Three Ways of Measuring Distance, Three Orbits, Three Subdegrees, or the Great Theorems of Cameron and Kantor

Shreeram S. Abhyankar

Finite Universe

Is our universe finite or infinite? As we travel further and further will our journey ever end or must we go on forever? The second possibility being frightening, it is convenient to assume the first. In other words, let us postulate that we live in the projective three-space. The quantum theorists have told us that matter, instead of being continuous, is discrete, so our universe has a finite number of points. The physicists also like to include time as the fourth dimension, and to represent further states, they even like the dimension to be any positive integer. So, as a thought experiment, we might as well suppose our universe U to be a finite projective space of any positive dimension N.

Thus the universe U consists of a finite number of points. Some points are collinear, i.e., they lie on a line. Any two points determine a line. Any three noncollinear points determine a plane. Any four noncoplanar points determine a solid. And so on. Finally $N+1$ points, not lying on any $(N-1)$-dimensional subspace, span the whole space U. An $(N-1)$-dimensional subspace of U is called a hyperplane.

Those properties of U which do not change when we change coordinates are more interesting than those which change. Making a coordinate change amounts to applying a *collineation* to U. A collineation is a bijection, i.e., a one-to-one onto map, of U onto itself which preserves collinearity, i.e., it sends collinear points to collinear points. We can follow up a collineation g by a collineation h to give us their composition hg. Also reversing g gives us its inverse g^{-1}. The set of all collineations of U thus forms a group $\Gamma(U)$.

A *perspectivity* is a collineation which fixes all points on a hyperplane. It will then also fix all hyperplanes through a certain point. If that point is on that hyperplane, then the perspectivity is an *elation*, otherwise a *homology*; see the 1920 projective geometry book by Veblen and Young. The subgroup of $\Gamma(U)$ generated by all elations is the little projective group denoted by $S(U)$. Likewise the group generated by all perspectivities is the full projective group $G(U)$. It is easily checked that the subgroup $S(U)$ is doubly transitive on U, i.e., any two points of U can be sent to any other two points of U by a suitable member of $S(U)$. One of the great theorems of Cameron-Kantor, Theorem I of their 1979 paper [6], says that conversely if a subgroup of the collineation group $\Gamma(U)$ is doubly transitive on U, then it must contain $S(U)$, with a few small exceptions which we shall mention in a moment.

Its Coordinates

How are the points of our universe U to be coordinatized? Now a point P in the affine, i.e., ordinary, N-dimensional space is referred to by an N-tuple $(b_1, \ldots, b_N)$. The passage from affine space to projective space is achieved by assigning to P a host of n-tuples $(c_1, \ldots, c_n)$, where $n = N+1$, with the understanding that all mutually proportional

Shreeram S. Abhyankar is professor of mathematics at Purdue University. His e-mail address is ram@cs.purdue.edu.

This work was partly supported by NSF grant DMS 99-88166 and NSA grant MDA 904-99-1-0019.

n-tuples give the same point, and the n-tuple with all zero entries is excluded. The n-tuples form an n-dimensional vector space V, and the projective space U may be identified with the set of all 1-dimensional subspaces of V. Now $(c_1,\dots,c_n)$ are referred to as homogeneous coordinates of the point P. Those points for which the last coordinate c_n is zero constitute the hyperplane at infinity. For points of U at finite distance, i.e., not on the hyperplane at infinity, we get back to the affine space by letting the point $(c_1,\dots,c_n)$ correspond to the point $(b_1,\dots,b_N) = (c_1/c_n,\dots,c_N/c_n)$. Thus the projective space may be formed by adding the points at infinity to the affine space.

Customarily the entries b_i and c_j are real numbers. Now real numbers can be added with associative addition $(a+b)+c = a+(b+c)$, with zero $a+0 = 0+a = a$; the addition is commutative, $a+b = b+a$, and we have negatives $-a+a = 0$; this gives us the additive abelian (= commutative) group R^+. Nonzero real numbers form the (commutative) multiplicative group $R^\times$ under multiplication. The two operations are linked by the distributive law $a(b+c) = ab+ac$. This is summarized by saying that the set R of all real numbers is a field. So is the set C of all complex numbers.

But these are infinite fields. For our universe to be finite, we had better take recourse to finite fields. The finite fields of prime order were discovered in 1830 by the youthful twenty-year-old Galois. Indeed, for any prime p, the integers $0,1,\dots,p-1$ form a field when they are added and multiplied modulo p, i.e., after adding or multiplying, the answer is to be divided by p and replaced by the remainder. This gives the Galois Field GF(p). At the Chicago World Fair of 1893, E. H. Moore extended Galois' thought by showing that for every power q of p, there is a field GF(q) of q elements. This is unique up to isomorphism, i.e., between any two such fields there is a one-to-one onto map preserving sums and products. For our universe, the entries b_i and c_j of the N-tuples $(b_1,\dots,b_N)$ and the n-tuples $(c_1,\dots,c_n)$ are to be in GF(q). Thus we refer to U as an N-dimensional projective space over GF(q) and to V as an n-dimensional vector space over GF(q).

American mathematical research was started by the students of Klein and Sylvester around 1880, but it took firmer roots through the work of Moore and his forty Ph.D. students; see the Parshall-Rowe book [11]. Amongst Moore's students there was Oswald Veblen, cited above, who developed the Princeton mathematics department, and also there were G. D. Birkhoff and R. L. Moore who went on to develop the mathematics departments at Harvard and Texas, respectively. E. H. Moore's first student was L. E. Dickson, who was very instrumental in further developing the mathematics department of the University of Chicago. In his 1901 book, when he was only twenty-seven, Dickson gave a masterly treatment of the fields GF(q) as well as many interesting groups based on them such as $S(U)$ and $G(U)$. The GF(p) versions of these groups were already studied by Jordan in his 1870 book which was the first expansion of Galois' ideas on equation solving.

Galois Theory

Indeed, in the eventful year 1830, the young Galois introduced the Galois group of a polynomial equation $f(Y) = 0$ as a way of estimating the difficulty of solving it. Suppose

$$f(Y) = Y^d + a_1 Y^{d-1} + \cdots + a_d$$
$$= (Y-\alpha_1)\cdots(Y-\alpha_d)$$

with coefficients $a_1,\dots,a_d$ in a field K and assume that the roots $\alpha_1,\dots,\alpha_d$ taken in some overfield of K are all distinct. By an overfield of K we mean a field in which K is embedded. The Galois group of f over K, denoted by Gal(f,K), is the group of all relation-preserving permutations of the roots, i.e., the set of all σ in S_d such that for every polynomial relation $\Theta(\alpha_1,\dots,\alpha_d) = 0$ over K we have $\Theta(\sigma(\alpha_1),\dots,\sigma(\alpha_d)) = 0$. As usual S_d is the symmetric group on d letters, which this time we take to be the roots $\alpha_1,\dots,\alpha_d$. This is Galois' original definition. According to the modern definition we take the splitting field K^* of K, i.e., $K^* = K(\alpha_1,\dots,\alpha_d)$, and we define the Galois group of K^* over K, denoted by Gal(K^*,K), to be the group of all K-automorphisms of K^*. It is clear

