

Viliam Chval; Rastislav Jurga

Tangents of conics in Hjelmslev planes over a local ring of even characteristic

Mathematica Slovaca, Vol. 48 (1998), No. 1, 69--78

Persistent URL: <http://dml.cz/dmlcz/130139>

Terms of use:

© Mathematical Institute of the Slovak Academy of Sciences, 1998

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

TANGENTS OF CONICS IN HJELMSLEV PLANES OVER A LOCAL RING OF EVEN CHARACTERISTIC

VILIAM CHVÁL — RASTISLAV JURGA

(Communicated by Anatolij Dvurečenskij)

ABSTRACT. In this paper, combinatorial properties of conics in the Desarguesian Hjelmslev plane over a finite local ring of even characteristic are investigated. The main result of this paper is a statement about the total number of tangents to the given conic.

In this paper, we will prove some combinatorial results concerning conics in the Desarguesian Hjelmslev plane over a special local ring of even characteristic. The analogous problem in the case of a projective plane — combinatorics of conics (and more generally of ovals) in the Desarguesian projective planes is now classical and closed following to the papers of B. Segre and his school.

The authors obtained some results concerning conics in the Desarguesian Hjelmslev plane over a special local ring of characteristic odd in [3], [4].

1. Concepts and notations

In this paper, by *special local ring* we will understand a finite commutative local ring R the ideal I of divisors of zero of which is principal. Let us denote by g the generator of the ideal I . We will call the smallest integer $n \in \mathbb{N}$ such that $g^n = 0$ the *index of nilpotency* of the ring R . For $a \in I$ let us denote by the symbol $\nu(a)$ the smallest integer $\alpha \in \mathbb{N}$ for which $a = Ag^\alpha$, $A \in R - I$, and let $[a]$ denote the ideal generated by the element a . We will understand by the *annihilator* the set $\text{An } a = \{x \in R; xa = 0\}$.

Let us assume that R is not a field, and that the characteristic of the ring R is even. We will denote by the symbol \bar{R} the factor ring R/I , and by Ψ the

AMS Subject Classification (1991): Primary 51C05, 51E30.

Key words: Hjelmslev plane, conic, tangent of a conic, number of tangents of a conic.

canonical homomorphism R on \overline{R} . Furthermore, let us denote by the symbol R^* the set of regular elements of R , i.e., $R^* = R - I$. We will denote by $H(R)$ the Desarguesian Hjelmslev plane over the ring R . The symbol Ψ will also denote the canonical homomorphism $H(R)$ onto the projective plane $\pi(\overline{R})$.

A *conic* in $H(R)$ is the set of all points $[x_1; x_2; x_3] \in H(R)$ the coordinates of which satisfy the equation

$$\sum_{i,j=1}^3 a_{ij}x_i x_j = 0, \quad \exists a_{ij} \notin I. \quad (1)$$

We will also use the notation $[x; y; z]$ for the point $[x_1; x_2; x_3]$. Furthermore, we will assume that the conic is nondegenerate. For a nondegenerate conic (1) in a projective plane, there is a coordinate system in which the conic has the equation

$$\overline{x}^2 - \overline{y}\overline{z} = 0.$$

Let us denote by the symbol \overline{Q} the image of the conic Q in $H(R)$ under the canonical homomorphism Ψ . A *tangent* of Q is a line which meets Q in at least two neighbouring points. Let us note that points which a tangent has in common with the conic are neighbouring.

2. Tangents of the conic in the plane $H(R)$

Let Q be a nondegenerate conic in $H(R)$. Then we have:

LEMMA 2.1. *Let $|\overline{R}| \geq 4$. The conic Q has (at least) $|\overline{R}| + 1$ nonneighbouring points.*

