Can. J. Math., Vol. XXVI, No. 6, 1974, pp. 1281–1288

ON CONICS OVER A FINITE FIELD

FUANGLADA R. JUNG

1. Introduction. Let F denote a Galois field of order q and odd characteristic p, and $F^* = F\backslash\{0\}$. Let S_n denote an n-dimensional affine space with base field F. E. Cohen [**1**] had proved that if $n \geqq 4$, there is no hyperplane of S_n contained in the complement of the quadric Q_n of S_n defined by

$$(1.1) \qquad a = a_1x_1^2 + \ldots + a_nx_n^2 \quad (\alpha = a_1 \ldots a_n \neq 0)$$

and in S_3, there are $q + 1$ or 0 planes contained in the complement of Q_3 according as $-a\alpha$ is not or is a square of F.

In this paper, we determine the number of lines of S_2 contained in the complement of a given conic of S_2 (see Theorems 2 and 4). Moreover, we obtain directly from the proofs of Theorems 2 and 4, the number of lines of S_2 which are 1-dimensional subspaces of S_2 contained in the complement of a given conic of S_2 (see Theorems 3 and 5). We note that Theorems 2 and 3 are concerned with central conics and Theorems 4 and 5 with noncentral conics. Finally, by applying the preceding results, we obtain the number of planes of S_3 which are in the complement of the intersection of a diagonal quadric and a plane of S_3 and which are not parallel to the given plane (see Theorem 6).

2. Let $\Psi(a)$ denote the Legendre symbol in F; that is, $\Psi(a) = 1, -1$ or 0 according as a is a square, a nonsquare or zero in F. Furthermore, for any set S, let $|S|$ denote its cardinal number.

For any $a, a_1, a_2 \in F$ such that $a_1a_2 \neq 0$, let

$$N(a;\, a_1, a_2) = \{(x_1, x_2) \in F \times F | a_1x_1^2 + a_2x_2^2 = a\}$$

LEMMA 1 [**2**, §64]. *For any $a, a_1, a_2 \in F$ such that $\alpha = a_1a_2 \neq 0$,*

$$(2.1) \qquad |N(a;\, a_1, a_2)| = \begin{cases} q - \Psi(-\alpha) & \text{if } a \neq 0, \\ q + (q-1)\Psi(-\alpha) & \text{if } a = 0. \end{cases}$$

For convenience, we say that any two elements (x_1, x_2) and (y_1, y_2) of $F \times F$ are proportional, and write $(x_1, x_2) \sim (y_1, y_2)$ if and only if $(x_1, x_2) = (\rho y_1, \rho y_2)$ for some $\rho \in F^*$. Clearly, $\sim$ is an equivalence relation. We denote the equivalence class containing $(x_1, x_2) \in F \times F$ by $[x_1, x_2]$ and the quotient set $F \times F/\sim$ by Q, and let $Q^* = Q\backslash\{[0, 0]\}$.

2.1 *Remarks* (a). It follows from Lemma 1 that for any squares μ, ν in F^*, $|N(\mu;\, a_1, a_2)| = |N(\nu;\, a_1, a_2)|$, where $a_1, a_2 \in F^*$. Moreover, it is easily seen

Received May 16, 1972. This research was supported by NSF Grant GP-8742.

https://doi.org/10.4153/CJM-1974-122-9 Published online by Cambridge University Press

that any (x_1, x_2) in $N(\mu; a_1, a_2)$ is proportional to some element (y_1, y_2) in $N(\nu; a_1, a_2)$. Furthermore, since for any fixed nonsquare λ in F^*, $\{\lambda\rho^2|\rho \in F^*\}$ is the set of all nonsquares in F^*, the above remark also holds true when μ and ν are both nonsquares.

(b) It is easily seen that if

$$P(a; a_1, a_2) = \{[x_1, x_2] \in Q^*|(x_1, x_2) \in N(a; a_1, a_2)\},$$

then

$$|P(a; a_1, a_2)| = |N(a; a_1, a_2)|/2 \quad \text{or} \quad \{|N(a; a_1, a_2)| - 1\}/(q - 1)$$

according as $a \neq 0$ or $a = 0$.

