CONICS AND ORTHOGONAL PROJECTIVITIES IN A FINITE PLANE

W. L. EDGE

1. Introduction. The ternary orthogonal group of projectivities over a finite field leaves a non-singular conic χ invariant, but the geometry consequent thereupon does not appear to have been investigated. The group is isomorphic to a binary group of fractional substitutions over the same field and this fact may, since these binary groups and their subgroups are so well known, have inhibited projects to embark on a detailed description of the geometry of the ternary group. While, however, one may concede that no new intrinsic knowledge of the group can be gained, different representations of the same abstract group are apt to portray some of its attributes from different aspects and to display in different settings interrelations among its properties; and if one recalls the situation in the real or complex field the incentive to initiate some investigation becomes compelling.

The representation, over the real or complex field, of the points of a line λ by those of a conic Γ is now commonplace and goes back at least as far as Hesse. The involutions of pairs of points, as well as harmonic sets, seem more appositely carried on Γ than on λ. The Pascal property of Γ is simply, in essence, a statement about three involutions having a pair in common; but although these involutions can be carried on any rational curve, and the Pascal property interpreted in that context, it will be generally agreed, and not merely on historical grounds, that the conic is the most appropriate setting for it. The representation, too, of harmonic pairs on λ as pairs on Γ whose joins are conjugate has its advantages, and no apology is needed for undertaking some account of the corresponding representation when the base field is neither the real nor the complex field but a Galois field.

The paper falls into three sections. In the first (§§2–9) the foundations of the figure are laid and its fundamental properties established. It is explained how the points of the plane fall into 3 disjoint classes according as they are exterior to, on, or interior to χ; this phenomenon is known **(10)**, but we proceed to discuss the pairing, on various lines, of conjugate points. This pairing is basically relevant, and the description of it has to take account of whether or not -1 is a square in the base field. The number of canonical triangles—triangles, that is, in reference to which χ is given by equating the unit quadratic form to zero—is calculated.

The second section (§§10–17) introduces the orthogonal group of projectivities and stresses the presence in it of involutions (of two kinds) and octahedral subgroups. The subgroup, of index 2, which subjects the points

Received October 6, 1955.

of χ to even permutations is the main focus of interest and a criterion is given for the octahedral subgroups to belong to it. They do, or do not, belong to it according as it permutes the canonical triangles intransitively or transitively. Other subgroups are found as the stabilisers of points in the plane.

The third section (§§18–32) is devoted to a detailed description of the geometry when the base field is $GF(p)$ and $p = 5, 7, 11$. For these values of p, but not for any higher values, the orthogonal group has a representation as a permutation group of degree p; such representations are found in the 3 planes. The geometry has many features of interest, such as the multiple perspectivities between certain pairs of canonical triangles and, when $p = 11$, the distribution of the points external to χ in sets of 6, the 15 joins of points of such a set being all skew to χ and concurrent in threes at 10 different points all internal to χ.

Conics and their Canonical Triangles

2. The number q of marks in a finite field F is always a power of a prime p. Every non-zero mark satisfies $x^{q-1} = 1$, and there always occur primitive marks of which no power lower than the $(q-1)$th is 1. All the non-zero marks are powers of any primitive mark j. We suppose throughout that $p > 2$. Then j cannot be the square of any mark of F because, if $j = i^2$,

$$j^{\frac{1}{2}(q-1)} = i^{q-1} = 1,$$

contradicting the primitiveness of j. Nor can any odd power of j be a square; it is impossible to extract a square root of any odd power of j without enlarging F. All even powers of j, on the other hand, are clearly squares of marks of F. The non-zero marks are thus half of them squares and the other half non-squares.

The product and quotient of two non-squares are always squares.

Take, as an example, $q = p = 7$. We may label the marks

$$-3, -2, -1, 0, 1, 2, 3$$

and regard them as the residue classes to modulus 7. The primitive marks are 3 and -2. The squares are

$$1 = 3^6 = (-2)^6, \quad -3 = 3^4 = (-2)^2, \quad 2 = 3^2 = (-2)^4,$$

while the non-squares are

$$-1 = 3^3 = (-2)^3, \quad 3 = 3^1 = (-2)^5, \quad -2 = 3^5 = (-2)^1.$$

It is important, with a view to the geometry, to distinguish between fields wherein -1 is, or is not, a square. Since -1 is $j^{\frac{1}{2}(q-1)}$, this power of j not being 1 and yet a square root of 1,

-1 is a square whenever $q \equiv 1 \pmod 4$,

-1 is a non-square whenever $q \equiv -1 \pmod 4$.

3. The marks of F will serve as homogeneous coordinates of points and lines in a plane; each point or line answers to a vector of 3 components not all of which are 0. There are $q^3 - 1$ such vectors; but the $q - 1$ non-zero multiples of any given vector represent the same point, or line, so that the plane consists of

$$(q^3 - 1)/(q - 1) = q^2 + q + 1$$

points and of the same number of lines. When it is necessary to distinguish point and line the coordinates of a point may be written as a column vector and those of a line as a row vector. The number of points on a line and of lines through a point is

$$(q^2 - 1)/(q - 1) = q + 1.$$

4. We take for granted **(3**, p. 158**)** the fact that every non-singular conic can, by appropriate choice of the triangle of reference, be given by equating to zero the unit quadratic form $x^2 + y^2 + z^2$. Let us, before embarking on the main task of exposition, enquire into the geometrical significance of this canonical form. It certainly refers the conic to a self-polar triangle, but there is more to say than this because a conic has self-polar triangles which, when used as triangle of reference, do not permit this canonical form unless F is enlarged. The complete explanation has to take account of whether or not -1 is a square in F. The line $x = 0$ meets the conic where $y^2 + z^2 = 0$; if -1 is a square this yields two intersections, whereas if -1 is not a square there are no intersections; and the like occurs on $y = 0$ and on $z = 0$. If we describe any triangle which permits the canonical form $x^2 + y^2 + z^2 = 0$ as a *canonical triangle* and denote it by Δ then

if $q \equiv 1 \pmod 4$ the sides of any Δ are all *chords* of the conic,

if $q \equiv -1 \pmod 4$ the sides of any Δ are all *skew* to the conic.

The number, $q(q^2 - 1)/24$, of Δ is found below in §§7, 8.

Note that there is, on any side of any Δ, a unique pair of points that is both harmonic to the vertices of Δ and conjugate for the conic; on $x = 0$ this pair is given by $y^2 = z^2$, and that whether $x = 0$ is a chord or is skew to the conic. The three such pairs on the sides of a Δ are the vertices of a quadrilateral Q having Δ for its diagonal triangle; Δ and Q each determine the other uniquely. When Δ is the triangle of reference the sides of Q are

$$x + y + z = 0, \quad -x + y + z = 0, \quad x - y + z = 0, \quad x + y - z = 0.$$

5. Let χ denote the conic $x^2 + y^2 + z^2 = 0$. The polar of $P(\alpha, \beta, \gamma)$ is $\alpha x + \beta y + \gamma z = 0$, and passes through P if and only if P is on χ; χ is the aggregate of points that lie on their own polars.

If the polar of P passes through $P'(\alpha', \beta', \gamma')$ then $\alpha\alpha' + \beta\beta' + \gamma\gamma' = 0$ and the polar of P' passes through P; P, P' are then *conjugate* with respect to χ.

Does the polar of P meet χ? At least one coordinate of P, say γ, is not zero; then, for points of χ on the polar,

$$\gamma^2(x^2 + y^2) + (\alpha x + \beta y)^2 = 0,$$
$$(\gamma^2 + \alpha^2)x^2 + 2\alpha\beta xy + (\gamma^2 + \beta^2)y^2 = 0.$$

The discriminant of this quadratic is

$$\alpha^2\beta^2 - (\gamma^2 + \alpha^2)(\gamma^2 + \beta^2) \equiv -\gamma^2(\alpha^2 + \beta^2 + \gamma^2),$$

so that the quadratic has, or has not, roots in F according as $-\alpha^2 - \beta^2 - \gamma^2 \equiv -\Sigma\alpha^2$ is, or is not, a square.

