Here using $\beta = \frac{1}{2} - a + o(1)$, we get with some computation that for $0 \leqslant a \leqslant \frac{1}{2} + o(1)$

$$G = G(a, \beta) = G(a) \geqslant G(0) = \frac{1}{\sqrt{e}} - \frac{1}{2} - o(1), \tag{2.26}$$

which proves Lemma 2.

Thus we have from formulae (2.2), (2.15), (2.11), (2.12) and (2.16)

$$\sum_{d \leqslant x} \frac{\theta(d)}{d} = \frac{1}{x} \sum_{n \leqslant x} g(n) + O(1) \leqslant \frac{1}{x} \sum_{n \leqslant x} g'(n) + O(1) \tag{2.27}$$

$$\leqslant \log x \left(1 - \frac{2U'}{\log x} + o(1)\right) \leqslant \log x \left(2\left(1 - \frac{1}{\sqrt{e}}\right) + o(1)\right).$$

### References


[1] D. A. Burgess, *The distribution of quadratic residues and non residues*, Mathematika 4 (1957), pp. 106–112.

[2] — *Estimating* $L_\chi(1)$, Norske Vid. Selsk. Forh. (Trondheim) 39 (1966), pp. 101–108.

[3] — *On character sums and L-series II*, Proc. London Math. Soc. 12 (1962), pp. 193–206.

[4] S. Chowla, *Bounds for the fundamental unit of a real quadratic field*, Norske Vid. Selsk. Forh. (Trondheim) 37 (1964), pp. 85–87.

[5] — *Application of a theorem of A. Weil to improvement of bounds for class numbers of quadratic fields*, ibid. 38 (1965), pp. 84–85.

[6] E. Landau, *Abschätzungen von Charactersummen, Einheiten und Klassenzahlen*, Göttinger Nachrichten 1918, pp. 79–97.

[7] G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste*, ibid. pp. 21–29.

[8] P. J. Stephens, *Optimizing the size of* $L(1, \chi)$, Proc. London Math. Soc. (3) 24 (1972), pp. 1–14.


EÖTVÖS LORAND UNIVERSITY
DEPARTMENT OF ALGEBRA AND NUMBER THEORY
Budapest, Hungary

*Received on 20. 10. 1975* (781)

ACTA ARITHMETICA
XXXII (1977)

# The factorization of $Q(L(x_1), \ldots, L(x_k))$ over a finite field where $Q(x_1, \ldots, x_k)$ is of first degree and $L(x)$ is linear

by

L. Carlitz (Durham, N. C.) and A. F. Long, Jr. (Greensboro, N. C.)

**1. Introduction.** Let $\mathrm{GF}(q)$ denote the finite field of order $q = p^n$ where $p$ is prime and $n \geqslant 1$. Let $\Gamma(p)$ denote the algebraic closure of $\mathrm{GF}(p)$. A polynomial $Q \in \mathrm{GF}[q; x_1, \ldots, x_k]$ is *absolutely irreducible* if $Q$ has no nontrivial factors over $\Gamma(p)$. Throughout this paper, the term irreducible will mean absolutely irreducible.

A polynomial with coefficients in $\mathrm{GF}(q)$ of the form

$$L(x) = \sum_{i=0}^{r} c_i x^{q^i}$$

is called a linear polynomial. The requirement that the coefficients be in $\mathrm{GF}(q)$ insures that the operation of mapping composition for linear polynomials is commutative. Corresponding to the linear polynomial $L(x)$ we have the ordinary polynomial

$$l(x) = \sum_{i=0}^{r} c_i x^i.$$

We shall assume in the following that $c_0 \neq 0$; this avoids multiple factors in $L(x)$ and insures that there is a smallest integer $r$ such that $l(x)$ divides $x^r - 1$. We say that $l(x)$ has *exponent* $r$.

Let $Q(x_1, \ldots, x_k) = a_1 x_1 + \ldots + a_k x_k + 1$ where $[\deg a_1, \ldots, \deg a_k] = s$ (if $a \in \mathrm{GF}(q^s)$ but $a \notin \mathrm{GF}(q^t)$, $1 \leqslant t < s$, we say that the *degree of* $a$ *relative to* $\mathrm{GF}(q)$ is $s$ and write $\deg a = s$). We shall assume that $\{a_1, \ldots, a_k\}$ are linearly independent over $\mathrm{GF}(q)$; otherwise $Q(x_1, \ldots, x_k)$ can be reduced at once to a polynomial in $m$ variables by suitable first degree transformations, where $m$ is the number of elements in a maximal linearly independent subset of $a_1, \ldots, a_k$.

In this paper we describe the factorization of $Q(L(x_1), \ldots, L(x_k))$. (We note that it is possible to have $Q(L(x_1), \ldots, L(x_k))$ reduce to a polynomial in fewer than $k$ variables even though $\{a_1, \ldots, a_k\}$ are linearly independent over GF$(q)$; see Example 5.1.) If $s\nmid r$, we shall show that $Q(L(x_1), \ldots, L(x_k))$ is absolutely irreducible. If $s|r$, the character of the factorization depends on $L(x)$. For $L(x) = x^{q^r}-x$, we obtain factors of degree one, for $L(x) = x^{q^{r-1}}+x^{q^{r-2}}+\ldots+x$ we obtain absolutely irreducible factors of degree $q^{k-1}$, and for arbitrary $L(x)$ we obtain absolutely irreducible factors of degree $q^{r-jk+u}$ where $u$ and $j$ are determined by $L(x)$. For the precise statement of this result, see Theorem 5.1. For convenience in Sections 3 and 4, we shall describe the factorization for $Q(x, y) = ax+by+1$ and then indicate how the results may be extended to more than two variables.

The results for the homogenous case

$$Q(x_1, \ldots, x_k) = a_1x_1+\ldots+a_kx_k$$

are similar.

The factorizations considered in this paper are motivated by the multiple variable factorizations for $L(x) = x^{q^r}-x$ obtained by Long in [2] and [3] and the single variable results for arbitrary $L(x)$ obtained by Long and Vaughan in [4] and [5]. It is interesting to note that the case $s\nmid r$ behaves like a result of Ehrenfeucht and Pełczyński [1]: The polynomial $f(x)+g(y)+h(z)$ is absolutely irreducible over the complex number field for any polynomials $f$, $g$ and $h$. However in the case of finite fields, $f(x)+g(y)+h(z)$ may indeed factor when $s|r$.