that every σ in $\mathrm{Gal}(K^*, K)$ corresponds to a relation-preserving permutation of the roots and conversely. Thus $\mathrm{Gal}(f, K)$ is a permutation representation of $\mathrm{Gal}(K^*, K)$. Again according to Galois, a finite group G is *simple* if G has no proper normal subgroup. Here proper means a nonidentity subgroup different from G. A subgroup H of G is normal if for every g in G we have $gHg^{-1} = H$. We denote subgroup by writing $H \leq G$ and normal subgroup by writing $H \lhd G$. Now every finite group G can be expressed as $1 = H_1 \lhd H_2 \lhd \cdots \lhd H_r = G$ where the factor group H_i/H_{i-1} is simple for $2 \leq i \leq r$. If all these simple groups are cyclic, that is, generated by single elements, then G is said to be solvable; otherwise it is unsolvable. This mimics the idea of solving an equation by radicals, i.e., by repeatedly finding square roots, cube roots, and so on. With these definitions at hand Galois proved his celebrated theorem according to which the equation $f = 0$ can be solved by radicals if and only if $\mathrm{Gal}(f, K)$ is solvable. From this he deduced that the general equation of degree $d \geq 5$ cannot be solved by radicals because then the alternating group A_d is simple and hence the symmetric group S_d is unsolvable. In addition to proving the simplicity of A_d for $d \geq 5$, he also proved the simplicity of $S(U)$ for $(n, q) = (2, p)$ with $p \geq 5$. Jordan extended this by proving the simplicity of $S(U)$ for $n \geq 3$ and $q = p$. Then Moore proved it for $n = 2$ and $q > p \geq 2$, and finally Dickson proved it for $n \geq 3$ and $q > p \geq 2$.

Most algebra textbooks, after defining the Galois group and proving the impossibility of solving general equations of degree ≥ 5 by radicals, give very few examples of Galois groups. Many of them stop after proving that the Galois group of a binomial $Y^d - a_d$ is cyclic provided K contains d distinct dth roots of 1. Note that this implies d is nondivisible by the characteristic of K. If $1 + 1 + \cdots$ is never zero in a field K, then K is said to be of characteristic 0. Otherwise $1 + 1 + \cdots + 1 = 0$ when 1 is repeated a certain number of times, and the smallest such number is easily seen to be a prime number, which is then called the characteristic of K. For instance the real and complex fields are of characteristic zero, and the field $\mathrm{GF}(q)$ is of characteristic p.

Trinomials

The goal of this article is to give more interesting examples of Galois groups. Namely, we show that various finite classical groups can be realized as Galois groups of specific concrete polynomials. We use as essential tools the great theorems of Cameron and Kantor.

So recall that in our universe q is a power of a prime p, and consider the nice trinomial

$$F(Y) = Y^{\langle N \rangle} + Y + X$$

over $k(X)$ where X and Y are indeterminates over a field k of characteristic p and we are using the abbreviation

$$\langle N \rangle = 1 + q + q^2 + \cdots + q^N,$$

i.e., $\langle N \rangle$ is the size $|U|$ of our universe which is an N-dimensional projective space over $\mathrm{GF}(q)$. Indeed, as we have said, we identify U with the set of all 1-dimensional subspaces of an n-dimensional vector space V over $\mathrm{GF}(q)$ where $n = N + 1$, and hence $|U| = \frac{q^n - 1}{q - 1} = \langle N \rangle$. As a consequence of Cameron-Kantor's Theorem I, in [2] it is shown that if $k = \mathrm{GF}(p)$, then $\mathrm{Gal}(F, k(X)) =$ the collineation group $\Gamma(U)$, and if $k = \mathrm{GF}(q)$, or more generally if k is an overfield of $\mathrm{GF}(q)$, then $\mathrm{Gal}(F, k(X)) =$ the full projective group $G(U)$. As a slight deformation of F we get the trinomial

$$F^*(Y) = Y^{\langle N \rangle} + XY + (-1)^n.$$

As another consequence of Theorem I, in [2] it is shown that if k is an overfield of $\mathrm{GF}(q)$, then $\mathrm{Gal}(F, k(X)) =$ the little projective group $S(U)$.

As usual let $\mathrm{GL}(n, q)$ be the group of all $n \times n$ matrices over $\mathrm{GF}(q)$ with nonzero determinant, and let $\mathrm{SL}(n, q)$ be the subgroup of $\mathrm{GL}(n, q)$ consisting of all matrices with determinant 1. Thinking of $\mathrm{GL}(n, q)$ as the group of all nonsingular linear transformations of V, we may regard it as a subgroup of the group $\Gamma\mathrm{L}(n, q)$, the group of all nonsingular *semilinear transformations* of V. A semilinear transformation is an additive isomorphism g of V such that for all λ in $\mathrm{GF}(q)$ and v in V we have $g(\lambda v) = \tau(\lambda) g(v)$ where τ is an automorphism of $\mathrm{GF}(q)$ which depends only on g and not on λ or v; we then say that g is τ-linear; note that the group $\mathrm{Aut}(\mathrm{GF}(q))$ of all automorphisms of $\mathrm{GF}(q)$ is a cyclic group of order u where $q = p^u$. Finally let $\mathrm{HL}(n, q)$ be the set of all $n \times n$ nonsingular scalar matrices over $\mathrm{GF}(q)$. Then $\mathrm{HL}(n, q)$ is a normal subgroup of $\mathrm{GL}(n, q)$ as well as $\Gamma\mathrm{L}(n, q)$. The abbreviations GL, SL, and HL stand for the general linear group, the special linear group, and the homothety group, respectively. For a study of homothetic figures, i.e., similar figures, see Askwith's 1920 *Pure Geometry* which, like the Veblen-Young book, is another projective geometry classic.

Clearly every member of $\Gamma\mathrm{L}(n, q)$ gives rise to a collineation of U, and members of $\mathrm{HL}(n, q)$ correspond to the trivial collineation. Thus there is a natural homomorphic map of $\Gamma\mathrm{L}(n, q)$ into $\Gamma(U)$, and its kernel is $\mathrm{HL}(n, q)$. Part of the fundamental theorem of projective geometry says that this map is surjective, that is, onto. So we may identify $\Gamma(U)$ with the factor group $\mathrm{P}\Gamma\mathrm{L}(n, q) = \Gamma\mathrm{L}(n, q)/\mathrm{HL}(n, q)$, and we may identify $G(U)$ and $S(U)$ with the respective images $\mathrm{PGL}(n, q)$ and $\mathrm{PSL}(n, q)$ of $\mathrm{GL}(n, q)$ and $\mathrm{SL}(n, q)$ under the natural epimorphism

$\Gamma L(n,q) \to P\Gamma L(n,q)$. Now the above consequences of Theorem I may be restated by saying that:

Result (1). *If* $k = \mathrm{GF}(p)$, *then* $\mathrm{Gal}(F, k(X)) = P\Gamma L(n,q)$, *and if* $\mathrm{GF}(q) \subset k$, *then* $\mathrm{Gal}(F, k(X)) = \mathrm{PGL}(n,q)$ *and* $\mathrm{Gal}(F^*, k(X)) = \mathrm{PSL}(n,q)$.

As in [2], these results are "vectorized" by putting

$$E(Y) = YF(Y^{q^{n-1}}) = Y^{q^n} + Y^q + XY$$

and

$$E^*(Y) = YF^*(Y^{q^{n-1}}) = Y^{q^n} + XY^q + (-1)^n Y$$

and deducing that:

Result (2). *If* $k = \mathrm{GF}(p)$, *then* $\mathrm{Gal}(E, k(X)) = \Gamma L(n,q)$, *and if* $\mathrm{GF}(q) \subset k$, *then* $\mathrm{Gal}(E, k(X)) = \mathrm{GL}(n,q)$ *and* $\mathrm{Gal}(E^*, k(X)) = \mathrm{SL}(n,q)$.