(c) Throughout the remainder of the paper, for any $b, b_1, b_2 \in F$, where at least one of b_1 and b_2 is nonzero, let $L(b; b_1, b_2)$ denote the line of S_2 which is represented by the equation

$$b = b_1x_1 + b_2x_2. \tag{2.2}$$

We observe that $L(0; b_1, b_2)$ and $L(0; b_1', b_2')$ are the same if and only if $[b_1, b_2] = [b_1', b_2']$.

THEOREM 1. *Let a, b, a_1, a_2, b_1, b_2 denote elements of F such that $a_1a_2 \neq 0$ and at least one of b_1 and b_2 is nonzero. If $\alpha = a_1a_2$ and $\beta = b_1^2/a_1 + b_2^2/a_2$, then the system of equations*

$$\begin{aligned} a &= a_1x_1^2 + a_2x_2^2 \\ b &= b_1x_1 + b_2x_2 \end{aligned}$$

is not solvable if and only if either $\beta \neq 0$, $\Psi(-\alpha(b^2 - a\beta)) = -1$ or $\beta = b = 0 \neq a$, $\Psi(-\alpha) = 1$.

Proof. The proof follows immediately from [**1**, Theorem 2].

THEOREM 2. *Let S_2 denote a 2-dimensional affine space with base field F and Q_2 a conic of S_2 defined by*

$$a = a_1x_1^2 + a_2x_2^2 \quad (\alpha = a_1a_2 \neq 0), \tag{2.3}$$

where $a, a_1, a_2 \in F$. If N denotes the set of all lines of S_2 contained in the complement of Q_2, then

$$|N| = \begin{cases} q^2 - 1 & \text{if } a = 0,\ \Psi(-\alpha) = -1, \\ 0 & \text{if } a = 0,\ \Psi(-\alpha) = 1, \\ 2 + \frac{1}{2}q(q-1) & \text{if } a \neq 0,\ \Psi(-\alpha) = 1, \\ \frac{1}{2}(q+1)(q-2) & \text{if } a \neq 0,\ \Psi(-\alpha) = -1. \end{cases}$$

Proof. Let N_0 and N_1 denote the sets of homogeneous and nonhomogeneous lines in N, respectively. Then $N = N_0 \cup N_1$ and $|N| = |N_0| + |N_1|$. Since we are only interested in $|N_0|$ and $|N_1|$, it suffices to consider only those lines in N_1 of the form (2.2) with $b = 0$ or 1. Moreover, it is clear that $L(b; b_1, b_2) \in N$ if and only if the equations (2.2) and (2.3) have no common solutions. For convenience, we write $N(\beta; a_1^{-1}, a_2^{-1}) = N(\beta)$, for any $\beta \in F$. Clearly,

$N(\beta) \cap N(\gamma) = \emptyset$, for any $\gamma \neq \beta$. To complete the proof we evaluate $|N_0|$ and $|N_1|$ in the following cases.

Case 1 ($a = 0$, $\Psi(-\alpha) = 1$). By Theorem 1, $|N_0| = |N_1| = 0$. Hence $|N| = 0$.

Case 2 ($a = 0$, $\Psi(-\alpha) = -1$). By Theorem 1

$$(2.4) \qquad |N_0| = 0$$

and

$$|N_1| = \left|\left\{(b_1, b_2) \in (F \times F)^* \middle| (b_1, b_2) \in \bigcup_{\beta \in F^*} N(\beta)\right\}\right| = \sum_{\beta \in F^*} |N(\beta)|,$$

where $(F \times F)^* = F \times F \backslash \{(0, 0)\}$. Hence, $|N_1| = q^2 - 1$ by virtue of (2.1), so that $|N| = |N_1| = q^2 - 1$.

