ON GALOIS GEOMETRIES

By BENIAMINO SEGRE

1. Introduction

Finite spaces, i.e. finite sets of point-elements on which some geometric structure is superimposed, are of importance in many branches of applied mathematics, e.g. statistics (Bose[6], Seiden[57]). Quite recently, they have been used in various efforts to build up a geometry which would be better adapted to the quantistic theories (Järnefelt[23, 24], Järnefelt and Kustaanheimo[25], Kustaanheimo[27–32]).

The present exposition will dwell chiefly on the geometric aspects in the study of the simplest and more important among finite spaces, the so-called *Galois spaces*, $S_{r,q}$, i.e. the linear spaces—of any dimension r—over a $GF(q)$. These spaces can be characterized as those finite graphic (or projective) spaces where Fano's postulate (existence of at least three distinct points on every line) and Desargues' theorem (on homological triangles) hold, the latter condition being a consequence of the former if $r \geqslant 3$. In every graphic space satisfying these conditions Pappus's theorem also holds, which is tantamount to the Maclagan–Wedderburn theorem affirming the commutativity of every finite field. Attempts at proving this theorem geometrically—by directly showing the validity of Pappus's or equivalent theorems in those spaces—have also been made (cf., for example, Locher[34]), but up to now without success (cf. Artin[1], p. 75). Quite recently I have added a fresh attempt [Segre[54]], with a view to a geometric proof of the Maclagan–Wedderburn theorem through a study of certain properties of non-linear non-commutative geometry, concerning reguli in projective spaces over a skew field and their plane sections.

Many of the ideas and results of algebraic geometry can be adapted to Galois spaces without difficulty, paying attention to the fact that the ground field $GF(q)$ of a $S_{r,q}$ has non-zero characteristic p (where $q = p^h$, for some positive integer h), and that the field is not algebraically closed. Additional questions and properties arise from the finiteness of the field, and some of them are dealt with in § 2.

In § 3 we briefly indicate how certain algebraic subvarieties of $S_{r,q}$ can be characterized by means of very simple properties of a numerical and graphical character.

Finally, §§ 4 and 5 concern the study of *k-sets*, i.e. sets of k points of

$S_{r,q}$, for $r = 2$ and $r \geqslant 3$ respectively; and it has to be noticed that each of them can always be considered, in different ways, as the set of points of an algebraic variety. The theory has been recently developed for certain k-sets of special interest, called *k-arcs* and *k-caps*; but very much remains to be done in this direction.

Our exposition—while rather sketchy—will implicitly suggest a number of further questions which, however, we shall pass over for lack of time.

2. Some properties of algebraic varieties

Projective geometry and non-Euclidean geometry of $S_{r,q}$ have many interesting group-theoretic aspects, which were substantially known a long time ago (Jordan[26], Dickson[10]). However, only recently have appropriate geometric terminology and reasoning been employed in order to clarify them, particularly for the smallest values of r and q. Thus the geometry of $S_{r,3}$ has been investigated in detail for $r \leqslant 4$ (Edge[11, 13]), and used for studying the group of the 27 lines of the general cubic surface and its separation into 25 conjugate classes (Edge[16]), as well as other group properties in $S_{5,3}$ (Edge[18]). Also the geometry of $S_{2,q}$ has been described, especially for $q = 5, 7, 11$ (Edge[14, 17]), and suggestive geometric arguments have been devised for establishing the known isomorphism between the linear fractional group $LF(4, 2)$ and the alternating group A_8 (Edge[12]), and between $LF(2, 9)$ and A_6 (Edge[15]).

