the terms in Z is for $k > c_{15}$

$$\leqslant 2\log k\cdot c_7 \log\big(k(1+\log k)\big) < 3c_7\log^2 k. \tag{4.5}$$

Hence if we determine $\omega+1$ as the exponent realizing the maximum on the left of (1.7) and take

$$N = 3c_7\log^2 k,$$

(2.3) is not violated and thus

$$|Z| \geqslant \left(\frac{3c_7\log^2 k}{22\,(\log^2 k\log\log k + 3c_7\log^2 k)}\right)^{3c_7\log^2 k}$$

or for $k > c_{16}$

$$|Z| > e^{-4c_7\log^2 k\log\log\log k}$$

Putting this, (4.1) and (4.2) into (3.4) and taking in account that owing to $\gamma \geqslant \frac{1}{2}$ we have for $k > c_{17}$

$$P^{\frac{2}{5}} < \tfrac{1}{2}P^{\frac{1}{2}-\frac{3c_7+1}{\log\log k}}\cdot e^{-4c_7\log^2 k\log\log\log k} \leqslant \tfrac{1}{2}P^{\gamma-\frac{3c_7+1}{\log\log k}}\cdot e^{-4c_7\log^2 k\log\log\log k},$$

we get, using also (2.3),

$$\max_{1\leqslant v\leqslant P}|U(v,\chi)| > (2e\log\log k)^{-(\omega+1)}\tfrac{1}{2}P^{\gamma-\frac{3c_7+1}{\log\log k}}\cdot e^{-4c_7\log^2 k\log\log\log k}$$

$$> P^{\gamma-\frac{4c_7}{\log\log k}}\cdot e^{-\frac{3}{2}\log^2 k\log\log k\log\log\log k}$$

$$> P^{\gamma}\cdot e^{-2\log^2 k\log\log k\log\log\log k} = P^{\gamma-2\frac{\log\log\log k}{\log\log k}},$$

which proves the theorem.

References

[1] E. Landau, *Über die Klassenzahl imaginärquadratischer Zahlenkörper*, Gött. Nachr. 1918, p. 285-295.

[2] A. Page, *On the numbers of primes in an arithmetical progression*, Proc. of London Math. Soc., Ser. 2, 39.2 (1935) p. 116-142.

[3] C. L. Siegel, *Über die Klassenzahl quadratischer Zahlkörper*, Acta Arithmetica 1 (1935), p. 83-86.

[4] E. C. Titchmarsh, *A divisor problem*, Rend. Circ. Mat. Palermo 54 (1930), p. 414-429.

[5] P. Turán, *Eine neue Methode in der Analysis und deren Anwendungen*, Budapest 1953.

[6] — and Vera T. Sós, *On some new theorems in the theory of diophantine approximations*, Acta Math. Hung. VII. 3-4 (1955), p. 241-255.

Reçu par la Rédaction le 2. 1. 1959

ACTA ARITHMETICA
V (1959)

On complete caps and ovaloids in three-dimensional Galois spaces of characteristic two

by

B. Segre (Rome)

Summary

§ 1. Introduction

The study of the geometry of a *Galois space* $S_{r,q}$, i. e. of a projective r-dimensional space over a Galois field of order

$$q = p^h,$$

where p, h are positive integers and p is a prime (the characteristic of the field), has recently been pursued and developed along new lines (1). In it, both algebraic-geometric and arithmetical methods have been applied, including the use of electronic calculating machines; moreover, some of the problems dealt with are deeply connected with information theory, especially with the construction of q-ary error-correcting codes. It is actually a chapter of ***arithmetical geometry***, which reduces to the investigation of certain questions on congruences mod p in the particular case when $h = 1$.

A set of k distinct points of $S_{r,q}$, no three of which lie on a line, is denoted by $k_{r,q}$ and called a *k-arc* if $r = 2$ and a *k-cap* if $r \geqslant 3$; any such $k_{r,q}$ is said to be *complete* when it is not a subset of a $(k+1)_{r,q}$. For given r and q, a $k_{r,q}$ having maximum k is called an *oval* if $r = 2$ and an *ovaloid* if $r \geqslant 3$, and then it is consequently always complete.

(1) See especially [8]; further historical and bibliographical informations are contained in [7].

When q is odd (i. e., if $p>2$), every *oval* is given by the points of an irreducible conic (cf. [5], the converse being also true), and consists of $k=q+1$ points. Likewise, when q is odd, every *ovaloid* of $S_{3,q}$ is given by the *points of an elliptic* (i. e., non-ruled) *quadric* ([1], [2]), and consists of $k=q^2+1$ points.

The situation is not so simple when q is even (i. e., $p=2$ and $q=2^h$). Then we obtain an *oval* (having $k=q+2$) by aggregating to the points of an irreducible conic the nucleus of the conic, namely, the point of concurrence of its tangents (the existence of such a point being a consequence of the fact that the ground field has now the characteristic $p=2$); but, with the only exception of some first few values of h, *there are ovals not obtainable in this way* [6]. As for the *ovaloids* of $S_{3,q}$ with even q, it is known that, if $q=2$, they are given by the $k=8$ points of $S_{3,2}$ outside a plane; if $q>2$ (i. e., $h>1$), they consist of $k=q^2+1$ points, an example being offered even now by the *points of an elliptic quadric*, which is the only possible case of ovaloid if $q=4$ ([3], [1]).

In the present paper we show that, *if $q=2^h\geqslant 8$, there may exist ovaloids of $S_{3,q}$ which are not quadric*, an explicit example being constructed for $q=8$ (§ 7). We also prove that any ovaloid defines a *null polarity* (§ 5), and establish a number of results on plane sections of an ovaloid (§ 6), as well as the existence of some *complete* $(2q+4)_{3,q}$ for $q=4$ (§ 2), and of some *complete* $(3q+2)_{3,q}$ for any $q=2^h$ (§ 3).

We now recall some simple known results (see e. g. [4], [8]), required later on.

The number of points of any $S_{r,q}$ is $q^r+q^{r-1}+\ldots+q+1$, and so $q+1$ is the number of the points lying on a line (as well as of the lines of a pencil), etc. The section of an arbitrary $k_{r,q}$ of $S_{r,q}$ with any subspace $S_{r',q}$ of $S_{r,q}$, if not empty, is necessarily a $k'_{r',q}$ (where $1\leqslant r'\leqslant r-1$, $1\leqslant k'\leqslant k$).