P r o o f. Let the equation of the conic be

$$\sum_{i,j=1}^3 a_{ij}x_i x_j = 0. \quad (2)$$

Then the conic \overline{Q} in the projective plane $\pi(\overline{R})$ has equation

$$\sum_{i,j=1}^3 \overline{a}_{ij}\overline{x}_i \overline{x}_j = 0. \quad (3)$$

There are at least four points on the conic \overline{Q} . Let us choose a point $\overline{X} \in \overline{Q}$. There is a regular transformation \overline{P} such that

$$\overline{X}\overline{P}^{-1} = \overline{Y} = [0; 1; 0],$$

and the conic \overline{Q} has the equation

$$\overline{y}_1^2 - \overline{y}_2\overline{y}_3 = 0. \quad (4)$$

The transformation $X = YP$ maps the conic (2) into the form

$$ay_1^2 + by_1y_2 + cy_1y_3 + dy_2^2 + ey_2y_3 + fy_3^2 = 0. \quad (5)$$

With regard to the relation (4), we have $b, c, d, f \in I$ and $\bar{e} = -1$. Because the point $[0; 1; 0]$ is on the conic (4), we will seek the point $Y = [0; 1; k]$, $k \in I$, which is on the conic (5). A necessary and sufficient condition for this is

$$d + ek + fk^2 = 0. \quad (6)$$

We will consider now the mapping $\varphi: I \rightarrow I$ defined by the relation

$$\varphi(k) = fk^2 + ek + d.$$

The mapping φ is injective. Indeed, if

$$d + ek + fk^2 = d + eK + fK^2,$$

then

$$(k - K)[e + f(k + K)] = 0.$$

Because $e + f(k + K) \in I$, $e \notin I$, $f \in I$, we have

$$k - K = 0.$$

Thus the mapping φ is injective. Thus there exists $k \in I$ such that $\varphi(k) = fk^2 + ek + d = 0$. For this k , the point $[0; 1; k]$ is on (5). Then the point $X = YP$ is on the conic (1), and its image is just \overline{X} . Because \overline{X} is any point of the conic \overline{Q} , the result is proved. \square

The following result is proved using Lemma 2.1.

THEOREM 2.1. *Let Q be a conic in the plane $H(R)$. Then there is a linear transformation which transforms the equation of the conic to the form*

$$x^2 - yz = 0.$$

P r o o f. According to Lemma 2.1, there exist four nonneighbouring points E_1, E_2, E_3, E_4 on the conic Q which we will choose as vertices of the coordinate system: $E_1 = [1; 0; 0]$, $E_2 = [0; 1; 0]$, $E_3 = [0; 0; 1]$, $E_4 = [1; 1; 1]$. In this coordinate system, the conic Q has equation

$$ax_1x_2 + bx_1x_3 + cx_2x_3 = 0, \quad (7)$$

and from the regularity of Q , it follows that $a, b, c \notin I$. Let $a = 1$. Using the transformation with matrix

$$\begin{bmatrix} -c & 0 & -c \\ 0 & -b & -b \\ 0 & 0 & 1 \end{bmatrix}$$

one obtains

$$z_3^2 - z_1 z_2 = 0,$$

as was to be proved. □

Using Lemma 2.1 we will prove the following result.

THEOREM 2.2. *Let Q be a conic in the plane $H(R)$. Then for the number of points of the conic Q we have*

$$|Q| = (|\bar{R}| + 1)|I|.$$

Proof. Let us choose any point $\bar{P}_0 = [\bar{x}_0; \bar{y}_0; \bar{z}_0]$ of the conic Q which has exactly $|\bar{R}| + 1$ points. At least one coordinate of the point \bar{P}_0 must be nonzero. Let $\bar{P}_0 = [\bar{x}_0; 1; \bar{x}_0^2]$. Certainly, for every $x_0 \in R$ such that $\Psi(x_0) = \bar{x}_0$ the point $P_0 = [x_0; 1; x_0^2]$ is on the conic Q and it satisfies $\Psi(P_0) = \bar{P}_0$. Then it maps into every point $\bar{P}_0 \in \bar{Q}$ exactly $|I|$ points of the conic Q . □

DEFINITION 2.1. Let Q be a conic in the plane $H(R)$. We will call a point $P \in H(R)$ a *nucleus* of the conic Q in the plane $H(R)$ if and only if \bar{P} is a nucleus of the conic \bar{Q} in $\pi(\bar{R})$.

Consequently, if the conic Q has the equation $x^2 = yz$, nuclei of the conic Q are the points $[1; j; k]$, $j, k \in I$.