Case 3 ($a \neq 0$, $\Psi(-\alpha) = 1$). By Theorem 1, $L(b; b_1, b_2)$, where $b = 0$ or 1, is in N if and only if either $\beta \neq 0$, $\Psi(b^2 - a\beta)) = -1$ or $\beta = b = 0$, where $\beta = b_1^2/a_1 + b_2^2/a_2$. Hence, by 2.1(c),

$$(2.5) \qquad |N_0| = \left|\left\{[b_1, b_2] \in Q^* \middle| \text{either } (b_1, b_2) \in \bigcup_{\beta \in F^*, \Psi(-a\beta) = -1} N(\beta) \text{ or } (b_1, b_2) \in N(0)\right\}\right|$$

and

$$(2.6) \qquad |N_1| = \left|\left\{(b_1, b_2) \in (F \times F)^* \middle| (b_1, b_2) \in \bigcup_{\beta \in T} N(\beta)\right\}\right| = \sum_{\beta \in T} |N(\beta)|,$$

where $T = \{\beta \in F^* | \Psi(1 - a\beta) = -1\}$. Hence, by 2.1($a$), 2.1($b$), (2.1) and (2.5)

$$(2.7) \qquad |N_0| = |P(0; a_1^{-1}, a_2^{-1})| + |P(\beta_0; a_1^{-1}, a_2^{-1})| = 2 + \tfrac{1}{2}(q - 1),$$

where $\beta_0 \in F^*$ such that $\Psi(-a\beta_0) = -1$. Moreover, since, for any $\beta \in T$, $N(\beta) = q - 1$ by virtue of (2.1) and since $|T|$ is equal to the number of nonsquares in $\{1 - a\beta | \beta \in F^*, \beta \neq a^{-1}\} = F^* \backslash \{1\}$, it follows from (2.6) that

$$|N_1| = (q - 1)|T| = \tfrac{1}{2}(q - 1)^2.$$

Hence, $|N| = |N_0| + |N_1| = 2 + q(q - 1)/2$.

Case 4 ($a \neq 0$, $\Psi(-\alpha) = -1$). By an argument similar to that used in Case 3, we have

$$(2.8) \qquad |N_0| = |P(\beta_0; a_1^{-1}, a_2^{-1})| = \tfrac{1}{2}(q + 1),$$

and

$$(2.9) \qquad |N_1| = \sum_{\beta \in T'} |N(\beta)| = \tfrac{1}{2}(q + 1)(q - 3),$$

where $\beta_0 \in F^*$ such that $\Psi(-a\beta_0) = 1$ and $T' = \{\beta \in F^* | \Psi(1 - a\beta) = 1\}$. Consequently, by (2.8) and (2.9), $|N| = (q + 1)(q - 2)/2$.

The proof of the theorem is now complete.

The following result is obtained directly from the proof of Theorem 1.

THEOREM 3. *With the same notation of Theorem 2, if H denotes the number of lines in N which are 1-dimensional subspaces of S_2, then*

$$H = \begin{cases} 2 + \frac{1}{2}(q-1) & \text{if } a \neq 0,\ \Psi(-\alpha) = 1, \\ \frac{1}{2}(q+1) & \text{if } a \neq 0,\ \Psi(-\alpha) = -1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Since $H = |N_0|$, the theorem follows immediately from (2.4), (2.7), (2.8) and the fact that $|N| = 0$ if $a = 0$ and $\Psi(-\alpha) = 1$.

THEOREM 4. *Let C_2 denote the conic of S_2 defined by*

$$a = \sigma x_1^2 + \lambda x_2,$$

where $a, \sigma, \lambda \in F$, $\sigma \neq 0 \neq \lambda$. If N denotes the set of all lines of S_2 contained in the complement of C_2, then $|N| = q(q-1)/2$.

Proof. We may (and shall) assume without loss of generality that $\sigma = 1$. Let N_0 and N_1 denote the sets of homogeneous and nonhomogeneous lines in N, respectively. Then $N = N_0 \cup N_1$ and $|N| = |N_0| + |N_1|$. In order to evaluate $|N_0|$ and $|N_1|$ we consider two cases in accordance with $a \neq 0$ or $a = 0$.

