ON THE REPRESENTATION OF A POLYNOMIAL IN A GALOIS FIELD AS THE SUM OF AN EVEN NUMBER OF SQUARES*

BY

LEONARD CARLITZ†

1. **Introduction.** Let $GF(p^n)$ denote a fixed Galois field of order p^n, p being any *odd* prime, and n an arbitrary positive integer; let $\mathfrak{D}(x, p^n)$ denote the totality of polynomials in an indeterminate, x, with coefficients in $GF(p^n)$. In this paper we seek simple expressions for the number of representations of a polynomial in $\mathfrak{D}$ as a sum of squares of polynomials in $\mathfrak{D}$ that satisfy certain restrictions.

More precisely, suppose that F is a *primary* polynomial, that is, the coefficient of the highest power of x occurring in F is the 1 element of the Galois field. Let s be a positive integer; $\alpha_1, \cdots, \alpha_s, \beta_1, \cdots, \beta_s$, $2s$ elements of the Galois field such that

$$\gamma_i = \alpha_i + \beta_i \neq 0 \qquad (i = 1, \cdots, s).$$

Then

(A) If F is of even degree, $2k$, and

$$\gamma = \gamma_1 + \gamma_2 + \cdots + \gamma_s \neq 0,$$

we seek the number of solutions of

$$\gamma F = \alpha_1 X_1^2 + \beta_1 Y_1^2 + \cdots + \alpha_s X_s^2 + \beta_s Y_s^2 \tag{1}$$

in primary polynomials X_i, Y_i, each of degree k.

(B) If F is of *arbitrary* degree f, $2k$ is any even integer $>f$, α any non-zero element of the Galois field, and

$$\gamma_1 + \gamma_2 + \cdots + \gamma_s = 0,$$

we seek the number of solutions of

$$\alpha F = \alpha_1 X_1^2 + \beta_1 Y_1^2 + \cdots + \alpha_s X_s^2 + \beta_s Y_s^2 \tag{2}$$

in primary polynomials X_i, Y_i, each of degree k.

The solution of (A) is expressed in terms of one of the functions $\rho_t(F)$, $\omega_t(F)$, defined thus:

* Presented to the Society, August 30, 1932; received by the editors June 23, 1932.

† This paper was written when the author was an International Research Fellow at Cambridge University.

$$\rho_t(F) = \left(1 - \frac{1}{p^{nt}}\right) \sum_{M|F}^{m>k} |M|^t + \sum_{M|F}^{m=k} |M|^t, \quad |M| = p^{nm}, \tag{3}$$

where m denotes the degree of M: the first summation is over all primary M dividing F, and of degree $>k$, the second is over all primary M dividing F and of degree $=k$;

$$\omega_t(F) = \left(1 + \frac{1}{p^{nt}}\right) \sum_{M|F}^{m>k} (-1)^m |M|^t + \sum_{M|F}^{m=k} (-1)^m |M|^t, \tag{4}$$

the summations having the same meaning as in (3). If now

$$(-1)^s \alpha_1 \cdots \alpha_s \beta_1 \cdots \beta_s \tag{5}$$

is a square in $GF(p^n)$, then the number of solutions of (1) is $\rho_{s-1}(F)$; if the expression (5) is a non-square of $GF(p^n)$, then the number of solutions is $\omega_{s-1}(F)$.

Case (B) involves a modification of the ρ and ω functions: if (5) is a square, the number of solutions of (2) is

$$p^{n(s-1)(2k-f)} \rho_{s-1}^k(F),$$

where

$$\rho_t^k(F) = \left(1 - \frac{1}{p^{nt}}\right) \sum_{M|F}^{m>f-k} |M|^t + \sum_{M|F}^{m=f-k} |M|^t; \tag{6}$$

if (5) is a non-square, the number of solutions is

$$p^{n(s-1)(2k-f)} \omega_{s-1}^k(F),$$

where

$$(-1)^f \omega_t^k(F) = \left(1 + \frac{1}{p^{nt}}\right) \sum_{M|F}^{m>f-k} (-1)^m |M|^t + \sum_{M|F}^{m=f-k} (-1)^m |M|^t. \tag{7}$$

If $k>f$, the second sum in (6) and (7) is vacuous and denotes zero.

We first treat case (A); then, making use of the results for this case, it is easy to deduce the results (6) and (7) for case (B). The method used is quite elementary, and presupposes only some well known general theorems concerning Galois fields.*

It should be emphasized that the results of this paper hold for all positive s. This is rather surprising when comparison is made with the known results concerning the number of representations of an ordinary integer as the sum of $2s$ squares: in the latter problem, while the cases $2s=2, 4, 6, 8$ admit of

* These theorems will be found in Dickson's *Linear Groups*, 1901, pp. 3–54.

simple expressions in terms of divisor functions, this is no longer true for $2s>8$. While comparison of the problem of this paper with the ordinary problem is of some interest, actually, since we are considering representations in terms of *primary* polynomials, the analogy is closer with the question of the number of representations of an integer as the sum of squares of *positive* integers.