We have:

THEOREM 2.3. *Let $A \in Q$, and let P be a nucleus of the conic Q . Then the line AP is a tangent of the conic Q .*

Proof. Without loss of generality, it can be assumed that $Q : x^2 = yz$, $A = [x_0; 1; x_0^2]$, and $P = [1; j; k]$, $j, k \in I$. Obviously, the line $\bar{t} = \overline{AP}$ is a tangent of the conic \bar{Q} in the projective plane $\pi(\bar{R})$. Therefore $t \cap Q$ cannot include nonneighbouring points. Let us prove that the line $t = AP$ has at least two further neighbouring points in common with the conic. The line t (which is incident to the nucleus) has the equation

$$(-bj - ck)x + by + cz = 0.$$

Because $A \in t$, we have

$$(-bj - ck)x_0 + b + cx_0^2 = 0.$$

TANGENTS OF CONICS IN HJELMSLEV PLANES

For $i \in I$ let us denote $A(i) = [x_0 + i; 1; (x_0 + i)^2] \in Q$. $A(i) \in t$ if and only if

$$(-bj - ck)(x_0 + i) + b + c(x_0 + i)^2 = 0,$$

i.e.,

$$(-bj - ck) + 2cx_0i + ci^2 = 0$$

or

$$i(-bj - ck + 2cx_0i + ci) = 0. \quad (9)$$

If $-bj - ck + 2cx_0 = B \in I$, then the equation (9) has the form

$$i(B + ci) = 0.$$

The last equation holds for every $i \in I$ with $\nu(i) \geq n - \nu(B)$. □

THEOREM 2.4. *If t is a tangent of the conic Q , then the line t is incident to a nucleus.*

Proof. Obviously, \bar{t} is the tangent of the conic in the projective plane $\pi(\bar{R})$, and it is incident to the nucleus $\bar{P} = [1; 0; 0]$. Therefore, there is a point on the line t neighbouring with the point $P = [1; 0; 0]$. □

THEOREM 2.5. *The line $ax + by + cz = 0$ incident to a point of the conic $x^2 = yz$ is tangent to it if and only if $a \in I$.*

Proof.

1. Let $a \in I$, $b \notin I$. The line $ax + by + cz = 0$ is incident to the nucleus $[1; 0; -\frac{a}{b}]$ and then is a tangent of Q . Analogously, for $c \notin I$.

2. Let the line $ax + by + cz = 0$ be a tangent of Q . According to Theorem 2.4, the line is incident to the nucleus $[1; j; k]$, consequently,

$$a + bj + ck = 0,$$

and the result is obvious. □

Remark. It follows from Theorem 2.5 that if a tangent is incident to the point $[x_0; 1; x_0^2]$, then its equation can be expressed in the form

$$z = ix + ky, \quad i \in I,$$

and tangents that are incident to the point $[y_0; y_0^2; 1]$ have the equation

$$y = ix + kz, \quad i \in I.$$

THEOREM 2.6. *Exactly $|I|$ tangents are incident to each point of the conic.*

Proof. For the tangent which is incident to the point $A = [x_0; 1; x_0^2]$ of the conic we have

$$x_0^2 = ix_0 + k$$

and $k = x_0^2 - ix_0$. It follows from this that the number of tangents is equal to the number of possibilities for $i \in I$, from which the result follows immediately. □

3. Properties of the set $M(b)$

In this part of the paper, we will prove some algebraic-combinatorial results which are necessary for the proof of the main results in part 4.

For $b \in I$ let us denote

$$M(b) = \{a \in I, a(a+b) = 0\}.$$

We have:

LEMMA 3.1. $M(rg^\beta) = M(g^\beta)$, $r \in R - I$.

Proof. Obviously, $a(a+g^\beta) = 0 \iff ra(ra+rg^\beta) = 0$, then $a \in M(g^\beta) \iff ra \in M(rg^\beta)$. \square

LEMMA 3.2. Let $b = g^\beta$. If $\beta < \lceil \frac{n}{2} \rceil$, then $\text{An}b \cap (-b + \text{An}b) = \emptyset$.