If $-\Sigma\alpha^2$ is a square we call the polar a c-line or *chord*, and say that P is *external* to χ.

If $\Sigma\alpha^2 = 0$, P is *on* χ and the polar a t-line or *tangent*. It does not meet χ elsewhere.

If $-\Sigma\alpha^2$ is a non-square we call the polar an s-line; it is *skew* to χ, and P *internal* to χ.

This separation by a conic of the points of a plane into disjoint classes is noted by Qvist **(10**, pp. 9 and 19**)** but he does not proceed further, save to remark on the numbers of tangents through the points. If a tangent passes through P then the polar of P passes through the "contact" of the tangent, and conversely; hence there pass

two t-lines through any external point,

one t-line through any point of χ,

no t-line through any internal point.

We may call external points e-points, and internal points i-points .

Every t-line consists of $q + 1$ points; one is the contact, but the remaining q have all to be e. It follows, on polarising, that there are $q + 1$ lines through any point of χ, one line being the tangent and the remaining q all c. Hence, since q chords pass through any point of χ, χ consists of $q + 1$ points. Since the number of c-lines is $\frac{1}{2}q(q + 1)$ and of t-lines is $q + 1$, the number of s-lines is

$$q^2 + q + 1 - \tfrac{1}{2}q(q + 1) - (q + 1) = \tfrac{1}{2}q(q - 1),$$

and this must also be the number of i-points. Thus χ separates the $q^2 + q + 1$ points of the plane into disjoint batches of

$$\tfrac{1}{2}q(q + 1), \qquad q + 1, \qquad \tfrac{1}{2}q(q - 1)$$

and likewise the $q^2 + q + 1$ lines into these numbers of c-lines, t-lines, s-lines, respectively.

Any two t-lines intersect, and the $\frac{1}{2}q(q+1)$ e-points are thus accounted for.

6. Of the $q - 1$ points of a c-line, not on χ, half are i and half are e. For let $(\alpha_1, \beta_1, \gamma_1)$ and $(\alpha_2, \beta_2, \gamma_2)$ be any two distinct points of χ; any point on the

https://doi.org/10.4153/CJM-1956-041-6 Published online by Cambridge University Press

c-line which joins them is $(\alpha_1 + k\alpha_2, \beta_1 + k\beta_2, \gamma_1 + k\gamma_2)$ where k runs through the $q - 1$ non-zero marks of F. This point is e or i according as

$$-\Sigma(\alpha_1 + k\alpha_2)^2 \equiv -2k\Sigma\alpha_1\alpha_2$$

is, or is not, a square; it cannot be zero since the point is not on χ. But when k runs through the $q - 1$ non-zero marks, $-2k\Sigma\alpha_1\alpha_2$ does likewise, and since, of these marks, $\frac{1}{2}(q-1)$ are squares and the others not, it follows that, of the $q - 1$ points of the c-line not on χ, $\frac{1}{2}(q-1)$ are e and the others i. It follows too, on polarising, that through each e-point there pass, with 2 t-lines, $\frac{1}{2}(q-1)$ c-lines and $\frac{1}{2}(q-1)$ s-lines.

Since there are $\frac{1}{2}(q-1)$ i-points on each of the $\frac{1}{2}q(q+1)$ c-lines there pass, through each i-point,

$$\tfrac{1}{2}q(q+1) \,.\, \tfrac{1}{2}(q-1)/\tfrac{1}{2}q(q-1) = \tfrac{1}{2}(q+1)$$

c-lines, and so $\frac{1}{2}(q+1)$ s-lines too. Polarisation then discloses that, of the $q + 1$ points on any s-line, half are e and half i.

7. Call two points, neither of them on χ, *similar* if they are either both e or both i; otherwise *opposite*.

Consider the pairing, as conjugate to one another, of the $q - 1$ points on c that are not on χ. Any conjugate pair is given by

$$(\alpha_1 \pm k\alpha_2, \quad \beta_1 \pm k\beta_2, \quad \gamma_1 \pm k\gamma_2)$$

for some non-zero k. Now the marks $\pm 2k\Sigma\alpha_1\alpha_2$ are both squares or both non-squares if -1 is a square, whereas if -1 is not a square one of the two marks is a square and the other not. Hence, for -1 not a square, the conjugates of the $\frac{1}{2}(q-1)$ e-points on c are the $\frac{1}{2}(q-1)$ i-points on c; conjugate points on c are opposite. If, however, -1 is a square conjugate points on c are similar; the $\frac{1}{2}(q-1)$ e-points consist of $\frac{1}{4}(q-1)$ conjugate pairs, as do the $\frac{1}{2}(q-1)$ i-points. Let, -1 being a square, the pole of c be e_0, and let e_1 and e_2 be any one of the $\frac{1}{4}(q-1)$ pairs of conjugate e-points on c; then each vertex of the triangle $e_0e_1e_2$ is an e-point and the triangle, being self-polar for χ, is a canonical triangle Δ. Since we may choose c, with its pole, in $\frac{1}{2}q(q+1)$ ways and, thereafter, take any of the $\frac{1}{4}(q-1)$ conjugate pairs of e-points on c the number of Δ is, since each of its 3 sides may be used to begin its construction,

$$\tfrac{1}{2}q(q+1) \,.\, \tfrac{1}{4}(q-1) \,.\, \tfrac{1}{3} = q(q^2-1)/24,$$

and each e-point is a vertex of $\frac{1}{4}(q-1)$ of them. The lowest value of q for which -1 is a square is 5; there are then 5Δ whose 15 vertices account for the 15 e-points just once. When $q = 9$ there are 30Δ, each of the $45e$-points being a vertex of 2 of them.

8. The relation between conjugate points on s can be deduced from that on c. Suppose that e_1 and e_2, two external points on s, are conjugate; their polars

c_1 and c_2 pass through e_2 and e_1, respectively and meet at i_0, the pole of s. Hence conjugate points on c are opposite and -1 is not a square. But if e_1 and i_2 are conjugate points on s their polars c_1 and s_2 pass through i_2 and e_1 respectively and meet at i_0; hence conjugate points on c are similar and -1 a square. It follows that, when -1 is a square, conjugate points on s are opposite; the conjugates of the $\frac{1}{2}(q+1)$ i-points are the $\frac{1}{2}(q+1)$ e-points. But if -1 is not a square conjugate points on s are similar; there are $\frac{1}{4}(q+1)$ conjugate pairs of i-points and $\frac{1}{4}(q+1)$ of e-points.

When -1 is not a square each Δ has s-lines for its sides and i-points for its vertices. In order to construct a Δ we may choose any one of the $\frac{1}{2}q(q-1)$ s-lines as a side, and thereafter any of the $\frac{1}{4}(q+1)$ pairs of conjugate i-points on it as vertices. Since the construction may set out from any of the 3 sides the number of Δ is

$$\tfrac{1}{2}q(q-1) \cdot \tfrac{1}{4}(q+1) \cdot \tfrac{1}{3} = q(q^2-1)/24,$$

and each i-point is a vertex of $\frac{1}{4}(q+1)$ of them. The lowest value of q for which -1 is a non-square is 3; there is then a unique Δ and its vertices are the only i-points in the plane. When $q = 7$ there are 14Δ, each of the 21 i-points being a vertex of 2 of them; when $q = 11$ there are 55Δ, each of the 55 i-points being a vertex of 3 of them.

9. Let ABC be any Δ and take e, distinct from B and C whether the vertices be e-points or i-points, on BC (there is no such e if $q = 5$). The t-lines through e are harmonic to eBC and eA, and harmonic inversions in vertices and opposite sides of ABC yield a second pair of t-lines whose intersection is the harmonic conjugate of e in regard to B and C. These 4 t-lines form a quadrilateral U with ABC as diagonal triangle; U is the same as Q if $p = 3$, though not otherwise.

When the vertices of Δ are e the e-points on BC afford $\frac{1}{4}(q-5)$ pairs harmonic to B and C; Δ gives rise to $\frac{1}{4}(q-5)$ U, of which it is the diagonal triangle, whose sides account for all $q+1$ t-lines save those 6 which pass 2 through each of A, B, C. Every Δ provides such a partitioning of the t-lines. The lowest relevant values of q are 9 (when the U are also Q) and 13.