Case 1 ($a \neq 0$). As in the proof of Theorem 2, we assume that any line in N_1 is of the form (2.2) with $b = 1$. Clearly, $L(b; b_1, b_2) \in N$ if and only if the system of equations

$$\begin{aligned} a &= x_1^2 + \lambda x_2 \\ b &= b_1 x_1 + b_2 x_2 \end{aligned} \tag{2.10}$$

is not solvable. If $b_2 = 0$, (2.10) is always solvable. Assume now that $b_2 \neq 0$; then eliminating x_2 and completing the squares, (2.10) yields

$$a - \lambda b_2^{-1} b + \tfrac{1}{4}\lambda^2 b_2^{-2} b_1^2 = (x_1 - \tfrac{1}{2}\lambda b_2^{-1} b_1^2)^2.$$

Hence, (2.10) is not solvable if and only if $\Psi(4ab_2^2 - 4\lambda b_2 b + \lambda^2 b_1^2) = -1$, where $b = 0$ or 1. Consequently, it follows from 2.1(c) and the above consideration that

$$|N_0| = |\{[b_1, b_2] \in Q^* | \Psi(4ab_2^2 + \lambda^2 b_1^2) = -1\}|, \tag{2.11}$$

and

$$|N_1| = |\{(b_1, b_2) \in F \times F \backslash \{(0,0)\} | \Psi(4ab_2^2 - 4\lambda b_2 + \lambda^2 b_1^2) = -1\}|. \tag{2.12}$$

Hence, if S_{t_0} denotes the number of solutions of the equation

$$4ax_1^2 + \lambda^2 x_2^2 = t_0,$$

where t_0 is any nonsquare in F^*, then

$$|N_0| = \tfrac{1}{2} S_{t_0} = \tfrac{1}{2}(q - \Psi(-a)) \tag{2.13}$$

https://doi.org/10.4153/CJM-1974-122-9 Published online by Cambridge University Press

by virtue of 2.1(a), 2.1(b), (2.1) and (2.11). Moreover by (2.12),

$$|N_1| = \sum_{t \in F^*, \Psi(t) = -1} T_t,$$

where T_t denotes the number of solutions of the equation

$$4ax_2^2 - 4\lambda x_2 + \lambda^2 x_1^2 = t. \tag{2.14}$$

By completing the square (2.14) becomes

$$4a(x_2 - \lambda/2a)^2 + \lambda^2 x_1^2 = t + \lambda^2/a$$

so that, by (2.1)

$$T_t = \begin{cases} q - \Psi(-a) & \textit{if } t + \lambda^2/a \neq 0, \\ q + (q-1)\Psi(-a) & \textit{if } t + \lambda^2/a = 0. \end{cases}$$

Hence

$$|N_1| = \begin{cases} \frac{1}{2}(q-1)^2 & \textit{if } \Psi(-a) = 1 \\ \frac{1}{2}(q-3)(q+1) + 1 & \textit{if } \Psi(-a) = -1. \end{cases}$$

It now follows from (2.13) and (2.15) that $|N| = q(q-1)/2$.

Case 2 ($a = 0$). By an argument similar to that used in Case 1,

$$N_0 = 0, \tag{2.16}$$

and

$$N_1 = \sum_{t \in F^*, \Psi(t) = -1} R_t,$$

where R_t denotes the number of solutions of (2.14) with $a = 0$. Clearly, by assigning arbitrary values in F to x_1, we can determine x_2. Hence, $R_t = q$ for all $t \in F^*$ such that $\Psi(t) = -1$. Consequently, $N = N_1 = q(q-1)/2$.

The theorem is now established.

The following theorem concerned with a subset of N is essentially obtained from the proof of Theorem 4.

THEOREM 5. *With the same notation of Theorem* 4, *let H denote the number of lines in N which are* 1-*dimensional subspaces of S_2. Then $H = 0$ or $(q - \Psi(-a))/2$ according as $a = 0$ or $a \neq 0$.*

Proof. Since $H = |N_0|$, the theorem follows immediately from (2.13) and (2.16).