Finally, we remark that it is possible, by methods similar to those used here, to determine the number of representations of a polynomial by means of any *odd* number of squares (that satisfy certain conditions). As we shall show in another paper, the final formulas are of quite a different type; they are no longer functions of divisors but involve sums of quadratic characters.

2. **Notation; preliminary lemmas.*** We shall employ the following notation. Polynomials will be denoted by large italic letters; unless the contrary be explicitly stated, a polynomial will always be assumed primary. Ordinary integers will be denoted by small italic letters, elements of the Galois field by small Greek letters. The degree of a polynomial will be denoted by the corresponding small letter, and we shall write

$$f = \deg F, \quad |F| = p^{nf}.$$

(A, B) is the "greatest" common divisor of A and B.

Using this notation, we have the following lemmas.

LEMMA 1. *The number of sets of polynomials* $[A, B]$ *such that*

$$\deg A = a, \ \deg B = b, \ (A, B) = 1,$$

is

$$\psi(a, b) = \begin{cases} p^{a+b} - p^{a+b-1} & \text{for } ab \neq 0, \\ p^{a+b} & \text{for } ab = 0. \end{cases}$$

This lemma is a special case of a more general theorem to be proved elsewhere. For completeness we give the following simple proof. Let us classify the $p^{n(a+b)}$ sets of polynomials $[A, B]$, $\deg A = a$, $\deg B = b$, according to their g.c.d. Then, if $1 \leqq a \leqq b$,

$$p^{n(a+b)} = \sum_{m \leqq a} |M| \psi(a - m, b - m), \tag{8}$$

the sum being extended over all M of degree $\leqq a$. The right member of (8) is

$$\psi(a, b) + \sum_{m=1}^{a} p^{nm} \psi(a - m, b - m)$$
$$= \psi(a, b) + p^{n(a+b-1)},$$

whence the lemma.

* The results of §§2, 3 hold for all p.

LEMMA 2. *Let F, A, B be of degree f, a, b, respectively*; $(A, B)=1$.

(I) *If $a+b \leqq f$, and α and β are two non-zero elements of $GF(p^n)$ such that $\alpha+\beta \neq 0$, then the number of solutions of*

$$(\alpha+\beta)F = \alpha AU + \beta BV, \quad |AU| = |BV|, \tag{9}$$

in polynomials U, V, is $|F/(AB)| = p^{n(f-a-b)}$.

(II) *If k is an integer $>f$, $a+b \leqq k$, and α is any non-zero element of $GF(p^n)$, then the number of solutions of*

$$\alpha F = AU - BV, \quad |AU| = |BV| = p^{nk}, \tag{10}$$

is

$$p^{n(k-a-b)} = p^{n(k-f)} \cdot |F| \cdot |AB|^{-1}.$$

It will suffice to prove (II) alone. From (10), we have

$$\begin{aligned} U &\equiv A' \pmod{B}, \quad a' < b, \\ V &\equiv B' \pmod{A}, \quad b' < a, \end{aligned} \tag{11}$$

where A' and B' are not necessarily primary. Since

$$u = \deg U = k - a \geqq b, \text{ and } v \geqq a,$$

the congruences (11) may be written in the form

$$U = A' + BU', \quad V = B' + AV' \quad (u' = v' = k - a - b),$$

where now U' and V' are primary. Then (10) becomes

$$\frac{\alpha F - AA' - BB'}{AB} = U' - V'. \tag{12}$$

But since $(A, B)=1$, there is a unique pair of polynomials A', B', such that $a'<b$, $b'<a$, and the left member of (12) is integral. If then V' be any (primary) polynomial of degree $v'=k-a-b$, U' is uniquely determined, and, retracing the steps that led from (10) to (12), U, V are uniquely determined. Since V' can be chosen in

$$p^{nv'} = p^{n(k-a-b)}$$

ways, this proves case (II). The proof of case (I) is very much the same.

3. **Theorems on the ρ and ω functions.** We now prove certain formulas concerning the functions $\rho_t(F)$ and $\omega_t(F)$ defined in the Introduction. As we shall see in the next section, these formulas enable us to solve our problem concerning (1); furthermore, the formulas seem to be of some interest in themselves.

