second line through A) is a projective transformation, we now observe that the linear fractional transformation of four collinear points A, B, C, D into four collinear points may be regarded as the product of two projective linear fractional transformations of the kind just considered (Fig. 7). The points A, B, C, D are first transformed into A, B', C', D_1, four points of the line AD_1, and these points are then transformed into A_1, B_1, C_1, D_1 of the given line through D_1.

It has now been proved that the group $LF(k+1, p^n)$ is the projective group of the $PG(k, p^n)$. This projective group is the sub-group (A_0) of the group (A_k) given in the last part of § 6. In the $PG(k, p)$, i. e., when

$n = 1$, the group (A_k) consists only of the transformations A_0, and the projective group is the same as the collineation group.

The $PG(k, p^n)$ may now be regarded as a defining invariant for the group $LF(k+1, p^n)$, (under projective transformations of course, although when $n = 1$ this is the same as saying under collineations). If there be left off from the $PG(k, s)$, $s = p^n$, the points of a single $PG(k-1, s)$, there will remain

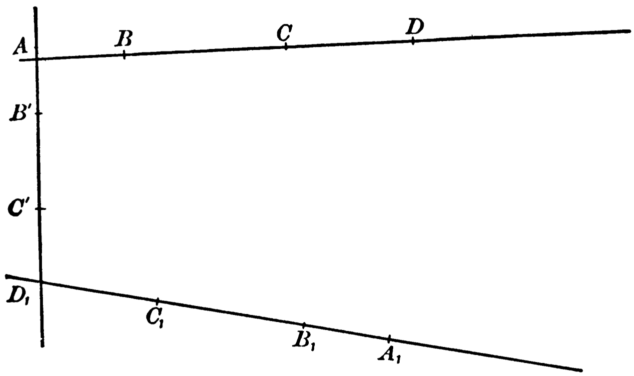


FIG. 7.

a configuration analogous to ordinary euclidean k-space. It is denoted by the symbol $EG(k, s)$. The $PG(k, s)$ may be thought of as arranged in $(s^{k+1}-1)/(s-1)$ geometries of the type $PG(k-1, s)$. The leaving off of the single $PG(k-1, s)$ takes from each remaining $PG(k-1, s)$ a single $PG(k-2, s)$. This leaves as the $EG(k, s)$ a configuration consisting of s^k points arranged in

$$\frac{s^{k+1}-1}{s-1} - 1 = \frac{s(s^k-1)}{s-1}$$

sets of s^{k-1} points each, each set being an $EG(k-1, s)$. Let $x_{k+1} = 0$ be the equation of the $PG(k-1, s)$ which was left off. The subgroup of the $LF(k+1, s)$, consisting of those transformations which leave invariant the $PG(k-1, s)$ whose equation is $x_{k+1} = 0$, is the linear group, $L(k, s)$, in k variables. It may be thought of as the group for which the $EG(k, s)$ is a defining invariant (under projective transformations, of course). The subgroup of the linear group $L(k, s)$, consisting of those transformations which leave invariant the origin of coördinates, is the general linear homogeneous group $GLH(k, s)$ in k variables. The configuration which is a defining invariant for this group is the configuration obtained by leaving off from the $EG(k, s)$ a single point and every $EG(k-1, s)$ containing it.

§ 8. *Second degree loci.*

A *point conic* is defined as the locus of the point of intersection of corresponding lines of two projective pencils of lines. A *line conic* is defined as consisting of the lines that join corresponding points of two projective ranges of points. If a tangent to a point conic be defined as a line that has one and only one point in common with the point conic, it can be proved (cf. *Notes*, p. 110), that the tangents to a point conic constitute a line conic. This being so, it is convenient to use the word *conic* to denote the self-dual figure that consists of a point conic and its tangents. The number of points of a point conic is equal to $s+1$, the number of lines in a pencil; the number of lines of a line conic is $s+1$, the number of points in a range. Therefore a conic consists of $s+1$ points and $s+1$ lines.