2.2 *Remark.* If L denotes a line of S_2, then the number of lines contained in the complement of L is $q - 1$ and if L denotes two parallel lines of S_2, then the number of lines contained in the complement of L is $q - 2$.

Finally, as a consequence of a complete evaluation of the number of lines contained in the complement of a conic of S_2, we obtain the following theorem.

THEOREM 6. *Let Q_3 denote a quadric of S_3 defined by*

$$a = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \quad (a_1a_2a_3 \neq 0),$$

and P_2 a plane of S_3 defined by

$$c = c_1x_1 + c_2x_2 + c_3x_3.$$

If N_3 denotes the number of planes of S_3 which are not parallel to P_2 and which are in the complement of $Q_3 \cap P_2$, then under the assumption that $Q_3 \cap P_2 \neq \emptyset$, we have

$$N_3 = \begin{cases} q(q-1) & \text{if } \gamma = c = a = 0, \\ q(q-2) & \text{if } \gamma = 0 = c,\ \Psi(-a\alpha) = 1, \\ \frac{1}{2}q^2(q-1) & \text{if } \gamma = 0 \neq c, \\ 2q + \frac{1}{2}q^2(q-1) & \text{if } \gamma \neq 0 \neq C,\ \Psi(-\alpha\gamma) = 1, \\ \frac{1}{2}q(q+1)(q-2) & \text{if } \gamma \neq 0 \neq C,\ \Psi(-\alpha\gamma) = -1, \\ q(q^2-1) & \text{if } \gamma \neq 0 = C,\ \Psi(-\alpha\gamma) = -1, \\ 0 & \text{if } \gamma \neq 0 = C,\ \Psi(-\alpha\gamma) = 1, \end{cases}$$

where $\gamma = c_1^2/a_1 + c_2^2/a_2 + c_3^2/a_3$, $C = c^2 - a\gamma$ and $\alpha = a_1a_2a_3$.

2.4 *Remark.* By [**1**, Theorem 2], $Q_3 \cap P_2 = \emptyset$ if and only if $\gamma = 0 = c$ and $\Psi(-a\alpha) = -1$.

Proof. Since $Q_3 \cap P_2$ is a conic in S_2 and since, for any given line, there are $q + 1$ distinct planes passing through it, $N_3 = qL$, where L denotes the number of lines of S_2 contained in the complement of $Q_3 \cap P_2$.

Now, consider the system of equations

$$\text{(2.17)} \quad \begin{aligned} a &= a_1x_1^2 + a_2x_2^2 + a_2x_3^2 \qquad (\alpha = a_1a_2a_3 \neq 0) \\ c &= c_1x_1 + c_2x_2 + c_3x_3. \end{aligned}$$

We may assume without loss of generality that $c_1 \neq 0$. Then eliminating x_1, (2.17) yields

$$\text{(2.18)} \quad a - \zeta c^2 = (\gamma_1x_2^2 + \gamma_2x_3^2 + 2\zeta c_2c_3x_2x_3) - 2\zeta c(c_2x_2 + c_3x_3),$$

where $\zeta = a_1c_1^{-2}$, $\gamma_1 = \zeta c_2^2 + a_2$ and $\gamma_2 = \zeta c_3^2 + a_3$. The discriminant of the quadratic form enclosed in parentheses in (2.18) is $c_1^{-2}\alpha\gamma$.