## 2. Preliminaries

Lemma 2.1. *Let $\boldsymbol{x} = (x_1, x_2, \ldots, x_k)$, that is let $\boldsymbol{x}$ denote a vector with components $x_1, \ldots, x_k$. Let $f(x)\in$ GF$[q; x]$. For any integer $j\geqslant 1$, $y^{p^j}+f(\boldsymbol{x})$ is absolutely irreducible if and only if $f(\boldsymbol{x})$ is not a $p$-th power in any extension of* GF$(q)$.

Remark. If $j = 0$, $y+f(\boldsymbol{x})$ is obviously an absolutely irreducible first degree polynomial.

Proof. To show necessity, let $f(\boldsymbol{x}) = [a(\boldsymbol{x})]^p$ in GF$[q, \boldsymbol{x}]$. Then for $j\geqslant 1$, we have

$$y^{p^j}+f(\boldsymbol{x}) = [y^{p^{j-1}}+a(\boldsymbol{x})]^p.$$

The proof of sufficiency will be by induction on $j$. Let $j = 1$. If $f(\boldsymbol{x})$ is not a $p$th power, then any factorization of $y^p+f(\boldsymbol{x})$ in some extension field of GF$(q)$ would be of the form

$$y^p+f(\boldsymbol{x}) = \varphi(y, \boldsymbol{x})\psi(y, \boldsymbol{x}) \tag{2.1}$$

where $\varphi$ is an absolute irreducible and $\psi$ is either irreducible or a product of irreducibles. If the factorization is nontrivial, $y$ actually appears in $\varphi$ and $\psi$. We consider separately the two cases $(\varphi, \psi) = 1$ and $(\varphi, \psi) \neq 1$.



Case I. $(\varphi, \psi) = 1$. On differentiating (2.1) with respect to $y$ we have

$$\varphi\psi_y+\psi\varphi_y = 0. \tag{2.2}$$

Now (2.2) implies that $\varphi|\psi\varphi_y$. Since $(\varphi, \psi) = 1$ we have $\varphi|\varphi_y$, which is impossible unless $\varphi_y = 0$. Similarly $\psi_y = 0$. But $\varphi_y = 0$ implies $\varphi = \varphi_1(y^p, \boldsymbol{x})$ with $y^p$ actually appearing. Similarly $\psi_y = 0$ implies $\psi = \psi_1(y^p, \boldsymbol{x})$ with $y^p$ actually appearing. Consequently the product $\varphi\psi$ contains a term with $y^{2p}$ and this clearly contradicts the choice of $\varphi$ and $\psi$ in (2.1).

Case II. $(\varphi, \psi) \neq 1$. We may assume the factorization in the form

$$y^p+f(\boldsymbol{x}) = \varphi^k(y, \boldsymbol{x}) \tag{2.3}$$

where $\varphi$ is absolutely irreducible over GF$(q)$ and $k$ is an integer $\geqslant 1$. (If $y^p+f(\boldsymbol{x}) = \varphi^k\psi$ with $(\varphi^k, \psi) = 1$, we may apply the argument of Case I.)

If $k \equiv 0 \pmod p$, then $y^p+f(\boldsymbol{x})$ is a $p$th power and this contradicts the hypotheses on $f(\boldsymbol{x})$ since this would imply $f(\boldsymbol{x})$ is a $p$th power. Thus $k \not\equiv 0 \pmod p$. On differentiating (2.3) we have

$$k\varphi^{k-1}\varphi_y = 0. \tag{2.4}$$

Since $k \not\equiv 0 \pmod p$, and $\varphi^{k-1} \neq 0$, we have $\varphi_y = 0$. Hence $\varphi(y, \boldsymbol{x}) = \varphi_1(y^p, \boldsymbol{x})$ and

$$y^p+f(\boldsymbol{x}) = \varphi_1^k(y^p, \boldsymbol{x}) \tag{2.5}$$

where $y^p$ actually appears in $\varphi_1$. In order that the degree of $y$ in both members of (2.5) be $p$, we must have $k = 1$. Thus $y^p+f(\boldsymbol{x})$ is absolutely irreducible over GF$(q)$.

Assume that the lemma is true for $j = r-1$.

Case I. $(\varphi, \psi) = 1$. For $j = r$, we have as before

$$y^{p^r}+f(\boldsymbol{x}) = \varphi_1(y^p, \boldsymbol{x})\psi_1(y^p, \boldsymbol{x}). \tag{2.6}$$

Let $z = y^p$ so that (2.6) becomes

$$z^{p^{r-1}}+f(\boldsymbol{x}) = \varphi_1(z, \boldsymbol{x})\psi_1(z, \boldsymbol{x}). \tag{2.7}$$

By the induction hypothesis $z^{p^{r-1}}+f(\boldsymbol{x}) = y^{p^r}+f(\boldsymbol{x})$ is absolutely irreducible over GF$(q)$.

Case II. $(\varphi, \psi) \neq 1$. For $j = r$ we have

$$y^{p^r}+f(\boldsymbol{x}) = \varphi_1^k(y^p, \boldsymbol{x}). \tag{2.8}$$

Again set $z = y^p$ and (2.8) becomes

$$z^{p^{r-1}}+f(\boldsymbol{x}) = \varphi_1^k(z, \boldsymbol{x}) \tag{2.9}$$

which is absolutely irreducible by the induction hypothesis.

LEMMA 2.2. *Let $\beta$ belong to $\Gamma(p)$. Then $x^{q^r}+x+\beta$ is never a $p$-th power.*

Proof. The derivative of $x^{q^r}+x+\beta$ with respect to $x$ is 1; the derivative of a $p$th power is 0. Hence $x^{q^r}+x+\beta$ is not a $p$th power.