When the vertices of Δ are i the partitioning of t-lines is simpler; each Δ gives rise to $\frac{1}{4}(q+1)$ U, the e-points on any s-line falling into $\frac{1}{4}(q+1)$ pairs harmonic to the vertices of any Δ of which this s-line is a side; these e-points can be paired not only in the involution I_0 of pairs conjugate for χ, but in $\frac{1}{4}(q+1)$ involutions I_k each having the vertices on s of a Δ for foci. No two of these $\frac{1}{4}(q+5)$ involutions are the same, and I_0 commutes with all the others since the foci of any of these form a pair of I_0. When $q = 7$ the pairing of the 4 e-points is as follows:

e_1, e'_1 and e_2, e'_2 in I_0;
e_1, e_2 and e'_1, e'_2 in I_1, with foci i_1, i'_1;
e_1, e'_2 and e'_1, e_2 in I_2, with foci i_2, i'_2.

Here i_2, i'_2 must be a pair of I_1; i_1, i'_1 a pair of I_2; not only do I_1 and I_2 commute with I_0, they commute with each other. Their product, in either order, is I_0 as is seen by observing the permutations imposed on the e when I_1 and I_2 act in succession.

The Ternary Orthogonal Group of Projectivities

10. Suppose now that a projectivity leaves χ invariant. It must permute the Δ among themselves, so that the sides $x = 0$, $y = 0$, $z = 0$ of any given Δ become the sides $\xi = 0$, $\eta = 0$, $\zeta = 0$ of (the same or) some other Δ. Here ξ, η, ζ are linearly independent linear forms in x, y, z; and since χ admits both the equations

$$x^2 + y^2 + z^2 = 0, \qquad \xi^2 + \eta^2 + \zeta^2 = 0,$$

the left-hand side of either equation is a scalar multiple of the left-hand side of the other. Thus

$$\Xi = \begin{bmatrix} \xi \\ \eta \\ \zeta \end{bmatrix} = \mathbf{M} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \mathbf{M}\,\mathbf{x}$$

where $\mathbf{M}$ is a three-rowed non-singular matrix whose elements are all in F, and

$$\mathbf{x}'\mathbf{x} = x^2 + y^2 + z^2 = \lambda(\xi^2 + \eta^2 + \zeta^2) = \lambda\,\Xi'\,\Xi = \lambda\mathbf{x}'\mathbf{M}'\mathbf{M}\mathbf{x},$$

so that

$$\lambda\mathbf{M}'\mathbf{M} = \mathbf{I}, \tag{10.1}$$

the unit matrix. Here λ is a mark of F; indeed it is a square because, on taking determinants in 10.1,

$$\lambda^3|\mathbf{M}|^2 = 1.$$

The projectivity is, however, unaffected if $\mathbf{M}$ is replaced by any scalar multiple of itself; if $\mathbf{H} = m^{-1}\mathbf{M}$ with m either square root of λ then, from 10.1,

$$\mathbf{H}'\mathbf{H} = \mathbf{I}.$$

Then $|\mathbf{H}|^2 = 1$, and we choose m to be that square root of λ for which $|\mathbf{H}|$ is $+1$; the projectivity is imposed by an orthogonal matrix of determinant $+1$. Conversely: this matrix is uniquely determined. For the only matrices which impose the same projectivity as $\mathbf{H}$ imposes are those of the form $\omega\mathbf{H}$ with ω a non-zero mark of F; the orthogonality condition demands that $\omega^2 = 1$ and the determinantal condition that $\omega^3 = 1$, which together require $\omega = 1$.

These projectivities, as likewise the unimodular orthogonal matrices that impose them, form a group $\Omega(3, q)$: the orthogonal group in 3 variables over F.

11. Note, in passing, the *involutions* in $\Omega(3, q)$, namely the harmonic inversions whose centre and axis are pole and polar for χ. Since the matrix imposing such an involution satisfies $\mathbf{H}^2 = \mathbf{I}$ as well as $\mathbf{H}'\mathbf{H} = \mathbf{I}$ it is symmetric as well as orthogonal. There are $\frac{1}{2}q(q+1)$ *hyperbolic involutions* whose centres are e-points and axes c-lines; the $q-1$ points of χ not on the axis are transposed in pairs. There are $\frac{1}{2}q(q-1)$ *elliptic involutions* whose centres are i-points and axes s-lines; the $q+1$ points of χ are transposed in pairs. One of the two consecutive integers $\frac{1}{2}(q \pm 1)$ is odd so that there are always in $\Omega(3, q)$ involutions that impose odd permutations on the points of χ—the hyperbolic ones if $q \equiv -1 \pmod 4$, the elliptic ones if $q \equiv 1 \pmod 4$.

12. The conditions, expressed by $\mathbf{H}'\mathbf{H} = \mathbf{I}$, for

$$\mathbf{H} = \begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{bmatrix}$$

with all its elements in F, to be orthogonal are

$$\Sigma\alpha_1^2 = \Sigma\alpha_2^2 = \Sigma\alpha_3^2 = 1, \tag{12.1}$$

$$\Sigma\alpha_2\alpha_3 = \Sigma\alpha_3\alpha_1 = \Sigma\alpha_1\alpha_2 = 0. \tag{12.2}$$

These conditions can be interpreted geometrically when each column of $\mathbf{H}$ is regarded as the coordinate vector of a point of the plane; 12.2 then demands that the 3 points form a self-polar triangle for χ and 12.1 that their coordinate vectors be normalised. It is not possible to normalize any vector unless $\Sigma\alpha^2$ is a square; hence if -1 is a square internal points, and if -1 is a non-square external points, cannot have their coordinates normalised. But when it is possible to normalise a vector it admits two normalised forms $\pm(\alpha, \beta, \gamma)$.

If -1 is a square, each column of $\mathbf{H}$ is one of two normalised coordinate vectors of one of three mutually conjugate e-points; that is, the columns of $\mathbf{H}$ answer one to each vertex of a Δ. The vertices of Δ can be taken in any order and, with this order chosen, four of the eight combinations of sign are permitted by the stipulation that $|\mathbf{H}| = +1$. Hence the number of such orthogonal matrices is

$$\frac{q(q^2-1)}{24} \cdot 3! \cdot 4 = q(q^2-1).$$

If -1 is not a square, the calculation leads to the same result; it is governed by the columns representing vertices of a Δ and is not affected by these vertices being e or i. *The order of the group* $\Omega(3, q)$ *is* $q(q^2-1)$.

The triangle of reference is itself a Δ, and the 24 matrices, obtained from $\mathbf{I}$ by imposing the 3! permutations on its columns and using the 4 choices of sign permitted for each permutation, form that subgroup of $\Omega(3, q)$ for which the triangle of reference is invariant. It is an octahedral subgroup; indeed it acts as the symmetric group $\mathfrak{S}_4$ on the sides of the Q associated with the

triangle of reference, imposing all 4! permutations on them. When $q = 3$ this $\mathfrak{S}_4$ is the whole orthogonal group; otherwise it is one among $q(q^2 - 1)/24$ octahedral subgroups of $\Omega(3, q)$. The involutions in $\mathfrak{S}_4$ are those three whose centres are vertices of Δ and those six whose centres are vertices of Q. The former answer to the diagonal matrices $\mathrm{diag}(1, -1, -1)$, $\mathrm{diag}(-1, 1, -1)$, $\mathrm{diag}(-1, -1, 1)$ and the latter to the matrices

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{bmatrix},$$
$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{bmatrix}.$$

13. $\Omega(3, q)$ acts as a permutation group on the $q + 1$ points of χ: should any of its operations subject these points to an odd permutation precisely one half of them must do so, and those operations that impose even permutations will then form a normal subgroup of index 2. We have, however, already noted the presence, in every group $\Omega(3, q)$, of involutions that impose odd permutations; hence $\Omega(3, q)$ has a normal subgroup $\Omega^+(3, q)$ of order $\frac{1}{2}q(q^2 - 1)$. Those involutions that belong to $\Omega^+(3, q)$ are the $\frac{1}{2}q(q + 1)$ hyperbolic involutions if $q \equiv 1 \pmod 4$, whereas they are the $\frac{1}{2}q(q - 1)$ elliptic evolutions if $q \equiv -1 \pmod 4$; in other words they are always those involutions whose centres are vertices of Δ.