Proof. Let $x \in \text{An}b \cap (-b + \text{An}b)$, $x \neq 0$, $x = Xg^\eta = Yg^\epsilon - g^\beta$, $\eta, \epsilon \geq \frac{n}{2}$. Then $Xg^\eta = g^\beta(Yg^{\epsilon-\beta} - 1)$, which is impossible because $\beta < \lceil \frac{n}{2} \rceil \leq \frac{n}{2} < \eta$. \square

If $x = o \text{An}b \cap (-b + \text{An}b)$, then $o = -b + x$, $x \in \text{An}b$, i.e., $b = x \in \text{An}b$, which is the contradiction with $\beta < \lceil \frac{n}{2} \rceil$.

LEMMA 3.3. If $b = g^\beta$, $\beta \geq \frac{n}{2}$, then $M(b) = [g^{\lceil \frac{n}{2} \rceil}]$.

Proof.

1. Let $a = Ag^\alpha$, $\alpha \geq \frac{n}{2}$. Then $2\alpha \geq n$, $\alpha + \beta \geq n$, and $a(a+b) = a^2 + ab = A^2g^{2\alpha} + Ag^{\alpha+\beta} = 0$, i.e., $a \in M(b)$.

2. If $\alpha < \lceil \frac{n}{2} \rceil$, then $2\alpha < n$, $a(a+b) = Ag^\alpha(Ag^\alpha + g^\beta) = Ag^{2\alpha}(A + g^{\beta-\alpha}) \neq 0$ because $g^{2\alpha} \neq 0$ and $A + g^{\beta-\alpha} \notin I$. \square

LEMMA 3.4. If $\beta < \lceil \frac{n}{2} \rceil$, $b = g^\beta$, then $M(b) = \text{An}b \cup (-b + \text{An}b)$.

Proof.

1. Let $a \in M(b)$.

a) Let $\nu(a) > \beta$. Then $\text{An}(a+b) = \text{An}b$, and then $a \in M(b)$, i.e., $a(a+b) = 0$, $a \in \text{An}(a+b)$.

b) Let $\nu(a) = \nu(b) = \beta$. Then $a+b \in \text{An}a = \text{An}b$.

c) Let $\nu(a) < \nu(b)$, then $(a+b)a = 0 \implies a+b \in \text{An}a \subset \text{An}b$.

2. Let $a \in \text{An}b$, then $\nu(a) = \alpha \geq \lceil \frac{n}{2} \rceil$. Then $a(a+b) = a^2 + ab = A^2g^{2\alpha} + Ag^{\alpha+\beta} = 0$. Thus $ab = 0$ because $a \in \text{An}b$, $Ag^{2\alpha} = 0$ for $\alpha \geq \lceil \frac{n}{2} \rceil$.

3. Let $a+b \in \text{An}b$, then $b(a+b) = 0$. Let us distinguish the cases:

(i) $\nu(a) \geq \nu(b)$: now $g^\alpha \cdot (a+b) = g^{\alpha-\beta}g^\beta(a+b) = g^{\alpha-\beta} \cdot b(a+b) = 0$,

(ii) $\nu(a) < \nu(b)$: in this case, $b(a+b) = 0$, then $g^\beta(Ag^\alpha + g^\beta) = g^{\beta+\alpha} \cdot (A + g^{\beta-\alpha}) = 0$. This is a contradiction because $\alpha + \beta < 2\beta < n$.

□

We will determine the cardinality of the set $M(b)$ for $b = g^\beta$.

LEMMA 3.5. For $0 < \alpha < n$, $|[g^\alpha]| = |\overline{R}|^{n-\alpha}$.

Proof. The ideal $[g^\alpha]$ is generated by the elements ag^α , $a \in R$. For $a, b \in R$, we have $ag^\alpha = bg^\alpha$ if and only if $(a - b)g^\alpha = 0$, i.e., if $a - b \in \text{An } g^\alpha$. Then the number of elements $a \in R$ which give the same element ag^α is equal to $|\text{An } g^\alpha| = |\overline{R}|^\alpha$. Thus

$$|[g^\alpha]| = \frac{|R|}{|\overline{R}|^\alpha} = |\overline{R}|^{n-\alpha}$$

because, in a local ring, we have $|R| = |\overline{R}|^n$.

□

THEOREM 3.1. If $\beta < \lceil \frac{n}{2} \rceil$, then $|M(b)| = 2|\overline{R}|^\beta$.