The number of linear subspaces of $S_{r,q}$ of a given dimension can be easily obtained (Segre[46], n. 159); thus, for instance, the number of points of $S_{r,q}$ is $1+q+q^2+\ldots+q^r$. Similar questions may be asked for any algebraic variety of $S_{r,q}$; but the answer is then usually far less simple and not precisely known. Estimates for the number of points lying on certain algebraic varieties have been obtained, and in special cases reasonably simple exact expressions of this number were given, by means of deep and often rather intricate algebraic and analytic arguments (Châtelet[9], Vandiver[64, 65], Hua and Vandiver[19–22], Weil[66], Lang and Weil[33], Carlitz[8]). Here we confine ourselves to quoting the result (Hua and Vandiver[22]) $N = (q-1)[(q-1)^{r-1}+(-1)^r]/q$ concerning the number N of solutions $x \in GF(q)$, with $x_1 x_2 \ldots x_r \neq 0$, of the equation $c_1 x_1^{n_1} + c_2 x_2^{n_2} + \ldots + c_r x_r^{n_r} = 0$, where the c's are given non-zero elements of $GF(q)$, the n's are integers satisfying $0 < n_i < q-1$ such that the numbers $(n_i, q-1)$ are relatively prime in pairs, and $r > 2$.

Some of the questions of the type indicated above can be conveniently treated by means of purely combinatorial and geometric methods. For instance, a well-known algebraic result (Dickson[10]) can be stated by saying that *every irreducible conic of* $S_{2,q}$ *contains precisely* $q+1$ *points*, and this has also been freshly proved by showing directly that in $S_{2,q}$ there are as many irreducible conics as there are conics containing exactly $q+1$ points, both numbers of conics being equal to q^5-q^2 (Segre[53]). Thus the whole theory of quadratic forms over $GF(q)$ can be geometrized (Primrose[39]), and partially new results can be obtained as follows (Segre[55]).

If $r = 2s$ is even ($s \geqslant 1$), the non-singular quadrics of $S_{r,q}$ are two by two homographic, and every one of them contains a positive number of linear subspaces $S_{n,q}$ of $S_{r,q}$, of each dimension $n = 0, 1, \ldots, s-1$, this number being

$$\prod_{i=0}^{n} (q^{s-i}-1) \prod_{i=s-n}^{s} (q^i+1) \Big/ \prod_{i=0}^{n} (q^{n-i+1}-1).$$

If $r = 2s-1$ is odd, the non-singular quadrics of $S_{r,q}$ fall into two different types, the *hyperbolic* and the *elliptic*, those of the same type being two by two homographic. Every hyperbolic quadric contains a positive number of $S_{n,q}$, of each dimension $n = 0, 1, \ldots, s-1$, this number being

$$\prod_{i=0}^{n} (q^{s-i}-1) \prod_{i=s-n-1}^{s-1} (q^i+1) \Big/ \prod_{i=0}^{n} (q^{n-i+1}-1)$$

(as usual, the spaces of maximum dimension $s-1$ then constitute two different systems, and those of lower dimension a single one). Every elliptic quadric contains no $S_{s-1,q}$ and a positive number of $S_{n,q}$, of each dimension $n = 0, 1, \ldots, s-2$, this number being

$$\prod_{i=0}^{n} (q^{s-i-1}-1) \prod_{i=s-n}^{s} (q^i+1) \Big/ \prod_{i=0}^{n} (q^{n-i+1}-1).$$

It has to be noticed that a non-singular quadric f of $S_{r,q}$ defines a polarity, which is a null system if, and only if, $p = 2$ (i.e., if q is even). In this case, the polarity is non-singular if r is odd, while it has one, and only one, singular point O if r is even; the point O is called the *kernel* of f, does not lie on f and is the point of concurrence of all the tangent primes of f. This is but an example of the discrepancies which may appear in algebraic geometry between the case where the characteristic of the ground field has the value $p = 2$ and the case $p \neq 2$; further examples have been investigated (Boughon, Nathan and Samuel[7], Segre[50]), and deep reasons for the occurrence of such discrepancies have been given (Segre[55]).

Other special algebraic varieties of a Galois space have been studied, as for instance the rational normal curves of $S_{r,q}$ (Segre[49]), and the cubic surfaces of $S_{3,q}$, with odd q. It has been shown (Rosati[42]) that the equation of the 27 lines and the equation of the 45 tritangent planes of such a surface are always reducible, and the various kinds of reducibility have been classified; moreover, the exact number of points lying on the surface has been obtained in several cases (Rosati[41]). Another interesting result is the coincidence between the locus of the kernels of the conics lying on the Veronesean representing the quadrics of $S_{r,q}$, with even q, and the Grassmannian of the lines of $S_{r,q}$ (Tallini).

An upper bound for the number of the points of an algebraic curve will be given later (§ 4).