In particular, with respect to a given $k_{r,q}$, the lines of the ambient $S_{r,q}$ can be classified in three kinds: (i) *secant* lines or *chords*, containing two distinct points of $k_{r,q}$; (ii) *external* lines, containing no point of $k_{r,q}$; (iii) *tangent* lines, containing a single point of $k_{r,q}$, called the *point of contact* between the line and $k_{r,q}$: then we say that each of these lines *touches* $k_{r,q}$ at their respective point of contact. At every point P of $k_{r,q}$ there is always the same number (possibly zero) of tangents, i. e., of lines having P as their point of contact with $k_{r,q}$, this number being $q^{r-1}+q^{r-2}+\ldots+q-k+2$.

The $q+1$ lines touching an ovaloid of $S_{3,q}$ at any of its points, P say, are the $q+1$ lines of a pencil [1], and so they lie on a plane, which is called the *tangent plane* of the ovaloid at P. It follows easily that the planes of $S_{3,q}$ which are not tangent planes are q^3+q in number, and that each of them intersects the ovaloid in a $(q+1)$-arc.

§ 2. Construction of a complete $(2q+4)_{3,q}$ for $q=4$

We begin by proving the following

LEMMA I. *If $\mathcal{C}$ and $\mathcal{C}'$ are any two ovals of a given $S_{2,4}$, free from common points, then no line of $S_{2,4}$ can be external to both $\mathcal{C}$ and $\mathcal{C}'$.*

In fact, both $\mathcal{C}$ and $\mathcal{C}'$ consist of $q+2=6$ points. Through each point of $\mathcal{C}$ there are on the whole $q+1=5$ lines of $S_{2,4}$, and each of these lines meets $\mathcal{C}$ at a further point; moreover, exactly 3 among the 5 lines just considered meet $\mathcal{C}'$ (in a pair of points), the remaining 2 lines being external to $\mathcal{C}'$. It follows that the number of the lines of $S_{2,4}$ meeting both $\mathcal{C}$ and $\mathcal{C}'$ is given by $6\cdot 3/2=9$; and that the number of the lines of $S_{2,4}$ meeting $\mathcal{C}$ but not $\mathcal{C}'$ (or, likewise, meeting $\mathcal{C}'$ but not $\mathcal{C}$) is given by $6\cdot 2/2=6$. The number of the lines of $S_{2,4}$ having some point in common with $\mathcal{C}\cup\mathcal{C}'$ is consequently $9+6+6=21$, which is also the total number $(1+4+4^2)$ of the lines of $S_{2,4}$, whence the lemma.

We can now establish

THEOREM I. *If π and π_1 are two distinct planes of an $S_{3,4}$, and r is their line of intersection, let us consider in π an oval $\mathcal{C}$ and in π_1 an oval $\mathcal{C}_1$, both ovals having no common point with r. Then the $6+6=12$ points of $\mathcal{C}\cup\mathcal{C}_1$ constitute a complete $12_{3,4}$.*

First of all, it is clear that no three points of $\mathcal{C}\cup\mathcal{C}_1$ can be collinear, and so the set of the points of $\mathcal{C}\cup\mathcal{C}_1$ is in fact a 12-caps of $S_{3,4}$. In order to prove the completeness of this $12_{3,4}$, it suffices to show that through every point P of $S_{3,4}$ there is some line meeting $\mathcal{C}\cup\mathcal{C}_1$ at two distinct points. This is obvious if P lies in π or in π_1, on account of the completeness of the ovals $\mathcal{C}$ and $\mathcal{C}_1$. If P lies outside π and π_1, let us project $\mathcal{C}_1$ from P upon π; the projection is an oval $\mathcal{C}'$ of π, and both $\mathcal{C}$ and $\mathcal{C}'$ have then no common point with r. From the lemma it follows that $\mathcal{C}$ and $\mathcal{C}'$ must consequently have some point in common: the line joining such a point with P meets actually $\mathcal{C}\cup\mathcal{C}_1$ in two distinct points, and this completes the proof of the theorem.

§ 3. Construction of a complete $(3q+2)_{3,q}$ for any $q=2^h$

We now assume that the character q has an arbitrary even value ($q=2^h$), and we establish the following

LEMMA II. *If π and π_1 denote two distinct planes of an $S_{3,q}$, and r is their line of intersection, let us consider in π an irreducible conic $\mathcal{C}$ and in π_1 an irreducible conic $\mathcal{C}_1$, both conics touching r at the same point T and having the same nucleus O (necessarily situated on r and distinct from T). Moreover, we denote by A any of the q points of $\mathcal{C}$ distinct from T, and by A_1 any of the q points of $\mathcal{C}_1$ distinct from T. Then every point A_2 of intersection* *of two of the q^2 lines AA_1, and not situated on either π or π_1, lies always on q of these lines exactly: the points A_2 just considered are q in number, lie all on a certain plane π_2 (distinct from π, π_1) which contains the line r, and — together with T — they constitute the points of an irreducible conic, $\mathcal{C}_2$, which touches r at T and has O as its nucleus.*

Let AA_1, $A'A'_1$ be two of the q^2 lines defined above — where A, A' are two points of $\mathcal{C}$ and A_1, A'_1 are two points of $\mathcal{C}_1$ — and suppose that they meet at a point, A_2, not situated on either π or π_1 (so that the four points A, A', A_1, A'_1 are distinct). Then the projection of $\mathcal{C}_1$ from A_2 upon π is an irreducible conic having in common with the given conic $\mathcal{C}$ the points T, A, A' and having the same nucleus O; consequently, the two conics just considered on π have at those three points the same tangents, TO, AO, $A'O$, and so they coincide. It follows that A_2 must actually lie on exactly q of the q^2 lines defined above.

Conversely, if we fix arbitrarily one of these lines, AA_1 say, we see that precisely $q-1$ of the remaining ones are meeting it, and so the latter intersect AA_1 all at the same point, A_2. We obtain in fact each of the required lines by considering any one, R say, of the $q-1$ points of r distinct from T and O: if A', A'_1 denote the intersections of $\mathcal{C}$, $\mathcal{C}_1$ with RA, RA_1 residual to A, A_1 respectively, then the points A, A_1, A', A'_1 are in a plane, and so the lines AA_1, $A'A'_1$ intersect; and conversely.

If A_2 is — as above — the intersection of AA_1, $A'A'_1$, and A'_2 denotes the intersection of AA'_1, $A'A_1$, then the points A_2, A'_2, R are the diagonal points of the quadrangle of vertices A, A_1, A', A'_1. Hence they are collinear, since the ground field has now the characteristic $p=2$ ([4], n. 103), and so the line $A_2A'_2$ meets r.