LEMMA 2.3. *Let $f(x)$ be a polynomial with coefficients in $\mathrm{GF}(q^s)$, and let $G(x)$ be a linear polynomial of degree $q^j$ with coefficients in $\mathrm{GF}(q)$. If $f(x+c) = f(x)$ for all $c$ such that $G(c) = 0$ then $f(x) = \varphi(G(x))$ where $\varphi$ is a polynomial over $\mathrm{GF}(q^s)$.*

Proof. Using the division algorithm we may write

$$f(x) = \sum_{i=0}^{h} A_i(x)G^i(x) \qquad (\deg A_i(x) < q^j). \tag{2.10}$$

Since $f(x+c) = f(x)$, (2.10) becomes

$$f(x) = \sum_{i=0}^{h} A_i(x+c)G^i(x+c).$$

Since $G(x+c) = G(x)+G(c) = G(x)$ it follows that

$$f(x) = \sum_{i=0}^{h} A_i(x+c)G^i(x).$$

Since the coefficients in (2.10) are uniquely determined we have

$$A_i(x+c) = A_i(x)$$

for all $c$ such that $G(c) = 0$. Since $\deg A_i(x) < q^j$ and $\deg G(x) = q^j$, we immediately conclude that $A_i(x)$ is a constant.

LEMMA 2.4. *Let $f(x_1, \ldots, x_k)$ be a polynomial with coefficients in $\mathrm{GF}(q^s)$, and let $G(x)$ be a linear polynomial of degree $q^j$ with coefficients in $\mathrm{GF}(q)$. If $f(x_1+c_1, \ldots, x_k+c_k) = f(x_1, \ldots, x_k)$ for all $c_i$ such that $G(c_i) = 0$, $i = 1, \ldots, k$, then*

$$f(x_1, \ldots, x_k) = \varphi(G(x_1), \ldots, G(x_k))$$

*where $\varphi$ is a polynomial over $\mathrm{GF}(q^s)$.*

Proof. Use Lemma 2.3 and induction on $k$.

LEMMA 2.5. *Let*

$$f(x_1, \ldots, x_k) = \prod_{c_1, \ldots, c_k} \psi(x_1+c_1, \ldots, x_k+c_k)$$

*where the product is over all $c_i$, $1 \leqslant i \leqslant k$, such that $G(c_i) = 0$, $\psi$ is a polynomial over $\mathrm{GF}(q^s)$, and $G(x)$ is a linear polynomial over $\mathrm{GF}(q)$. Then*

$$f(x_1, \ldots, x_k) = \varphi(G(x_1), \ldots, G(x_k))$$

*where $\varphi$ is a polynomial over $\mathrm{GF}(q^s)$.*

Proof. This is an immediate corollary of Lemma 2.4.

LEMMA 2.6. *Let $x^r-1 = l(x)m(x)$. Let $L(x)$, $M(x)$ be the linear polynomials corresponding to $l(x)$, $m(x)$ respectively. If $Q(L(x), L(y)) = F(x, y)G(x, y)$, then*

$$Q(x^{q^r}-x, y^{q^r}-y) = F(M(x), M(y))G(M(x), M(y)).$$

Proof. Since $x^{q^r}-x = L(M(x))$, we have

$$Q(x^{q^r}-x, y^{q^r}-y) = Q(L(M(x)), L(M(y))) = F(M(x), M(y))G(M(x), M(y)).$$

Note that Lemma 2.6 can be immediately generalized to more than two variables. The lemma is of course also true for one variable.

LEMMA 2.7. *Let $G(x)$ be an arbitrary linear polynomial in $\mathrm{GF}[q; x]$. Let*

$$P(x_1, \ldots, x_k) = \prod_{c_1, \ldots, c_k} [a_1(x_1+c_1)+ \ldots +a_k(x_k+c_k)+a_0]$$

*where $a_i$, $0 \leqslant i \leqslant k$, are coefficients from $\mathrm{GF}(q^s)$ and the product is over all $c_i$, $1 \leqslant i \leqslant k$, such that $G(c_i) = 0$. For a given $k$-tuple $(c_1, \ldots, c_k)$ of roots of $G(x)$, define the class $C[c_1, \ldots, c_k]$ as follows:*

$$C[c_1, \ldots, c_k] = \{(d_1, \ldots, d_k) |\ G(d_i) = 0,\ 1 \leqslant i \leqslant k, \text{ and } a_1(x_1+d_1)+ \ldots \\ \ldots +a_k(x_k+d_k)+a_0 = a_1(x_1+c_1)+ \ldots +a_k(x_k+c_k)+a_0\}.$$

*These classes partition the $k$-tuples of roots of $G(x)$ and each class has the same cardinality.*

Proof. If $C[c_1, \ldots, c_k]$ and $C[c_1', \ldots, c_k']$ have a $k$-tuple in common, it follows that

$$a_1(x_1+c_1')+ \ldots +a_k(x_k+c_k')+a_0 = a_1(x_1+c_1)+ \ldots +a_k(x_k+c_k)+a_0.$$

Thus $(c_1', \ldots, c_k') \in C[c_1, \ldots, c_k]$ and conversely. Hence

$$C[c_1, \ldots, c_k] = C[c_1', \ldots, c_k'].$$

Let $C_0 = C[0, \ldots, 0]$. Then $(c_1, \ldots, c_k) \in C_0$ if and only if $a_1c_1+ \ldots \ldots +a_kc_k = 0$. Let $C_1 = C[d_1, \ldots, d_k]$ denote an arbitrary class. For each $(c_1, \ldots, c_k) \in C_0$, we have

$$a_1(d_1+c_1)+ \ldots +a_k(d_k+c_k) = a_1d_1+ \ldots +a_kd_k.$$

Thus $(d_1+c_1, \ldots, d_k+c_k) \in C_1$. Hence $|C_1| \geqslant |C_0|$. On the other hand if $(d_1', \ldots, d_k') \in C_1$, we have $(d_1'-d_1, \ldots, d_k'-d_k) \in C_0$. Thus $(d_1', \ldots, d_k') = (d_1+c_1, \ldots, d_k+c_k)$ for some $(c_1, \ldots, c_k) \in C_0$. Hence $|C_1| \leqslant |C_0|$. We conclude that $|C_1| = |C_0|$.