THEOREM 1. *If F is of even degree, $2k$; α, β two elements of $GF(p^n)$ such that $\alpha\beta(\alpha+\beta)\neq 0$; s, t two (real or complex) numbers; then*

$$\sum \rho_s(A)\rho_t(B) = \rho_{s+t+1}(F), \tag{13}$$

$$\sum \rho_s(A)\omega_t(B) = \omega_{s+t+1}(F), \tag{14}$$

$$\sum \omega_s(A)\omega_t(B) = \rho_{s+t+1}(F), \tag{15}$$

where, in each instance, the summation is extended over all (primary) polynomials A, B of degree $2k$, such that

$$(\alpha + \beta)F = \alpha A + \beta B.$$

The three formulas (13), (14), (15) may be proved simultaneously if ρ and ω be expressed in terms of the function $\Lambda_s(F, \lambda)$ now to be defined. We define the "character" $\lambda(B)$ by

$$\lambda(B) = (-1)^b, \quad b = \deg B, \tag{16}$$

and the function $\Lambda_s(F, \lambda^i)$ by

$$\Lambda_s(F, \lambda^i) = \left(1 - \frac{(-1)^i}{p^{ns}}\right) \sum_{M|F}^{m>k} \lambda^i(M)\,|M|^s + \sum_{M|F}^{m=k} \lambda^i(M)\,|M|^s. \tag{17}$$

It is obvious from the definitions (3) and (4) that

$$\rho_s(F) = \Lambda_s(F, 1), \quad \omega_s(F) = \Lambda_s(F, \lambda), \tag{18}$$

and therefore the several parts of Theorem 1 reduce to

$$\sum_{(\alpha+\beta)F=\alpha A+\beta B} \Lambda_s(A, \lambda^i)\Lambda_t(B, \lambda^j) = \Lambda_{s+t+1}(F, \lambda^{i+j}), \tag{19}$$

i, j integers which may be taken $=0$ or 1. We proceed to establish (19).

The left hand member of (19) is by (17)

$$\begin{aligned}\Big\{&\left(1 - \frac{(-1)^i}{p^{ns}}\right)\left(1 - \frac{(-1)^j}{p^{nt}}\right) \sum_{a<u,\,b<v} + \left(1 - \frac{(-1)^i}{p^{ns}}\right) \sum_{a<u,\,b=v} \\ &+ \left(1 - \frac{(-1)^j}{p^{nt}}\right) \sum_{a=u,\,b<v} + \sum_{a=u,\,b=v} \Big\} \lambda^i(U)\,|U|^s\,\lambda^j(V)\,|V|^t,\end{aligned} \tag{20}$$

where each summation is taken over all (primary) A, B, U, V satisfying $(\alpha+\beta)F=\alpha AU+\beta BV$ as well as the conditions indicated under each $\sum$. Call the sums $\sum_1, \sum_2, \sum_3, \sum_4$, respectively; then, since $a<u$ is equivalent to $a<k$,

$$\sum_1 = |F|^{s+t} \sum_{\substack{(\alpha+\beta)F=\alpha AU+\beta BV \\ a,b<k}} \lambda^i(A)\lambda^j(B)\,|A|^{-s}|B|^{-t}$$

$$= |F|^{s+t} \sum_{M|F}^{m<k} \lambda^{i+j}(M)\,|M|^{-s-t} S_M, \tag{21}$$

where

$$S_M = \sum_{\substack{(\alpha+\beta)FM^{-1}=\alpha AU+\beta BV \\ (A,B)=1;\, a,b<k-m}} \lambda^i(A)\lambda^j(B)\,|A|^{-s}|B|^{-t}$$

$$= \sum_{\substack{(A,B)=1 \\ a,b<k-m}} \lambda^i(A)\lambda^j(B)\,|A|^{-s}|B|^{-t} \sum_{(\alpha+\beta)FM^{-1}=\alpha AU+\beta BV} 1$$

$$= |FM^{-1}| \sum_{\substack{(A,B)=1 \\ a,b<k-m}} \lambda^i(A)\lambda^j(B)\,|A|^{-s-1}|B|^{-t-1},$$

by case (I) of Lemma 2. By the definition of $\psi(a, b)$ in Lemma 1, the last expression is equal to

$$|FM^{-1}| \sum_{a\ b<k-m} (-1)^{ia+jb} p^{-n(s+1)a-n(t+1)b}\psi(a, b). \tag{22}$$