3. Characterization of certain algebraic varieties

While every irreducible conic of $S_{2,q}$ consists of a set of $q+1$ points of $S_{2,q}$ (§ 2) no three of which are collinear, it has been proved that *the converse is true if, and only if, q is odd* (Segre[47,48]) *or if* $q = 2, 4$ (Segre[51]). Another similar result is that, if q is odd, any set of $q+1$ points of $S_{3,q}$ no four of which are in a plane consists of the points of a twisted cubic curve (Segre[49]). These very simple but rather unexpected results have been the starting-point of further investigations, some of which we shall now summarize.

In $S_{r,q}$, where q is odd and $r \geqslant 3$, let us consider any set of k points such that every line of $S_{r,q}$ containing three distinct points of the set consists entirely of points of the set. It has been proved (Tallini[58,59]) that, if $1+q+\ldots+q^{r-1} \leqslant k < 1+q+\ldots+q^r$, then the set can only be the set of all the points of one of the following algebraic varieties: (i) the variety consisting of a prime and a $S_{t,q}$ of $S_{r,q}$ $(t = -1, 0, 1, \ldots, r-1)$; (ii) a non-singular quadric in a space of even dimension, or a quadric cone projecting such a quadric from its vertex; (iii) a non-singular hyperbolic quadric in a space of odd dimension, or a quadric cone projecting such a quadric from its vertex. Also the case of q even has been treated (*l.c.*). Moreover, similar characterizations have been obtained for non-singular elliptic quadrics in spaces of odd dimension and their projecting cones (Tallini[60]), as well as for certain cubic surfaces of $S_{3,q}$ with odd q (Tallini[63]).

Finally, the Veronese surface of $S_{5,q}$ can be characterized as follows (Tallini[62]). In a $S_{r,q}$, where $r \geqslant 5$ and q is odd, consider any set of $k \geqslant q^2+q+1$ planes two by two incident, such that no three of these have a common point; then $r = 5$, $k = q^2+q+1$, and the set consists precisely of the tangent planes of a Veronese surface.

In the sequel we shall give some results improving those stated at the beginning of the present § 3. By using them suitably, similar improvements of the remaining results of this § 3 could be easily deduced.

4. On planar k-sets

With every k-set of $S_{2,q}$ we can associate, for any $n = 1, 2, \ldots$, an integer N_n given by the maximum number of points of the k-set which lie on some algebraic curve of order n. The consideration of N_n is significant only for the smallest values of n, precisely when $\frac{1}{2}n(n+3) < k$, and then we have $\frac{1}{2}n(n+3) \leqslant N_n \leqslant k$. Not much is known about these characters N_n; for instance, it has been proved (Segre[52]) that, *if* $N_1 = 2$ *and* $N_2 \geqslant \frac{1}{2}q+2$, *then* $N_2 = k$, i.e. the k-set lies entirely on a conic, *with only one possible exception for even* q, *when it can happen that* $N_2 = k-1$, the k-set consisting then of $k-1$ points of a conic and of the latter's kernel.

It may be noticed that the character N_1 can be defined—more generally—for k-sets belonging to any projective plane of order q, namely to a graphic finite plane, Π_q say, each line of which contains $q+1$ points. Of very particular importance are the k-sets of Π_q having $N_1 = 2$ (i.e. containing no triplet of collinear points), which are called simply *k-arcs*. It can be shown (Qvist[40]) that, for no k-arc of Π_q may k be greater than $q+1$ or $q+2$ according as q is odd or even, these maximum values of k being in fact reached by some k-arcs, called *ovals* (Segre[47, 48]).

The consideration and study of ovals are important also on planes Π_q which are non-Desarguesian, i.e. non-Galoisian (Ostrom[37]), as can be anticipated from the fact that, *when q is odd, every oval of $S_{2,q}$ is simply a conic* (§ 3). *When $q = 2^h$ is even,* we obtain an oval in a Galois plane $S_{2,q}$ by adding the kernel to the $q+1$ points of a conic of $S_{2,q}$ (§ 2); *this is then the only way of obtaining an oval if $h = 1, 2, 3$ (i.e. $q = 2, 4, 8$), but there are always ovals not obtainable in this manner if $h > 3$, with a single possible exception for $h = 6$* (Segre[51]). A complete classification of ovals in a plane $S_{2,q}$, with q even, remains however to be done.