LEMMA 2.8. *Let $G(x)$ be a linear polynomial over $\mathrm{GF}(q)$ having degree $q^w$. Let $h(x_1, \ldots, x_k) = a_1x_1+ \ldots +a_kx_k \in \mathrm{GF}[q^s; x_1, \ldots, x_k]$. Then the set of* *solutions* $\{(c_1, \ldots, c_k)\}$ *of* $h(x_1, \ldots, x_k) = 0$ *such that* $G(c_i) = 0$, $i = 1, \ldots, k$, *has cardinality* $q^u$ *where* $u$ *is an integer* $\geqslant 0$.

Proof. Let $W$ be the vector space of solutions of $G(x) = 0$ over $GF(q)$. By renumbering if necessary, let $S = \{a_1, \ldots, a_m\}$ be a maximal linearly independent subset of $\{a_1, \ldots, a_k\}$ over $W$. Thus for $j = 1, \ldots, k$, we may write

$$a_j = \sum_{i=1}^{m} b_{ij} a_i \qquad (b_{ij} \in W).$$

Then

$$\sum_{j=1}^{k} a_j c_j = \sum_{i=1}^{m} \Big( \sum_{j=1}^{k} b_{ij} c_j \Big) a_i = 0$$

implies

$$\sum_{j=1}^{k} b_{ij} c_j = 0 \qquad (i = 1, \ldots, m) \tag{2.11}$$

by the linear independence of $S$.

Let $V$ be the vector space of solutions of (2.11). Then $|V| = q^v$ for some integer $v \geqslant 0$. The set of solutions $\{(c_1, \ldots, c_k)\}$ of (2.11) such that $G(c_i) = 0$, $i = 1, \ldots, k$, is the vector space $W \cap V$. Since $|W| = q^w$ and $|V| = q^v$, we have $|W \cap V| = q^u$ for some integer $u \geqslant 0$.

**3. The factorization of** $a(x^{q^r} - x) + b(y^{q^r} - y) + 1$. Let $Q(x, y) = ax + by + 1 \in GF[q^s; x]$. Let $[\deg a, \deg b] = s$. We also require that $a$ and $b$ be linearly independent over $GF(q)$; if not, $Q(x, y)$ can be written as a polynomial $Q_1(z)$ in the variable $z = x + cy$ for some $c \in GF(q)$, and it is well known that the one-variable polynomial $Q_1(z^{q^r} - z)$ has first degree factors over $\Gamma(p)$. If $s | r$, we find that

$$\begin{aligned} Q(x^{q^r} - x, y^{q^r} - y) &= a(x^{q^r} - x) + b(y^{q^r} - y) + 1 \\ &= (ax + by)^{q^r} - (ax + by) + 1 = \prod_{\lambda} (ax + by + \lambda) \end{aligned} \tag{3.1}$$

where the product extends over all $\lambda$ satisfying $\lambda^{q^r} - \lambda + 1 = 0$. Thus we have:

THEOREM 3.1 ([2]). *Let* $Q(x, y) = ax + by + 1$ *where* $[\deg a, \deg b] = s$ *relative to* $GF(q)$. *If* $s | r$, *then* $Q(x^{q^r} - x, y^{q^r} - y)$ *factors into first degree factors over* $GF(q^r)$.

The proof for the homogeneous case is the same except that the product in (3.1) extends over all $\lambda$ such that $\lambda^{q^r} - \lambda = 0$. We have:

THEOREM 3.2 ([3]). *Let* $Q(x, y) = x + by$ *where* $\deg b = s$ *relative to* $GF(q)$. *If* $s | r$, *then* $Q(x^{q^r} - x, y^{q^r} - y)$ *factors into first degree factors over* $GF(q^r)$.



We now show that if $s \nmid r$ and if $a$ and $b$ are linearly independent over $GF(q)$, then $Q(x^{q^r} - x, y^{q^r} - y)$ is absolutely irreducible of degree $q^r$. Since $s \nmid r$, at least one of $\{\deg a, \deg b\}$ does not divide $r$. Consequently we may write

$$a = a^{q^r} + f(a), \qquad b = b^{q^r} + g(b) \tag{3.2}$$

with at least one of $\{f(a), g(b)\}$ non-zero. Thus

$$\begin{aligned} a(x^{q^r} - x) + b(y^{q^r} - y) + 1 &= (ax + by)^{q^r} - (ax + by) + 1 + f(a) x^{q^r} + g(b) y^{q^r} \\ &= W^{q^r} - W + 1 + X^{q^r} + Y^{q^r} \end{aligned} \tag{3.3}$$

where $W = ax + by$, $X = [f(a)]^{q^{-r}} x$, and $Y = [g(b)]^{q^{-r}} y$.

Let $T = X + Y$. Then (3.3) has the form

$$T^{q^r} + (W^{q^r} - W + 1). \tag{3.4}$$

By Lemma 2.2, $W^{q^r} - W + 1$ is not a $p$th power. Hence (3.4), and therefore (3.3), is absolutely irreducible by Lemma 2.1. We have proved:

THEOREM 3.3. *Let* $Q(x, y) = ax + by + 1$ *where* $[\deg a, \deg b] = s$ *relative to* $GF(q)$ *and* $a$ *and* $b$ *are linearly independent over* $GF(q)$. *If* $s \nmid r$, *then* $Q(x^{q^r} - x, y^{q^r} - y)$ *is absolutely irreducible.*

The proof for the homogeneous case is the same except that, with the same notation as before, we use Lemmas 2.1 and 2.2 to show that $T^{q^r} + (W^{q^r} - W)$ is absolutely irreducible.

We have:

THEOREM 3.4. *Let* $Q(x, y) = x + by$ *where* $\deg b = s$ *relative to* $GF(q)$ *and* 1 *and* $b$ *are linearly independent over* $GF(q)$. *If* $s \nmid r$, *then* $Q(x^{q^r} - x, y^{q^r} - y)$ *is absolutely irreducible.*

We note that minor modifications in the proofs permit Theorems 3.1–3.4 to be extended to more than two variables.