Applying Lemma 1, the sum becomes

$$\sum_{a=0}^{k-m-1} (-1)^{ia}p^{-nsa} + \sum_{b=1}^{k-m-1} (-1)^{jb}p^{-ntb} + \sum_{a,b=1}^{k-m-1} (-1)^{ia+jb}p^{-n(sa+tb)}(1-p^{-n})$$

$$= [k-m, i]_s[k-m, j]_t - p^{-n}[k-m, i]'_s[k-m, j]'_t,$$

where, for brevity, we put

$$[k, i]_s = \frac{1-(-1)^{ik}p^{-nsk}}{1-(-1)^i p^{-ns}},^*$$

$$[k, i]'_s = \frac{(-1)^i p^{-ns} - (-1)^{ik}p^{-nsk}}{1-(-1)^i p^{-ns}} = [k, i]_s - 1, \tag{23}$$

so that, by (21) and (22),

$$\sum_1 = \sum_{M|F}^{m>k} \lambda^{i+j}(M)\,|M|^{s+t+1}\{[m-k, i]_s[m-k, j]_t - p^{-n}[m-k, i]'_s[m-k, j]'_t\}. \tag{24}$$

The treatment of $\sum_2$ is much the same; we have

---

* For $s=i=0$, the symbol $[k, i]_s=k$.

$$\sum\nolimits_2 = |F|^{s+t} \sum_{\substack{(\alpha+\beta)F=\alpha AU+\beta BV \\ a<k,\, b=k}} \lambda^i(A)\lambda^j(B)\,|A|^{-s}\,|B|^{-t}$$

$$= |F|^{s+t} \sum_{M|F}^{m<k} \lambda^{i+j}(M)\,|M|^{-s-t} S_M,$$

where now

$$S_M = \sum_{\substack{(\alpha+\beta)FM^{-1}=\alpha AU+\beta BV \\ (A,B)=1;\, a<k-m=b}} \lambda^i(A)\lambda^j(B)\,|A|^{-s}\,|B|^{-t}$$

$$= |FM^{-1}| \sum_{\substack{(A,B)=1 \\ a<k-m=b}} \lambda^i(A)\lambda^j(B)\,|A|^{-s-1}\,|B|^{-t-1}$$

$$= |FM^{-1}| \sum_{a<k-m} (-1)^{ia+j(k-m)}\psi(a,\, k-m)\,p^{-n(s+1)a-n(t+1)(k-m)}$$

$$= |FM^{-1}|\,(-1)^{j(k-m)}p^{-nt(k-m)}\left\{[k-m,\, i]_s - p^{-n}[k-m,\, i]'_s\right\},$$

$[k, i]_s$ having the same meaning as in (23); therefore

$$\sum\nolimits_2 = \sum_{M|F}^{m>k} \lambda^{i+j}(M)\,|M|^{s+t+1}(-1)^{j(m-k)}p^{-nt(m-k)} \cdot \left\{[m-k,\, i]_s - p^{-n}[m-k,\, i]'_s\right\}. \tag{25}$$

Similarly

$$\sum\nolimits_3 = \sum_{M|F}^{m>k} \lambda^{i+j}(M)\,|M|^{s+t+1}(-1)^{i(m-k)}p^{-ns(m-k)} \cdot \left\{[m-k,\, j]_t - p^{-n}[m-k,\, j]'_t\right\}. \tag{26}$$

The sum $\sum_4$ is slightly different in that (A, B) may be of degree k; thus

$$\sum\nolimits_4 = |F|^{s+t} \sum_{M|F}^{m\leqq k} \lambda^{i+j}(M)\,|M|^{-s-t} S_M,$$

where

$$S_M = \sum_{\substack{(\alpha+\beta)FM^{-1}=\alpha AU+\beta BV \\ (A,B)=1;\, a=b=k-m}} \lambda^i(A)\lambda^j(B)\,|A|^{-s}\,|B|^{-t}$$

$$= |FM^{-1}| \sum_{\substack{(A,B)=1 \\ a=b=k-m}} \lambda^i(A)\lambda^j(B)\,|A|^{-s-1}\,|B|^{-t-1}$$

$$= |FM^{-1}|\,(-1)^{(i+j)(k-m)}\psi(k-m,\, k-m)\,p^{-n(s+t+2)(k-m)},$$

and therefore we have almost immediately

$$\sum\nolimits_4 = \sum_{M|F}^{m=k} \lambda^{i+j}(M)\,|M|^{s+t+1} + \sum_{M|F}^{m>k} \lambda^{i+j}(M)\,|M|^{s+t+1}(-1)^{(i+j)(m-k)}p^{-n(s+t)(m-k)}(1-p^{-n}). \tag{27}$$