Writing $\mathcal{P}(n-1,q)$ for the $(n-1)$-dimensional projective space U over $\mathrm{GF}(q)$ and denoting isomorphism by $\approx$, we precisely reformulate:

Cameron-Kantor's Theorem I. *If* $G \le \Gamma L(n,q)$ *is doubly transitive on* $\mathcal{P}(n-1,q)$, *then either* $\mathrm{SL}(n,q) \lhd G$, *or* $(n,q) = (4,2)$ *and* $A_7 \approx G \le \mathrm{SL}(4,2)$, *or* $(n,q) = (2,4)$ *and* $|G| \in \{20, 60\}$.

In general, to calculate the Galois group $G = \mathrm{Gal}(f, K)$, first note that G is a transitive subgroup of S_d if and only if f is irreducible in $K[Y]$. Next consider the one-point stabilizer G_{α_1} which by definition consists of all $\sigma \in G$ with $\sigma(\alpha_1) = \alpha_1$. We may regard G_{α_1} as a subgroup of S_d or as a subgroup of the permutation group S_{d-1} on the $d-1$ roots $\alpha_2, \ldots, \alpha_d$. As in [2] and [3], for calculating G_{α_1} we "throw away" the root α_1 by constructing the "twisted derivative"

$$f'(Y) = \frac{f(Y) - f(\alpha_1)}{Y - \alpha_1} \in K'[Y] \text{ with } K' = K(\alpha_1).$$

Then G_{α_1}, as a subgroup of S_{d-1}, is transitive if and only if f' is irreducible in $K'[Y]$. Hence $\mathrm{Gal}(f, K)$ is doubly transitive if and only if f is irreducible in $K[Y]$ and f' is irreducible in $K'[Y]$. On the other hand, if f is irreducible in $K[Y]$ but f' has e irreducible factors in $K'[Y]$, then $\mathrm{Gal}(f, K)$ is transitive Rank $e+1$, where the permutation rank of a transitive subgroup of S_d is defined to be the number of orbits of its one-point stabilizer as a subgroup of S_d. The sizes of these orbits are called its subdegrees, one of which is obviously 1.

In our situation, since F is linear in X, by applying Gauss's Lemma twice, we see that F is irreducible in $K[Y]$ with $K = k(X)$. Also $K' = k(X)(\alpha_1) = k(\alpha_1) \approx k(X)$ which makes it easier to check the irreducibility of F' over $K'[Y]$. So we may use the above Theorem I, after we make special considerations to show that the exceptions in the cases $(n,q) = (4,2)$ or $(2,4)$ do not occur. Similarly for F^*.

On the other hand, by "inserting" a few suitable terms in F, it can be arranged that F remains irreducible but F' factors into two irreducible factors of specified degrees. When this happens we shall be ready to apply other great theorems of Cameron and Kantor to produce further interesting examples of Galois groups. For this purpose we start by introducing some more classical groups.

Isometry Groups

In elementary geometry we learn to measure distance or length and to consider congruence of triangles and other geometric figures. We also measure angles. The measurements of distances and angles can be deduced from each other by the idea of inner products. The inner product between two vectors $x = (x_1, x_2)$ and $y = (y_1, y_2)$ in R^2 is given by the bilinear form $b(x,y) = x_1y_1 + x_2y_2$. This bilinear form is symmetric, i.e., $b(y,x) = b(x,y)$. The length of x, or rather its square $c(x)$, is given by the equation $c(x) = x_1^2 + x_2^2 = b(x,x)$. Similarly in R^n.

The absolute value square of a complex number z is given by $z\overline{z}$. This gives rise in C^2 to the hermitian form $b(x,y) = x_1\overline{y}_1 + x_2\overline{y}_2$. This is hermitian symmetric, i.e., $b(y,x) = \overline{b(x,y)}$. Similarly in C^n.

The bilinear form $b(x,y) = x_1y_2 - x_2y_1$ is an example of an antisymmetric bilinear form, i.e., a bilinear form for which $b(y,x) = -b(x,y)$. Similarly in R^n or C^n provided n is even.

These three different ways of measuring distance or angle give rise to three types of geometries: orthogonal, unitary, and symplectic.

The study of congruences of figures leads to the isometry group. This is the group of all distance- or angle-preserving transformations. For instance, a nonsingular linear transformation of R^2 is given by a 2×2 real matrix, with nonzero determinant. All such matrices form a group under matrix multiplication. This is denoted by $\mathrm{GL}(2,R)$, i.e., the 2-dimensional general linear group over R. Amongst these the distance-preserving transformations form a subgroup which is called the 2-dimensional orthogonal group and is denoted by $\mathrm{O}(2,R)$. The length $c(x) = x_1^2 + x_2^2$ of the vector $x = (x_1, x_2)$ is the distance between its end points. So $\mathrm{O}(2,R)$ may be called the isometry group of R^2 relative to c and denoted by $\mathrm{I}(R^2, c)$. We may also denote it by $\mathrm{I}(R^2, [b,c])$ or $\mathrm{I}(R^2, b)$ since it also preserves the inner product $b(x,y) = x_1y_1 + x_2y_2$. Similarly the distance-preserving transformations of R^n form the orthogonal group $\mathrm{O}(n,R)$, which is the isometry group $\mathrm{I}(R^n, [b,c])$ of R^n relative to the n-dimensional versions of b and c. In the etymology of the word "isometry", the piece "iso" refers to equal or preserving, and the piece "metry" refers to metric or distance.

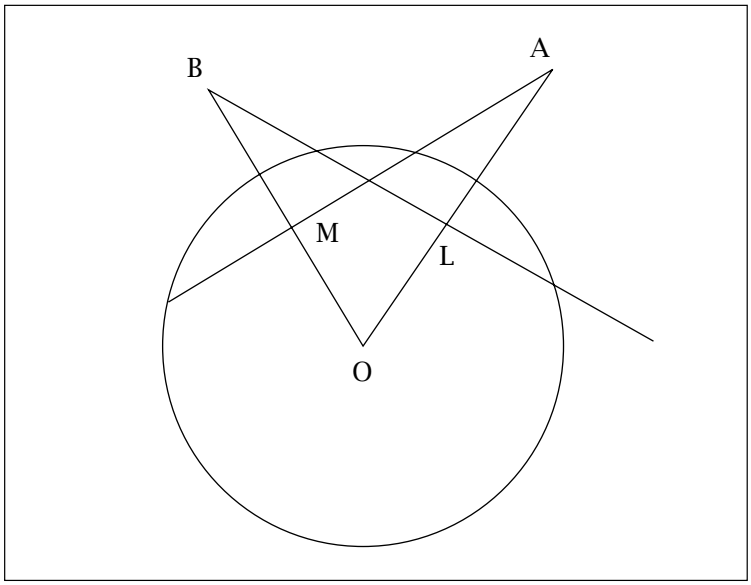
In the hermitian case, the isometry group $\mathrm{I}(C^n, b)$ is called the unitary group and is denoted by

$\mathrm{U}(n, C)$. In the antisymmetric case, the isometry group $\mathrm{I}(R^n, b)$ or $\mathrm{I}(C^n, b)$ is called the symplectic group and is denoted by $\mathrm{Sp}(n, R)$ or $\mathrm{Sp}(n, C)$, respectively.

