A Note on a Specific Pencil of Conics in the Galois Fields of Order 2^n

Metod Saniga

Astronomical Institute, Slovak Academy of Sciences, SK-059 60 Tatranská Lomnica,
The Slovak Republic
E-mail: msaniga@astro.sk

Abstract

The pencil of conics featuring three degenerate conics each of which is a line-pair is briefly inspected in a Galois field of characteristic two. It is shown that if two degenerates are conjugate imaginary line pairs, the third must be a *real* line pair; this contradicts Campbell's claim (Campbell 1927) that all the three singular conics are conjugate imaginary line pairs.

Our remark concerns the structure of the pencil of conics containing three degenerate conics of which two represent conjugate imaginary line pairs, i.e. the pencil defined by Eq. (24) in [1]. In what follows we will demonstrate that Campbell's claim that also the third singular conic 'must be a conjugate imaginary line pair' is false, because this conic is, in fact, a *real* line pair.

The proof relies on the following theorem: the expression

$$u^2 + v^2 + \Theta uv, \qquad \Theta \neq 0, \tag{1}$$

where u and v are regarded as variables and Θ is a parameter, is reducible or irreducible in the Galois field of order 2^n (GF(2^n)) iff, respectively,

$$D\left(1/\Theta^2\right) = 0, \tag{2}$$

or

$$D\left(1/\Theta^2\right) = 1, \tag{3}$$

where

$$D(w) \equiv w + w^2 + w^4 + \ldots + w^{2^{n-1}} \tag{4}$$

(see, e.g. [2]). The pencil of conics concerned is (see Eq. (24) of [1])

$$C(\lambda, \mu) \equiv \lambda C_1 + \mu C_2 \equiv \lambda\left(x^2 + y^2 + \alpha xy\right) + \mu\left(x^2 + z^2 + \beta xz\right), \tag{5}$$

where

$$\alpha\beta \neq 0, \quad \alpha \neq \beta. \tag{6}$$

If the conics $C_1 = 0$ and $C_2 = 0$ are to represent conjugate imaginary line pairs, both C_1 and C_2 must be *ir*reducible, i.e.

$$D\left(1/\alpha^2\right) = 1 = D\left(1/\beta^2\right). \tag{7}$$

Our task is to find the character of the third degenerate conic of the pencil, which is given by (see p. 405 of [1])

$$C_3 \equiv \left(\beta^2 + \alpha^2\right) x^2 + \beta^2 y^2 + \alpha^2 z^2 + \beta^2 \alpha xy + \beta\alpha^2 xz = 0. \tag{8}$$

To this end in view we first notice that with the help of the relation

$$(u+v)^2 = u^2 + v^2 \tag{9}$$

Eq. (8) can be cast into the form

$$\bar{C}_3 = x^2 + \left(\frac{\beta y + \alpha z}{\alpha + \beta}\right)^2 + \frac{\alpha\beta}{\alpha+\beta}\, x\, \frac{\beta y + \alpha z}{\alpha + \beta} = 0, \tag{10}$$

which, using a non-singular transformation

$$\begin{aligned} x' &= x, \\ y' &= \frac{\beta y + \alpha z}{\alpha + \beta}, \\ z' &= \frac{\alpha y + \beta z}{\alpha + \beta}, \end{aligned} \tag{11}$$

is sent into

$$C_3' = x'^2 + y'^2 + \gamma x' y' = 0, \tag{12}$$

where

$$\gamma \equiv \frac{\alpha\beta}{\alpha+\beta}. \tag{13}$$

The shape of C_3' is identical with that of Eq. (1) so that its character, in the light of the above-introduced theorem, depends solely on the value of $D\left(1/\gamma^2\right)$. In order to find the latter we first observe that

$$D\left(1/\gamma^2\right) = D\left(\frac{\alpha^2+\beta^2}{\alpha^2\beta^2}\right) = D\left(\frac{1}{\alpha^2} + \frac{1}{\beta^2}\right). \tag{14}$$

Further, from the definition of $D(w)$ and Eq. (9) it can easily be verified that

$$D(u+v) = D(u) + D(v), \tag{15}$$

which implies that

$$D\left(1/\gamma^2\right) = D\left(1/\alpha^2\right) + D\left(1/\beta^2\right) = 1 + 1 = 0 \tag{16}$$

where we also took into account Eq. (7) and the fact that $w + w = 0$ for any $w \in \mathrm{GF}(2^n)$. Eq. (16) tells us that C_3' is *reducible* and the corresponding conic $C_3' = 0$ thus, indeed, represents a *real* line pair.

References

[1] A. D. Campbell, Pencils of conics in the Galois fields of order 2^n, Amer. J. Math. 49 (1927) 401–406.

[2] J. W. P. Hirschfeld, "Projective Geometries over Finite Fields," Clarendon Press, Oxford, 1979.