14. There is a criterion which decides whether the octahedral subgroups of $\Omega(3, q)$ are also contained in $\Omega^+(3, q)$: they will not be so contained unless the vertices of Q are similar to those of Δ, for $\Omega^+(3, q)$ only contains either hyperbolic or elliptic involutions, never both. On the other hand, it does contain all the involutions of one of the two types. The test of $-\Sigma\alpha^2$ being, or not being, a square establishes that the vertices of Δ are similar to those of Q if, and only if, 2 is a square; for $-\Sigma\alpha^2$ is -1 at the vertices of the triangle of reference and -2 at those of its associated Q. When q is a prime p the similarity of the vertices requires that, in the common phraseology, 2 is a quadratic residue; this occurs **(11**, p. 110**)** whenever $p \equiv \pm 1 \pmod 8$, but not when $p \equiv \pm 3 \pmod 8$.

It is clear from §12 that $\Omega(3, q)$ permutes the Δ transitively; a given Δ is then invariant for

$$q(q^2 - 1) \div \frac{q(q^2 - 1)}{24} = 24$$

projectivities of $\Omega(3, q)$ and they form one of the octahedral subgroups. But if $\Omega^+(3, q)$ permutes the Δ transitively only 12 of its operations leave a given Δ invariant; they form a subgroup of index 2 in an octahedral group—a tetrahedral group that imposes the 12 even permutations on the sides of the associated Q. Should, therefore, $\Omega^+(3, q)$ contain the octahedral subgroups

it cannot act transitively on the Δ, which must then fall, under $\Omega^+(3, q)$, into two transitive sets of $q(q^2 - 1)/48$ each, sets which form two systems of imprimitivity for $\Omega(3, q)$ and which are transposed by any projectivity of $\Omega(3, q)$ that is outside $\Omega^+(3, q)$.

15. The rules (see §12) by which matrices of $\Omega(3, q)$ are formed show that the group is transitive not only on the Δ but also on those points that can serve as vertices of Δ; hence any such point B, and its polar b, are latent for a subgroup Ω_B, the stabiliser of B in $\Omega(3, q)$, of order

$$q(q^2 - 1) \div \tfrac{1}{2}q(q \pm 1) = 2(q \mp 1),$$

the upper or lower sign occurring according as B is e or i. Ω_B includes all the involutions whose centres are on b; they account for $q \mp 1$ of its operations and their matrices all have the coordinate vector of B latent, with multiplier -1. The other $q \mp 1$ operations of Ω_B form the group Ω_{B+} for which the coordinate vector of B is invariant, being associated with a latent root $+1$. Ω_{B+} is isomorphic to the binary orthogonal group which it induces on b, and we now show that it is cyclic. That it is abelian follows at once from the form of the 2-rowed orthogonal matrices of determinant 1 (**3**, p. 169); it can be asserted to be cyclic once the presence in it is detected of an operation whose period is the order of Ω_{B+}.

The binary orthogonal group consists of all matrices

$$\mathbf{U} = \begin{bmatrix} u & v \\ -v & u \end{bmatrix}$$

with $u^2 + v^2 = 1$ and both u, v belonging to $GF(q)$. Since $\mathbf{U}^2 = 2u\mathbf{U} - \mathbf{I}$ it follows (cf. **11**, p. 368) that, if h is a square root of -1,

$$2hv\mathbf{U}^n = \{(u + hv)^n - (u - hv)^n\}\mathbf{U} - \{(u + hv)^{n-1} - (u - hv)^{n-1}\}\mathbf{I},$$

and then that $\mathbf{U}^n = \mathbf{I}$ if, and only if,

$$(u + hv)^n = (u - hv)^n = 1.$$

Should B be an e then $h \in GF(q)$ and every $\mathbf{U}$ satisfies $\mathbf{U}^{q-1} = \mathbf{I}$; in order to find $\mathbf{U}$ with period $q - 1$ it is only necessary to choose $u + hv$, and therewith its reciprocal $u - hv$, to be a primitive mark.

If, however, B is an i then $u \pm hv$ do not belong to $GF(q)$ but to a quadratic extension $GF(q^2)$; they are conjugate marks therein, each the qth power of the other. Hence

$$(u + hv)^{q+1} = (u + hv)(u + hv)^q = (u + hv)(u - hv) = 1,$$

and every $\mathbf{U}$ satisfies $\mathbf{U}^{q+1} = \mathbf{I}$. A matrix of period $q + 1$ is found by choosing $u + hv$ in $GF(q^2)$ to be a primitive root of $x^{q+1} = 1$. The mark h, having served its purpose, falls out of the working and leaves only marks of $GF(q)$ in the final result.

Two examples may perhaps be given, with details of the calculations left out.

The quadratic $X^2 = X + 1$ is irreducible over $GF(7)$ and the adjunction of either root ζ extends the field to $GF(7^2)$. A primitive root of $x^8 = 1$ in $GF(7^2)$ is ζ^2, and so we take

$$u + \zeta^4 v = \zeta^2, \qquad u - \zeta^4 v = \zeta^{-2},$$

which give $u = v = -2$;

$$\mathbf{U} = \begin{bmatrix} -2 & -2 \\ 2 & -2 \end{bmatrix} \text{ has period 8 over } GF(7).$$

The quadratic $X^2 = X - 1$ is irreducible over $GF(11)$ and the adjunction of either root θ extends the field to $GF(11^2)$. A primitive root of $x^{12} = 1$ in $GF(11^2)$ is $2\theta + 2$ and we take

$$u + (4\theta - 2)v = 2\theta + 2, \qquad u - (4\theta - 2)v = -2\theta + 4,$$

which give $u = 3$, $v = -5$;

$$\mathbf{U} = \begin{bmatrix} 3 & -5 \\ 5 & 3 \end{bmatrix} \text{ has period 12 over } GF(11).$$

The operation of period 2 in Ω_{B+} is manifestly the involution with B as centre and this, since B is vertex of a Δ, belongs to $\Omega^+(3, q)$. But not all operations of Ω_{B+} so belong, and hence only half of them will do so. For Ω_B certainly contains operations outside $\Omega^+(3, q)$, namely those centred at $\frac{1}{2}(q \mp 1)$ points on b opposite to vertices of Δ; and when *all* involutions centred on b are jettisoned from Ω_B to leave Ω_{B+} only half these are outside $\Omega^+(3, q)$ and so not all the $q \mp 1$ operations of Ω_B outside $\Omega^+(3, q)$ are rejected. The consequence is that $\Omega^+(3, q)$ has subgroups Ω_B^+ of order $q \mp 1$ and cyclic subgroups Ω_{B+}^+ of order $\frac{1}{2}(q \mp 1)$, and is transitive on vertices of Δ.

It is perhaps not superfluous to remark that, as the involution centred at B imposes the identity projectivity on the points of b, the groups of projectivities on b are of orders one half those of the groups of orthogonal matrices; Ω_{B+}^+ imposes $\frac{1}{4}(q \mp 1)$ projectivities on b and is in (2, 1) homomorphism with this latter group.

16. There is a corresponding discussion for points D, opposite to vertices of Δ, and their polars d; $\Omega(3, q)$ has subgroups Ω_D of order $2(q \pm 1)$ and cyclic subgroups Ω_{D+} of order $q \pm 1$; $\Omega^+(3, q)$ has subgroups Ω_D^+ of order $q \pm 1$ and cyclic subgroups Ω_{D+}^+ of order $\frac{1}{2}(q \pm 1)$. There is a difference in that the "restriction" of the ternary quadratic form to the line d does not have the canonical form $\xi_1^2 + \xi_2^2$, that it had on the side of a Δ, but $\xi_1^2 + \nu\xi_2^2$ where ν is any fixed non-square of $GF(q)$. When the coordinates are transformed to correspond thereto the binary orthogonal projectivities answer to matrices **(3**, p. 161**)**

$$\mathbf{U} = \begin{bmatrix} u & v \\ -\nu v & u \end{bmatrix},$$

wherein $u^2 + \nu v^2 = 1$; but these also satisfy $\mathbf{U}^2 = 2u\mathbf{U} - \mathbf{I}$.