EXAMPLE 3.1. This example illustrates Theorem 3.1. Let $Q(x, y) = ax + a^2 y + 1$ where $a^2 = a + 1$ generates $GF(4)$. Let $L(x) = x^4 - x$. Then $s = 2$ and $r = 2$, so that $s | r$. Let $W = ax + a^2 y$. Then

$$Q(x^4 - x, y^4 - y) = W^4 + W + 1 = \prod_{i=0}^{3} (W - \beta^{2^i})$$

where $\beta^4 = \beta + 1$ generates $GF(16)$.

EXAMPLE 3.2. This example illustrates Theorem 3.3. Let $Q(x, y) = ax + a^2 y + 1$ where $a^2 = a + 1$ generates $GF(4)$. Let $L(x) = x^8 - x$. Then $s = 2$ and $r = 3$, so that $s \nmid r$. Thus

$$Q(x^8 - x, y^8 - y) = ax^8 + a^2 y^8 - ax - a^2 y + 1$$

is absolutely irreducible.

**4. The factorization of $a(L(x))+b(L(y))+1$ where $L(x) = x^{q^{r-1}}+ +x^{q^{r-2}}+\ldots+x$.** This substitution is of special interest since $L(x)$ is the trace function of $GF(q^r)$ over $GF(q)$. We note that the exponent of the corresponding ordinary polynomial $l(x)$ is either $r$ or $r-1$. The value $r-1$ occurs only when $p=2$ and $r=2$; in this case $L(x) = x^q-x$ and the factorization is described in Section 3. Consequently we shall exclude the case $p=r=2$, so that the exponent of $l(x)$ is $r$ throughout this section.

THEOREM 4.1. *Let $Q(x,y) = ax+by+1$ where $[\deg a, \deg b] = s$ relative to $GF(q)$ and $a$ and $b$ are linearly independent relative to $GF(q)$. Let*

$$L(x) = x^{q^{r-1}}+x^{q^{r-2}}+\ldots+x.$$

*Let the corresponding ordinary polynomial $l(x) = x^{r-1}+x^{r-2}+\ldots+1$ have exponent $r$. If $s\nmid r$, then $Q(L(x), L(y))$ is absolutely irreducible.*

Proof. Suppose that $Q(L(x), L(y)) = F(x,y)G(x,y)$. Then by Lemma 2.6,

$$Q(x^{q^r}-x, y^{q^r}-y) = F(x^q-x, y^q-y)G(x^q-x, y^q-y).$$

This factorization is in contradiction to Theorem 3.3 since $s\nmid r$.

Remark. The condition of linear independence over $GF(q)$ for $a$ and $b$ rules out the possibility of using a change of variable to transform $Q(L(x), L(y))$ to a polynomial in one variable when $L(x)$ is the trace function of $GF(q^r)$ over $GF(q)$.

The proof of Theorem 4.1 also applies to the case where $Q(x,y)$ is homogenous. We have:

THEOREM 4.2. *Let $Q(x,y) = x+by$ where $\deg b = s$ relative to $GF(q)$. Let $L(x) = x^{q^{r-1}}+x^{q^{r-2}}+\ldots+x$. Let the corresponding ordinary polynomial $l(x) = x^{r-1}+x^{r-2}+\ldots+1$ have exponent $r$. If $s\nmid r$, then $Q(L(x), L(y))$ is absolutely irreducible.*

THEOREM 4.3. *Let $Q(x,y)$, $L(x)$, $l(x)$, $s$ and $r$ be given as in Theorem 4.1. If $s\mid r$, then $Q(L(x), L(y))$ is the product of $q^{r-2}$ absolute irreducibles of degree $q$ in $x$ and $y$.*

Proof. Let $X = x^q-x$ and $Y = y^q-y$. Then, as in (3.1),

$$Q(L(X), L(Y)) = Q(x^{q^r}-x, y^{q^r}-y) = \prod_{\lambda}(ax+by+\lambda) \tag{4.1}$$

where the product extends over all $\lambda$ satisfying $\lambda^{q^r}-\lambda+1 = 0$.

Consider a fixed factor $ax+by+\lambda_0$ of (4.1). Let $c$ and $d$ independently satisfy the equation $x^q-x=0$, that is $c$ and $d$ belong to $GF(q)$. Since $a$ and $b$ are linearly independent, the factors

$$a(x+c)+b(y+d)+\lambda_0 \qquad (c, d\in GF(q)) \tag{4.2}$$



are all distinct. Furthermore they are all factors of $Q(L(X), L(Y))$. We now form the product of the factors (4.2) and obtain the polynomial $P(x,y)$ of degree $q^2$ in $x$ and $y$:

$$P(x,y) = \prod_{c,d\in GF(q)}[a(x+c)+b(y+d)+\lambda_0]. \tag{4.3}$$

By Lemma 2.5

$$P(x,y) = P_1(x^q-x, y^q-y) = P_1(X, Y),$$

and $P_1(X,Y)$ is a polynomial of degree $q$ in $X$ and $Y$.

We now show that $P_1(X,Y)$ is absolutely irreducible. If not, there exists a nontrivial absolutely irreducible factor of $P_1(X,Y)$, call it $R(X,Y)$. Replacing $X$ by $x^q-x$, and $Y$ by $y^q-y$, it is clear that $R(x^q-x, y^q-y)\mid P_1(x^q-x, y^q-y)$; this implies that $R$ is a product of some of the first degree factors (4.2). If we suppose that one first degree factor divides $R$, then it follows that all $q^2$ factors in (4.2) divide $R$. Hence $R(X,Y)$ is identical with $P_1(X,Y)$.

Thus the factors of (4.1) are grouped into $q^{r-2}$ products of the form $P(x,y)$ in (4.3). Each $P(x,y)$ has degree $q^2$ in $x$ and $y$ and can be written as an absolute irreducible of degree $q$ in $X$ and $Y$.

The same proof applies in the case where $Q(x,y)$ is homogeneous. We have:

THEOREM 4.4. *Let $Q(x,y)$, $L(x)$, $l(x)$, $s$ and $r$ be given as in Theorem 4.2. If $s\mid r$, then $Q(L(x), L(y))$ is the product of $q^{r-2}$ absolute irreducibles of degree $q$ in $x$ and $y$.*

Theorems 4.1 and 4.2 can be extended without modification to more than two variables. Theorems 4.3 and 4.4 require a slight change. We state only the theorem corresponding to Theorem 4.3; the homogeneous case is essentially the same.

