CONNECTION BETWEEN THE n-DIMENSIONAL AFFINE SPACE $A_{n,q}$ AND THE CURVE C, WITH EQUATION $y=x^q$, OF THE AFFINE PLANE A_{2,q^n} (*)

by J. A. THAS (in Gent) (**)

SOMMARIO. - *Indicata con C la curva di equazione $y = x^q$ nel piano affine A_{2,q^n} ($n \geq 1, q = p^h$), è definita una struttura d'incidenza $I(C)$ nel modo seguente: i punti sono gli elementi di C, le C-rette sono gli insiemi formati da q punti allineati di C e l'incidenza è quella stessa di A_{2,q^n}. $I(C)$ è lo spazio affine a n dimensioni su $GF(q)$, e due C-rette sono parallele se e solo se le rette corrispondenti di A_{2,q^n} sono parallele. Ne segue che la determinazione delle calotte di $A_{n,q}$ ($n > 2$) è equivalente alla determinazione delle intersezioni di C con gli archi del piano A_{2,q^n}.*

SUMMARY. - *If the curve, with equation $y = x^q$, of the affine plane A_{2,q^n} ($n \geq 1$, $q = p^h$) is denoted by C, then an incidence structure $I(C)$ is defined as follows: points are the elements of C, C-lines are the sets which consist of q collinear points of C, and incidence is that of A_{2,q^n}. $I(C)$ is the n-dimensional affine space over $GF(q)$, and two C-lines are parallel if and only if the corresponding lines of A_{2,q^n} are parallel. Consequently the determination of the caps of $A_{n,q}$ ($n > 2$) is equivalent to the determination of the intersections of C with the arcs of the plane A_{2,q^n}.*

1. Introduction.

Let $GF(q)$ denote the Galois field of q elements, where $q = p^h, p$ is a prime and h is a positive integer. Denote by $A_{n,q}$ the affine space of n dimensions defined over $GF(q)$.

(*) Pervenuto in Redazione il 30 ottobre 1970.

(**) Indirizzo dell'Autore: Seminar of higher geometry — University of Ghent — J. Plateaustraat 22 — 9000 Gent (Belgium).

The field $GF(q^n)$ is an algebraic extension of $GF(q)$, and each element of $GF(q^n)$ can be written in one and only one way in the form $a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1}$, with $a_i \in GF(q)$ and α a zero of a polynomial of order n which belongs to the field $GF(q)$ and is irreducible in it [2].

The curve of A_{2,q^n} ($n \geq 1$, $q = p^h$) with equation $y = x^q$ is denoted by C. It is seen at once that the curve C contains q^n points.

2. Lemma.

Every line of A_{2,q^n} which contains at least two distinct points of C, contains exactly q points of C.

PROOF: We consider two distinct points $P_1(x_1, x_1^q)$, $P_2(x_2, x_2^q)$ ($x_1 \neq x_2$) of the curve C. A general point P of the set $P_1P_2 \setminus \{P_1, P_2\}$ has coordinates $(x_1 h - x_2)(h-1)^{-1}$, $(x_1^q h - x_2^q)(h-1)^{-1}$, with $h \in GF(q^n) \setminus \{0, 1\}$. The point P belongs to C if and only if

$$(1) \qquad (x_1^q h - x_2^q)(h-1)^{-1} = (x_1 h - x_2)^q (h-1)^{-q}.$$

Since $f \colon GF(q^n) \to GF(q^n)$, $a \to a^q$ is an automorphism of the Galois field $GF(q^n)$ [2], (1) is equivalent to

$$(x_1^q h - x_2^q)(h^q - 1) = (x_1^q h^q - x_2^q)(h-1),$$

or

$$(x_1 - x_2)^q (h^q - h) = 0.$$

So we conclude that $P \in C$ if and only if $h^q = h$ (2). The equation (2) has $q-2$ distinct solutions in the set $GF(q^n) \setminus \{0, 1\}$. There follows that the line P_1P_2 contains exactly q distinct points of the curve C, and the lemma is proved.

3. Theorem.

An incidence structure $I(C)$ is defined as follows: points are the elements of C, C-lines are the sets which consist of q collinear points of C, and incidence is that of A_{2,q^n}. Then $I(C)$ is the n-dimensional affine space over the Galois field $GF(q)$.