17. The group $\Omega^+(3, q)$ is **(3**, p. 164**)** isomorphic to the linear fractional group $LF(2, q)$, and the subgroups that have just been obtained in the orthogonal representation were found in the linear fractional representation by Serret for the case $q = p$ **(11**, pp. 375, 379, 380; results which were given also in the earlier editions of this treatise**)** and by Dickson for q a power of a prime **(3**, pp. 263–4**)**. The 3 involutions centred at the vertices of any Δ are mutually commutative and form, with the identity, a 4-group; the orthogonal representation thus discloses the $q(q^2 - 1)/24$ 4-groups in $\Omega^+(3, q)$ at a glance. They are, of course, well known in the linear fractional representation **(3**, p. 268; **1**, p. 444**)**. Serret also obtained the p^2 involutions of the group of linear fractional transformations, pointing out **(11**, p. 382**)** that the number in $LF(2, p)$ is $\frac{1}{2}p(p + 1)$ or $\frac{1}{2}p(p - 1)$ according as $p \equiv 1$ or $-1 \pmod 4$.

The Details of the Geometry over the Smaller Fields

18. The remaining sections of the paper are given to describing the geometry for the smaller fields $q = 3, 5, 7, 11$. The figure for $q = 3$ has been described elsewhere **(4)**; the Δ and Q therein are unique, and the sides of Q are the tangents at the 4 points of χ. $\Omega(3, 3)$ is the octahedral, $\Omega^+(3, 3)$ the tetrahedral, group and the points of χ and sides of Q undergo the corresponding permutations. The subgroups Ω_B, one for each vertex of Δ, are the dihedral subgroups of order 8; Ω_{B+} the cyclic subgroups of order 4. There is only a single Ω_B^+, namely the 4-group that is a common subgroup of the 3 dihedral Ω_B, but there are 3 cyclic groups Ω_{B+}^+ of order 2.

19. Some description has also been printed **(5)** of the figure for $q = 5$, although in quite a different context and using a different nomenclature. An account of this figure from the standpoint of the present enquiry is therefore given now. Each of the 15 c-lines is a side of one, and only one, Δ; and since no vertex e of any Δ lies on χ the c-lines through a point of χ belong one to each of the 5Δ. The 6 points of χ are separated by the sides of any Δ into 3 pairs of a *syntheme* (i.e., 3 pairs which together account for all 6 points) and the 5 synthemes, one arising from each Δ, constitute a *synthematic total* T (i.e, 5 synthemes which together account, by 3 pairs in each, for all 15 pairs of the 6 points).

Since there are 3 c-lines through each i-point the points of χ fall, in 10 distinct ways, into 3 pairs which, since their joins are concurrent, are in involution on χ. Each involution yields a syntheme, and the 10 synthemes so arising are those extraneous to T. We may say, with Clebsch, that the points of χ form a hexagon endowed 10 times over with the Brianchon property.

Clebsch **(2**, p. 336**)** establishes the existence of such hexagons in the real projective plane; their vertices are not then on a conic, neither will they be when we encounter such hexagons again below with $q = 11$. They arose when Clebsch mapped his 'diagonal' cubic surface on the plane, the surface itself

having arisen by making certain transformations of a quintic equation. The presence of such hexagons in the real plane is however visually obvious: they are provided by sections of the 6 diagonals of a regular icosahedron in Euclidean 3-space, the Brianchon points being the sections of the 10 joins of centroids of pairs of opposite faces. Some approach, whether deliberate or not, to this aspect of the matter is made by Klein **(8**, p. 218**)** but he does not appear to record that mere section is enough to provide the figure. The simplest section, by a plane perpendicular to a diagonal of the icosahedron, gives a hexagon consisting of the 5 vertices and the centre of a regular pentagon.

20. Take now any two Δ; call them Δ_1 and Δ_2. Label the points of χ A, B', C, A', B, C' so that

$$BC',\ CA',\ AB' \text{ are sides of } \Delta_1,$$
$$B'C,\ C'A,\ A'B \text{ are sides of } \Delta_2.$$

Since no e-point can lie on sides of more than one Δ, BC' and $B'C$ meet at a point i_1; the remaining c through i_1 is AA'. Hence

$$AA',\ BC',\ B'C \text{ are concurrent at } i_1,$$
$$BB',\ CA',\ C'A \text{ are concurrent at } i_2,$$
$$CC',\ AB',\ A'B \text{ are concurrent at } i_3;$$

moreover i_1, i_2, i_3 lie on the Pascal line s_0 of the hexagon $AB'CA'BC'$. Thus Δ_1 and Δ_2 are in *fourfold perspective*. Since they are both self-polar for χ, any axis of perspective is the polar of the corresponding centre of perspective; the four axes of perspective are AA', BB', CC', s_0. The first three of these are concurrent at i_0, the pole of s_0; they are the c-lines which pass through i_0 and are sides one of each of the Δ other than Δ_1 and Δ_2. Every pair of the 5Δ is in this relation of fourfold perspectivity, and each of the 10 s-lines plays the role of s_0 for one pair of Δ The s-lines are sides of Q, and each pair of Q share one s-line, namely the Pascal line of the hexagon of which their diagonal triangles provide alternate sides.

21. $\Omega(3, 5)$ is of order 120 and subjects the 5Δ to all 5! permutations; the octahedral subgroup for which one Δ is invariant subjects the other 4Δ to all 4! permutations. $\Omega^+(3, 5)$ is of order 60 and subjects the 5Δ to all even permutations; it has no octahedral subgroups and permutes the Δ transitively. The coordinate vectors of the 3 vertices of any Δ can therefore be displayed as columns of a matrix of $\Omega^+(3, 5)$; for instance thus:

$$21.1 \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & -1 & -1 \\ -1 & 1 & 2 \\ -1 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -1 & 2 \\ -1 & 2 & -1 \\ 2 & -1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & -1 \\ 2 & 1 & -1 \\ -1 & -1 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix}.$$

Indeed these matrices are symmetric and so, apart from $\mathbf{I}$, represent involutions; the latent column vectors associated with the latent root $+1$ are found to be e, and so the involutions are hyperbolic and belong to $\Omega^+(3, 5)$.

Each matrix affords, by the 3! permutations of its columns and the 4 permissible signings for each permutation, 24 matrices of $\Omega(3, 5)$. If the permutations are restricted to be even, the 60 matrices so arising constitute $\Omega^+(3, 5)$; for the 12 arising from $\mathbf{I}$ form the tetrahedral subgroup of $\Omega^+(3, 5)$ for which the triangle of reference is invariant and these, when they postmultiply the other matrices of 21.1 impose even permutations on their columns.

The subgroups Ω_B are easily disposed of. If B is $y = z = 0$ the 8 matrices of Ω_B are

$$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix},\begin{bmatrix}1&0&0\\0&-1&0\\0&0&-1\end{bmatrix},\begin{bmatrix}1&0&0\\0&0&1\\0&-1&0\end{bmatrix},\begin{bmatrix}1&0&0\\0&0&-1\\0&1&0\end{bmatrix},\begin{bmatrix}-1&0&0\\0&1&0\\0&0&-1\end{bmatrix},$$
$$\begin{bmatrix}-1&0&0\\0&-1&0\\0&0&1\end{bmatrix},\begin{bmatrix}-1&0&0\\0&0&1\\0&1&0\end{bmatrix},\begin{bmatrix}-1&0&0\\0&0&-1\\0&-1&0\end{bmatrix},$$

the first 4 of which constitute Ω_{B+}, the first 2 Ω^+_{B+}. The 4 diagonal matrices constitute Ω^+_B, and the same subgroup Ω^+_B arises for the 3 vertices of any Δ. These are the 5 4-groups in $\Omega^+(3, 5)$. The 15 cyclic subgroups Ω^+_{B+} of order 2 are of course generated by the hyperbolic involutions.