Substituting from (24), $\cdots$, (27) into (20), we find that the left member of (19) is

$$(28)\qquad \sum_{M|F}^{m-k}\lambda^{i+j}(M)\,|\,M\,|^{s+t+1}+\sum_{M|F}^{m>k}\lambda^{i+j}(M)\,|\,M\,|^{s+t+1}\chi_m,$$

where

$$\begin{aligned}\chi_m &= \{1-(-1)^i p^{-ns}\}\{1-(-1)^j p^{-nt}\}\{[m-k,i]_s[m-k,j]_t\\ &\quad -p^{-n}[m-k,i]'_s[m-k,j]'_t\}\\ &\quad +\{1-(-1)^i p^{-ns}\}\{[m-k,i]_s-p^{-n}[m-k,i]'_s\}(-1)^{j(m-k)}p^{-nt(m-k)}\\ &\quad +\{1-(-1)^j p^{-nt}\}\{[m-k,j]_t-p^{-n}[m-k,j]'_t\}(-1)^{i(m-k)}p^{-ns(m-k)}\\ &\quad +(-1)^{i+j}p^{-n(s+t)(m-k)}(1-p^{-n})\\ &= 1-(-1)^{i+j}p^{-n(s+t+1)},\end{aligned}$$

as may be verified without any calculation by applying (23) and then grouping the terms in an obvious way. This evidently completes the proof of (19) and therefore of Theorem 1.

We next prove a group of formulas that will be needed in §5 in deriving the expression sought for the number of solutions of (2).

THEOREM 2. *If F is of arbitrary degree, f; $2k$ is an even integer $>f$; α is any non-zero element of $GF(p^n)$; s, t two (real or complex) numbers; then*

$$(29)\qquad \sum\rho_s(A)\rho_t(B)=p^{n(2k-f)(s+t+1)}\rho^k_{s+t+1}(F),$$

$$(30)\qquad \sum\rho_s(A)\omega_t(B)=p^{n(2k-f)(s+t+1)}\omega^k_{s+t+1}(F),$$

$$(31)\qquad \sum\omega_s(A)\omega_t(B)=p^{n(2k-f)(s+t+1)}\rho^k_{s+t+1}(F),$$

where, in each instance, the summation is extended over all polynomials A, B of degree $2k$, such that $\alpha F=A-B$; $\rho^k_t(F)$, $\omega_t(F)$ are defined by (6) *and* (7), *respectively.*

Exactly as in Theorem 1, the formulas (29), (30), (31) may be combined in a single relation involving the function $\Lambda^k_s(F,\lambda)$ defined by

$$(32)\qquad \lambda^i(F)\Lambda^k_s(F,\lambda^i)=\left(1-\frac{(-1)^i}{p^{ns}}\right)\sum_{M|F}^{m>f-k}\lambda^i(M)\,|\,M\,|^s+\sum_{M|F}^{m=f-k}\lambda^i(M)\,|\,M\,|^s,$$

$\lambda(F)$ being defined by (16). The equations (18) may then be replaced by

$$\rho^k_s(F)=\Lambda^k_s(F,1),\quad \omega^k_s(F)=\Lambda^k_s(F,\lambda),$$

and the formulas (29), (30), (31) by

$$(33)\qquad \sum_{\alpha F=A-B} \Lambda_s(A, \lambda^i)\Lambda_t(B, \lambda^j) = p^{n(2k-f)(s+t+1)}\Lambda^k_{s+t+1}(F, \lambda^{i+j}),$$

the summation being over all A, B of degree $2k$ for which $\alpha F = A - B$.

The proof of (33) is very similar to that of (19), except that wherever Lemma 2 is necessary, we now use case (II). It is scarcely necessary to give the proof in detail. We begin exactly as in (20), and we shall consider only the first sum, $\sum_1$; evidently

$$\begin{aligned}\sum\nolimits_1 &= \sum_{\substack{\alpha F=AU-BV\\ a,b<k}} \lambda^i(U)\lambda^j(V)\,|\,U\,|^s\,|\,V\,|^t \\ &= p^{2nk(s+t)} \sum_{\substack{\alpha F=AU-BV\\ a,b<k}} \lambda^i(A)\lambda^j(B)\,|\,A\,|^{-s}\,|\,B\,|^{-t} \\ &= p^{2nk(s+t)} \sum_{M|F}^{m<k} \lambda^{i+j}(M)\,|\,M\,|^{-s-t} S_M,\end{aligned}$$

where, exactly as in (21),

$$\begin{aligned}S_M &= \sum_{\substack{(A,B)=1\\ a,b<k-m}} \lambda^i(A)\lambda^j(B)\,|\,A\,|^{-s}\,|\,B\,|^{-t} \sum_{\substack{\alpha F M^{-1}=AU-BV\\ a+u=b+v=2k-m}} 1 \\ &= p^{2nk}\,|\,M\,|^{-1} \sum_{\substack{(A,B)=1\\ a,b<k-m}} \lambda^i(A)\lambda^j(B)\,|\,A\,|^{-s-1}\,|\,B\,|^{-t-1}\end{aligned}$$

by case (II) of Lemma 2. Therefore

$$S_M = p^{2nk}\,|\,M\,|^{-1} \sum_{a,b<k-m} (-1)^{ia+jb}\psi(a, b)p^{-n(s+1)a-n(t+1)b},$$