Proof. According to Lemma 3.2 and Lemma 3.4, we have, $M(b) = \text{An } b \cup (-b + \text{An } b)$ and $\text{An } b \cap (-b + \text{An } b) = \emptyset$. Thus $|M(b)| = |\text{An } b| + |(-b + \text{An } b)| = 2|\text{An } b| = 2|\overline{R}|^\beta$, where $b = g^\beta$.

□

THEOREM 3.2. If $\beta \geq \lceil \frac{n}{2} \rceil$, then $|M(b)| = |\overline{R}|^{n-\lceil \frac{n}{2} \rceil} = |\overline{R}|^{\lfloor \frac{n}{2} \rfloor}$.

Proof. The result is an immediate consequence of Lemma 3.3.

$$M(b) = |[g^{\lceil \frac{n}{2} \rceil}]| = |\overline{R}|^{n-\lceil \frac{n}{2} \rceil}.$$

□

LEMMA 3.6. $M(0) = [g^{\lceil \frac{n}{2} \rceil}]$.

Proof. If $a \in M(0)$, then $a(a + 0) = a^2 = 0$. For $a = Ag^\alpha$ then we have $2\alpha \geq n$. Conversely, if $\alpha > \frac{n}{2}$, certainly $a^2 = 0$, and consequently, $a \in M(0)$.

□

LEMMA 3.7. $|M(0)| = |\overline{R}|^{\lfloor \frac{n}{2} \rfloor} = |\overline{R}|^{n-\lceil \frac{n}{2} \rceil}$.

LEMMA 3.8. The set $M = \{b \in I; b = Bg^\beta, B \in R^*\}$ contains $\frac{|R^*|}{|\overline{R}|^\beta}$ elements.

Proof. The number of possibilities for b is equal to the number of regular elements $B \in R^*$, consequently, $Bg^\beta = B'g^\beta$, $B, B' \in R^*$. Then $(B - B')g^\beta = 0 \iff B - B' \in \text{An } g^\beta$. Thus $|\text{An } g^\beta| = |\overline{R}|^\beta$, and the total number of elements of the set M is

$$\frac{|R^*|}{|\overline{R}|^\beta}.$$

□

4. The number of tangents of the conic

Let A be a point of the conic Q , and let $[A]$ be the class of all points neighbouring with the point A .

THEOREM 4.1. *The total number of tangents which are incident to points from the class $[A]$ is equal to*

$$\sum_{b \in I} \frac{|I|}{M(b)}. \quad (10)$$

P r o o f. Let the line

$$z = ix + ky, \quad i \in I, \quad k \in R, \quad (11)$$

be a tangent of the conic $Q : x^2 - yz = 0$ at the point $A = [x_0; 1; x_0^2] \in Q$. From (11), we have

$$k = x_0^2 - ix_0. \quad (12)$$

Consequently, for given $i \in I$ the number of different k of form (12) is equal to the number of different tangents. Let us consider all the tangents incident to points $A' = [x'_0; 1; x'^2_0]$ neighbouring with the point A . For x_0 and x'_0 the relation (12) determines the same tangent if

$$x_0^2 - ix_0 = x'^2_0 - ix'_0,$$

from which it follows that

$$(x'_0 - x_0)(x_0 + x'_0 - i) = 0. \quad (13)$$

Let us denote $x'_0 - x_0 = a \in I$. Then (13) becomes

$$a(a + 2x_0 - i) = 0.$$

If we denote $2x_0 - i = b$, we obtain

$$a(a + b) = 0. \quad (14)$$

This means that the points $A = [x_0; 1; x_0^2]$, $A' = [x'_0; 1; x'^2_0]$ (A, A' are neighbouring) are incident to the same tangent (11) if and only if $a \in M(b)$. Because there are exactly $|I|$ points in the class $[A]$, the result follows. \square

Remark. (10) also holds when R is a field. Then we have $I = \{0\} - M(0)$.

Let us denote $\lfloor \frac{n}{2} \rfloor = m$, and let $S_1 = \sum_{\nu(b) \leq m-1} \frac{|I|}{|M(b)|}$, $S_2 = \sum_{\nu(b) \geq m} \frac{|I|}{|M(b)|}$, $S_3 = \frac{|I|}{|M(0)|}$ and $S = S_1 + S_2 + S_3$. We will now find the numbers S_1, S_2, S_3 .