22. The presence of axes of perspectivity is an immediate consequence of the factorisations of linear combinations of products of sides of any two Δ. For instance: the first and fifth of the matrices 21.1 provide, over $GF(5)$, the identities

$$(2x + y + z)(x + 2y + z)(x + y + 2z) + xyz \equiv (2x - y - z)(2y - z - x)(2z - x - y)$$
$$(2x + y + z)(x + 2y + z)(x + y + 2z) - xyz \equiv 2(x + y + z)(x^2 + y^2 + z^2),$$

and 9 other pairs of identities arise from these by applying the orthogonal transformations.

23. Suppose now that $q = 7$. All Δ and Q have i-points for their vertices, but whereas the sides of Δ are s those of Q are c. $\Omega^+(3, 7)$ has 14 octahedral subgroups, each acting as the symmetric group of 4! permutations of the sides of a Q.

Consider, for the moment, some one Δ. There are operations of $\Omega^+(3, 7)$ that permute its vertices cyclically; they leave one side c of the associated Q invariant while cyclically permuting the 3 i-points thereon. They cannot, being of odd period, transpose the two points of χ on c; nor can they, as not

imposing the identity projectivity on c, have any other latent point on c than these two; hence the 3 e-points on c are also permuted cyclically. Thus, on any c-line, the 3 i-points form an equianharmonic tetrad with either point of χ, as do likewise the 3 e-points. The two triads are analogous to a binary cubic and its cubic covariant, with their common Hessian pair.

24. The stabiliser Ω_B^+ of a given i-point, called for the moment B, in $\Omega^+(3, 7)$ is of order 8. There are 2 canonical triangles Δ, Δ' with B for vertex and these *are never transposed* by any operation of Ω_B^+. Δ is invariant for an octahedral subgroup of 24 operations of $\Omega^+(3, 7)$, and of these 8 leave B unaltered and so exhaust the stabiliser. The two octahedral subgroups associated with Δ and Δ' have this (dihedral) stabiliser in common. It follows that any operation of $\Omega(3, 7)$ that transposes Δ and Δ' lies outside $\Omega^+(3, 7)$. Any two Δ which share a vertex belong to different imprimitive systems.

It is then easy, starting from any one Δ (say the triangle of reference Δ_0), to obtain all the Δ and partition them into two sets of 7. There are 3, say Δ_1, Δ_2, Δ_3, which share a vertex with Δ_0 and so belong to the opposite set; each of them shares a vertex with two Δ other than Δ_0, and the 6Δ so arising all belong to the same set as Δ_0 and, indeed, complete it. We now display all 14Δ; each of the two horizontal strata consists of a set of 7 that are permuted transitively by $\Omega^+(3, 7)$. Each stratum is an imprimitive system for $\Omega(3, 7)$; whereas both strata are invariant for $\Omega^+(3, 7)$, they are transposed by those operations of $\Omega(3, 7)$ that lie outside $\Omega^+(3, 7)$.

$$\left|\begin{array}{ccc|ccc|ccc|ccc}
1 & 0 & 0 & 0 & -2 & -2 & 0 & 2 & -2 & 3 & 2 & -3 \\
0 & 1 & 0 & -2 & 3 & -3 & 2 & 3 & 3 & 2 & 0 & 2 \\
0 & 0 & 1 & -2 & -3 & 3 & -2 & 3 & 3 & -3 & 2 & 3 \\
\hline
-1 & 0 & 0 & 2 & 0 & 2 & -2 & 2 & 0 & 2 & -3 & -3 \\
0 & 2 & 2 & 0 & -1 & 0 & 2 & 2 & 0 & -3 & 2 & 3 \\
0 & 2 & -2 & 2 & 0 & -2 & 0 & 0 & -1 & -3 & 3 & 2
\end{array}\right|$$

$$\left|\begin{array}{ccc|ccc|ccc}
3 & -2 & 3 & 3 & -3 & -2 & 3 & 3 & 2 \\
-2 & 0 & 2 & -3 & 3 & -2 & 3 & 3 & -2 \\
3 & 2 & 3 & -2 & -2 & 0 & 2 & -2 & 0 \\
\hline
2 & -3 & 3 & 2 & 3 & -3 & 2 & 3 & 3 \\
-3 & 2 & -3 & 3 & 2 & -3 & 3 & 2 & 3 \\
3 & -3 & 2 & -3 & -3 & 2 & 3 & 3 & 2
\end{array}\right|$$

Each square block provides, by permutations and signings of its columns, 24 matrices of $\Omega(3, 7)$; all 336 operations of the group are thus accounted for. The upper stratum provides, from its 7 blocks, the 168 matrices of $\Omega^+(3, 7)$; the unit matrix provides those 24 matrices for which the triangle of reference is invariant. The other octahedral subgroups occur when these 24 matrices are transformed, in the sense $\mathbf{HMH}^{-1}$, by those of the other 13 blocks.

https://doi.org/10.4153/CJM-1956-041-6 Published online by Cambridge University Press

25. Each block is symmetric and therefore the matrix of an involution save when it is the unit matrix. The involutions of $\Omega^+(3, 7)$ are the 21 elliptic ones; of these 9 are provided by the matrices given in §12. There are 12 others, of which 6 are furnished by the blocks precisely as displayed; the outstanding 6 are got from these by changing the signs of those 4 marks that occur in the same row or column as the zero in the diagonal, these changes neither altering the value of the determinant nor destroying the orthogonality. The 28 hyperbolic involutions must be imposed by symmetric matrices, orthogonal and of determinant $+1$, whose columns, either themselves or their negatives, occur in the lower stratum. All the assemblages

$$\begin{vmatrix} 2 & 2 & 2 & -2 & -2 & 2 & -2 & -2 \\ 2 & -2 & -2 & -2 & 2 & 2 & -2 & 2 \end{vmatrix}$$

can play the part of that one which appears in any of its first three blocks; this accounts for 12 hyperbolic involutions. As for the remaining four blocks, not only does each provide a hyperbolic involution as it stands but it provides three others—by transposing any two of its three columns and multiplying by -1 either the untransposed column only or all three columns, whichever alternative is the one to restore symmetry to the matrix.

26. It is easy to give the explicit forms for the matrices of the stabiliser Ω_B when B is $y = z = 0$. There are 16 of them; those 8 of Ω_{B+} have $+1$ at their top left-hand corner, zeros elsewhere in the top row and left-hand column, and the residual block one of

$$\begin{matrix} 1 & 0 & -1 & 0 & 0 & 1 & 0 & -1 & 2 & -2 & -2 & 2 & 2 & 2 & -2 & -2 \\ 0 & 1 & 0 & -1 & -1 & 0 & 1 & 0 & 2 & 2 & -2 & -2 & -2 & 2 & 2 & -2 \end{matrix}.$$

The other 8 matrices have -1 in the top left-hand corner, and the residual blocks are the 8 two-rowed blocks just given but each with its bottom row changed in sign throughout. The 8 matrices with only $0, 1, -1$ for their elements constitute Ω_B^+; here, in contrast to $q = 3, 5$, the subgroups Ω_B^+ differ for different vertices of the same Δ.

The 4 e-points on $x = 0$, being those points for which

$$y = 2z, \quad y = -2z, \quad 2y = z, \quad -2y = z,$$

undergo a cyclic group of 4 permutations under Ω_B^+ when B is $y = z = 0$. Thus $\Omega^+(3, 7)$, transitive on the 4 c-lines through an i-point as well as on the 21 i-points, is transitive on the 28 c-lines, and the stabiliser of a given c-line in $\Omega^+(3, 7)$ is of order 6. Now any c-line is a side of 2 Q, each invariant for an octahedral subgroup of $\Omega^+(3, 7)$ imposing the 4! permutations on its sides; there are 3! operations of this subgroup for which c is invariant and which impose the 3! permutations on the remaining sides. These 3! operations exhaust the stabiliser: any projectivity of $\Omega(3, 7)$ that transposes 2 Q that share a side must lie outside $\Omega^+(3, 7)$. The 14 Q fall, with their diagonal triangles,

https://doi.org/10.4153/CJM-1956-041-6 Published online by Cambridge University Press

into 2 imprimitive systems of 7, and 2 Q with a common side always belong to opposite systems.