The results stated above concerning the maximum value of k, for k-arcs of Π_q, can be extended as follows (Barlotti[4]): *if, for a k-set of Π_q, the character $N_1 = n$ is such that $2 < n \leqslant q$, then $k \leqslant (n-1)q+n$ or $k \leqslant (n-1)q+n-2$ according as q is or is not divisible by n.*

It may be noticed that, if a k-set of $S_{2,q}$ lies on an algebraic curve of order $n \leqslant q$ free from rectilinear components, then the k-set has $N_1 \leqslant n$. The last result can in this case be refined, by proving (Segre[55]) that:

The number k of points of $S_{2,q}$ lying on an algebraic curve of order $n \leqslant q$ of $S_{2,q}$ satisfies the limitation $k \leqslant nq+1$, where the equality sign *occurs if, and only if, the curve consists of n distinct lines of a pencil. Moreover, if the curve does not break up into n lines, then*

$$k \leqslant (q+1)(n-1)-[\tfrac{1}{2}n]+1,$$

where the equality sign may occur only if n is even or if the curve has some rectilinear component.

We shall now confine ourselves to the study of the k-arcs of Π_q or, in particular, of $S_{2,q}$. Such a k-arc, K, is said to be *incomplete* or *complete* according as there is or there is not a $(k+1)$-arc containing it (for instance, every oval is manifestly complete); moreover, a line of the plane is said to be *external* to K or a *tangent*, or a *secant* of K according as it has 0, or 1, or 2 distinct points in common with K. Clearly, every point of K lies on $k-1$ secant lines and so on

$$t = q-k+2$$

distinct tangents (each of which is said *to touch K at the point*). To any point of the plane not lying on K we can attach an integer i, called the *index* of the point and satisfying the limitations

$$0 \leqslant i \leqslant [\tfrac{1}{2}k],$$

given by the number of distinct secants of K containing it. Denoting by c_i the number ($\geqslant 0$) of points of the plane not lying on K and having index i, K is obviously complete if, and only if, $c_0 = 0$; more generally, if $c_0 = c_1 = \ldots = c_{\alpha-1} = 0$, but $c_\alpha \neq 0$, K is said to be *complete of index* α.

The projective characters c_i, as well as other integers attached in a similar way to K, are connected by a system of Diophantine equations; and a simple discussion of this system gives necessary conditions in order that K be complete, possibly of a given index (Segre[55], Sce[44, 45]). The question of obtaining sufficient conditions is much more difficult, and has been studied only on Galois planes and in special cases.

For instance, it has been shown (Segre[49], Tallini[61]) that no q-arc of $S_{2,q}$ can be complete; on the contrary (Lombardo-Radice[35]), if $q \equiv 3 \pmod 4$, there certainly exist some complete $\frac{1}{2}(q+5)$-arcs in any $S_{2,q}$. Moreover (Segre[55]), while the necessary arithmetical conditions for completeness are, e.g. satisfied for $q = 13$, $k = 7$, there exists no complete 7-arc in $S_{2,13}$; finally (Segre[51, 55]), for the first non-trivial values of q:

$$q = 7, \quad q = 8, \quad q = 9,$$

the exact values of k, such that there exists some complete k-arc in $S_{2,q}$ are

$$k = 6, 8, \quad k = 6, 10, \quad k = 6, 7, 8, 10$$

respectively. The known complete k-arcs which are not ovals have been obtained by different methods (see also Scafati[43]), one of which (Lunelli and Sce[36]) has required the use of an electronic calculating machine; and many of those k-arcs are endowed with remarkable groupal properties.

Other results on completeness have been deduced from the following theorem (Segre[55]), established in its turn by means of certain considerations of algebraic geometry having a much wider applicability.