THEOREM 4.2. *We have*

$$S_1 = \frac{|I| \cdot |R^*|}{2|\overline{R}|^{2m-2}} \cdot \frac{|\overline{R}|^{2m-2} - 1}{|\overline{R}|^2 - 1}.$$

Proof. According to Lemma 3.1, for $b = Bg^\beta$ we have $M(b) = M(g^\beta)$. Using Theorem 3.1 and Lemma 3.8 we get

$$S_1 = \sum_{\beta=1}^{m-1} \frac{|I|}{2|\overline{R}|^\beta} \cdot \frac{|R^*|}{|\overline{R}|^\beta} = \frac{|I| \cdot |R^*|}{2} \cdot \sum_{\beta=1}^{m-1} \frac{1}{|\overline{R}|^{2\beta}},$$

after reordering, we obtain

$$\frac{|I| \cdot |R^*|}{2|\overline{R}|^{2m-2}} \cdot \frac{|\overline{R}|^{2m-2} - 1}{|\overline{R}|^2 - 1},$$

which was necessary to prove. \square

THEOREM 4.3. *We have*

$$S_2 = \frac{|I| \cdot |R^*|}{|\overline{R}|^{2n-m-1}} \cdot \frac{|\overline{R}|^{n-m} - 1}{|\overline{R}| - 1}.$$

Proof. Using Theorem 3.1 and Lemma 3.8, according to Lemma 3.1, we get

$$S_2 = \sum_{\beta=m}^{n-1} \frac{|I|}{|\overline{R}|^{n-m}} \cdot \frac{|R^*|}{|\overline{R}|^\beta} = \frac{|I| \cdot |R^*|}{|\overline{R}|^{n-m}} \sum_{\beta=m}^{n-1} \frac{1}{|\overline{R}|^\beta} = \frac{|I| \cdot |R^*|}{|\overline{R}|^{2n-m-1}} \cdot \frac{|\overline{R}|^{n-m} - 1}{|\overline{R}| - 1}.$$

\square

THEOREM 4.4. *We have*

$$S_3 = \frac{|I|}{|\overline{R}|^{n-m}}.$$

Proof. According to Lemma 3.7, we have

$$S_3 = \frac{|I|}{|M(0)|} = \frac{|I|}{|\overline{R}|^{n-m}}.$$

\square

COROLLARY 4.1. *The total number of tangents to the conic that are incident to points neighbouring with a given point of the conic is equal to $S_1 + S_2 + S_3$.*

Proof. This follows from Theorems 4.1, 4.2 and 4.3, and from Lemma 3.1. \square

COROLLARY 4.2. *The total number of tangents to the conic is given by the relation*

$$(S_1 + S_2 + S_3)(|\overline{R}| + 1).$$

Proof. This follows from Corollary 4.1 and the fact that the conic in $H(R)$ has exactly $|\overline{R}| + 1$ nonneighbouring points. \square

REFERENCES

- [1] BERZ, E. : *Kegelschnitte in Desarguesian Ebenen*, Math. Z. **78** (1962).
- [2] DEMBOWSKI, P. : *Finite Geometries*, Springer-Verlag, New-York Inc., 1968.
- [3] HUGHES, D. R.—PIPER, F. C. : *Projective Planes*, Springer-Verlag, New York-Heidleberg-Berlin, 1973.
- [4] CHVÁL, V. : *Some properties of quadrics in Hjelmslev plane*. Technical report I-4-2/9a, PF UPJŠ, Košice, 1975. (Slovak)
- [5] JURGA, R. : *Some combinatorial properties of conics in the Hjelmslev plane*, Math. Slovaca **45** (1995), 219–226.
- [6] PRIMROSE, E. J. F. : *Quadrics in finite geometries*, Proc. Cambridge Philos. Soc. **147** (1951).

Received August 30, 1994

Revised March 15, 1996

*Katedra hospodárskej informatiky
a matematiky
Podnikovohospodárska fakulta
v Košiciach
Ekonomickej univerzity
v Bratislave
Tajovského 11
SK-041 30 Košice
SLOVAKIA*