Metric Pairs

Until now we considered vectors in R^n, i.e., n-tuples $x = (x_1, \ldots, x_n)$ with coordinates x_i in R. By taking coordinates in the finite field $\mathrm{GF}(q)$, we get the n-dimensional vector space V over $k = \mathrm{GF}(q)$. Distances or lengths in V are measured by a univariate form $c(x)$ with values in k. Angles or inner products in V are measured by a bivariate form $b(x, y)$ with values in k. Together they constitute a metric pair $[b, c]$ over V. Now $\mathrm{GL}(n, q)$ is the group of all $n \times n$ nonsingular (= with nonzero determinant) matrices $g = (g_{ij})$ with g_{ij} in k. If we regard $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in V as column vectors, then the isometry group $\mathrm{I}(V, [b, c])$ consists of all g such that for all x, y we have $b(gx, gy) = b(x, y)$ and $c(gx) = c(x)$. In a moment we shall write down some explicit formulas for $[b, c]$ obtained by choosing suitable coordinate systems. Strangely these formulas are simplest in the symplectic case, and next in line is the unitary case. The orthogonal case bifurcates, or rather trifurcates, into three subcases. Although I write the explicit formulas to give the reader some flavor for the subject, the details of the formulas are not important to the subsequent discussion, and one may skim over the formulas without any loss.

In the orthogonal case, $c(x)$ will be a homogeneous polynomial of degree 2 in the variables $x_1, \ldots, x_n$, and so $c(x) = 0$ is an n-space generalization of the usual double cone in 3-space. Just as a 3-variable homogeneous equation of degree two can be interpreted as defining a conic in the projective plane, and a 4-variable homogeneous equation of degree two can be interpreted as defining a quadric in the projective 3-space, so the equation $c(x) = 0$ can be regarded as defining a hyperquadric in the $(n-1)$-dimensional projective space. Moreover, pictorially, the projective plane is not very different from R^2, and the projective 3-space is not very different from R^3. So we may use our geometric intuition accrued over the ages in studying conics and quadrics. Amazingly, in spite of the fact that in the symplectic and unitary cases the quadric is really not a quadric, and in spite of the fact that even in the orthogonal case we are working over a finite field, the intuition of conics in R^2 or quadrics in R^3 does work! For details see Sections 5 to 7 of [4]. What we are talking about is the correspondence which sends a subspace W of V to its complementary dimensional perp-space $W^{\perp_b} = \{v \in V : b(v, w) = 0 \text{ for all } w \in W\}$. In particular, a point P of $U = \mathcal{P}(n-1, q)$ corresponds to its polar hyperplane $\mathcal{P}(P^{\perp_b}) \subset \mathcal{P}(n-1, q)$ where we write $\mathcal{P}(P^{\perp_b})$ for the set of all "points" (= 1-dimensional subspaces) of $P^{\perp_b}$.



16. Prop. *If the polar of A goes through B, then the polar of B goes through A.*

Let *BL* be the polar of *A* cutting *OA* at right angles in *L*.

Draw *AM* at right angles to *OB*.

Then $OM.OB = OL.OA$ = sq. of radius,

$\therefore$ *AM* is the polar of *B*,

that is, *A* lies on the polar of *B*.

—*from* A Course of Pure Geometry, *E. H. Askwith, Cambridge University Press, 1917.*

At any rate, the foundation of all this theory is the basic pole-polar property of a circle which we (used to?) learn in school. Now the polar of a point relative to a fixed circle is the line joining the two points of contact with the circle of the two tangents which can be drawn from that point. The point is called the pole of the line. The pole-polar property says that if the polar of a point passes through a second point, then the polar of the second point passes through the first point. A proof of this can be found on page 14 of the Askwith book already cited when we spoke of homothetics. Incidentally, on page 17 of that book you will see a generalization of this property ascribed to George Salmon. See my recent historical article [1] in *Bull. Amer. Math. Soc.* where I implicitly call Salmon the father of algebraic geometry and his 1852 book on higher plane curves the cradle of that subject (see the letter from Salmon to Sylvester on the next page).

Turning to the explicit formulas, in the symplectic case, assuming $n = 2m$, and writing $[\phi, \psi]$ for $[b, c]$, we have

$$\phi(x, y) = \sum_{1 \le i \le m} (x_i y_{m+i} - x_{m+i} y_i)$$

and

$$\psi(x) = 0.$$

We let $\mathrm{Sp}(n, q) = \mathrm{I}(V, [\phi, \psi])$ and call it the symplectic group.

Railway Carriage, Staffordshire
April 14th 1852

My dear Sir
You will doubtless have discovered since that you understated your theorem last night & that the evectant

$$\left(x^n \frac{dR}{da} + \&c\right)$$

is a perfect n^{th} power when R is the discriminant & the curve has a double point. The proof is precisely the same as for two variables: Since if the equation be

$$ax^n + bx^{n-1}y + cx^{n-1}z + \&c$$

the form of the discriminant is

$$aL + b^2M + bcN + c^2P.$$

Th[u]s it at once solves the problem if a curve have a double point to find its coordinates.

The corresponding theorem is true for any number of variables. I think this theorem so pretty that it was almost worth coming from Dublin to be told it.

Give Cayley a good scolding for me. He undertook to walk part of the way home with me last night & we progressed Westward in a satisfactory manner till we got to the church (I forget its name) just beyond Temple Bar. There we made a complete circuit of the church. He had got on some interesting topic so that I never observed it & he left me with my face turned to the East & I did not discover my mistake till I found myself in St Paul's Church Yard.

I suppose you will have sent me my letters according to promise.

Very sincerely yours
Geo Salmon

Letter from George Salmon to J. J. Sylvester, April 14, 1852.
Reprinted by permission of the Master and Fellows of St. John's College, Cambridge, UK.

In the unitary case, assuming $q = q'^2$, we note that for all z in k we have $(z^{q'})^{q'} = z$ and hence $z^{q'}$ behaves like the complex conjugate of z. Now writing $[\phi^\dagger, \psi^\dagger]$ for $[b, c]$ we have

$$\phi^\dagger(x, y) = \sum_{1 \le i \le n} x_i y_i^{q'}$$

and

$$\psi^\dagger(x) = \sum_{1 \le i \le n} x_i^{q'+1}.$$

We let $\mathrm{U}(n, q) = \mathrm{I}(V, [\phi^\dagger, \psi^\dagger])$ and call it the unitary group.

In the orthogonal case, let m be the highest dimension of a linear subspace of V lying on the cone $c(x) = 0$. This number m is called the index of $[b, c]$; sometimes m is called the Witt index in honor of Witt who studied these cones in his 1937 paper in the *Crelle Journal*. If n is even, then $m = n/2$ or $(n/2) - 1$, and we call these the positive and negative subcases, respectively. If n is odd, then $m = (n/2) - (1/2)$, and we call this the ordinary subcase. In the positive subcase, writing $[\phi^+, \psi^+]$ for $[b, c]$, we have

$$\phi^+(x, y) = \sum_{1 \le i \le m} (x_i y_{m+i} + x_{m+i} y_i)$$

and

$$\psi^+(x) = \sum_{1 \le i \le m} x_i x_{m+i},$$

and we let $\mathrm{O}^+(n, q) = \mathrm{I}(V, [\phi^+, \psi^+])$ and call it the positive orthogonal group. In the negative subcase, writing $[\phi^-, \psi^-]$ for $[b, c]$, we have

$$\begin{aligned}\phi^-(x, y) =& x_{2m+1}(2y_{2m+1} + y_{2m+2}) \\ &+ x_{2m+2}(y_{m+1} + 2\zeta y_{2m+2}) \\ &+ \sum_{1 \le i \le m} (x_i y_{m+i} + x_{m+i} y_i)\end{aligned}$$