If $\gamma = c = a = 0$, then $Q_3 \cap P_2$ is a line; similarly, if $\gamma = c = 0$ and $\Psi(-a\alpha) = 1$, then $Q_3 \cap P_2$ consists of two parallel lines. Assume $\gamma = 0 \neq c$. Then at least two of the c_i are nonzero; we may assume without loss of generality that $c_1 \neq 0 \neq c_2$. By a simple calculaton, we see that (2.18) assumes the form

$$a - \zeta c^2 = a_3x_3^2 - 2\zeta cc_2x_2,$$

or

$$(a\gamma_1 - \zeta c^2a_2)/\gamma_1^2 = x^2 + 2c\gamma_1c_3a_3x_3,$$

https://doi.org/10.4153/CJM-1974-122-9 Published online by Cambridge University Press

where $x = x_2 + \gamma_2\zeta c_2^{-1}c_3^{-1}x_3 - c\zeta c_2\gamma_1^{-1}$, according as $c_3 = 0$ or $c_3 \neq 0$. We note that if $c_3 \neq 0 = \gamma$, then $\gamma_1 \neq 0$. Hence, by 2.2 and Theorem 4,

$$(2.19)\quad L = \begin{cases} q-1 & \text{if } \gamma = a = c = 0, \\ q-2 & \text{if } \gamma = c = 0,\ \Psi(-a\alpha) = 1, \\ \frac{1}{2}q(q-1) & \text{if } \gamma = 0 \neq c. \end{cases}$$

Assume now that $\gamma \neq 0$. If either γ_1 or γ_2 is nonzero, say $\gamma_1 \neq 0$, then the nonsingular transformation

$$y_2 = \gamma_1 x_1 + \zeta c_2 c_3 x_3$$
$$y_3 = x_3$$

takes (2.18) into

$$(2.20)\quad a - \zeta c^2 = \gamma_1^{-1}y_2^2 + c_1^{-2}\alpha\gamma\gamma_1^{-1}y_3^2 - 2\zeta c\gamma_1^{-1}(c_2y_2 + a_2c_3y_3).$$

Putting $w_2 = y_2 - \zeta cc_2$ and $w_3 = y_3 - a_1ca_2c_3$, (2.20) becomes

$$(2.21)\quad -\gamma^{-1}C = \gamma_1^{-1}w_2^2 + c_1^{-2}\alpha\gamma\gamma_1^{-1}w_3^2.$$

If $\gamma_1 = 0 = \gamma_2$, then $\Psi(-1) = 1$. Applying the nonsingular transformation

$$y_2 = \tfrac{1}{2}c_1^{-1}c_2x_2 + \tfrac{1}{2}c_1^{-1}c_3x_3$$
$$y_3 = \tfrac{1}{2}c_1^{-1}c_2x_2 - \tfrac{1}{2}c_1^{-1}c_3x_3$$

to (2.18) yields

$$(2.22)\quad a - \zeta c^2 = 2a_1y_2^2 - 2a_1y_3^2 - 4a_1cc_1^{-1}y_2.$$

If we put $y_2' = y_2 - cc_1^{-1}$, (2.22) becomes

$$(2.23)\quad -\gamma^{-1}C = 2a_1y_2'^2 - 2a_1y_3^2.$$

Hence, it follows from (2.21), (2.23) and Theorem 2 that

$$(2.24)\quad L = \begin{cases} 2 + q(q-1) & \text{if } C \neq 0,\ \Psi(-\alpha\gamma) = 1, \\ \frac{1}{2}(q+1)(q-2) & \text{if } C \neq 0,\ \Psi(-\alpha\gamma) = -1, \\ q^2 - 1 & \text{if } C = 0,\ \Psi(-\alpha\gamma) = -1, \\ 0 & \text{if } C = 0,\ \Psi(-\alpha\gamma) = 1. \end{cases}$$

Hence, the theorem follows from (2.19) and (2.24). This completes the proof of the theorem.

For an alternative proof of Theorem 6, see [**3**, §II.4].

References

1. E. Cohen, *Linear and quadratic equations in a Galois field with applications to geometry*, Duke Math. J. *32* (1965), 633–641.

https://doi.org/10.4153/CJM-1974-122-9 Published online by Cambridge University Press

2. L. E. Dickson, *Linear group, with an exposition of the Galois field theory*, (Lipezig, **1901**: reprinted by Dover, 1958).
3. F. R. Jung, Ph.D. thesis, Kansas State University, 1969.

Kansas State University,
Manhattan, Kansas;
Chulalongkorn University,
Bangkok, Thailand