A point which is the intersection of two tangents is said to be an *outside point*. A point which is neither a point of the conic nor an outside point is said to be an *inside point*. The total number of outside points is $\frac{1}{2}(s^2+s)$, the number of combinations of $s+1$ tangents taken two at a time. By subtraction from s^2+s+1, the number of points in the plane, the total number of inside points is found to be $\frac{1}{2}(s^2-s)$. By the principle of duality, the number of secants (a secant being a line that meets the conic in two points) is $\frac{1}{2}(s^2+s)$ and the number of lines that do not meet the conic is $\frac{1}{2}(s^2-s)$. On any secant there are $s-1$ points which are not points of the conic. Half of these are inside points and half are outside points, because *two* tangents meet in each outside point. This corresponds to the fact that in a Galois field there are as many squares as not squares since, as is proved below, a conic may be represented by an equation of the second degree.

Let $P=0$ and $Q=0$ be the equations of two lines in abridged notation. P and Q are linear homogeneous functions of the three variables x_1, x_2, x_3. The equation $\lambda P+\mu Q=0$, λ and μ being any marks of the $GF[s]$, is the equation of a line through the point of intersection of the lines $P=0$ and $Q=0$. Therefore the equation $\lambda P+\mu Q=0$, the domain for λ and μ being the $GF[s]$, represents the pencil of lines through the point of intersection of $P=0$ and $Q=0$. There is one and only one line of the pencil for every value of the fraction λ/μ. There are s values of this fraction in the $GF[s]$. When $\mu=0$ the fraction λ/μ is denoted by the symbol ∞, and the corresponding line of the pencil is the line $P=0$.

Consider two pencils of lines $\lambda P+\mu Q=0$ and $\lambda P'+\mu Q'=0$. A one to one correspondence between the two pencils may be established by taking as corresponding elements the two lines which correspond to the same value of the parameter λ/μ. That this correspondence is projective may be proved by observing that the linear fractional transformation [a transformation of the projective group of the $PG(2, s)$] which transforms the lines $P=0$, $Q=0$

and $P + Q = 0$ into the lines $P' = 0$, $Q' = 0$ and $P' + Q' = 0$, respectively, also transforms the line $\lambda P + \mu Q = 0$ into the line $\lambda P' + \mu Q' = 0$. The locus of the point of intersection of corresponding lines is obtained by eliminating λ and μ from the equations of the two pencils. The result is $PQ' + P'Q = 0$ which is a homogeneous equation of the second degree in x_1, x_2, x_3 since P, Q, P', and Q' are linear homogeneous functions. Similarly, using line coördinates, it may be proved that the line equation of a conic is a homogeneous equation of second degree in three variables.

As in ordinary analytic or synthetic geometry, pole and polar may be defined with reference to a conic, and the conic may be thought of as consisting of those points which are such that each is contained in its corresponding line in a polar system. (For a definition of polar system without reference to a conic, cf. *Notes*, p. 147.)

A configuration analogous to the non-euclidean plane geometry of LOBATCHEWSKY may be obtained by considering only the inside points of a conic. The number of points in such a configuration is $\frac{1}{2}(s^2 - s)$. These points will be arranged in s^2 lines, the tangents being the only lines of the plane which are excluded. Every secant line of the plane contains $\frac{1}{2}(s - 1)$ inside points, and every line of the plane which does not meet the conic contains $\frac{1}{2}(s + 1)$ inside points. Of course a line joining an inside point and an outside point does not necessarily meet the conic. The configuration may be thought of as consisting of $\frac{1}{2}(s^2 - s)$ points arranged in s^2 lines which are of two classes. In the first class there are $\frac{1}{2}(s^2 + s)$ lines containing $\frac{1}{2}(s - 1)$ points each. In the second class there are $\frac{1}{2}(s^2 - s)$ lines containing $\frac{1}{2}(s + 1)$ points each.

Configurations analogous to k-dimensional non-euclidean geometries may be obtained in a similar manner from second degree loci in k dimensions.