which may be evaluated by following the method applied to (22). Thus we find that

$$\begin{aligned}\sum\nolimits_1 &= p^{2nk(s+t+1)} \sum_{M|F}^{m<k} \lambda^{i+j}(M)\,|\,M\,|^{-s-t-1} \\ &\quad \cdot \{[k-m, i]_s[k-m, j]_t - p^{-n}[k-m, i]'_s[k-m, j]'_t\} \\ &= \lambda^{i+j}(F)p^{n(2k-f)(s+t+1)} \sum_{M|F}^{m>f-k} \lambda^{i+j}(M)\,|\,M\,|^{s+t+1} \\ &\quad \cdot \{[m+k-f, i]_s[m+k-f, j]_t - p^{-n}[m+k-f, i]'_s[m+k-f, j]'_t\}.\end{aligned} \tag{34}$$

Similarly, we find that

$$\begin{aligned}\sum\nolimits_2 &= \lambda^{i+j}(F)p^{n(2k-f)(s+t+1)} \sum_{M|F}^{m>f-k} \lambda^{i+j}(M)\,|\,M\,|^{s+t+1} \\ &\quad \cdot (-1)^{j(m+k-f)}p^{-nt(m+k-f)}\{[m+k-f, i]_s - p^{-n}[m+k-f, j]'_s\};\end{aligned} \tag{35}$$

$$(36)\quad \sum_3 = \lambda^{i+j}(F)p^{n(2k-f)(s+t+1)} \sum_{M|F}^{m>f-k} \lambda^{i+j}(M) \mid M \mid^{s+t+1} \cdot(-1)^{i(m+k-f)}p^{-ns(m+k-f)}\{[m+k-f,j]_i - p^{-n}[m+k-f,j]'_i\};$$

$$(37)\quad \sum_4 = \lambda^{i+j}(F)p^{n(2k-f)(s+t+1)}\Big\{ \sum_{M|F}^{m=f-k} \lambda^{i+j}(M) \mid M \mid^{s+t+1} + (1-p^{-n}) \sum_{M|F}^{m>f-k} \lambda^{i+j}(M) \mid M \mid^{s+t+1} \cdot(-1)^{(i+j)(m+k-f)}p^{-n(s+t)(m+k-f)} \Big\}.$$

Combining (34), $\cdots$, (37) exactly as in (28) (the corresponding point in the proof of Theorem 1) we complete the proof of (33) and therefore of Theorem 2.

4. **Number of solutions of (1).** We begin with the case $s=1$ and then proceed by induction to the formulas (3) and (4) for general s.

THEOREM 3. *If α is an element of $GF(p^n), \neq 0$ or 1; F is of even degree, $2k$; then the number of solutions of*

$$(38)\qquad (1-\alpha)F = X^2 - \alpha Y^2.$$

in (primary) X, Y of degree k, is

(I) $\sum_{M|F}^{m=k} 1$ *for α a square in $GF(p^n)$,*

(II) $\sum_{M|F}(-1)^m$ *for α a non-square in $GF(p^n)$.*

The case (I) is almost trivial. Let $\alpha \doteq \beta^2$, β in $GF(p^n)$ and $\neq \pm 1$, so that (38) becomes

$$F = \frac{X+\beta Y}{1+\beta}\,\frac{X-\beta Y}{1-\beta} = UV,$$

say. Evidently U and V are primary of degree k. But the number of solutions of $F=UV$, U and V of equal degree, is of course the number of divisors of F that are of degree k. Since U, V uniquely determines X, Y, this establishes the formula (I).

(II)* α is now not the square of any element of $GF(p^n)$; however it is a square in the Galois field of order p^{2n}, $GF(p^{2n})$, which contains the original

* This case can be deduced from the general theory of quadratic fields over $\mathfrak{D}$, worked out in detail by Artin, Mathematische Zeitschrift, vol. 19 (1924), pp. 153–246. However we shall make no use of this theory here.

$GF(p^n)$. Put $\alpha=\theta^2$, so that θ is in $GF(p^{2n})$ but not in $GF(p^n)$; in particular $\theta \neq \pm 1$. Then as above

$$F = \frac{X+\theta Y}{1+\theta}\,\frac{X-\theta Y}{1-\theta} = UV,$$

U and V now being over $GF(p^{2n})$ and of equal degree. Put

$$U = A + \theta B,\ V = A' + \theta B',$$

where A, B, A', B' are all over $GF(p^n)$; A and A' are primary and of degree k; B and B' are of degree less than k and not necessarily primary. Then

$$X + \theta Y = (1+\theta)(A+\theta B),$$
$$X - \theta Y = (1-\theta)(A'+\theta B'),$$

whence $A=A'$, $B=-B'$. Therefore we seek the number of solutions of

$$F = (A+\theta B)(A-\theta B), \tag{39}$$

where A is primary of degree k, and B is of lesser degree and need not be primary. This can be determined readily if we make use of two well known properties of polynomials over a Gälois field: first, *an irreducible polynomial over $GF(p^n)$ factors in $GF(p^{2n})$ if and only if its degree is even*; second, *a polynomial over $GF(p^n)$ can be expressed as a product of irreducible polynomials over $GF(p^n)$ in essentially one way.*