PROOF: Each element of $GF(q^n)$ can be written in one and only one way in the form $a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{n-1}\alpha^{n-1}$, with $a_i \in GF(q)$ and α a zero of a polynomial of order n which belongs to the field $GF(q)$ and is irreducible in it. With the point $P(x, x^q)$ of C, $x = \sum_{i=0}^{n-1} a_i \alpha^i$, we let correspond the point $P^*(a_0, a_1, \dots, a_{n-1})$ of $A_{n,q}$. In this way we obtain a bijection g of the pointset of C onto the pointset of the affine space $A_{n,q}$. Now we prove that every C-line of $I(C)$ is mapped by g onto a line of $A_{n,q}$.

For this purpose we consider two different points $P_1(x_1, x_1^q)$ and $P_2(x_2, x_2^q)$ of C, where $x_j = \sum_{i=0}^{n-1} a_i^{(j)} \alpha^i$ $(j = 1, 2)$. The points of the C-line P_1P_2 are the point P_1 and the points with coordinates $(x_1h - x_2)(h-1)^{-1}$, $(x_1^q h - x_2^q)(h-1)^{-1}$, with $h^q = h$ and $h \neq 1$ (see 2.). We remark that $h^q = h$ is equivalent to $h \in GF(q)$. Consequently, the points of the C-line $P_1 P_2$ are mapped onto the points $P_j^*(a_0^{(j)}, a_1^{(j)}, \dots, a_{n-1}^{(j)})$ and $((a_0^{(1)}h - a_0^{(2)})(h-1)^{-1}, (a_1^{(1)}h - a_1^{(2)})(h-1)^{-1}, \dots, (a_{n-1}^{(1)}h - a_{n-1}^{(2)})(h-1)^{-1})$, where $h \in GF(q) \setminus \{0, 1\}$. We conclude that the C-line P_1P_2 is mapped by g onto the line $P_1^*P_2^*$ of the affine space $A_{n,q}$.

Conversely, every line of $A_{n,q}$ corresponds with a C-line. Indeed, from the preceding there follows immediately that the line $Q_1^*Q_2^*$ of $A_{n,q}$ corresponds with the C-line Q_1Q_2, where $Q_i = g^{-1}(Q_i^*)$ $(i = 1, 2)$.

So we conclude that $I(C)$ is the n-dimensional affine space over the Galois field $GF(q)$.

4. Theorem.

Two C-lines of $I(C)$ are parallel if and only if the corresponding lines of A_{2,q^n} are parallel.

PROOF: We consider two C-lines P_1P_2 and P_3P_4, where P_j has coordinates x_j, x_j^q $(j = 1, 2, 3, 4)$. If $x_j = \sum_{i=0}^{n-1} a_i^{(j)} \alpha^i$ $(j = 1, 2, 3, 4)$, then from 3. it follows immediately that the C-lines P_1P_2 and P_3P_4 of $I(C)$ are parallel if and only if there exists an element $\varrho \in GF(q) \setminus \{0\}$ for which $a_i^{(3)} - a_i^{(4)} = \varrho(a_i^{(1)} - a_i^{(2)})$, $i = 1, 2, \dots, n-1$. Consequently the C-lines P_1P_2 and P_3P_4 are parallel if and only if $GF(q) \setminus \{0\}$ contains an element ϱ for which $x_3 - x_4 = \varrho(x_1 - x_2)$.

The lines $P_1 P_2$ and $P_3 P_4$ of A_{2, q^n} are parallel if and only if there exists an element $\varrho' \in GF(q^n) \setminus \{0\}$ such that $x_3 - x_4 = \varrho' (x_1 - x_2)$ and $x_3^q - x_4^q = \varrho' (x_1^q - x_2^q)$. So these lines are parallel if and only if $GF(q^n) \setminus \{0\}$ contains an element ϱ' such that $x_3 - x_4 = \varrho' (x_1 - x_2)$ and $\varrho'^q = \varrho'$. Consequently the lines $P_1 P_2$ and $P_3 P_4$ of A_{2, q^n} are parallel if and only if $GF(q) \setminus \{0\}$ contains an element ϱ' for which $x_3 - x_4 = \varrho' (x_1 - x_2)$.

So we conclude that the C-lines $P_1 P_2$ and $P_3 P_4$ of $I(C)$ are parallel if and only if the corresponding lines of A_{2, q^n} are parallel.