27. There is a symmetric (3, 3) correspondence between Δ in opposite systems; two Δ, one of each system, correspond when they share a vertex. There is also a symmetric (4, 4) correspondence between Δ in opposite systems; two Δ, one of each system, correspond when the Q associated with them share a side. This latter is of course the same as the correspondence between Δ of opposite systems that do *not* share a vertex; such Δ are in a certain geometrical relation that will now be obtained.

Let c be one side of a Q; i_1, i_2, i_3 the vertices of Q on c; i'_1, i'_2, i'_3 its opposite vertices. Each pair of opposite vertices is conjugate for χ. The diagonal triangle Δ is $j_1 j_2 j_3$ where j_1 is common to $i_2 i'_3$ and $i'_2 i_3$, and so on. The polars $j_1 i'_1, j_2 i'_2, j_3 i'_3$ of i_1, i_2, i_3 are concurrent at e, the pole of c; the intersection e_1 of c and $j_1 i'_1$ is the point on c conjugate to i_1, and likewise for e_2 and e_3. The s-lines through j_1 join it to the i on $j_2 j_3$ and so meet c at i_1, i_2, i_3, e_1. Thus $j_1 e_2$ and $j_1 e_3$ are c-lines as, likewise, are $j_2 e_3$, $j_2 e_1$, $j_3 e_1$, $j_3 e_2$, and the *only* c-lines through, say, e_1 are $e_1 j_2$, $e_1 j_3$, $i_1 i_2 i_3$.

Take, now, the other Q of which c is a side; it also has i_1, i_2, i_3 for vertices but has another diagonal triangle $k_1 k_2 k_3$; and the *only* c-lines through e_1 are $e_1 k_2$, $e_1 k_3$, $i_1 i_2 i_3$. This implies, since k_1, like j_1, is on ee_1, that $j_1 j_2 j_3$ and $k_1 k_2 k_3$ are in perspective from e_1. Similarly they are in perspective from e_2 and e_3. And they are manifestly in perspective from e.

Two Δ, in opposite systems and not sharing a vertex, are therefore in quadruple perspective. Their centres of perspective are all e-points and the polar of one of them contains the other three and is the common side of the two Q associated with these Δ.

Just as for $q = 5$, so for $q = 7$; the axes of perspectivity of two Δ can be displayed as factors of linear combinations of the products of their sides. The simplest such identities occur when one Δ is the triangle of reference and the other, to be selected from the lower stratum but not to be any of the first three blocks therein, is the Δ answering to the last block, since the product of its three sides is a symmetric function of the coordinates. The identities, over $GF(7)$, are

$$(2x + 3y + 3z)(3x + 2y + 3z)(3x + 3y + 2z) - xyz \equiv 2(2x - y - z)(2y - z - x)(2z - x - y),$$

$$(2x + 3y + 3z)(3x + 2y + 3z)(3x + 3y + 2z) + xyz \equiv -3(x + y + z)(x^2 + y^2 + z^2 + yz + zx + xy).$$

The centres of perspectivity of these two triangles are then (1, 1, 1) and the three e-points

$$(2, -1, -1), \quad (-1, 2, -1), \quad (-1, -1, 2)$$

on its polar. The Q associated with these Δ are that whose sides are

$$x + y + z = 0, \quad y + z - x = 0, \quad z + x - y = 0, \quad x + y - z = 0,$$

and that whose sides are

$$x + y + z = 0, \quad y + z + 2x = 0, \quad z + x + 2y = 0, \quad x + y + 2z = 0.$$

Each of the 28 c-lines is a common side of two Q, whose diagonal triangles are in quadruple perspective in the manner described above; there are 28 pairs of identities of which the pair displayed is one, and the other 27 pairs are derivable from this one pair by applying the orthogonal transformations.

28. The symmetrical (3, 3) correspondence between two sets of 7 objects must occur in any representation of $\Omega^+(3, 7)$. For Klein's representation as a group of ternary substitutions over the complex field there occur **(9a**, p. 715; **7**, p. 443**)** two sets of 7 conics; every conic of either set meets Klein's non-singular plane quartic in the 8 contacts of 4 bitangents, and the 7 sets of 4 bitangents answering to the 7 conics of either set account for all 28 bitangents. Each bitangent belongs to one, and only one, quadruple of either set **(9a**, p. 712**)** and a symmetrical correspondence between the two sets of 7 conics is set up if conics, one in each set, correspond when the quadruples do not have a bitangent in common.

But perhaps the representation of $\Omega^+(3, 7)$ that most simply displays the (3, 3) correspondence (although the two sets do not now consist of like objects) is the group of 168 projectivities of the 7-point plane $\tilde{\omega}$, a point and line corresponding when they are incident. In $\tilde{\omega}$ each of the 7 lines contains 3 points and each of the 7 points lies on 3 lines.

29. It was announced by Galois **(6**, p. 412**)** that $LF(2, q)$ has a permutation representation of degree q for $q = 5, 7, 11$; this is never so if $q > 11$. The isomorphic group $\Omega^+(3, q)$ must therefore also admit such a representation in the finite plane; one has already been encountered for $q = 5, 7$, when the q objects permuted are canonical triangles: for $q = 5$ the whole set, for $q = 7$ the members of either imprimitive system. And so the question is clamant: what geometrical entities supply a representation of $\Omega^+(3, 11)$ as a permutation group of degree 11?

In the finite plane corresponding to $q = 11$ there are, as we shall see, Clebsch hexagons; hexagons, that is, endowed in 10 ways with the Brianchon property of concurrence of 3 diagonals. Given the conic χ there are 22 Clebsch hexagons $\mathscr{C}$ all of whose vertices are e-points and diagonals s-lines; each of the 66 e-points is a vertex of 2 $\mathscr{C}$ that belong one to each of 2 imprimitive systems of 11 $\mathscr{C}$. Either system supplies a representation of $\Omega^+(3, 11)$ as a permutation group of degree 11. The operations of $\Omega(3, 11)$ that are outside $\Omega^+(3, 11)$ transpose the 2 systems.

30. Take χ, $x^2 + y^2 + z^2 = 0$, and the triangle of reference Δ. Suppose that an s-line meets both $y = 0$ and $z = 0$ in points e neither of which is a

vertex of Q; such points are $(c, 0, 1)$ and $(b, 1, 0)$ with b, c both marks of $GF(11)$ and both b^2 and c^2 neither 0 nor 1. Moreover, the points being e, neither $b^2 + 1$ nor $c^2 + 1$ can be a square. Since, in $GF(11)$,

$$1,\quad 4,\ -2,\quad 5,\quad 3 \text{ are the squares,}$$
and $$-1,\ -4,\quad 2,\ -5,\ -3 \text{ the non-squares,}$$

b^2 and c^2 can only be -2 or 5. But the join

$$x = by + cz$$

is not an s-line unless $b^2 + c^2 + 1$ is a square; this prevents $b^2 + c^2$ from being -4 or -1 and forces it to be 3; b^2 and c^2 are, in either order, the two marks -2 and 5, squares of ± 3 and $\pm\frac{1}{3}$. This yields 2 quadrangles whose 4 vertices are e and 6 joins s, two of the joins being $y = 0$ and $z = 0$; one has vertices $(\pm 3, 1, 0)$ and $(1, 0, \pm 3)$; the other has vertices $(1, \pm 3, 0)$ and $(\pm 3, 0, 1)$.