and

$$\begin{aligned}\psi^-(x) = &\left(x_{2m+1}^2 + x_{2m+1}x_{2m+2} + \zeta x_{2m+2}^2\right) \\ &+ \sum_{1 \le i \le m} x_i x_{m+i}\end{aligned}$$

where $\zeta \in k$ is such that $Y^2 + Y + \zeta$ is irreducible in $k[Y]$, and we let $\mathrm{O}^-(n, q) = \mathrm{I}(V, [\phi^-, \psi^-])$ and call it the negative orthogonal group. Finally, in the ordinary subcase, writing $[\phi^0, \psi^0]$ for $[b, c]$, we have

$$\begin{aligned}\phi^0(x, y) =& 2x_{2m+1}y_{2m+1} \\ &+ \sum_{1 \le i \le m} (x_i y_{m+i} + x_{m+i} y_i)\end{aligned}$$

and

$$\psi^0(x) = x_{2m+1}^2 + \sum_{1 \le i \le m} x_i x_{m+i},$$

and we let $\mathrm{O}^0(n, q) = \mathrm{I}(V, [\phi^0, \psi^0])$ and call it the ordinary orthogonal group. Collectively we denote the groups O^+, O^-, and O^0 by $\mathrm{O}(n, q)$ and call them orthogonal groups.

The definition of index can be suitably extended to apply to the symplectic and unitary cases, and then in the symplectic case its value is $n/2$, and in the unitary case it is the largest integer $\le n/2$. In all this we are assuming $[b, c]$ to be nondefective, i.e., there is no vector x with $c(x) \ne 0$ such that $b(x, y) = 0$ for all y.

The above neat formulas evolved gradually. For orthogonal groups in case of $p \ne 2$, the original formulas in Dickson's book are more involved, and he has to deal with many situations, such as $n \equiv 1 \bmod 4$ or $n \equiv 3 \bmod 4$, separately. One advantage of Dickson's formulas is that they involve more square terms as opposed to more cross terms in the above formulas. So they are closer to the familiar equation of a hypersphere $x_1^2 + \cdots + x_n^2 = 0$.

Orbits and Subdegrees

Referring for details to Sections 5 to 7 of [4], here is a brief review on orbits and subdegrees. But let us first define nondegenerate and nondefective metric pairs and embed the isometry groups into the corresponding similarity and semisimilarity groups.

Recall that V is the n-dimensional vector space k^n over $k = \mathrm{GF}(q)$ with $n > 1$, and U is the associated projective space $\mathcal{P}(n-1, q)$. Let $[b, c]$ be a symplectic or unitary or orthogonal (= quadratic)

name	metric pair	proper isometries	special isometries	isometries	similarities	semi-similarities
(0) general case	$[b,c]$		$\mathrm{SI}(V,[b,c])$	$\mathrm{I}(V,[b,c])$	$\mathrm{GI}(V,[b,c])$	$\Gamma\mathrm{I}(V,[b,c])$
(1) symplectic $n=2m$	$[\phi,\psi]$			$\mathrm{Sp}(n,q)$	$\mathrm{GSp}(n,q)$	$\Gamma\mathrm{Sp}(n,q)$
(2) unitary $q=q'^2$	$[\phi^\dagger,\psi^\dagger]$		$\mathrm{SU}(n,q)$	$\mathrm{U}(n,q)$	$\mathrm{GU}(n,q)$	$\Gamma\mathrm{U}(n,q)$
(3) orthogonal $n=2m$	$[\phi^+,\psi^+]$	$\Omega^+(n,q)$	$\mathrm{SO}^+(n,q)$	$\mathrm{O}^+(n,q)$	$\mathrm{GO}^+(n,q)$	$\Gamma\mathrm{O}^+(n,q)$
(4) orthogonal $n=2m+2$	$[\phi^-,\psi^-]$	$\Omega^-(n,q)$	$\mathrm{SO}^-(n,q)$	$\mathrm{O}^-(n,q)$	$\mathrm{GO}^-(n,q)$	$\Gamma\mathrm{O}^-(n,q)$
(5) orthogonal $n=2m+1, q$ odd	$[\phi^0,\psi^0]$	$\Omega^0(n,q)$	$\mathrm{SO}^0(n,q)$	$\mathrm{O}^0(n,q)$	$\mathrm{GO}^0(n,q)$	$\Gamma\mathrm{O}^0(n,q)$
(6) orthogonal $n=2m+1, q$ even	$[\phi^0,\psi^0]$	$\Omega^0(n,q)$	$\mathrm{SO}^0(n,q)$	$\mathrm{O}^0(n,q)$	$\mathrm{GO}^0(n,q)$	$\Gamma\mathrm{O}^0(n,q)$

metric pair. This means that in the symplectic case $b : V \times V \to k$ is a bilinear form which is alternating, i.e., $b(v,v) = 0$ for all $v \in V$; in the unitary case $b : V \times V \to k$ is a left linear form which is hermitian, i.e., assuming $q = q'^2$ where q' is a power of p, for all v, w in V we have $b(w,v) = b(v,w)^{q'}$, and in both the cases $c(v) = b(v,v)$ for all $v \in V$. In the orthogonal case, $c : V \to k$ is a quadratic function, i.e., $c(\lambda v) = \lambda^2 c(v)$ for all $\lambda \in k$ and $v \in V$, and its biassociate $b : V \times V \to k$ is bilinear where b is defined by saying that for all v, w in V we have $c(v+w) = c(v) + b(v,w) + c(w)$. In all three cases, we say that $[b,c]$ is nondegenerate if there is no $v \in V$ with $v \neq 0$ such that $b(v,w) = 0$ for all $w \in V$, and we say that $[b,c]$ is nondefective if there is no $v \in V$ with $c(v) \neq 0$ such that $b(v,w) = 0$ for all $w \in V$. It can be shown that, except in the orthogonal case with n odd and q even, nondegenerate and nondefective are equivalent. Moreover, if n is odd and q is even, then there is no nondegenerate orthogonal metric pair. Given any other symplectic or unitary or orthogonal metric pair $[b',c']$ on V: (i) by an isometry (resp., a special isometry) of $(V,[b,c])$ onto $(V,[b',c'])$ we mean $g \in \mathrm{GL}(V)$ (resp., $g \in \mathrm{SL}(V)$) such that for all v, w in V we have $b'(g(v), g(w)) = b(v,w)$ and for all v in V we have $c'(g(v)) = c(v)$; (ii) by a similarity of $(V,[b,c])$ onto $(V,[b',c'])$ we mean $g \in \mathrm{GL}(V)$ for which there exists $\lambda \in k^\times$ such that for all v, w in V we have $b'(g(v), g(w)) = \lambda b(v,w)$ and for all v in V we have $c'(g(v)) = \lambda c(v)$; (iii) by a semisimilarity of $(V,[b,c])$ onto $(V,[b',c'])$ we mean $g \in \Gamma\mathrm{L}(V)$, with its associated $\tau \in \mathrm{Aut}(k)$, for which there exists $\lambda \in k^\times$ such that for all v, w in V we have $b'(g(v), g(w)) = \lambda\tau(b(v,w))$ and for all v in V we have $c'(g(v)) = \lambda\tau(c(v))$; (iv) the metric pair $[b,c]$ is said to be isometric (resp., similar) to the metric pair $[b',c']$ if there exists an isometry (resp., a similarity) of $(V,[b,c])$ onto $(V,[b',c'])$.