THEOREM 4.5. *Let $Q(x_1, \ldots, x_k) = a_1x_1+\ldots+a_kx_k+1$ where $[\deg a_1, \ldots \ldots, \deg a_k] = s$ relative to $GF(q)$ and $\{a_1, \ldots, a_k\}$ are linearly independent relative to $GF(q)$. Let*

$$L(x) = x^{q^{r-1}}+x^{q^{r-2}}+\ldots+x.$$

*Let $l(x) = x^{r-1}+x^{r-2}+\ldots+1$ have exponent $r$. If $s\mid r$, then $Q(L(x_1), \ldots \ldots, L(x_k))$ is the product of $q^{r-k}$ absolute irreducibles of degree $q^{k-1}$ in $x_1, \ldots, x_k$.*

Proof. We first note that the condition of linear independence on $\{a_1, \ldots, a_k\}$ insures that $s\geqslant k$ and hence $r\geqslant k$. For if we consider $GF(q^s)$ as a vector space of dimension $s$ over $GF(q)$, a maximal linearly independent set of elements in $GF(q^s)$ has cardinality $s$.

The proof is the same as that for Theorem 4.3 except that (4.1) becomes

$$Q(L(X_1), \ldots, L(X_k)) = \prod_{\lambda}[a_1x_1+\ldots+a_kx_k+\lambda] \tag{4.4}$$

where the product is over all $\lambda$ such that $\lambda^{q^r}-\lambda+1=0$. Thus (4.3) becomes

$$(4.5)\quad P(x_1,\dots,x_k)=\prod_{c_1,\dots,c_k\in GF(q)}[a_1(x_1+c_1)+\dots+a_k(x_k+c_k)+\lambda] = P_1(X_1,\dots,X_k)$$

where $X_i=x_i^q-x_i$ for $1\leqslant i\leqslant k$. As before, it can be shown that $P_1(X_1,\dots,X_k)$ is absolutely irreducible of degree $q^{k-1}$ in its variables, and the factors of (4.4) are partitioned to form $q^{r-k}$ such absolute irreducibles.

In the preceding theorems we have assumed that the coefficients of the variables are linearly independent relative to $GF(q)$. We now describe what occurs if this is not the case. We illustrate with the generalization of Theorem 4.5 where $s|r$ and we also describe the case when $s\nmid r$.

THEOREM 4.6. *Let $Q(x_1,\dots,x_k)=a_1x_1+\dots+a_kx_k+1$ and, by renumbering if necessary, let $\{a_1,\dots,a_m\}$ be a maximal linearly independent subset of $\{a_1,\dots,a_k\}$ relative to $GF(q)$. Let $L(x)$ and $l(x)$ be given as in Theorem 4.5. If $s|r$, then $Q(L(x_1),\dots,L(x_k))$ is the product of $q^{r-m}$ absolute irreducibles of degree $q^{m-1}$ in $x_1,\dots,x_k$.*

Proof. By writing the coefficients $a_{m+1},\dots,a_k$ as linear combinations of $\{a_1,\dots,a_m\}$ over $GF(q)$, we may use first degree transformations of the variables $x_1,\dots,x_k$ to rewrite $Q$ in the form $Q(y_1,\dots,y_m)=a_1y_1+\dots+a_my_m+1$. The result follows from Theorem 4.5 since $\{a_1,\dots,a_m\}$ are linearly independent over $GF(q)$ and $Q(L(y_1),\dots,L(y_m))=Q(L(x_1),\dots,L(x_k))$.

THEOREM 4.7. *Let the hypotheses of Theorem 4.6 be satisfied. If $s\nmid r$, $Q(L(x_1),\dots,L(x_k))$ is absolutely irreducible unless all the ratios $a_j/a_1$, $1\leqslant j\leqslant k$ are in $GF(q)$. In that case $Q(L(x_1),\dots,L(x_k))$ is the product of first degree factors.*

Proof. As in the proof of Theorem 4.6, we have a polynomial $Q(L(x_1),\dots,L(x_k))$ which may reduce to an $m$-variable polynomial. Now $m=1$ if and only if $a_j/a_i$ belongs to $GF(q)$ for $1\leqslant j\leqslant k$. If $m>1$, $Q(L(x_1),\dots,L(x_k))$ is absolutely irreducible by Theorem 4.1 or its generalization. If $m=1$, first degree factorization is always possible.

EXAMPLE 4.1. This example illustrates Theorem 4.1. Let $Q(x,y)=ax+a^2y+1$ where $a^2=a+1$ generates $GF(4)$. Let $L(x)=x^4+x^2+x$. Then $s=2$, $r=3$ and $s\nmid r$. Thus

$$Q(x^4+x^2+x,y^4+y^2+y)=ax^4+a^2y^4+ax^2+a^2y^2+ax+a^2y+1$$

is absolutely irreducible.

EXAMPLE 4.2. This example illustrates Theorem 4.3. Let $Q(x,y)=ax+a^2y+1$ where $a^2=a+1$ generates $GF(4)$. Let $L(x)=x^8+x^4+x^2+x$. Then $s=2$, $r=4$ and $s|r$. Let $W=ax+a^2y$ and $Z=x^2+y^2$. Then if $\beta^4=\beta+1$ generates $GF(16)$, we have

$$(4.6)\quad Q(L(x),L(y))=(Z+W^2+W)^4+(Z+W^2+W)+1 = \prod_{i=0}^{3}[(Z+W^2+W)-\beta^{2^i}]=\prod_{i=0}^{3}[a(x^2-x)+a^2(y^2-y)-\beta^{2^i}].$$

Each factor in (4.6) is absolutely irreducible, and thus $Q(L(x),L(y))$ is the product of 4 absolute irreducibles of degree 2.

EXAMPLE 4.3. This example illustrates Theorem 4.3. Let $Q(x,y)=\lambda x+y+1$ where $\lambda^3=\lambda+2$ generates $GF(3^3)$. Let $L(x)=x^9+x^3+x$. Then $s=3$, $r=3$ and $s|r$. Let $Z=\lambda^9x^3+y^3+2\lambda x+2y$.

$$(4.7)\quad Q(L(x),L(y))=\prod_{i=0}^{2}[Z+(2\lambda)^{3^i}]=[Z+2\lambda][Z+2\lambda+1][Z+2\lambda+2]$$

where each factor in the right member of (4.7) is absolutely irreducible of degree 3.

