APOLARITY IN THE GALOIS FIELDS OF ORDER 2^n*

BY A. D. CAMPBELL

Let us consider an m-ary quadratic in the Galois fields of order 2^n

$$(1) \qquad f(x_1, x_2, \cdots, x_m) \equiv \sum a_{ij}x_ix_j = 0,$$

where

$$i, j = 1, 2, \cdots, m; j \geqq i; a_{ji} = 0 \text{ if } j \neq i.$$

If m is even, the discriminant of (1) is†

$$(2) \qquad \Delta \equiv \begin{vmatrix} 0 & a_{12} & a_{13} \cdots a_{1m} \\ a_{12} & 0 & a_{23} \cdots a_{2m} \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ a_{1m} & a_{2m} & a_{3m} \cdots 0 \end{vmatrix}.$$

If m is odd, the discriminant of (1) is*†

$$(3) \qquad \Delta \equiv \tfrac{1}{2}\begin{vmatrix} 2a_{11} & a_{12} \cdots a_{1m} \\ a_{12} & 2a_{22} \cdots a_{2m} \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ a_{1m} & a_{2m} \cdots 2a_{mm} \end{vmatrix}.$$

We note that in the expansion of (2) we shall have terms like $2a_{12}a_{23}a_{34} \cdots a_{1m} \equiv 0$ modulo 2. Hence (2), when expanded, is of the form

$$a_{12}^2a_{34}^2a_{56}^2 \cdots a_{m-1m}^2 + a_{13}^2a_{24}^2 \cdots + \cdots$$
$$+ (a_{12}a_{34}a_{56} \cdots a_{m-1m} + a_{13}a_{24} \cdots + \cdots)^2.$$

Let us consider a pencil of m-ary quadratics

$$(4) \qquad \sum(\lambda b_{ij} + \mu a_{ij})x_ix_j = 0,$$

with b_{ij} and a_{ij} like a_{ij} in (1).

---

* Presented to the Society, December 28, 1931.

† See A. D. Campbell, *The discriminant of the m-ary quadratic in the Galois fields of order* 2^n, Annals of Mathematics, (2), vol. 29 (1928), No. 3, pp. 395–398.

If m is even and we apply (2) to (4), we have

$$(5)\quad \{(\lambda b_{12}+\mu a_{12})(\lambda b_{34}+\mu a_{34})\cdots(\lambda b_{m-1m}+\mu a_{m-1m})+\cdots\}^2.$$

If we equate to zero the square root of the coefficient of $\lambda^2\mu^{m-2}$ in (5), we obtain the invariant

$$(6)\quad b_{12}(a_{34}a_{56}\cdots a_{m-1m}+\cdots)+b_{13}(a_{24}a_{56}\cdots+\cdots)+\cdots=0.$$

If m is odd and we apply (3) to (4), we have

$$(7)\quad \frac{1}{2}\begin{vmatrix} 2(\lambda b_{11}+\mu a_{11}) & \lambda b_{12}+\mu a_{12} & \cdots & \lambda b_{1m}+\mu a_{1m} \\ \vdots & \vdots & & \vdots \\ \lambda b_{1m}+\mu a_{1m} & \lambda b_{2m}+\mu a_{2m} & \cdots & 2(\lambda b_{mm}+\mu a_{mm}) \end{vmatrix}.$$

If we equate to zero the coefficient of $\lambda\mu^{m-1}$ in (7), we obtain the invariant

$$(8)\qquad \sum b_{ij}A_{ij}=0,$$

where

$$i,j=1,2,\cdots,m;\ j\geqq i;\ b_{ji}=0 \text{ if } j\neq i,$$

and where A_{ij} is the cofactor of a_{ij} in a determinant like (2), only with m odd. Thus we have

$$A_{11}=\begin{vmatrix} 0 & a_{23} & \cdots & a_{2m} \\ a_{23} & 0 & \cdots & a_{3m} \\ \vdots & \vdots & & \vdots \\ a_{2m} & a_{3m} & \cdots & 0 \end{vmatrix},\qquad A_{12}=\begin{vmatrix} a_{12} & a_{13} & \cdots & a_{1m} \\ a_{23} & 0 & \cdots & a_{3m} \\ \vdots & \vdots & & \vdots \\ a_{2m} & a_{3m} & \cdots & 0 \end{vmatrix},\ \text{etc.}$$