The previous argument gives immediately that the meeting points outside π, π_1 of two (and therefore of q) lines AA_1 are q in number; and that the join of any one of them with any point of $\mathcal{C}$ distinct from T meets $\mathcal{C}_1$ at a point (also distinct from T). If A_2 and A'_2 are any two distinct of those meeting points, let us choose any point A of $\mathcal{C}$ distinct from T, and denote by A_1, A'_1 the points where the lines AA_2, AA'_2 respectively intersect $\mathcal{C}_1$. Then the line $A_1A'_1$ will meet r at a point, R say (distinct from T, O), and the line RA will intersect $\mathcal{C}$ — residually to A — at a point A' (distinct from T). From the above, it follows that the lines $A_2A'_2$ and r intersect; hence the q meeting points defined in the lemma are two by two in a plane through r, and so they must all lie in a single fixed plane, π_2 say, containing r. Those q points can therefore be obtained by projecting on π_2 the points A_1 ($\neq T$) of $\mathcal{C}_1$ from any chosen point A ($\neq T$) of $\mathcal{C}$; consequently, they all lie on a conic $\mathcal{C}_2$ of π_2, which touches r at T and has O as its nucleus.

Lemma II is thus established. We see, moreover, that the relation among the three conics $\mathcal{C}$, $\mathcal{C}_1$, $\mathcal{C}_2$ is symmetric, any two of them being perspective from a point — distinct from T — arbitrarily chosen on the third conic.

We prove now

THEOREM II. *With the notation of lemma II, the point-set $\mathcal{C}\cup\mathcal{C}_1\cup O$ constitutes an incomplete $(2q+2)$-cap. Every $k_{3,q}$ containing this $(2q+2)$-cap can be obtained by aggregating to it some points conveniently chosen on the plane π_2; it follows that the number k of its points satisfies the limitation $k\leqslant 3q+2$, the maximum $k=3q+2$ being actually reached by certain $(3q+2)_{3,q}$, each of which is therefore complete.*

First of all, the definition of k-cap (§ 1) gives at once that $\mathcal{C}\cup\mathcal{C}_1\cup O$ is a $(2q+2)_{3,q}$. Since $\mathcal{C}\cup O$ is an oval of π (§ 1), no further point of π (and, likewise, of π_1) can be aggregated to this $(2q+2)_{3,q}$, if we wish to obtain still a cap. On the other hand, each line AA_1 (joining a point $A\neq T$ of $\mathcal{C}$ and a point $A_1\neq T$ of $\mathcal{C}_1$, and so containing a point A_2 of $\mathcal{C}_2$) has exactly $(q+1)-3=q-2$ points outside the planes π, π_1, π_2; since the lines AA_1 are q^2 in number and — by lemma II — none of the points just considered can be situated on more than one of those lines, thus the total number of these points is $q^2(q-2)$, and so it coincides with the number

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

of the points of $S_{3,q}$ which lie outside the three planes π, π_1, π_2. It follows that each of the latter points lies on one, and only one, line AA_1; therefore none of them can be aggregated to $(2q+2)_{3,q}$, if we wish to obtain still a cap.

In conclusion, in order to amplify $(2q+2)_{3,q}$ in a cap, we may only aggregate to it some points of π_2. From lemma II, none of the additional points can lie on $\mathcal{C}_2$; moreover, since π_2 meets $(2q+2)_{3,q}$ in the two points T and O, the additional points can be chosen freely in π_2, outside $\mathcal{C}_2$, with the only further condition that the set of points obtained by aggregating T and O to them is a k'-arc of π_2. As $k'\leqslant q+2$ (§ 1), the number of additional points is never greater than $(q+2)-2=q$, this maximum being reached if (and only if) the q additional points — together with the points T and O — constitute an oval, having no point distinct from T in common with $\mathcal{C}_2$.

We obtain such an oval by considering in π_2 the pencil of conics determined by $\mathcal{C}_2$ and the line r counted twice, and aggregating the point O to the $q+1$ points of any of its conics distinct from the two conics by means of which we have defined the pencil. Theorem II is thus completely proved.

§ 4. Two additional lemmas

We now give a couple of additional lemmas, to be applied later on, the first of which can be conveniently compared with lemma II (§ 3).

LEMMA III. *If π and π_1 are two distinct planes of an S_3 over an arbitrary perfect (possibly infinite) field of characteristic 2, and r denotes their line of intersection, let us consider in π an irreducible conic $\mathcal{C}$ and in π_1 an irreducible conic $\mathcal{C}_1$, the two conics having the same nucleus, O (situated on r), and touching r at two distinct points T, T_1. Then a third plane ω — passing through r — is defined, the points of which not lying on r constitute the locus of those points of $S_3-(\pi\cup\pi_1)$ which lie on just one line meeting both $\mathcal{C}$ and $\mathcal{C}_1$.*

We can introduce in S_3 homogeneous coordinates (x_1, x_2, x_3, x_4), in such a way that T, T_1 have the coordinates (1000), (0100), and that (0010), (0001) are two further points of $\mathcal{C}$, $\mathcal{C}_1$ respectively. Then, by a proper choice of the unity point, the coordinates of O become (1100) and the equations of $\mathcal{C}$, $\mathcal{C}_1$ can be reduced to the form:

$$\mathcal{C}:\quad x_4=0,\quad (x_1+x_2)x_3+x_2^2=0,$$

$$\mathcal{C}_1:\quad x_3=0,\quad (x_1+x_2)x_4+x_1^2=0.$$

The points A, A_1 of $\mathcal{C}$, $\mathcal{C}_1$, different from T, T_1 respectively, are those of coordinates

$$A:\quad x_1=\lambda^2+\lambda,\quad x_2=\lambda,\quad x_3=1,\quad x_4=0,$$

$$A_1:\quad x_1=\mu,\quad x_2=\mu^2+\mu,\quad x_3=0,\quad x_4=1,$$

where the parameters λ, μ vary arbitrarily in the ground field. The coordinates of any point P of S_3 not situated in π or π_1 can be written in the form

$$P:\quad x_1=a,\quad x_2=b,\quad x_3=c,\quad x_4=1,$$

with $c\neq 0$; then A, A_1, P are collinear if, and only if,

$$a=c(\lambda^2+\lambda)+\mu,\qquad b=c\lambda+(\mu^2+\mu).$$

On eliminating μ among these relations, we obtain:

$$c^2\lambda^4+c(c+1)\lambda^2+(a+b+a^2)=0;$$

and the last equation has just one root λ in the ground field if, and only if, $c+1=0$: this is tantamount to supposing that the point P lies on the plane $x_3+x_4=0$, which is therefore the plane ω of the lemma.