Suppose now $F=Q^l$, Q irreducible of degree q. Clearly if l and q are both odd, there are no factorizations (39); if q is odd but l is even, there is one such factorization. However if q is even, there are $l+1$ factorizations. In other words the number of solutions of (39) in this case is

$$1 + (-1)^q + \cdots + (-1)^{lq}.$$

Similarly if $F=\Pi Q^l$, Q irreducible, the number of solutions of (39) is

$$\prod_{Q|F}\{1 + (-1)^q + \cdots + (-1)^{ql}\} = \sum_{M|F}(-1)^m.$$

This completes the proof of formula (II).

We are now able to prove our first principal result.

THEOREM 4. *If $\alpha_1, \cdots, \alpha_s, \beta_1, \cdots, \beta_s$ are non-zero elements of $GF(p^n)$, such that*

$$\gamma_i = \alpha_i + \beta_i \neq 0,$$
$$\gamma = \gamma_1 + \cdots + \gamma_s \neq 0;$$

F is of even degree, $2k$; then the number of solutions of (1) *is $\rho_{s-1}(F)$ if*

$$(-1)^s\alpha_1 \cdots \alpha_s\beta_1 \cdots \beta_s \tag{40}$$

is a square in $GF(p^n)$; and is $\omega_{s-1}(F)$ if (40) *is a non-square in $GF(p^n)$.*

The case $s=1$ of this theorem is clearly true by virtue of Theorem 3 and the definition of $\rho_0(F)$ and $\omega_0(F)$. Assume the theorem true for all values up to and including s. In order to effect the induction it is necessary to consider two cases: (I) for some $j \leqq s+1$,

$$\gamma^{(s+1)} = \sum_{i=1}^{s+1} \gamma_i \neq \gamma_j; \tag{41}$$

(II) for no j is (41) satisfied.

(I) Assume the notation is such that $\gamma^{(s)}=\gamma_1+\cdots+\gamma_s\neq 0$. By hypothesis $\gamma_{s+1}\neq 0$, $\gamma^{(s+1)}\neq 0$. If we put

$$\begin{gathered}\gamma^{(s+1)}(F) = \gamma^{(s)}A + \gamma_{s+1}B,\\ |A| = |B| = |F|,\end{gathered} \tag{42}$$

then, since our theorem is assumed true for s, it is obvious that the number of solutions in question for $s+1$ is

$$\begin{aligned} &\text{(i)} \quad \textstyle\sum \rho_{s-1}(A)\rho_0(B), && \text{(ii)} \quad \textstyle\sum \rho_{s-1}(A)\omega_0(B),\\ &\text{(iii)} \quad \textstyle\sum \omega_{s-1}(A)\rho_0(B), && \text{(iv)} \quad \textstyle\sum \omega_{s-1}(A)\omega_0(B), \end{aligned} \tag{43}$$

according as

(i) (5) and $-\alpha_{s+1}\beta_{s+1}$ are both squares,
(ii) (5) is a square, $-\alpha_{s+1}\beta_{s+1}$ a non-square,
(iii) (5) a non-square, $-\alpha_{s+1}\beta_{s+1}$ a square,
(iv) (5) and $-\alpha_{s+1}\beta_{s+1}$ both non-squares;

the sums (43) being taken over all A, B satisfying (42). If now we apply Theorem 1, it is clear that the induction is complete for case (I).

(II) Since (41) is satisfied for no j, it is clear that $\gamma_1=\gamma_2=\cdots=\gamma_{s+1}$, and therefore s is a multiple of p. As a consequence of this,

$$\gamma^{(s-1)} = \gamma_1 + \cdots + \gamma_{s-1} \neq 0,\ \gamma_s + \gamma_{s+1} \neq 0.$$

Let us now put, in place of (42),

$$\gamma^{(s+1)}F = \gamma^{(s-1)}A + (\gamma_s + \gamma_{s+1})B^*,\ |A| = |B| = |F|; \tag{44}$$

in place of (43) we now have

$$\textstyle\sum \rho_{s-2}(A)\rho_1(B),\ \sum \rho_{s-2}(A)\omega_1(B),\ \text{etc.},$$

summed over all A, B satisfying (42). The induction is completed as in case (I).