We define the polar (or tangent) hyperplane of any point $P'(x_1',x_2',\cdots,x_m')$ with respect to (1) by the equation

$$(9)\qquad \sum\frac{\partial f}{\partial x_i'}x_i=0,\qquad (i=1,2,\cdots,m).$$

To find the equation of (1) in hyperplane coordinates we seek the condition that the tangent hyperplane (9) shall be the same as

$$(10)\qquad \sum u_ix_i=0,$$

and that (10) shall pass through P'. We get equations of the form

$$
(11) \qquad \begin{aligned} -\rho u_1 + 2a_{11}x_1' + a_{12}x_2' + \cdots + a_{1m}x_m' &= 0, \cdots, \\ \sum u_i x_i' &= 0. \end{aligned}
$$

If m is even, the determinant of the coefficients of the equations (11), considered as equations in the unknowns ρ, x_1', x_2', $\cdots$, x_m', vanishes identically because this determinant is then a skew-symmetric determinant of odd order (modulo 2). The vanishing of this determinant means that, for m even, the hyperplane (9) always passes through P' even when (9) is only a polar (and not a tangent) hyperplane with respect to (1). Therefore, for m even, we define the equation of (1) in hyperplane coordinates as having the form

$$
(12) \qquad \frac{1}{2} \begin{vmatrix} 2a_{11} & a_{12} & \cdots & a_{1m} & u_1 \\ a_{12} & 2a_{22} & \cdots & a_{2m} & u_2 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ a_{1m} & a_{2m} & \cdots & 2a_{mm} & u_m \\ u_1 & u_2 & \cdots & u_m & 0 \end{vmatrix} \equiv \sum A'_{ij} u_i u_j = 0,
$$

where $A'_{ij}(i \neq j)$ is defined as A_{ij} for (8) and $A'_{ji} = 0$ if $j \neq i$, but $A'_{ii} = \frac{1}{2}A_{ii}$.

For m odd, we define the equation of (1) in hyperplane coordinates as having the form

$$
(13) \qquad \begin{vmatrix} 0 & a_{12} & \cdots & a_{1m} & u_1 \\ a_{12} & 0 & \cdots & a_{2m} & u_2 \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ a_{1m} & a_{2m} & \cdots & 0 & u_m \\ u_1 & u_2 & \cdots & u_m & 0 \end{vmatrix} \equiv \sum A_{ii} u_i^2 = 0,
$$

where A_{ii} is defined as for (8). We note that, for m even, there is no term in (5) of the form $\alpha\lambda\mu^{m-1}$. Even if we define apolarity as the relation given by the invariant (6), this has no simple geometrical meaning.

For m odd, the equations

$$
(14) \qquad \begin{aligned} 2a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m &= 0, \\ a_{12}x_1 + 2a_{22}x_2 + a_{23}x_3 + \cdots + a_{2m}x_m &= 0, \cdots, \text{ (modulo 2)} \end{aligned}
$$

have a common solution, since the determinant of the coefficients vanishes (being skew-symmetric and of odd order). Geometrically, this means that all the polar and tangent hyperplanes of (1) pass through a common point P, for m odd.