We pass now to

LEMMA IV. *Let K be a k-cap contained in an irreducible quadric Q of $S_{3,q}$, with arbitrary (even or odd) $q\geqslant 4$; and suppose that*

$$k\geqslant (q^2+q+4)/2.$$

Then Q is elliptic, and every cap containing K lies entirely in Q.

Q is elliptic, since otherwise K could have at most two points on each of the $q+1$ generators of Q of one system, and so $k\leqslant 2q+2$, in contrast with our hypotheses.

If a cap containing K does not lie entirely on Q, and so it possesses (at least) one point — O say — not situated on Q, then there are exactly $q+1$ points of Q joined to O by a tangent and the k points of K are joined to O by k distinct lines. Hence at least

$$k-(q+1)\geqslant (q^2-q+2)/2$$

of these lines do not touch Q, and each of them meets consequently Q in two distinct points. The points thus defined on Q and the points of contact of the tangents of Q passing through O are distinct, and at least

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

in number. But this is impossible, since the quadric Q — being elliptic — contains q^2+1 points exactly; and this contradiction completes the proof of the lemma.

§ 5. The polarity defined by an ovaloid

We now consider an arbitrary ovaloid K of $S_{3,q}$, with $q=2^h\geqslant 4$, and any plane π of $S_{3,q}$. From § 1 there are only two cases to be distinguished, according as π intersects K in a single point, P say (and then π is the tangent plane of K at P), or in a $(q+1)$-arc. In the first case, the tangent lines of K lying in π are clearly the $q+1$ lines of π containg P. In the second case, the $(q+1)$-arc is contained in just one oval ([8], n. 30), obtainable by aggregating to it a uniquely determined point, P say; in other words, the $q+1$ tangents to the $(q+1)$-arc (one at each of its points) are the lines of the pencil of centre P, and they are manifestly the only tangents of K lying in π. In either case, the above defined point P will be called the *pole* of π with respect to K.

We shall prove

THEOREM III. *The correspondence associating to every plane of $S_{3,q}$ its pole with respect to K is always a null polarity. The linear complex of the lines of $S_{3,q}$ which are transformed into themselves by this polarity, consists precisely of the tangent lines of K; hence the tangent lines of K containing an arbitrarily given point of $S_{3,q}$ are $q+1$ in number, and constitute* *a pencil. Moreover, the polarity transforms every chord of K into an external line, and conversely.*

We show first that the correspondence $\pi \to P$ — defined in the first paragraph of the present section — is one-to-one, namely that each point P of $S_{3,q}$ lies on exactly $q+1$ tangents of K, constituting a pencil. For this purpose, we denote by t_P the number of tangents of K containing P, and we remark firstly that

$$t_P \geqslant q+1.$$

In fact — if we suppose $t_P \leqslant q$ — we deduce the existence of some plane, α say, containing P but none of the t_P tangents of K issued from P; this, however, would lead to a contradiction, since we know that on α there is a pencil of tangent lines of K, and so at least one of these lines should contain P.

On the other hand, K admits $q+1$ tangents at each of its q^2+1 points, and $(q+1)(q^2+1)$ is the total number of points of $S_{3,q}$ (§ 1). By evaluating in two different manners the number of pairs formed by a tangent of K and one of its $q+1$ points, we then obtain the equality

$$\sum_P t_P = (q+1)^2(q^2+1),$$

where the sum runs over all the points P of $S_{3,q}$. Hence in none of the previous limitations the inequality sign may hold, i. e., we must have $t_P = q+1$ for every P, since otherwise — by adding them — we should obtain a contradiction. We notice now that the $q+1$ tangents of K issued from P lie necessarily on a plane (to be called the *polar plane* of P). For, if that would not be so, there should be some plane containing P and none of these tangents; but this, from what we have previously seen, would not be possible.

In order to complete the proof of theorem III, there remains only to be shown that, if r denotes any line of $S_{3,q}$, when a plane π of $S_{3,q}$ turns about r its pole P describes a line, r' say; and that r' coincides with r if r is a tangent, while otherwise r' is external or is a secant with respect to K according as r is a secant or is an external line.

The stated properties being all obvious when r is a tangent, let us suppose that r is a secant of K. If A, B are the two (distinct) points of K lying on r, we denote by α, β the tangent planes of K at A, B respectively, and by r' the line of intersection of α, β. Clearly, r' contains none of the points A, B, and so it is external with respect to K (A, B being the only points of K lying on α, β). Any plane π containing r intersects α, β in two lines touching K (at A, B respectively); hence these two lines meet at a point P, intersection of π and r', which — from the very definition of pole — is precisely the pole of π with respect to K. And we should notice that the pencil described by π and the line described by P are homographic, since they are mutually perspective.

Finally, let us consider the remaining case — when r is external to K — and denote by π, π_1, π_2 any three distinct planes of $S_{3,q}$ containing r, and by P, P_1, P_2 the poles of π, π_1, π_2 with respect to K. We remark that none of these points can lie on r, as otherwise r would touch K at such a point, and so P, P_1, P_2 are certainly distinct. Hence any point O of r is joined to P, P_1, P_2 by three distinct lines, which — from the definition of pole — are three tangents of K issued from O, and so they are coplanar. Since O is an arbitrary point of r, it follows that P, P_1, P_2 must lie on a line (skew to r). By keeping π_1 and π_2 fixed, and making π turn about r, we see consequently that the pole P of π lies on the fixed line $r' = P_1P_2$. This line is certainly not a tangent, as this would imply the coincidence of r and r'. In order to prove that r' is now a chord of K, on using the results of the previous paragraph it suffices to show that:

Any ovaloid admits the same number of chords and of external lines.

In fact, the total number of lines of $S_{3,q}$ is ([4], n. 159):

$$(q^2+1)(q^2+q+1);$$

moreover, an ovaloid of $S_{3,q}$ has manifestly $(q+1)(q^2+1)$ tangents and $\binom{q^2+1}{2}$ chords. Hence the latter number is actually the same as that of the external lines, since

$$(q^2+1)(q^2+q+1) = (q+1)(q^2+1)+2\binom{q^2+1}{2}.$$

Theorem III is thus established. From it we deduce at once

COROLLARY I. *When a point describes a tangent line of an ovaloid, its polar plane turns about the same line, corresponding homographically to it.*

Another immediate consequence of theorem III is expressed by

COROLLARY II. *The tangent planes of any given ovaloid constitute the dual of an ovaloid, the lines situated on two (and so on only two) distinct of those planes being the lines external to the given ovaloid.*

§ 6. On the plane sections of an ovaloid

We shall establish later on (§ 7) the existence of ovaloids which are not quadrics; and now we investigate some properties of the plane sections of such ovaloids.