EXAMPLE 4.4. This example illustrates Theorem 4.6. Let $Q(x,y,z)=x+ay+a^2z+1$ where $a^2=a+1$ generates $GF(3^2)$. Let $L(x)=x^3+x$. Then $s=r=2$ and $s|r$. Now if we let $w=x+z$ and $v=y+z$, we have

$$Q(x,y,z)=(x+z)+a(y+z)+1=w+av+1.$$

The coefficients of $w$ and $v$ are linearly independent over $GF(3)$, so that $m=2$. Theorem 4.6 predicts $3^0=1$ absolute irreducible of degree $3^1=3$. We have

$$Q(L(x),L(y),L(z))\equiv Q(L(w),L(v))=w^3+w+a(v^3+v)+1,$$

an absolute irreducible of degree 3.

## 5. The factorization of $a_1L(x_1)+\dots+a_kL(x_k)+1$ where $L(x)$ is an arbitrary linear polynomial

THEOREM 5.1. *Let $Q(x_1,\dots,x_k)=a_1x_1+\dots+a_kx_k+1$ where $[\deg a_1,\dots,\deg a_k]=s$ over $GF(q)$ and $\{a_1,\dots,a_k\}$ are linearly independent over $GF(q)$. Let $L(x)\in GF[q,x]$ be a linear polynomial with corresponding ordinary polynomial $l(x)=b_0+b_1x^{e_1}+\dots+b_tx^{e_t}$, $0<e_1<\dots<e_t$, belonging to the exponent $r$. Let $g(x)$ be defined by $l(x)g(x)=x^r-1$ and suppose that $g(x)$ has degree $j$. Let $G(x)$ be the linear polynomial corresponding to $g(x)$. Let $q^u$ be the number of solutions $\{c_1,\dots,c_k\}$ of*

$$(5.1)\quad a_1c_1+\dots+a_kc_k=0$$

*where $G(c_i)=0$, $1\leqslant i\leqslant k$.*

*If $s\nmid r$, then $Q(L(x_1),\dots,L(x_k))$ is absolutely irreducible. If $s|r$ and $s|e_i$, $1\leqslant i\leqslant t$, then $Q(L(x_1),\dots,L(x_k))$ is the product of first degree factors* *over $\Gamma(p)$ (and indeed over $\mathrm{GF}(q^r)$). If $s|r$ and $s\nmid e_i$ for at least one $i$, $1\leqslant i\leqslant t$, then $Q\big(L(x_1),\ldots,L(x_k)\big)$ is the product of $q^{r-jk+u}$ absolute irreducibles of degree $q^{j(k-1)-u}$.*

Proof. If $s\nmid r$, the proof of Theorem 4.1 applies. If $s|r$ and $s|e_i$, $1\leqslant i\leqslant t$, then $Q\big(L(x_1),\ldots,L(x_k)\big)$ can be written as a polynomial in one variable $z$ where $z=a_1x_1+\ldots+a_kx_k$. We therefore have first degree factors over $\Gamma(p)$. The factors actually have coefficients in $\mathrm{GF}(q^r)$ by Corollary 3.2 of [4].

Now assume that $s|r$ and $s\nmid e_i$ for at least one $i$, $1\leqslant i\leqslant t$. Now

$$Q\Big(L\big(G(x_1)\big),\ldots,L\big(G(x_k)\big)\Big)=Q(x_1^{q^r}-x_1,\ldots,x_k^{q^r}-x_k)=\prod_{\lambda}(a_1x_1+\ldots+a_kx_k+\lambda)\tag{5.2}$$

where the product extends over all $\lambda$ satisfying $\lambda^{q^r}-\lambda+1=0$.

For a fixed $\lambda$, consider the product

$$P(x_1,\ldots,x_k)=\prod_{c_1,\ldots,c_k}[a_1(x_1+c_1)+\ldots+a_k(x_k+c_k)+\lambda]\tag{5.3}$$

where $G(c_i)=0$. Since the roots of $G(x)$ are in $\mathrm{GF}(q^r)$, it follows that the factors of (5.3) occur in (5.2). Although $\{a_1,\ldots,a_k\}$ are linearly independent over $\mathrm{GF}(q)$, they may not be linearly independent over $W$, the subspace generated by the roots of $G(x)$. Thus there may be repeated factors in (5.3). By Lemma 2.7 and 2.8, each distinct factor appears with the same cardinality $q^u$ where $u\geqslant 0$. By Lemma 2.5, we then have

$$P(x_1,\ldots,x_k)=\Big[P_1\big(G(x_1),\ldots,G(x_k)\big)\Big]^{q^u}\tag{5.4}$$

where $P_1\big(G(x_1),\ldots,G(x_k)\big)$ is absolutely irreducible of degree $q^{j(k-1)-u}$. The total number of such absolute irreducibles formed from the factors of (5.2) is $q^{r-jk+u}$ since (5.2) is of degree $q^{r-j}$ in the variables $G(x_1),\ldots,G(x_k)$. (Note that each factor $P_1\big(G(x_1),\ldots,G(x_k)\big)$ appears exactly once in the factorization of (5.2).)

Corollary 5.1. *For the case $s|r$ and $s\nmid e_i$ for at least one $i$, $1\leqslant i\leqslant t$, of Theorem 5.1, if $\{a_1,\ldots,a_k\}$ are linearly independent over $W$, the vector space of roots of $G(x)=0$, then $Q\big(L(x_1),\ldots,L(x_k)\big)$ is the product of $q^{r-jk}$ absolute irreducibles of degree $q^{j(k-1)}$.*

Proof. Under the hypothesis of linear independence over $W$, (5.1) has only the trivial solution $(c_1,\ldots,c_k)=(0,\ldots,0)$. Consequently the cardinality of the vector space $V$ of solutions of (5.1) is 1, and therefore $|W\cap V|=q^u=1$ (see Lemma 2.6). We conclude that $u=0$.