Theorem. If K denotes any k-arc of $S_{2,q}$ for which (putting as above $t = q-k+2$) $t > 0$, then it is possible to associate with K an algebraic envelope of lines of $S_{2,q}$, Γ say, containing no pencil of lines with the centre on K as a component, and such that:

if q is even, Γ has class t, and the t lines of Γ issuing from any point of K coincide with the t distinct tangents of K at the same point;

if q is odd, Γ has class $2t$, without being an envelope of class t counted twice, and the $2t$ lines of Γ issuing from any point of K coincide with the t distinct tangents of K at the same point, each counted twice.

In the first of the two cases considered in the theorem, the envelope Γ has therefore class t and contains as elements each of the

$$kt = t(q-t+2)$$

tangents of K. From the dual of a previous result we see that, if q is sufficiently large with respect to t, the envelope Γ must contain some pencil of lines as a component; the centre of such a pencil does not lie on K and, by aggregating it to K, we obtain a $(k+1)$-arc containing K, so that K is certainly incomplete. The argument now sketched, suitably completed, shows for instance that:

If q is even and $t = 1, 2, 3, 4$, there exists no complete $(q-t+2)$-arc in $S_{2,q}$, save for just one exception, given by the complete 6-arcs of $S_{2,8}$.

The argument can be further developed, and also suitably modified so as to adapt to the second case of the theorem (q odd); thus new results can be established, whose qualitative content is expressed by the following theorem.

If a denotes any non-negative constant and $k \geqslant q-a$, where q is sufficiently large with respect to a, then every k-arc of $S_{2,q}$ is contained in one and only one oval (i.e. a conic, if q is odd), and is therefore incomplete if it is not an oval.

5. On spatial k-sets

The notion of k-arc can be extended to higher spaces, by considering in $S_{r,q}$ sets of k points any $s+1$ distinct of which are linearly independent

$(2 \leqslant s \leqslant r)$; such a set will be denoted by $k^s_{r,q}$, and the maximum of k for given r, q, s will be indicated by $m^s_{r,q}$. Of particular importance are the cases when $s = r$ or $s = 2 < r$: then the k-set will be called a *k-arc* or a *k-cap* of $S_{r,q}$ respectively.

If c is an integer satisfying $1 \leqslant c \leqslant r-2$, $c < k$, then the projection of any $k-c$ points of a k-arc of $S_{r,q}$, from the $S_{c-1,q}$ joining the remaining c points, onto a $S_{r-c,q}$ skew to $S_{c-1,q}$, is clearly a $(k-c)$-arc of $S_{r-c,q}$. By applying the last theorem of § 4 and this remark, we obtain (Segre[55]) that:

If q is odd and sufficiently large with respect to r, then $m^r_{r,q} = q+1$, the k-arcs with maximum k $(= q+1)$ being the rational normal curves of $S_{r,q}$. If, moreover, q is sufficiently large with respect to $q-k$, then every k-arc of $S_{r,q}$ is contained in a rational normal curve of $S_{r,q}$.

The characters m of the k-caps have a special significance in statistics. For them, the following results have been proved:

$$\left.\begin{array}{ll} m^2_{3,q} = q^2+1 & \text{if } q \text{ is odd,} \\ q^2+1 \leqslant m^2_{3,q} \leqslant q^2+q+2 & \text{if } q \text{ is even,} \\ m^2_{r,2} = 2^r & \text{for any } r \geqslant 2, \end{array}\right\} \quad \text{(Bose[6]).}$$

$$m^2_{3,4} = 17 \qquad \text{(Seiden[57], Barlotti[2]).}$$

$$m^2_{r,q} \leqslant q^{r-1} - (q-5)\sum_{i=0}^{r-4} q^i + 1 \qquad \text{if } q \text{ is odd and } r \geqslant 4 \quad \text{(Barlotti[5]).}$$

$$m^2_{4,q} \geqslant 2q^2 + 2(q+1)\left[\tfrac{1}{4}q\right] - 6q - 2 \qquad \text{(Segre[55]).}$$

Moreover, it has been established (Barlotti[2]) that:

If q is odd, the k-caps of $S_{3,q}$ having maximum k $(= q^2+1)$ coincide with the sets of points of an elliptic quadric of $S_{3,q}$.

If $q > 17$, this property is a particular case of the following (given by Segre[55], and also including another result by Barlotti[3]):

If q is odd and $k \geqslant q^2-q+19$, every k-cap of $S_{3,q}$ lies in an elliptic quadric of $S_{3,q}$.