If K is any ovaloid of $S_{3,q}$, with even q, let π be any of the q^3+q planes of $S_{3,q}$ which do not touch K; then π intersects K in a $(q+1)$-arc, Γ say, giving an oval by aggregating to it the pole P of π with respect to K (§ 5). About Γ, we can distinguish from § 1 the following three possibilities:

(i) Γ is a conic (and then P is its nucleus).

(ii) Γ can be obtained from a conic by aggregating its nucleus, O, and suppressing one of its points, coinciding with P. We shall then say that Γ is a *pointed conic*, having as *nucleus* the point O (which is a well defined point of Γ if $q > 4$); and we notice that the tangent of Γ at O is the line OP.

(iii) The oval $\Gamma \cup P$ can be obtained in no way from a conic, by aggregating the nucleus to it.

If K is a quadric, only case (i) can arise; and the converse is also true (cf. theorem V). We shall say that K is *singular* or *regular* according as some or none of its plane sections presents case (iii). No singular ovaloid can therefore be a quadric. On the other hand, from known results [6], we have that *every ovaloid is regular for $h = 4$ and for $h = 8$*; and we shall not investigate the question of existence of singular ovaloids for $h > 8$.

We prove first

THEOREM IV. *All the pointed conics lying on an ovaloid K of $S_{3,q}$, which have as nucleus a given point O of K (if any), must admit a common tangent at O.*

It suffices to show that, if π, π_1 are two distinct planes of $S_{3,q}$ containing O and meeting K in two pointed conics, Γ, Γ_1 say, of nucleus O, then the line $r = \pi\pi_1$ touches K at O. For this purpose, let us suppose that r intersects K at a point, T say, distinct from O, so that the poles of π, π_1 with respect to K are two points P, P_1 (of π, π_1 respectively) not lying on r. Moreover, on π, π_1 we have two conics $\mathcal{C}$, $\mathcal{C}_1$, both having O as nucleus and touching r at T, such that

$$\Gamma \cup P = \mathcal{C} \cup O, \qquad \Gamma_1 \cup P_1 = \mathcal{C}_1 \cup O;$$

we then designate by $\mathcal{H}$, $\mathcal{H}_1$ the quadric cones projecting $\mathcal{C}$, $\mathcal{C}_1$ from P_1, P respectively.

From lemma II and the proof of theorem II (§ 3), we see that $\mathcal{C}$, $\mathcal{C}_1$ define a certain plane π_2 containing r, and that the lines joining the single points of

$$\Gamma - (O \cup T) = \mathcal{C} - (P \cup T)$$

with the single points of

$$\Gamma_1 - (O \cup T) = \mathcal{C}_1 - (P_1 \cup T)$$

fill up

$$S_{3,q} - (\pi_2 \cup \mathcal{H} \cup \mathcal{H}_1)$$

completely. Consequently, since K is a cap, the points of $K - (\Gamma \cup \Gamma_1)$ must lie on $\pi_2 \cup \mathcal{H} \cup \mathcal{H}_1$, and so their number cannot be greater than $3q$. But the total number of the points just considered actually is $(q^2+1) - 2q$; and this number is greater than $3q$, since now $q \geqslant 8$ (otherwise K would not contain any pointed conic (cf. § 1)).

This contradiction proves the theorem, as an immediate consequence of which we obtain

COROLLARY III. *Any point of an ovaloid of $S_{3,q}$ is the nucleus of at most q of its pointed conics.*

We proceed to establish

THEOREM V. *Any ovaloid K of $S_{3,q}$ ($q \geqslant 8$) containing (at least) $(q^3 - q^2 + 2q)/2$ conics is consequently an elliptic quadric.*

We begin by showing that we can find on K two distinct points, A, B say, such that:

(i) there exist (at least) $q^2/2+1$ distinct conics lying on K and containing A;

(ii) there exist (at least) $q/2+1$ distinct conics lying on K and containing both A and B.

If it should be impossible to choose a point A for which (i) holds, then each of the q^2+1 points of K would lie on at most $q^2/2$ conics. By evaluating in two different ways the number of pairs formed by a conic of K and one of its $q+1$ points, we then obtain:

$$(q+1)\cdot(q^3 - q^2 + 2q)/2 \leqslant (q^2+1)\cdot q^2/2 .$$

This inequality being not satisfied, it follows that we can in fact choose A such as (i) holds.

If it should be impossible to associate to A another point B of K for which (ii) holds, then A and any of the q^2 points of K distinct from A would lie both on no more than $q/2$ conics of K. By evaluating in two different ways the number of pairs formed by a conic of K containing A and one of its q points distinct from A, and using (i), we then obtain:

$$(q^2/2+1)\cdot q \leqslant q^2 \cdot q/2 .$$

This inequality being not satisfied, also part (ii) of our assertion is proved.

If A, B are two distinct points of K for which (i) and (ii) hold, we denote by α, β the planes touching K at A, B, by $\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{q/2}$ $q/2+1$ distinct conics of K containing A, B, and by $\mathcal{D}$ a conic of K containing A but not B. The plane of $\mathcal{D}$ will then meet α in a line touching at most one of the $\mathcal{C}$'s at A. Hence it is not restrictive to suppose that the plane of $\mathcal{D}$ intersects the planes of $\mathcal{C}_1, \ldots, \mathcal{C}_{q/2}$ in chords of K; if $P_1, \ldots, P_{q/2}$ denote the points distinct from A where these chords meet K, then P_i is a common point of $\mathcal{C}_i$ and $\mathcal{D}$ $(i = 1, \ldots, q/2)$.

The quadric — Q say — defined by the condition of containing $\mathcal{C}_1$, $\mathcal{C}_2$ and P_3, meets $\mathcal{D}$ at P_1, P_2, P_3 and (having α as its tangent plane at A) it touches $\mathcal{D}$ at A. Therefore the conic $\mathcal{D}$ lies on Q; and so does the conic $\mathcal{C}_i$ ($i = 3, \ldots, q/2$), since $\mathcal{C}_i$ contains the point P_i of $\mathcal{D}$, hence of Q, and it touches Q at A and B.

From (i), (ii) we see that on K there exist conics containing A, but not B, which do not touch $\mathcal{C}_0$ at A. By substituting such a conic for $\mathcal{D}$ in the previous argument, we infer that $\mathcal{C}_0$ must lie on a quadric containing at least $q/2-1$ of the conics $\mathcal{C}_1, \ldots, \mathcal{C}_{q/2}$; hence also $\mathcal{C}_0$ is situated on Q.