---

* Or $F=-A+2B$.

COROLLARY. *Let F be of degree $2k$ over $GF(p^n)$, s not a multiple of p. Then the number of solutions of*

$$2sF = X_1^2 + X_2^2 + \cdots + X_{2s}^2$$

in (primary) X_i of degree k is $\rho_{s-1}(F)$ if

(i) *s is even,*

(ii) *s is odd, n is even,*

(iii) *s and n are odd, $p \equiv 1 \pmod 4$;*

the number of solutions is $\omega_{s-1}(F)$ otherwise, that is, if

(iv) *s and n are odd, $p \equiv 3 \pmod 4$.*

5. **Number of solutions of (2).** Our second principal result is contained in the following theorem.

THEOREM 5. *If $\alpha, \alpha_1, \cdots, \alpha_s, \beta_1, \cdots, \beta_s$ are non-zero elements of $GF(p^n)$, such that*

$$\gamma_i = \alpha_i + \beta_i \neq 0, \quad \gamma = \gamma_1 + \cdots + \gamma_s = 0;$$

F is of arbitrary degree, f; $2k$ is an even integer $> f$; then the number of solutions of (2) is

$$p^{n(s-1)(2k-f)}\rho_{s-1}^k(F) \quad \text{or} \quad p^{n(s-1)(2k-f)}\omega_{s-1}^k(F)$$

according as (40) is or is not a square in $GF(p^n)$.

Take first $s = 1$; we may write (2) in the form

$$\alpha F = X^2 - Y^2, \quad \deg X = \deg Y = k \tag{45}$$

(so that (40) is necessarily a square). But (45) is equivalent to

$$F = UV, \quad \deg U = k, \quad \deg V = f - k;^*$$

therefore the number of solutions of (45) is the number of divisors of F of degree $f-k$, i.e.

$$\sum_{M \mid F}^{m=f-k} 1 = \rho_0^k(F).$$

Since (40) is necessarily a square, our theorem holds for $s = 1$.

For $s > 1$, we make use of Theorem 4. Since $\gamma = 0, \gamma_1 \neq 0$, plainly $\gamma - \gamma_1 \neq 0$. Let us put

$$\alpha F = \gamma_1 A + (\gamma - \gamma_1)B, \quad \deg A = \deg B = 2k. \tag{46}$$

---

* U and V are of course primary.

By Theorem 4 we may express the number of solutions of

$$\gamma_1 A = \alpha_1 X_1^2 + \beta_1 Y_1^2,\ (\gamma - \gamma_1)B = \alpha_2 X_2^2 + \cdots + \beta_s Y_s^2,$$

in terms of $\rho_0(A)$, $\omega_0(A)$; $\rho_{s-2}(A)$, $\omega_{s-2}(A)$, respectively. Thus, if $-\alpha_1\beta_1$ and $(-1)^{s-1}\alpha_2 \cdots \beta_s$ are both squares, the number of solutions of (2) is

$$\sum \rho_0(A)\rho_{s-2}(B)$$

summed over all A, B satisfying (46). Applying Theorem 2, this sum is

$$p^{n(s-1)(2k-f)}\overset{k}{\rho}_{s-1}(F),$$

which proves the theorem in this case. The proof is exactly the same in each of the remaining three cases and need not be repeated. This completes the proof of Theorem 5.

COROLLARY 1. *If all the hypotheses of Theorem* 5 *are true, and in addition* $k>f$, *then the number of solutions of* (2) *is*

$$\left(1 - \frac{1}{p^{n(s-1)}}\right)p^{n(s-1)(2k-f)} \sum_{M|F} |M|^{s-1}$$

or

$$\left(1 - \frac{1}{p^{n(s-1)}}\right)p^{n(s-1)(2k-f)} \sum_{M|F} (-1)^{f-m} |M|^{s-1}$$

according as (40) *is or is not a square in* $GF(p^n)$, *the summations now being taken over all* M *dividing* F.

COROLLARY 2.* *Let* F *be of degree* f *over* $GF(p^n)$, $2k$ *an even integer* $>f$, s *a multiple of* p, $\alpha \neq 0$. *Then the number of solutions of*

$$\alpha F = X_1^2 + \cdots + X_{2s}^2$$

in (primary) X_i *of degree* k *is*

$$p^{n(s-1)(2k-f)}\overset{k}{\rho}_{s-1}(F)$$

if $ns(p-1)/2$ *is even; the number of solutions is*

$$p^{n(s-1)(2k-f)}\overset{k}{\omega}_{s-1}(F)$$

if $ns(p-1)/2$ *is odd.*

* Cf. the corollary to Theorem 4.

DUKE UNIVERSITY,
DURHAM, N.C.