For an orthogonal pair $[b,c]$, the explicit formulas of the previous section are meant to conform with the above equation $c(v+w) = c(v) + b(v,w) + c(w)$ and its consequence $2c(v) = b(v,v)$. If we had arranged matters to agree with the usual distance and inner product in R^n, then we would have required $c(v+w) = c(v) + 2b(v,w) + c(w)$ and $c(v) = b(v,v)$. However, for $p = 2$ this would have caused serious problems because then c would be identically zero and it would not determine b. This is why we have "absorbed" the 2 inside the b and postulated the equation $c(v+w) = c(v) + b(v,w) + c(w)$ with its consequence $2c(v) = b(v,v)$. Now everything works smoothly in all characteristics including 2. Historically it seems to have taken a long time to evolve this solution. For instance in Artin's 1957 book on geometric algebra and in Jacobson's 1974–1980 book on basic algebra, while dealing with quadratic forms, they simply declare their characteristic to be different from 2.

In the same vein, for a symplectic pair $[b,c]$ we have chosen the alternating property $b(v,v) = 0$ as the defining property rather than the antisymmetry $b(v,u) = -b(u,v)$, because the former always implies the latter, whereas the latter implies the former only when the characteristic is not 2.

For a metric pair $[b,c]$ on V, the set of all isometries (resp., special isometries, similarities, semisimilarities) of $(V,[b,c])$ onto itself is the isometry group $\mathrm{I}(V,[b,c])$ (resp., special isometry group $\mathrm{SI}(V,[b,c])$, similarity group $\mathrm{GI}(V,[b,c])$, semisimilarity group $\Gamma\mathrm{I}(V,[b,c])$). Referring to the table above, this gives us the sequence of groups $\mathrm{SI}(V,[b,c]) \le \mathrm{I}(V,[b,c]) \le \mathrm{GI}(V,[b,c]) \le \Gamma\mathrm{I}(V,[b,c])$ in the 0th row.

The rest of the table is almost self-explanatory. Rows (1) to (6) are obtained from the 0th row by writing $\mathrm{Sp},\dots,\mathrm{O}^0$ for I. In each case m is the Witt index, with the understanding that in row (2) we have $n = 2m$ or $2m+1$ according as n is even or odd. Row (3) says that if $n = 2m$, then any nondegenerate orthogonal pair $[b,c]$ of index m on V is isometric to the nondegenerate positive orthogonal pair $[\phi^+,\psi^+]$ of the previous section; for this pair we denote the groups $\mathrm{SI}(V,[\phi^+,\psi^+]) \le \mathrm{I}(V,[\phi^+,\psi^+]) \le \mathrm{GI}(V,[\phi^+,\psi^+]) \le \Gamma\mathrm{I}(V,[\phi^+,\psi^+])$ by $\mathrm{SO}^+(n,q) \le \mathrm{O}^+(n,q) \le \mathrm{GO}^+(n,q) \le \Gamma\mathrm{O}^+(n,q)$. Similarly for other rows. In row (1) there is nothing under SI because all symplectic isometries are special. In cases (1) to (5) the pair is nondegenerate, and in case (6) it is degenerate but nondefective. In cases (3) to (5), Ω is a subgroup of SO of index 2; Ω is the commutator subgroup of O except when $n/2 = m = q = 2$, in which case $\Omega^+(4,2)$ is defined to be the subgroup of $\mathrm{SO}^+(4,2)$ consisting of products of an even number of reflections, where a reflection is a map of the form $r_v : V \to V$ given by $r_v(w) = w - b(v,w)c(v)^{-1}$ for all $w \in V$ for some $v \in V$ with $c(v) \neq 0$; note that the commutator subgroup G' of a group G is the subgroup of G generated by the commutators $ghg^{-1}h^{-1}$ of all pairs of elements g,h of G. In case (6) we put $\Omega^0 = \mathrm{SO}^0$.

For details of the "eccentric" case (6) see Sections 8 to 10 of [4]. Henceforth in this article we shall exclude this case by assuming the metric pair $[b,c]$ to be nondegenerate. Also assuming $n > 2$, it can be shown that, in the symplectic or unitary or orthogonal cases, the isometry group $\mathrm{I}(V,[b,c])$ has, respectively, one or two or three orbits on the projective space $U = \mathcal{P}(n-1,q)$, except in the orthogonal case of even q when there are only two orbits. In each case one of the orbits is the hyperquadric $\Theta \subset U$ defined by the homogeneous equation $c = 0$, i.e., $\Theta = \{P \in U : c(v) = 0 \text{ for all } v \in P\}$. As above let $m > 0$ be the index, and let m' and m^* be the defect and the tag defined by putting

$$m' = n - 2m \text{ and } m^* = \begin{cases} 1 & \text{in the symplectic case,} \\ 1/2 & \text{in the unitary case,} \\ 0 & \text{in the orthogonal case.} \end{cases}$$

It can be shown that then

$$|\Theta| = (1 + q + \cdots + q^{m-1})(1 + q^{m^*+m'+m-1})$$

and, for any $P \in \Theta$, the orbits of $\mathrm{I}(V,[b,c])_P$ on $\Theta \setminus \{P\}$ are

$$\Gamma = (\Theta \setminus \{P\}) \cap \mathcal{P}(P^{\perp_b}) \quad \text{and} \quad \Delta = \Theta \setminus \mathcal{P}(P^{\perp_b})$$

and their sizes are

$$|\Gamma| = (1 + q + \cdots + q^{m-2})(q + q^{m^*+m'+m-1})$$

and

$$|\Delta| = q^{m^*+m'+2m-2}.$$

In an appropriate obvious sense, in cases (1) to (5), let $\Omega = \mathrm{Sp}$ or SU or Ω^+ or Ω^- or Ω^0. Then it can be shown that for any group G between $\Omega(V,[b,c])$ and $\Gamma\mathrm{I}(V,[b,c])$, the orbits of G on U are the same as the orbits of $\mathrm{I}(V,[b,c])$ on U, and for any $P \in \Theta$ the orbits of G_P on $\Theta \setminus \{P\}$ are the same as the orbits of $\mathrm{I}(V,[b,c])_P$ on $\Theta \setminus \{P\}$. In particular, G is transitive Rank 3 on Θ. Note that in the symplectic case $\Theta = U$. Now part of Theorem IV of the Cameron-Kantor paper [6] says that the converse of this is true. More precisely we have:

Cameron-Kantor's Theorem IV (Partial Statement). *If $q > 2$ and $[b,c]$ is a nondegenerate metric pair on V for whose Witt index m we have $m > 3$, then for any $G \le \Gamma\mathrm{I}(V,[b,c])$ which is transitive Rank 3 on the hyperquadric $\Theta = \{P \in U : c(v) = 0 \text{ for all } v \in P\}$ we have $\Omega(V,[b,c]) \lhd G$, where in an appropriate obvious sense, in cases (1) to (5), we have put $\Omega = \mathrm{Sp}$ or SU or Ω^+ or Ω^- or Ω^0.*

Here is another great theorem of Kantor:

Kantor's Rank 3 Theorem (Running Formulation). *If $[b,c]$ is a nondegenerate metric pair on V for whose Witt index m we have $m > 3$, and if G is a transitive Rank 3 permutation group whose subdegrees coincide with the subdegrees of $\Gamma\mathrm{I}(V,[b,c])$, then G is isomorphic to a subgroup of $\Gamma\mathrm{I}(V,[b,c])$.*

In the above formulation of Theorem IV we have assumed $q > 2$ and $m > 3$ to avoid including the long list of exceptions, for which we refer to the original paper [6]. For similar reasons of brevity we have given only a running formulation of the Rank 3 Theorem, for the detailed version of which we refer to Kantor's original 1975 paper in the *Journal of Algebra*.