The points of $\mathcal{C}_0 \cup \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_{q/2} \cup \mathcal{D}$ are at least

$$2+(q/2+1)(q-1)+(q/2-1) > (q^2+q+4)/2$$

in number. Since they lie on both K and Q, from lemma IV (§ 4) it follows that K is an elliptic quadric, and that K is contained in Q. Hence K and Q must coincide, as they contain the same number (q^2+1) of points.

Thus theorem V is proved. From it we shall draw as a consequence (to be compared with corollary III) the following:

COROLLARY IV. *On every regular ovaloid K of $S_{3,q}$, which is not a quadric, there exist some point which is the nucleus of at least $q/2+1$ of its pointed conics.*

For, if every point of K should be the nucleus of no more than $q/2$ pointed conics, then K could contain on the whole at most $(q^2+1)q/2$ pointed conics, and so at least

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

conics, in contrast with theorem V.

§ 7. On ovaloids of $S_{3,q}$ which are not quadrics

Let us now suppose that K is an ovaloid of $S_{3,q}$ ($q = 2^h \geqslant 8$), containing $l+2$ ($\geqslant 2$) pointed conics

$$\Gamma, \Gamma_1, \Delta_1, \ldots, \Delta_l$$

with the same nucleus, O say, and denote by ω the tangent plane of K at O. Then, from theorem IV, the planes $\pi, \pi_1, \chi_1, \ldots, \chi_l$ of these pointed conics must all contain a fixed line, r say, touching K at O; moreover, from theorem III (§ 5), their respective poles

$$T, T_1, U_1, \ldots, U_l$$

must be distinct points of r. If $l > 0$, we see from corollary I (§ 5) that the points $O, T, T_1, U_1, \ldots, U_l$ must correspond homographically to the planes $\omega, \pi, \pi_1, \chi_1, \ldots, \chi_l$. In any case, from the definition of pointed conics, we obtain the existence of $l+2$ conics

$$\mathcal{C}, \mathcal{C}_1, \mathcal{D}_1, \ldots, \mathcal{D}_l,$$

lying in $\pi, \pi_1, \chi_1, \ldots, \chi_l$ and touching r at $T, T_1, U_1, \ldots, U_l$ respectively, such that

$$\Gamma = (\mathcal{C} \cup O)-T, \quad \ldots, \quad \Delta_l = (\mathcal{D} \cup O)-U_l.$$

The plane through r associated — from lemma III (§ 4) — with any two of the conics $\mathcal{C}, \mathcal{C}_1, \mathcal{D}_1, \ldots, \mathcal{D}_l$, e. g. with $\mathcal{C}$ and $\mathcal{C}_1$, has certainly no point in common with K outside r; hence it must coincide with the plane ω previously considered, which touches K at O.

In order to construct an ovaloid K presenting the peculiarities specified above, in the case when l reaches its maximum value, $q-2$ (see corollary III, § 6), we define $GF(2^h)$ as the field generated over the field $GF(2)$ (consisting of the elements 0 and 1, to be added and multiplied mod 2) by a *root x of an irreducible equation of degree h over $GF(2)$*, e. g.— if $h = 3$ or $h = 4$ (but not if $h = 5$) — of the equation

$$x^h = x+1;$$

and we denote by $a_1, a_2, \ldots, a_{q-2}$ the *elements of $GF(q)$ different from 0 and 1* taken in any order. Moreover, we recall ([4], n. 80) that an element a of $GF(2^h)$ is said to be *of the 1st* or *of the 2nd category* according as the equation

$$\xi^2+\xi+a = 0$$

has two roots ξ or has no roots in $GF(2^h)$ (which is tantamount to saying that $a^{2^{h-1}}+a^{2^{h-2}}+\ldots+a^2+a$ has then the value 0 or 1 respectively); and that *the sum of two elements of the same or opposite categories is always of the 1st or 2nd category respectively.*

We shall presently give the required construction, leading to the following

THEOREM VI. *In $S_{3,q}$ (with $q = 2^h \geqslant 8$) there exists some ovaloid containing q pointed conics with the same nucleus, if it is possible to choose $q-2$ (not necessarily distinct) elements $b_1, b_2, \ldots, b_{q-2}$ of the 2nd category of $GF(q)$, such that also each of the elements $a_i b_j + a_j b_i$ ($i, j = 1, 2, \ldots, q-2$; $i \neq j$) is of the 2nd category.*

Let us consider the Galois space $S_{3,q}$, with homogeneous point coordinates (x_1, x_2, x_3, x_4) over $GF(q)$, and denote by r the line $x_3 = x_4 = 0$. The $q+1$ points of r are then

$$O(1000), \quad T(0100), \quad T_1(1100), \quad U_i(\sqrt{a_i}100),$$

where $i = 1, 2, \ldots, q-2$, and they correspond homographically to the planes

$$\omega:\ x_3 = 0,\qquad \pi:\ x_4 = 0,\qquad \pi_1:\ x_4 = x_3,\qquad \chi_i:\ x_4 = \sqrt{a_i}\,x_3$$

containing r. The conics

$$\begin{aligned}
\mathcal{C}&: & x_4 &= 0, & x_1^2+x_2x_3 &= 0,\\
\mathcal{C}_1&: & x_4 &= x_3, & x_1^2+x_2x_3+x_2^2 &= 0,\\
\mathcal{D}_i&: & x_4 &= \sqrt{a_i}\,x_3, & x_1^2+x_2x_3+a_ix_2^2+b_ix_3^2 &= 0
\end{aligned}$$

lie on the planes π, π_1, χ_i, touch r at the points T, T_1, U_i respectively, and each of them has O as its nucleus.

Theorem VI will now be proved if we show that, on taking the b's in the demanded manner, we obtain a cap by aggregating the point O to the $q\cdot q = q^2$ points which lie on the q conics just defined, and are distinct from their respective point of contact with r. This is tantamount to proving that three of these q^2 points, arbitrarily chosen on three different conics, are then never collinear. Later on, we shall refer to the last requirement as the *ϑ-condition for the three conics*.

We begin by noticing that the q points of the q point-sets $\mathcal{C}-T$, $\mathcal{C}_1-T_1$, $\mathcal{D}_i-U_i$ $(i = 1, 2, \ldots, q-2)$ are those given by

$$\begin{aligned}
P&:\quad x_1 = \lambda,\quad x_2 = \lambda^2,\quad x_3 = 1,\quad x_4 = 0,\\
P_1&:\quad x_1 = \mu^2+\mu,\quad x_2 = \mu^2,\quad x_3 = 1,\quad x_4 = 1,\\
Q_i&:\quad x_1 = \sqrt{a_i}\nu_i^2+\nu_i+\sqrt{a_i}b_i,\quad x_2 = \nu_i^2+b_i,\quad x_3 = 1,\quad x_4 = \sqrt{a_i}
\end{aligned}$$

respectively, when the parameters λ, μ, ν_i vary in $GF(q)$.