Consider now the first of these quadrangles. Through each vertex pass, in addition to its joins to the other vertices, 2 further s-lines; the 8 s-lines so arising are found to meet 4 at each of 2 e-points on $x = 0$ and these 8 s-lines, with $x = 0$ and the 6 joins of the quadrangle, are the 15 joins of 6 e-points, namely of

$$\text{30.1}\qquad \begin{matrix} 3 & 1 & 0 & -3 & 1 & 0 \\ 1 & 0 & 3 & 1 & 0 & -3 \\ 0 & 3 & 1 & 0 & -3 & 1. \end{matrix}$$

Verification is immediate. And the 15 s-lines are sides of the following 5Δ:

$$\begin{aligned} &\Delta_0: && xyz = 0 \\ &\Delta_1: && (5x - 4y - 2z)(-2x + 5y - 4z)(-4x - 2y + 5z) = 0 \\ \text{30.2}\quad &\Delta_2: && (5x + 4y + 2z)(-2x - 5y + 4z)(-4x + 2y - 5z) = 0 \\ &\Delta_3: && (-5x - 4y + 2z)(2x + 5y + 4z)(4x - 2y - 5z) = 0 \\ &\Delta_4: && (-5x + 4y - 2z)(2x - 5y - 4z)(4x + 2y + 5z) = 0. \end{aligned}$$

Denote by $\mathscr{C}$ the hexagon whose vertices are 30.1. Each Δ_j in 30.2 answers to a syntheme of vertices of $\mathscr{C}$; the 5 synthemes, one for each Δ_j, constitute a synthematic total T. Each of the 10 synthemes extraneous to T provides 3 pairs whose joins concur: $\mathscr{C}$ has the Clebsch property. The concurrencies are all at points i, and normalized coordinate vectors for them are

$$\text{30.3}\qquad \begin{matrix} 0 & 5 & 3 & 0 & -5 & 3 & -2 & 2 & 2 & 2 \\ 3 & 0 & 5 & 3 & 0 & -5 & 2 & -2 & 2 & 2 \\ 5 & 3 & 0 & -5 & 3 & 0 & 2 & 2 & -2 & 2. \end{matrix}$$

Each of these points is the concurrence of sides of 3 of the 5 Δ_j; and each of these 3 sides is an axis of perspective of the 2 remaining Δ_j. The triple perspectivity of Δ_0 and Δ_1 accords with the identity, over $GF(11)$,

$$\begin{aligned} &(5x - 4y - 2z)(-2x + 5y - 4z)(-4x - 2y + 5z) + xyz \\ &\qquad \equiv 4(5x + 4y + 2z)(2x + 5y + 4z)(4x + 2y + 5z). \end{aligned}$$

Other identities derived from this by imposing the orthogonal transformations exhibit other pairs of canonical triangles in triple perspective.

One may, in passing, note the relation between the Q associated with such triangles; they are found to have a common side, the line on which the 3 centres of perspective of their diagonal triangles lie, and their 2 sets of 3 vertices thereon account for all e-points on the side.

31. The elliptic involution centred at a vertex of Δ_0 leaves Δ_0 invariant while transposing the other Δ_j as two pairs; the analogous situation holds for the involution centred at any vertex of any Δ_j, and the Δ_j thus undergo the 15 even permutations of period 2 of the alternating group $\mathfrak{A}_5$. The 15 involutions all belong to $\Omega^+(3, 11)$ and generate a subgroup thereof; this is icosahedral, being isomorphic to $\mathfrak{A}_5$ because any projectivity which imposes the identity permutation of the Δ_j must impose it on the points 30.3 (each of which is determined by those 3 Δ_j whose sides intersect there) and so be the identity projectivity.

$\mathscr{C}$ is not invariant for the whole group $\Omega^+(3, 11)$, it is changed to other hexagons by the involutions centred at the points 30.3; the subgroup for which it is invariant is thus a maximal icosahedral subgroup of order 60, and $\mathscr{C}$ is one of

$$660 \div 60 = 11$$

Clebsch hexagons permuted transitively by $\Omega^+(3, 11)$. The other 10 $\mathscr{C}$ are obtained at once by imposing the involutions centred at the points 30.3; taking, for example, the last of these points $x = y = z$ we have

$$\begin{bmatrix} -4 & -3 & -3 \\ -3 & -4 & -3 \\ -3 & -3 & -4 \end{bmatrix} \begin{bmatrix} 3 & 1 & 0 & -3 & 1 & 0 \\ 1 & 0 & 3 & 1 & 0 & -3 \\ 0 & 3 & 1 & 0 & -3 & 1 \end{bmatrix} = \begin{bmatrix} -4 & -1 & -2 & -2 & -5 & 5 \\ -2 & -4 & -1 & 5 & -2 & -5 \\ -1 & -2 & -4 & -5 & 5 & -2 \end{bmatrix}.$$

The vertices of the 11 $\mathscr{C}$ account for all 66 e-points, and the Δ_j which belong 5 to each $\mathscr{C}$ account for all 55Δ.

32. The 11 $\mathscr{C}$ only provide one half of the figure; there is a second set of 11 Clebsch hexagons $\mathscr{D}$ equally well supplying a permutation representation. These are obtained by starting, instead of from 30.1, from

$$\begin{matrix} 1 & 3 & 0 & 1 & -3 & 0 \\ 3 & 0 & 1 & -3 & 0 & 1 \\ 0 & 1 & 3 & 0 & 1 & -3 \end{matrix}$$

which affords, by a synthematic total of its vertices, the 5 Δ got by transposing y and z throughout 30.2. This transposition is effected by using the involution whose matrix is

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix};$$

https://doi.org/10.4153/CJM-1956-041-6 Published online by Cambridge University Press

its centre (0, 1, 1) is an e-point so that it is hyperbolic and, although belonging to $\Omega(3, 11)$, it does not belong to $\Omega^+(3, 11)$. Thus $\Omega(3, 11)$ is transitive on 22 Clebsch hexagons $\mathscr{C}$ and $\mathscr{D}$; these form imprimitive systems for $\Omega(3, 11)$ and each set of 11 is a transitive set for $\Omega^+(3, 11)$.

Each e-point is a vertex of a single $\mathscr{C}$ and a single $\mathscr{D}$; there is a symmetrical (6, 6) correspondence between the $\mathscr{C}$ and $\mathscr{D}$ wherein corresponding hexagons share a vertex. Alternatively, one may use the symmetrical (5, 5) correspondence wherein corresponding hexagons do not have a vertex in common. These correspondences between 2 sets of 11 objects will occur in other representations of $\Omega^+(3, 11)$. Klein, in 1879, found a representation as a group of quinary linear substitutions over the complex field, and when the 5 variables on which the substitutions operate are used as homogeneous coordinates in [4] there do occur two sets of 11 quadrics with each quadric of either set linearly dependent on 5 of the other **(9b**, p. 429**)**.

References

1. W. Burnside, *Theory of groups of finite order* (Cambridge, 1911).

2. A. Clebsch, *Über die Anwendung der quadratischen Substitution auf die Gleichung 5ten Grades und die geometrische Theorie des ebenen Fünfseits*, Math. Ann., *4* (1871), 284–345.

3. L. E. Dickson, *Linear groups, with an exposition of the Galois field theory* (Leipzig, 1901).

4. W. L. Edge, *Geometry in three dimensions over GF*(3), Proc. Royal Soc. A*222* (1953), 262–286.

5. ———, *31-point geometry*, Math. Gazette, *39* (1955), 113–121.

6. E. Galois, *Lettre de Galois à M. Auguste Chevalier*, J. de math. pures et appliquées, *11* (1846), 408–415.

7. F. Klein, *Über die Transformation siebenter Ordnung der elliptischen Funktionen*, Math Ann., *14* (1879), 428–471.

8. ———, *Vorlesungen über des Ikosaëder* (Leipzig, 1884).

9a, b. F. Klein and R. Fricke, *Vorlesungen über die Theorie der elliptischen Modulfunktionen* (Leipzig, 1890 and 1892).

10. B. Qvist, *Some remarks concerning curves of the second degree in a finite plane.* Annales Academiae Scientiarum Fennicae A., No. 134 (1952).

11. J. A. Serret, *Cours d'algèbre supérieure* (5th ed.), tome 2 (Paris, 1885).

University of Edinburgh