Result (3). *As an application of the above two theorems, by "inserting" suitable terms in the vectorial trinomial $E(Y) = Y^{q^n} + Y^q + XY$, in [3] we establish nice quartinomials, quintinomials, and sextinomials with Galois groups $\mathrm{SU}(n,q)$, $\mathrm{Sp}(n,q)$, and $\Omega^-(n,q)$, respectively, where in the unitary case n is assumed odd.*

Actually the above assertion about the unitary quartinomial is only wishful thinking. In other

words, we hope to deduce it from the above two theorems. Currently we have to fall back on the following powerful result proved in Liebeck's paper [9] by using CT = the Classification Theorem of finite simple groups. Again for brevity, we give only a rough formulation of the Liebeck Theorem.

Liebeck's Orbit Size Theorem (Rough Formulation). *If $[b,c]$ is a nondegenerate unitary or orthogonal pair on V for whose Witt index m we have $m > 3$, and if $G \leq \Gamma\mathrm{L}(V)$ has the same orbit sizes on U as $\Gamma\mathrm{I}(V,[b,c])$, then, with Ω as in Theorem IV, we have $\Omega(V,[b,c]) \lhd G \leq \Gamma\mathrm{I}(V,[b,c])$.*

Result (4). *As another application of Liebeck's Theorem, in a 2001 paper in* Trans. Amer. Math. Soc., *Nick Inglis and I have established nice polynomials with Galois groups $\mathrm{SU}(n,q)$, $\Omega^+(n,q)$, and $\Omega^0(n,q)$, respectively, where in the unitary case n is assumed even.*

Comments on Cameron-Kantor's Theorems II, III, V

Although the main aim of Cameron-Kantor's paper [6] is to prove Theorem I on double transitivity, for induction purposes they have to deal with antiflag transitive groups which is a larger class of groups. An antiflag in U is a point-hyperplane pair (P,H) with $P \notin H$. A subgroup G of $\Gamma\mathrm{L}(V)$ is said to be antiflag transitive on U if it can send any antiflag (P,H) to any other antiflag (P',H'). Moreover, the stabilizer group $G_W = \{g \in G : g(W) = W\}$ is said to be antiflag transitive on the hyperplane W of U if any antiflag in W can be sent to any other antiflag in W by a member of G_W. Cameron and Kantor can start off their induction because of a basic theorem proved in Wagner's 1961 *Math. Zeit.* paper which says that if $G \leq \Gamma\mathrm{L}(V)$ is doubly transitive on U, then G is antiflag transitive on U and, for every hyperplane W in U, the group G_W is antiflag transitive on W. Indeed, like Higman and McLaughlin who in their 1965 *Crelle Journal* paper initiated the study of Rank 3 subgroups of symplectic and unitary groups, and like Perin who in his 1972 paper [12] continued it, Wagner was an early pioneer in the robust revival of projective geometry around 1960, after a long slumber of over forty years. It is this slumber which perhaps caused my Guru Zariski to try to dampen my undue exuberance at the end of his beautiful course on projective geometry which I took under him in 1951, by saying to me that "Projective geometry is a beautiful dead subject. Do not try to do research in it." Indeed, it seems to be a prevalent view among young mathematicians that projective geometry is still slumbering. To dispel this myth is indeed my primary aim in writing this essay, and I propose to continue this task in my forthcoming commutative algebra textbook, to be published by the World Scientific Press.

Oscar Zariski

Two prominent players in this revival of projective geometry are Buekenhout and Shult who in their 1974 paper put forth the one-or-all axiom as the foundation of polar geometry. This codifies the property of points and lines on a hyperquadric which says that a point not on a line can either be joined to exactly one point of the line or to all of them. This paper is what Kantor built his Rank 3 Theorem on. In turn, the Buekenhout-Shult paper is heavily based on the previous work of Veldkamp. Another basic building block for the Cameron-Kantor paper [6] is the graph theoretic theorem of Feit and Higman on the nonexistence of most generalized polygons; incidentally this is Graham Higman, as opposed to Donald Higman who was cited above.

All this should explain why Theorems II and III, dealing with antiflag transitivity, are an integral part of Theorem I. Another fact achieved in Cameron-Kantor's Theorem II as well as Theorem V is a Rank 4 characterization of Dickson's simple group G_2. This group is the finite field version of the automorphism group of Caley's octonians which, in a way, are the eight-dimensional nonassociative incarnation of Hamilton's four-dimensional noncommutative quaternions. As shown in a forthcoming paper, as an application of Cameron-Kantor's Rank 4 characterization, I have constructed a nice equation with Galois group G_2.

It may be noted that the work of Perin [12] on the Rank 3 characterization of the symplectic and unitary groups was supplemented by the Rank 3 characterization of the orthogonal groups given by Kantor-Liebler in their 1982 paper [8], where on page 30 they say that it "uses classification theorems which depend upon deep results concerning the classification of finite simple groups." It needs to be checked how far these Rank 3 characterizations apply to semisimilarities and not just to similarities or isometries.

The fundamental paper [6] of Cameron-Kantor is very difficult to read and, as evolved in my recent discussions with Cameron, checking the details is a formidable task, in part because of the dependence on other difficult papers that themselves have substantial prerequisites. For instance, for Rank 3 characterizations of subgroups of semisimilarities,

Cameron-Kantor refer to the above-mentioned work of Perin and Kantor-Liebler. Moreover, the imprimitive case considered in Section 7 of the Cameron-Kantor paper needs to be augmented by the group $\Gamma L(n,4)$ inside $\Gamma L(n,16)$ studied in Proposition B on page 45 of the 1990 memoir [10] of Liebeck-Praeger-Saxl. The importance of the Cameron-Kantor paper is underscored by the fact that it is an essential building block of the equally versatile Singer cycle paper [7] of Kantor, which we shall cite in a moment. So it is very desirable to produce a revised transparent stand-alone version of the Cameron-Kantor paper. My forthcoming paper [5] with Inglis is a first shot at the revision project.

Iteration of Vectorial Polynomials and Kantor's $C^2 = R^4$ Theorem

As said above, as an application of Cameron-Kantor's Theorem I, in [2] it is shown that for the vectorial trinomial

$$E(Y) = Y^{q^n} + Y^q + XY$$

we have

$$\mathrm{Gal}(E, \mathrm{GF}(q)(X)) = \mathrm{GL}(n,q)$$

but

$$\mathrm{Gal}(E, \mathrm{GF}(p)(X)) = \Gamma L(n,q).$$

So how can it be arranged that the Galois group over $\mathrm{GF}(p)$ is $\mathrm{GL}(n,q)$? In other words, given any integer $\nu > 0$, how can we modify E to get a polynomial $\widetilde{E}$ so that $\mathrm{Gal}(\widetilde{E}, \mathrm{GF}(q)(X)) = \mathrm{GL}(n, q^\nu)$? Here the ideas of Carlitz, coupled with Kantor's Singer cycle paper [7], come to the rescue. Now $\mathrm{GF}(q^\nu)$ is obtained from $\mathrm{GF}(q)$ by adjoining a root of a monic irreducible polynomial

$$s(T) = \sum_{0 \le j \le \nu} s_j T^j$$

over $\mathrm{GF}(q)$ with $s_j \in \mathrm{GF}(q)$ and $s_\nu = 1$. Generalizing E, let

$$k = \mathrm{GF}(q) \subset \hat{k} \subset K$$

be fields, and consider a monic "vectorial q-polynomial"

$$\hat{E}(Y) = Y^{q^n} + \sum_{1 \le i \le n} A_i Y^{q^{n-i}}$$
$$\text{with } A_i \in \hat{k} \text{ and } s(A_n) \neq 0$$

over K, and following Carlitz and Drinfeld, let us define its generalized sth iterate $\hat{E}^{[s]}(Y)$ by putting

$$\hat{E}^{[s]}(Y) = \sum_{0 \le j \le \nu} s_i \hat{E}^{[[j]]}(Y)$$

where

$$\hat{E}^{[[j]]}(Y) = \hat{E}(\hat{E}(\cdots \hat{E}(Y) \cdots)) \text{ taken } j \text{ times}$$

is the ordinary jth iterate with $\hat{E}^{[[0]]}(Y) = Y$.