Next we remark that, from the above, the line PP_1 meets the plane χ_i $(x_4 = \sqrt{a_i}x_3)$ at the point

$$x_1 = (\sqrt{a_i}+1)\lambda+\sqrt{a_i}(\mu^2+\mu),\qquad x_2 = (\sqrt{a_i}+1)\lambda^2+\sqrt{a_i}\mu^2,$$
$$x_3 = 1,\qquad x_4 = \sqrt{a_i};$$

hence, by expressing that this point lies on $\mathcal{D}_i$, we obtain

$$b_i = \xi^2+\xi\quad\text{where}\quad \xi = (a_i+\sqrt{a_i})(\lambda^2+\mu^2).$$

The last two equations have no common roots ξ, λ, μ in $GF(q)$ if, and only if, *b_i is of the 2nd category*; this is therefore the ϑ-condition for the conics $\mathcal{C}$, $\mathcal{C}_1$ and $\mathcal{D}_i$.

We now denote by i, j any two distinct numbers $1, 2, \ldots, q-2$, and notice that the line Q_iQ_j meets the plane π $(x_4 = 0)$ at the point of coordinates:

$$\begin{aligned}
x_1 &= \sqrt{a_j}(\sqrt{a_i}\nu_i^2+\nu_i+\sqrt{a_i}b_i)+\sqrt{a_i}(\sqrt{a_j}\nu_j^2+\nu_j+\sqrt{a_j}b_j),\\
x_2 &= \sqrt{a_j}(\nu_i^2+b_i)+\sqrt{a_i}(\nu_j^2+b_j),\\
x_3 &= \sqrt{a_i}+\sqrt{a_j},\\
x_4 &= 0;
\end{aligned}$$

hence, by expressing that this point lies on $\mathcal{C}$, we obtain

$$a_ib_j+a_jb_i = \xi^2+\xi,\quad\text{where}\quad \xi = \sqrt{a_ia_j}(\nu_i^2+\nu_j^2+b_i+b_j).$$

The last two equations have no common roots ξ, ν_i, ν_j in $GF(q)$ if, and only if, *$a_ib_j+a_jb_i$ is of the 2nd category*; this is therefore the ϑ-condition for the conics $\mathcal{D}_i$, $\mathcal{D}_j$ and $\mathcal{C}$.

We see likewise that the line Q_iQ_j meets the plane π_1 $(x_4 = x_3)$ at the point of coordinates:

$$\begin{aligned}
x_1 &= (1+\sqrt{a_j})(\sqrt{a_i}\nu_i^2+\nu_i+\sqrt{a_i}b_i)+(1+\sqrt{a_i})(\sqrt{a_j}\nu_j^2+\nu_j+\sqrt{a_j}b_j),\\
x_2 &= (1+\sqrt{a_j})(\nu_i^2+b_i)+(1+\sqrt{a_i})(\nu_j^2+b_j),\\
x_3 &= x_4 = \sqrt{a_i}+\sqrt{a_j};
\end{aligned}$$

hence, by expressing that this point lies on $\mathcal{C}_1$, we obtain

$$b_i+b_j+(a_ib_j+a_jb_i) = \xi^2+\xi,$$

where

$$\xi = (1+\sqrt{a_i})(1+\sqrt{a_j})(\nu_i^2+\nu_j^2+b_i+b_j).$$

The last two equations have no common roots ξ, ν_i, ν_j in $GF(q)$ if, and only if, *$b_i+b_j+(a_ib_j+a_jb_i)$ is of the 2nd category*; this is therefore the ϑ-condition for the conics $\mathcal{D}_i, \mathcal{D}_j$ and $\mathcal{C}_1$, and — from the above — it is a *consequence* of the ϑ-conditions for the triplets $(\mathcal{C}, \mathcal{C}_1, \mathcal{D}_i)$, $(\mathcal{C}, \mathcal{C}_1, \mathcal{D}_j)$ and $(\mathcal{D}_i, \mathcal{D}_j, \mathcal{C})$.

Finally, on denoting by i, j, l any three distinct numbers $1, 2, \ldots, q-2$, we remark that the line Q_iQ_j meets the plane χ_l $(x_4 = \sqrt{a_l}x_3)$ at the point of coordinates

$$\begin{aligned}
x_1 &= (\sqrt{a_j}+\sqrt{a_l})(\sqrt{a_i}\nu_i^2+\nu_i+\sqrt{a_i}b_i)+(\sqrt{a_i}+\sqrt{a_l})(\sqrt{a_j}\nu_j^2+\nu_j+\sqrt{a_j}b_j),\\
x_2 &= (\sqrt{a_j}+\sqrt{a_l})(\nu_i^2+b_i)+(\sqrt{a_i}+\sqrt{a_l})(\nu_j^2+b_j),\\
x_3 &= \sqrt{a_i}+\sqrt{a_j},\\
x_4 &= \sqrt{a_l}(\sqrt{a_i}+\sqrt{a_j});
\end{aligned}$$

hence, by expressing that this point lies on $\mathcal{D}_l$, we obtain

$$(a_j b_l + a_l b_j) + (a_l b_i + a_i b_l) + (a_i b_j + a_j b_i) = \xi^2 + \xi$$

where

$$\xi = (a_l + \sqrt{a_j a_l + a_l a_i + a_i a_j})(\nu_i^2 + \nu_j^2 + b_i + b_j).$$

These two equations have no common roots ξ, ν_i, ν_j in $GF(q)$ if $(a_j b_l + a_l b_j) + (a_l b_i + a_i b_l) + (a_i b_j + a_j b_i)$ *is of the 2nd category*; hence the last property implies the ϑ-condition for the conics $\mathcal{D}_i$, $\mathcal{D}_j$ and $\mathcal{D}_l$, and — from the above — it is a consequence of the ϑ-conditions for the triplets $(\mathcal{D}_j, \mathcal{D}_l, \mathcal{C})$, $(\mathcal{D}_l, \mathcal{D}_i, \mathcal{C})$ and $(\mathcal{D}_i, \mathcal{D}_j, \mathcal{C})$.