If $P(X_1, X_2, \cdots, X_m)$ is this common solution, we have

$$X_1 = k_1A_{11},\ X_2 = k_1A_{12}, \cdots, X_m = k_1A_{1m},$$
$$X_1 = k_2A_{12},\ X_2 = k_2A_{22}, \cdots, X_m = k_2A_{2m},$$
$$X_1 = k_3A_{13}, \text{ etc.}$$

But A_{11} has the form α_{11}^2, being a skew-symmetric determinant of even order, like (2). Similarly, $A_{22}=\alpha_{22}^2, \cdots, A_{mm}=\alpha_{mm}^2$. Also we have

$$X_1X_2 = k_1k_2A_{12}^2,\ X_1 = \frac{k_1A_{12}^2}{A_{22}} = k_1A_{11};$$

hence $A_{12}^2=A_{11}A_{22}=\alpha_{11}^2\alpha_{22}^2$, so that $A_{12}=\alpha_{11}\alpha_{22}$. But

$$X_1 = k_2A_{12} = k_2\alpha_{11}\alpha_{22} = k_1A_{11} = k_1\alpha_{11}^2;$$

therefore

$$k_1\alpha_{11}^2 = k_2\alpha_{11}\alpha_{22}, \text{ and } \frac{k_1}{k_2} = \frac{1/\alpha_{11}}{1/\alpha_{22}},$$

so that $k_1=c/\alpha_{11}$, and $k_2=c/\alpha_{22}$, where c is an arbitrary constant. Finally we have

$$X_1 = k_1A_{11} = \frac{c}{\alpha_{11}}\alpha_{11}^2 = c\alpha_{11},$$

and $X_2=c\alpha_{22}$. Similarly

$$A_{1i}^2 = \alpha_{11}^2\alpha_{ii}^2, \qquad \frac{k_1}{k_i} = \frac{1/\alpha_{11}}{1/\alpha_{ii}},$$

so that $k_1=c/\alpha_{11}$ and $k_i=c/\alpha_{ii}$; therefore $X_i=c\alpha_{ii}$.

From the above discussion we see that the equations (14) have the common solution

$$(15)\quad P(X_1, X_2, \cdots, X_m) = P\{(A_{11})^{1/2}, (A_{22})^{1/2}, \cdots, (A_{mm})^{1/2}\},$$

with A_{ii} defined as for (8). If we call (8) the relation of apolarity between the point quadratic $\sum b_{ij}x_ix_j=0$ and the quadratic in hyperplane coordinates given by (13), we see that (8) is the condition that $P(X_i \equiv (A_{ii})^{1/2})$ shall lie on the apolar quadratic $\sum b_{ij}x_ix_j = 0$.

Finally we note that if we expand (3) m times, first using the elements of the first column and their cofactors, then the elements of the second column and their cofactors, and in like manner to the last column, and if we then add our results and equate Δ to zero (removing the odd factor m), we get (3) in the form $\sum a_{ij}A_{ij} = 0$, where a_{ij} and A_{ij} are the same as for (8). This shows us that for (1) to be a degenerate quadratic, when m is odd, the point P in (15) must lie on (1). There is no similar simple geometrical description when m is even and (1) is degenerate.

SYRACUSE UNIVERSITY

A CLASS OF UNIVERSAL FUNCTIONS*

BY GORDON PALL

Let a, b, c, d be integers, $a \neq 0$. The function $f(x, y)$ defined by the equation

(1) $$f(x, y) = axy + bx + cy + d$$

will be called *universal* if $f(x, y)$ represents all integers for integral values of x and y.

THEOREM 1. *A necessary and sufficient condition for* (1) *to be universal is that*

(2) $$b \equiv \pm 1 \text{ or } c \equiv \pm 1 \pmod{a},$$

or $a = 6$, $b \equiv \pm 3$, $c \equiv \pm 2$ (mod 6), *or vice versa for* b *and* c.†

The sufficiency is evident. For, if $b = \pm 1 + Ba$,

$$f(x, -B) = \pm x + d - Bc.$$

* Presented to the Society, December 28, 1931.

† The writer was led to the exceptional form $6xy+3x+2y$ as in the analysis below, but through an oversight he thought it did not represent 7. The error was, fortunately, pointed out by W. L. G. Williams before this paper went to press.