In the geometry of three-space a quadric may be defined by means of two correlative bundles (a bundle of lines correlated with a bundle of planes). The quadric consists of the points in which a line of one bundle meets its corresponding plane in the other. This, the general definition of a quadric in projective geometry, includes the special cases of ruled quadric and quadric cone. A *ruled quadric* may be defined as the points of a set of lines each of which meets three given skew lines; or it may be thought of as the points of the lines of intersection of two projective axial pencils whose axes have no common point. A *quadric cone* is defined in like manner by means of projective axial pencils whose axes do have a common point. From either definition it appears that one ruling of a ruled quadric consists of $s + 1$ lines of $s + 1$ points each, i. e., the surface consists of $(s + 1)^2$ points. A quadric cone consists of $s + 1$ lines having a point in common, the total number of points being $s^2 + s + 1$. This is the number of points in a plane, or of lines in a bundle, or of planes in a bundle. The number of points of the general quadric is $s^2 + 1$. As in ordinary projective geometry, it may be seen that any plane section of a quadric is a conic.

§ 9. *Derived tactical configurations.*

The finite projective geometries may be used to build a practically endless sequence of tactical configurations.* For example, in a three dimensional geometry, systems of lines may be obtained analogous to the ordinary linear congruence. Any three lines of the system determine a set of $p^n + 1$ lines, namely, the lines of the same ruling in the quadric determined by the three. We thus have a generalization from the case p to the case p^n of the configuration of all the chains in a line (cf. § 5).

The configurations just named seem not to be in the literature, but all the other configurations discussed above have been known previously for the cases where p^n is a simple prime. The references, so far as we have been able to find them, are given below. We have found no previous mention of a case p^n where $n > 1$.

The $PG(2, 2)$ is the same configuration as the triple system Δ_7 in seven elements mentioned in § 1 and § 3.

The $PG(k-1, 2)$ is the same configuration as the *linear triple system* Δ_{2^k-1} in $2^k - 1$ elements, defined and studied by MOORE.†

The $EG(k, 3)$ is a triple system Δ_{3^k} in 3^k elements. The number of triples is $\frac{1}{6}3^k(3^k - 1)$.

The $PG(k, p)$ is the same as the linear fractional configuration $LFCf[(p^k - 1)/(p-1)]$ obtained by MOORE ‡ as a defining tactical invariant for the linear fractional group $LF(k+1, p)$. Paragraph 7 of this paper may be regarded as a generalization by a different method of the $LF(k+1, p)$ to the $LF(k+1, p^n)$, $n > 1$.

The $PG(k, p)$ has been defined synthetically by FANO § and analytically by HESSENBURG.|| Neither FANO nor HESSENBERG seems to have studied its group properties or its geometrical theory. MOORE studied only the group properties. He obtained the configuration from the $GF[p^k]$ instead of from the $GF[p]$ as in this paper.

* For the general definition of tactical configuration and a rich collection of examples, cf. E. H. MOORE, *Tactical memoranda*, American Journal of Mathematics, vol. 18 (1896), p. 264.

† *Concerning the general equations of the seventh and eighth degrees*, Mathematische Annalen, vol. 51 (1898), pp. 417–444.

‡ *Concerning Jordan's linear groups*, Bulletin of the American Mathematical Society, ser. 2, vol. 2 (1895–96), pp. 33–43.

§ *Sui postulati fondamentali della geometria projettiva*, Giornale di Matematiche, vol. 30 (1892). p. 106.

|| *Über die projective Geometrie*, Sitzungsberichte der Berliner mathematischen Gesellschaft, 1902–03, pp. 36–40.

The $EG(k, p)$ is the linear configuration $LCf[p^k]$ obtained by MOORE * as a defining tactical invariant for the linear group $L(k, p)$. The linear homogeneous configuration $LHCf(p^k - 1)$, obtained by MOORE * as a defining tactical invariant for the general linear homogeneous group $GLH(k, p)$, is the same configuration, for the case $s = p$, as the one obtained as a defining invariant for the general case of the same group at the end of § 7 of this paper.

The $EG(3, 2)$ is MOORE's quadruple system $\square_8$.† The planes of the $EG(3, 2)$ are the quadruples.

* Bulletin of the American Mathematical Society, loc. cit.

† Mathematische Annalen, loc. cit., § 5. In this paper, MOORE points out that the $PG(3, 2)$ [his Δ_{15}] leads to a solution of KIRKMAN's fifteen-schoolgirl problem.