I conjecture that, perhaps excluding some special values of n and ν, we have $\mathrm{Gal}(E^{[s]}, \hat{k}(X)) = \mathrm{GL}(n, q^\nu)$. To state a possibly easier conjecture, let us say that we are in the Generic Case means that $K = \hat{k}(A_1, \ldots, A_n)$ and the elements $A_1, \ldots, A_n$ are algebraically independent over $\hat{k}$. In his path-breaking paper of 1896, Moore showed that in the Generic Case we have $\mathrm{Gal}(\hat{E}, K) = \mathrm{GL}(n,q)$; for a delightful discussion of how Moore and Carlitz were the forerunners of Drinfeld Module Theory, see Goss's 1996 Springer-Verlag book. The easier Generic Conjecture mentioned predicts that in the generic case we have $\mathrm{Gal}(\hat{E}^{[s]}, K) = \mathrm{GL}(n, q^\nu)$.

Just as the complex 2-space C^2 may be identified with the real 4-space R^4, which gives an embedding of $\mathrm{GL}(C^2)$ into the much larger group $\mathrm{GL}(R^4)$, similarly, upon letting $n' = n\nu$, we may regard $\mathrm{GL}(n, q^\nu)$ to be a subgroup of $\mathrm{GL}(n', q)$. In his Singer cycle paper [7], Kantor shows that such subgroups are essentially those subgroups which contain a Singer cycle. Note that a Singer cycle is a member of $\mathrm{GL}(n', q)$ whose order is $e = q^{n'} - 1$, as an element of the symmetric group S_e it is an e-cycle in the usual sense. Here is the precise version of

Kantor's Singer Cycle Theorem. *If $G \le \mathrm{GL}(n', q)$ contains a Singer cycle, then we have $\mathrm{GL}(n'/\mu, q^\mu) \lhd G$ for some μ.*

Result (5). *As an application of Kantor's Singer Cycle Theorem, in my forthcoming paper in the* Proceedings of the MSRI von Neumann Symposium *of 1999, I have proved the Generic Conjecture under the assumption that n is square-free and $\mathrm{GCD}(n, \nu) = 1 = \mathrm{GCD}(n, p)$.*

Result (6). *As another application of Cameron-Kantor's Theorem I, in our 2001 paper in the* Proceedings of the Indian Academy of Sciences, *Keskar and I proved the Generic Conjecture under the assumption that $\nu < n$ and $\mathrm{GCD}(n, \nu) = 1$.*

As I have noted at the end of [1], the symbol $\hat{E}$ is meant to remind us of elliptic curves and more generally of abelian varieties, and the notation $\hat{E}^{[s]}$ is meant to remind us of s-division points of abelian varieties, since in the theory of generalized iteration I am trying to mimic Serre's characteristic zero work on division points of elliptic curves and his unpublished generalization of it to abelian varieties.

Summary: An Overview

Postulating a finite universe, the three ways of measuring distance give rise to various finite classical groups as isometry groups. Their orbit sizes and subdegrees provide tools for constructing nice

polynomial equations having these isometry groups as Galois groups. An essential ingredient for this are the great theorems of Cameron and Kantor which recognize these groups by their transitivity properties. This they do mostly in terms of the subdegrees. A powerful theorem of Liebeck does the same thing in terms of orbit sizes. As a starting point we have the double transitivity theorem of Cameron and Kantor which gives rise to a trinomial having the collineation group as Galois group. The generalized iteration method of the Moore-Carlitz-Drinfeld module theory enables us to descend this Galois group down to the level of the full projective group. This descent is made possible by Kantor's Singer cycle theorem. The generalized iteration itself is a finite field analog of Serre's characteristic zero work on division points on elliptic curves and abelian varieties. Dickson's exceptional simple group is the finite field version of the automorphism group of Cayley's octonians which themselves are an eight-dimensional nonassociative incarnation of Hamilton's four-dimensional noncommutative quaternions. Cameron and Kantor's characterization of the Dickson group as a Rank 4 permutation group leads to a nice polynomial equation having that group as its Galois group.

The new revival of projective geometry underlies most of these advances in group theory. On one hand this revival was led by the pioneering work of Wagner who showed that double transitivity on points induces antiflag transitivity on hyperplanes and thus provided an inductive key to the work of Cameron and Kantor. This was followed up by the Rank 3 characterization of the symplectic and unitary groups first by Higman-McLaughlin and then by Perin, which was supplemented by the Rank 3 characterization of the orthogonal groups by Kantor-Liebler. On the other hand the said revival was led by the polar space characterization of Veldkamp which was continued first by Tits and then by Buekenhout and Shult. Yet another foundation of the Cameron-Kantor theory was provided by the graph theoretic theorem of Feit-Higman on the nonexistence of most types of generalized polygons.

References

[1] S. S. Abhyankar, Resolution of singularities and modular Galois theory, *Bull. Amer. Math. Soc.* **125** (2001), 1643–50.

[2] ____ , Nice equations for nice groups, *Israel J. Math.* **88** (1994), 1–24.

[3] ____ , Factorizations over finite fields, *Finite Fields and Applications,* London Math. Soc. Lecture Notes Ser., vol. 223, 1996, pp. 1–21.

[4] ____ , Symplectic groups and permutation polynomials, Part I, *Proceedings of the International Colloquium on Algebra, Arithmetic, and Geometry, held at Tata Institute of Fundamental Research in January 2000*, Narosa Publishing House (distributed by the American Mathematical Society), 2002.

[5] S. S. Abhyankar and N. F. J. Inglis, Thoughts on symplectic groups and symplectic equations, *Proceedings of the Purdue Conference on Algebraic Geometry and its Applications, in honor of Abhyankar's 70th Birthday*, Springer-Verlag, 2002.

[6] P. J. Cameron and W. M. Kantor, 2-Transitive and antiflag transitive collineation groups of finite projective spaces, *J. Algebra* **60** (1979), 384–422.

[7] W. M. Kantor, Linear groups containing a Singer cycle, *J. Algebra* **62** (1980), 232–4.

[8] W. M. Kantor and R. L. Liebler, The rank 3 permutation representations of the finite classical groups, *Trans. Amer. Math. Soc.* **271** (1982), 1–71.

[9] M. W. Liebeck, Characterization of classical groups by orbit sizes on the natural module, *Proc. Amer. Math. Soc.* **124** (1996), 2961–6.

[10] M. W. Liebeck, C. Praeger, and J. Saxl, The maximal factorizations of the finite simple groups and their automorphism groups, *Mem. Amer. Math. Soc.* **86** (1990), Number 432, 1–151.

[11] K. H. Parshall and D. E. Rowe, *The Emergence of the American Mathematical Research Community, 1876–1900: J. J. Sylvester, Felix Klein, and E. H. Moore*, History of Mathematics, vol. 8, American Mathematical Society, 1994.

[12] D. Perin, On collineation groups of finite projective spaces, *Math. Zeit.* **126** (1972), 135–42.