Theorem VI now follows at once. We shall complete its content in the first two cases, $h = 3$ and $h = 4$, by establishing

THEOREM VII. *While it is possible to satisfy all the conditions stated in theorem* VI *if we suppose* $q = 8$, *these conditions are incompatible for* $q = 16$.

On assuming firstly $q = 8$ (i. e., $h = 3$), we can define $GF(8)$ in the manner specified in the paragraph before theorem VI, and assume precisely:

$$a_1 = x, \qquad a_3 = x^2, \qquad a_5 = x^2 + x,$$

$$a_2 = x+1, \qquad a_4 = x^2+1, \qquad a_6 = x^2 + x + 1,$$

where $x^3 = x+1$. From the obvious rules of addition and multiplication among these elements (for the multiplication cf. [6], § V), we see that

$$0, a_1, a_3, a_5$$

are of the 1st category, and

$$1, a_2, a_4, a_6$$

are of the 2nd category; and that all the conditions stated in theorem VI are verified if e. g. we assume

$$b_1 = b_6 = a_4, \qquad b_2 = b_3 = a_6, \qquad b_4 = b_5 = a_2.$$

Let us secondly suppose $q = 16$ (i. e., $h = 4$). Now we define $GF(16)$ in the manner specified in the paragraph before theorem VI, and assume precisely:

$$a_1 = x, \qquad a_2 = x+1, \qquad a_3 = x^2,$$

$$a_4 = x^2+1, \qquad a_5 = x^2+x, \qquad a_6 = x^2+x+1,$$

$$a_7 = x^3, \qquad a_8 = x^3+1, \qquad a_9 = x^3+x,$$

$$a_{10} = x^3+x+1, \qquad a_{11} = x^3+x^2, \qquad a_{12} = x^3+x^2+1,$$

$$a_{13} = x^3+x^2+x, \qquad a_{14} = x^3+x^2+x+1,$$

where now $x^4 = x+1$. We see without difficulty that, at present,

$$0, 1, a_1, a_2, \ldots, a_6$$

are the elements of the 1st category, and so

$$a_7, a_8, \ldots, a_{14}$$

are those of the 2nd category; besides, we can dress the table

	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}
a_7	*		*		*		*	
a_8		*		*		*		*
a_9	*		*			*		*
a_{10}		*		*	*		*	
a_{11}	*			*	*			*
a_{12}		*	*			*	*	
a_{13}	*			*		*	*	
a_{14}		*	*		*			*

where the crossing of a line a_i and a column a_j is empty or is marked by an asterisk, according as the product $a_i a_j$ is of the 1st or 2nd category.

From the above, in order that b_7 and b_8 are of the 2nd category we must have

$$b_7 = a_i, \qquad b_8 = a_j,$$

where i, j are any two (possibly coincident) among the numbers $7, 8, \ldots, 14$. Then, on using the table, and recalling that the sum of two elements of $GF(q)$ is of the 2nd category if and only if the two elements are of opposite categories, we see that the condition for $a_7 b_8 + a_8 b_7 = a_7 a_j + a_8 b_i$ to be of the 2nd category gives:

$$i \equiv j \pmod 2.$$

If l denotes any of the numbers $9, 10, \ldots, 14$, the table shows that $a_7 b_l$ and $a_8 b_l$ are of opposite categories. Hence, in order that

$$a_7 b_l + a_l b_7 \quad \text{and} \quad a_8 b_l + a_l b_8$$

are of the 2nd category, it is necessary that

$$a_l b_7 = a_l a_i \quad \text{and} \quad a_l b_8 = a_l a_j$$

are of opposite categories. But now, again from the table, we see that (for no choice of i, j satisfying the conditions given in the preceding paragraph) the last property actually holds for all values of $l = 9, 10, \ldots, 14$; and this proves the second part of theorem VII.

As an immediate consequence of theorems III, VI and of the first part of theorem VII, we obtain

THEOREM VIII. *In $S_{3,8}$ there exist ovaloids which are not quadrics. However, each of them defines a null polarity, exactly in the same way as it was a quadric.*

References

[1] A. Barlotti, *Un'estensione del teorema di Segre-Kustaanheimo*, Boll. Un. Mat. Ital., (3) 10 (1955), p. 498-506.

[2] G. F. Panella, *Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito*, Boll. Un. Mat. Ital. (3) 10 (1955), p. 507-513.

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

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

[5] — *Ovals in a finite projective plane*, Canadian Journ. of Math. 7 (1955), p. 414-416.

[6] — *Sui k-archi nei piani finiti di caratteristica due*, Revue de Math. pures et appl. 2 (1957), p. 283-294.

[7] — *On Galois geometries* (Lecture given at the Edinburgh Internat. Congr. of Math., on August 19, 1958).

[8] — *Le geometrie di Galois*, Annali di Mat. (4) 48 (1959), p. 1-97.

Reçu par la Rédaction le 4. 3. 1959

ACTA ARITHMETICA
V (1959)

Les points exceptionnels rationnels sur certaines cubiques du premier genre

par

T. NAGELL (Uppsala)

§ 1. Les points exceptionnels sur une cubique

1. Soit donnée la cubique C de genre un représentée par l'équation

$$F(x, y, z) = 0 \tag{1}$$

en coordonnées homogènes. Soit P un point sur la cubique. La tangente à la cubique en ce point rencontre la cubique en un second point P_1, le *point tangentiel* de P. Soit ensuite P_2 le point tangentiel de P_1 et soit P_3 le point tangentiel de P_2 et ainsi de suite. Nous aurons alors une suite infinie de points,

$$P = P_0, P_1, P_2, P_3, \ldots, P_m, \ldots, \tag{2}$$

où P_m est le point tangentiel de P_{m-1}. Si tous ces points sont distincts, nous appelons le point P *point normal*. Dans le cas contraire, il n'y a qu'un nombre fini de points distincts, et nous appelons le point P *point exceptionnel*. J'ai proposé cette notion dans un travail publié en 1935, voir [1], [2] et [3] (1). Si le point P est exceptionnel, tous les autres points dans la suite (2) sont aussi exceptionnels.

Les neuf points d'inflexion sont évidemment des points exceptionnels.

Choisissons la représentation paramétrique des coordonnées de la cubique (1) par des fonctions elliptiques de telle façon que le point d'argument $u = 0$ corresponde à un point d'inflexion. Soit u l'argument du point P. L'argument du point tangentiel P_1 est alors $-2u$ et l'argument du point P_m dans la suite (2) est $(-2)^m u$. Si, dans la suite (2), tous les points coincident, le point initial P est un point d'inflexion.

(1) Les numéros figurant entre crochets renvoient à la Bibliographie placée à la fin de ce travail.