COROLLARIES: *a*) The points at infinity of the affine space $I(C)$ can be identified with the points at infinity $(1, x^{q-1}, 0)$, $x \in GF(q^n) \setminus \{0\}$, of the affine plane A_{2, q^n}.

b) If P_{2, q^2} is the projective plane defined over $GF(q^2)$, then the $q^2 + q + 1$ points (x, x^q, a) $(x \in GF(q^2), a \in \{0, 1\})$, a and x not both zero) constitute a Baer subplane [1] of P_{2, q^2}.

c) If A_n, $n \geq 3$, is a finite n-dimensional affine space then there always exists a finite Desarguesian affine plane A_2 satisfying the following conditions

1^0 the pointset of A_n is a subset of the pointset of A_2;

2^0 the intersection of a line of A_2 and the pointset of A_n is a line of A_n, a point or the void set;

3^0 every line of A_n is subset of a line of A_2;

4^0 two lines of A_n are parallel if and only if the corresponding lines of A_2 are parallel.

5. k-arcs and k-caps.

A k-arc (resp. k-cap) of $A_{2, q}$ (resp. $A_{n, q}$, $n > 2$) is a set of k points of $A_{2, q}$ (resp. $A_{n, q}$), no three of which are collinear.

The caps of the affine space $A_{n, q} = I(C)$ $(n > 2)$ evidently are the intersections of C with the arcs of the affine plane A_{2, q^n}.

Three distinct points $P_1 (x_1, x_1^q)$, $P_2 (x_2, x_2^q)$, $P_3 (x_3, x_3^q)$ of the curve C are not collinear if and only if

$$(3) \qquad \begin{vmatrix} x_1 & x_1^q & 1 \\ x_2 & x_2^q & 1 \\ x_3 & x_3^q & 1 \end{vmatrix} \neq 0.$$

Since

$$\begin{vmatrix} x_1 & x_1^q & 1 \\ x_2 & x_2^q & 1 \\ x_3 & x_3^q & 1 \end{vmatrix} = (x_1 - x_3)(x_2 - x_3) \begin{vmatrix} 1 & (x_1 - x_3)^{q-1} & 0 \\ 1 & (x_2 - x_3)^{q-1} & 0 \\ x_3 & x_3^q & 1 \end{vmatrix} =$$

$$= (x_1 - x_3)(x_2 - x_3)((x_2 - x_3)^{q-1} - (x_1 - x_3)^{q-1})$$

and since x_1, x_2, x_3 are distinct elements of $GF(q^n)$, (3) is equivalent to

$$\left(\frac{x_1 - x_3}{x_2 - x_3}\right)^{q-1} \neq 1.$$

So we conclude that P_1, P_2, P_3 are not collinear if and only if

$$\frac{x_1 - x_3}{x_2 - x_3} \notin GF(q) \subset GF(q^n).$$

Consequently the determination of the k-caps (k-arcs when $n = 2$) of $A_{n,q}$ $(n \geq 2)$ is equivalent to the determination of the sets $\{x_1, x_2, \dots, x_k\}$, $x_i \in GF(q^n)$, with

$$\frac{x_i - x_l}{x_j - x_l} \notin GF(q) \subset GF(q^n),$$

$\forall\, i, j, l \in \{1, 2, \dots, k\}$ and i, j, l distinct.

Other interpretation: the determination of the k-caps (k-arcs when $n = 2$) of $A_{n,q}$ $(n \geq 2)$ is equivalent to the determination of the pointsets $\{Q_1, Q_2, \dots, Q_k\}$ of the affine line A_{1,q^n}, for which

$$\frac{Q_i Q_l}{Q_j Q_l} \notin GF(q) \subset GF(q^n),$$

$\forall\, i, j, l \in \{1, 2, \dots, k\}$ and i, j, l distinct.

Remark: If $q = 3$ then the three distinct points $P_1(x_1, x_1^3)$, $P_2(x_2, x_2^3)$, $P_3(x_3, x_3^3)$ of the curve C of the plane $A_{2,3^n}$ $(n \geq 2)$ are not collinear if and only if

$$\frac{x_1 - x_3}{x_2 - x_3} \notin \{0, 1, -1\}. \tag{4}$$

Since x_1, x_2, x_3 are distinct elements of $GF(3^n)$, (4) is equivalent to

$$\frac{x_1 - x_3}{x_2 - x_3} \neq -1.$$

So we conclude that P_1, P_2, P_3 are not collinear if and only if

$$x_1 + x_2 + x_3 \neq 0.$$

BIBLIOGRAPHY

[1] P. DEMBOWSKI, *Finite geometries*, Springer-Verlag, Berlin-Heidelberg New York (1968).

[2] B. SEGRE, *Lectures on modern geometry*, Edizioni Cremonese, Roma (1961).