Stronger improvements can be derived from the last theorems of § 4. Thus, for instance (Segre[55]),

If a denotes any positive constant, and q is odd and sufficiently large with respect to a, then any k-cap of $S_{3,q}$ for which $k \geqslant q^2 - aq$ is contained in an elliptic quadric of $S_{3,q}$; moreover, under the same conditions for q and if $r \geqslant 4$, for every k-cap of $S_{r,q}$ we have $k < q^{r-1} - aq^{r-2}$.

Also the case when q is even has been studied further, even if not so extensively as the case when q is odd. First of all, one of the results by Bose previously quoted has been completed by proving (Barlotti[2]) that, *if* $q > 2$ *is even, then* $m^2_{3,q} = q^2+1$. Moreover, it has been shown that, for even q (e.g. for $q = 8$), *there exist* (q^2+1)*-caps of* $S_{3,q}$ *which are not quadrics*; however, *any such* (q^2+1)*-cap defines a null polarity*, exactly in the same way as in the case of a quadric (cf. Segre[56]).

We conclude by remarking that the sets $k^s_{r,q}$, considered above, are in their turn generalized by the k-sets of $S_{r,q}$ such that, if they contain any $(s+1)$-subset of linearly dependent points, then the space joining such a subset wholly consists of points of the k-set. Every k-set of this type defines a non-negative index δ, and can therefore be indicated by $k^{s,\delta}_{r,q}$, δ being the maximum dimension of the subspaces of $S_{r,q}$ lying entirely in the k-set (clearly, the $k^{s,0}_{r,q}$'s thus coincide with the $k^s_{r,q}$'s). Up to now, only the $k^{2,\delta}_{r,q}$'s (or k-caps of index δ) have been studied (Tallini[59]); and we have already given some of the results concerning them.

REFERENCES

[1] Artin, A. *Geometric Algebra.* Interscience Publ., New York, 1957.

[2] Barlotti, A. Un'estensione del teorema di Segre–Kustaanheimo. *Boll. Un. mat. ital.* (3), 10, 498–506 (1955).

[3] Barlotti, A. Un'osservazione sulle k-calotte degli spazi lineari finiti di dimensione tre. *Boll. Un. mat. ital.* (3), 11, 248–252 (1956).

[4] Barlotti, A. Sui $\{k; n\}$-archi di un piano lineare finito. *Boll. Un. mat. ital.* (3), 11, 553–556 (1956).

[5] Barlotti, A. Una limitazione superiore per il numero di punti appartenenti a una calotta $\mathscr{C}(k, 0)$ di uno spazio lineare finito. *Boll. Un. mat. ital.* (3), 12, 67–70 (1957).

[6] Bose, R. C. Mathematical theory of factorial design. *Sankhyā,* 8, 107–166 (1947).

[7] Boughon, P., Nathan, J. and Samuel, P. Courbes planes en caractéristique 2. *Bull. Soc. math. Fr.* 83, 275–278 (1955).

[8] Carlitz, L. A note on nonsingular forms in a finite field. *Proc. Amer. Math. Soc.* 7, 27–29 (1956).

[9] Châtelet, F. Les courbes de genre 1 dans un champ de Galois. *C.R. Acad. Sci., Paris,* 224, 1616–1618 (1947).

[10] Dickson, L. E. *Linear Groups with an Exposition of the Galois Field Theory.* Teubner, Leipzig, 1901.

[11] Edge, W. L. Geometry in three dimensions over $GF(3)$. *Proc. Roy. Soc.* A, 222, 262–286 (1953).

[12] Edge, W. L. The geometry of the linear fractional group $LF(4, 2)$. *Proc. Lond. Math. Soc.* (3), 4, 317–342 (1954).

[13] Edge, W. L. Line geometry in three dimensions over $GF(3)$, and the allied geometry of quadrics in four and five dimensions. *Proc. Roy. Soc.* A, 228, 129–146 (1955).

[14] Edge, W. L. 31-point Geometry. *Math. Gaz.* 39, 113–121 (1955).
[15] Edge, W. L. The isomorphism between $LF(2, 3^2)$ and $\mathscr{A}_6$. *J. Lond. Math. Soc.* 30, 172–185 (1955).
[16] Edge, W. L. The conjugate classes of the cubic surface group in an orthogonal representation. *Proc. Roy. Soc.* A, 233, 126–146 (1955).
[17] Edge, W. L. Conics and orthogonal projectivities in a finite plane. *Canad. J. Math.* 8, 362–382 (1956).
[18] Edge, W. L. The geometry of an orthogonal group in six variables. *Proc. Lond. Math. Soc.* (3), 8, 416–446 (1958).
[19] Hua, L. K. and Vandiver, H. S. On the existence of solutions of certain equations in a finite field. *Proc. Nat. Acad. Sci., Wash.*, 34, 258–263 (1948).
[20] Hua, L. K. and Vandiver, H. S. Characters over certain types of rings with applications to the theory of equations in a finite field. *Proc. Nat. Acad. Sci., Wash.*, 35, 94–99 (1949).
[21] Hua, L. K. and Vandiver, H. S. On the number of solutions of some trinomial equations in a finite field. *Proc. Nat. Acad. Sci., Wash.*, 35, 477–481 (1949).
[22] Hua, L. K. and Vandiver, H. S. On the nature of the solutions of certain equations in a finite field. *Proc. Nat. Acad. Sci., Wash.*, 35, 481–487 (1949).
[23] Järnefelt, G. A plane geometry with a finite number of elements. *Veröf. finn. geod. Inst.* n. 36 (1949).
[24] Järnefelt, G. Reflections on a finite approximation to Euclidean geometry. Physical and astronomical prospects. *Ann. Acad. Sci. Fenn.*, ser. A, 1, n. 96 (1951).
[25] Järnefelt, G. and Kustaanheimo, P. An observation on finite geometries. *Comptes Rendus XI Congr. Math. Scand.* 166–182. Trondheim, 1949.
[26] Jordan, C. *Traité des substitutions et des équations algébriques*. Paris, 1870.
[27] Kustaanheimo, P. A note on a finite approximation of the Euclidean plane geometry. *Soc. Sci. Fenn. Comm. Phys.-Math.* 15, 19 (1950).
[28] Kustaanheimo, P. On the fundamental prime of a finite world. *Ann. Acad. Sci. Fenn.*, ser. A, 1, n. 129 (1952).
[29] Kustaanheimo, P. Über die Versuche, ein logisch finites Weltbild aufzubauen. *Actes congr. int. Un. int. Phil. Sci.* 2, 60–65. Zürich, 1954.
[30] Kustaanheimo, P. On the relation of order in geometries over a Galois field. *Soc. Sci. Fenn. Comm. Phys.-Math.* 20, 8 (1957).
[31] Kustaanheimo, P. On the relation of congruence in finite geometries. *R.C. Mat. pura appl.* 16, 286–291 (1957).
[32] Kustaanheimo, P. On the relation of order in finite geometries. *R.C. Mat. pura appl.* 16, 292–296 (1957).
[33] Lang, S. and Weil, A. Number of points of varieties in finite fields. *Amer. J. Math.* 76, 819–827 (1954).
[34] Locher, L. Struktur der Axiome der projectiven Geometrie. *C.R. Congr. Int. Oslo 1936*, 2, 167–168 (1937).
[35] Lombardo-Radice, L. Sul problema dei k-archi completi di $S_{2,q}$. *Boll. Un. mat. ital.* (3), 11, 178–181 (1956).
[36] Lunelli, L. and Sce, M. Sulla ricerca dei k-archi completi mediante calcolatrice elettronica. *R.C. Convegno Reticoli geom. proi.* 81–86. Palermo, 1957.
[37] Ostrom, T. G. Ovals, dualities, and Desargues's theorem. *Canad. J. Math.* 7, 417–431 (1955).

[38] Panella, G. F. Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito. *Boll. Un. mat. ital.* (3), 10, 507–513 (1955).

[39] Primrose, E. J. F. Quadrics in finite geometries. *Proc. Camb. Phil. Soc.* 47, 299–304 (1951).

[40] Qvist, B. Some remarks concerning curves of the second degree in a finite plane. *Ann. Acad. Sci. Fenn.* ser. A, I, no. 134 (1952).

[41] Rosati, L. A. Sul numero dei punti di una superficie cubica in uno spazio lineare finito. *Boll. Un. mat. ital.* (3), 11, 412–418 (1956).

[42) Rosati, L. A. L'equazione delle 27 rette della superficie cubica generale in un corpo finito (Note I, II). *Boll. Un. mat. ital.* (3), 12, 612–626 (1957); (3), 13, 84–99 (1958).

[43] Scafati, M. Sui 6-archi completi di un piano lineare $S_{2,8}$. *R.C. Conv. Reticoli geom. proi.* 128–132. Palermo, 1957.

[44] Sce, M. Sui k_q-archi di indice h. *R.C. Conv. Reticoli geom. proi.* 133–135. Palermo, 1957.

[45] Sce, M. Sulla completezza degli archi nei piani proiettivi finiti. *R.C. Acc. Naz. Lincei*, (8), 25, 43–51 (1958).

[46] Segre, B. *Lezioni di geometria moderna.* I. Zanichelli, Bologna, 1948.

[47] Segre, B. Sulle ovali dei piani lineari finiti. *R.C. Acc. Naz. Lincei*, (8), 17, 141–142 (1954).

[48] Segre, B. Ovals in a finite projective plane. *Canad. J. Math.* 7, 414–416 (1955).

[49] Segre, B. Curve razionali normali e k-archi negli spazi finiti. *Ann. Mat.* (4), 39, 357–379 (1955).

[50] Segre, B. Intorno alla geometria sopra un corpo di caratteristica due. *Rev. Fac. Sci. de l'Univ. d'Istanbul* (A), 21, 97–123 (1956).

[51] Segre, B. Sui k-archi nei piani finiti di caratteristica due. *Rev. Math. pures appl.* 2, 283–294 (1957).

[52] Segre, B. Sulle geometrie proiettive finite. *R.C. Conv. Reticoli geom. proi.* 46–61. Palermo, 1957.

[53] Segre, B. Sulla geometria sopra un campo a caratteristica. *Archimede*, 10, 53–60 (1958).

[54] Segre, B. Fondamenti di geometria non lineare sopra un corpo sghembo. *R.C. circ. mat. Palermo*, (2), 7, 81–122 (1958).

[55] Segre, B. Le geometrie di Galois. (Due to appear in *Ann. Mat.*)

[56] Segre, B. On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two. (Due to appear in *Acta Arithm.*)

[57] Seiden, E. A theorem in finite projective geometry and an application to statistics. *Proc. Amer. Math. Soc.* 1, 282–286 (1950).

[58] Tallini, G. Sulle k-calotte degli spazi lineari finiti (Note I, II). *R.C. Acc. Naz. Lincei*, (8), 20, 311–317, 442–446 (1956).

[59] Tallini, G. Sulle k-calotte di uno spazio lineare finito. *Ann. Mat.* (4), 42, 119–164 (1956).

[60] Tallini, G. Caratterizzazione grafica delle quadriche ellittiche negli spazi finiti. *R.C. Mat. pura appl.* 16, 328–352 (1957).

[61] Tallini, G. Sui q-archi di un piano lineare finito di caratteristica $p=2$. *R.C. Acc. Naz. Lincei*, (8), 23, 242–245 (1957).

[62] Tallini, G. Una proprietà grafica caratteristica della superficie di Veronese negli spazi finiti (Note I, II). *R.C. Acc. Naz. Lincei*, (8), 24, 19–23, 135–138 (1958).

[63] Tallini, G. Caratterizzazione grafica di certe superficie cubiche di $S_{3,q}$. (Due to appear in *R.C. Acc. Naz. Lincei.*)

[64] Vandiver, H. S. Limits for the number of solutions of certain general types of equations in a finite field. *Proc. Nat. Acad. Sci., Wash.*, 33, 236–242 (1947).

[65] Vandiver, H. S. Quadratic relations involving the numbers of solutions of certain types of equations in a finite field. *Proc. Nat. Acad. Sci., Wash.*, 35, 681–685 (1949).

[66] Weil, A. Number of solutions of equations in finite fields. *Bull. Amer. Math. Soc.* 55, 497–508 (1949).