Remark. In Theorems 4.1, 4.3, 4.5, and 4.6, $G(x)=x^q-x$. Thus the hypothesis of linear independence of the $a_i$ over $\mathrm{GF}(q)$ in these theorems insures that $u=0$.



In general, $u$ is a function of $r$, $s$, $k$, and the degree of linear dependence of $\{a_1,\ldots,a_k\}$ over $W$. Thus it does not appear convenient to give an algorithm for computing $u$. The following example shows that values of $u>0$ can be obtained.

Example 5.1. Let $\theta$ be a root of $x^9+x+1$, an irreducible of degree 9 over $\mathrm{GF}(2)$, so that $\theta$ generates $\mathrm{GF}(2^9)$. Let $\beta$ be a root of $x^3+x+1$, an irreducible of degree 3 over $\mathrm{GF}(2)$; $\beta$ generates $\mathrm{GF}(2^3)$. Let $Q(x_1,x_2)=\theta x_1+\beta\theta x_2+1$. Let $L(x)=x^{2^6}+x^{2^3}+x$ with corresponding ordinary polynomial $l(x)=x^6+x^3+1$. Here $k=2$, $r=9$, $g(x)=x^3-1$, $j=3$, and $G(x)=x^{2^3}-x$. Since $s=[\deg\theta,\deg\beta\theta]=9$, we have $s|r$. But $s$ does not divide $e_1=6$ and $e_2=3$. The vector space $W$ of roots of $G(x)$ is $\mathrm{GF}(8)$. Since $\theta c_1+\beta\theta c_2=0$ implies $c_1=-\beta c_2$, each element $c_2$ of $\mathrm{GF}(8)$ determines a $c_1\in\mathrm{GF}(8)$. Hence $\theta c_1+\beta\theta c_2=0$ has $2^3$ solutions $\{(c_1,c_2)\}$ where $c_1$ and $c_2$ are roots of $G(x)=0$. We have $u=3$ and $Q\big(L(x_1),L(x_2)\big)$ factors into $q^{r-jk+u}=2^6$ absolute irreducibles of degree $q^{j(k-1)-u}=1$.

We observe that the polynomial can be written

$$Q\big(L(x_1),L(x_2)\big)=\theta X^{2^6}+\theta X^{2^3}+\theta X+1\tag{5.5}$$

where $X=x_1+\beta x_2$. Since (5.5) is a polynomial in the single variable $X$ it is the product of (absolutely irreducible) first degree factors in $x_1$ and $x_2$.

Corollary 5.2. *If $L(x)=x^{q^{r-1}}+x^{q^{r-2}}+\ldots+x^q+x$ has corresponding ordinary polynomial $l(x)$ with exponent $r$ in Theorem 5.1 and $s|r$, then $Q\big(L(x_1),\ldots,L(x_k)\big)$ is the product of $q^{r-k}$ absolute irreducibles of degree $q^{k-1}$.*

Remark. Note that Corollary 5.2 is the same as Theorem 4.5.

Proof. Since $G(x)=x^q-x$, the coefficients $a_1,\ldots,a_k$ of $Q(x_1,\ldots,x_k)$ are linearly independent over $W$, the vector space of roots of $G(x)=0$, by the hypothesis that $\{a_1,\ldots,a_k\}$ are linearly independent over $\mathrm{GF}(q)$. If $s=1$, this hypothesis insures that $k=1$ and we have $q^{r-1}$ first degree factors of $Q\big(L(x_1),\ldots,L(x_k)\big)$.

If $s>1$, then $s\nmid e_1=1$ since the term $x^q$ appears in $L(x)$. Consequently Corollary 5.1 is satisfied with $j=1$, and we have $q^{r-k}$ absolute irreducibles of degree $q^{k-1}$.

## References


[1] J. W. S. Cassels, *Factorization of polynomials in several variables*, Proceedings of the 15th Scandinavian Congress, Springer Lecture Notes in Mathematics No. 118, 1970, pp. 1–17.

[2] Andrew F. Long, *A theorem on factorable irreducible polynomials in several vari-*

*ables over a finite field with the substitution $x_i^{q^r} - x_i$ for $x_i$*, Math. Nachr. 63 (1974), pp. 123–130.

[3] Andrew F. Long, *Classification of irreducible factorable polynomials over a finite field*, Acta Arith. 12 (1967), pp. 301–313.

[4] Andrew F. Long and Theresa P. Vaughan, *Factorization of $Q(h(T)(x))$ over a finite field where $Q(x)$ is irreducible and $h(T)(x)$ is linear I*, Linear Algebra and Appl. 13 (1976), pp. 207–221.

[5] — — *Factorization of $Q(h(T)(x))$ over a finite field where $Q(x)$ is irreducible and $h(T)(x)$ is linear II*, ibid. 11 (1975), pp. 53–72.

[6] Oystein Ore, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc. 36 (1934), pp. 243–274.

DUKE UNIVERSITY
Durham, North Carolina
UNIVERSITY OF NORTH CAROLINA
Greensboro, North Carolina

*Received on 12. 11. 1975* (793)



| Les volumes IV et suivants sont à obtenir chez | Volumes from IV on are available at | Die Bände IV und folgende sind zu beziehen durch | Томы IV и следующие можно получить через |
|---|---|---|---|

Ars Polona, Krakowskie Przedmieście 7, 00-068 Warszawa

| Les volumes I–III sont à obtenir chez | Volumes I–III are available at | Die Bände I–III sind zu beziehen durch | Томы I–III можно получить через |
|---|---|---|---|

Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y.

## BOOKS PUBLISHED BY THE POLISH ACADEMY OF SCIENCES INSTITUTE OF MATHEMATICS

S. Banach, Oeuvres, vol. I, 1967, p. 381.
S. Mazurkiewicz, Travaux de topologie et ses applications, 1969, p. 380.
W. Sierpiński, Oeuvres choisies, vol. I, 1974, 360 pp.; vol. II, 1975, 780 pp.; vol. III, 1976, 688 pp.

### MONOGRAFIE MATEMATYCZNE

41. H. Rasiowa and R. Sikorski, The mathematics of metamathematics, 3 rd ed., revised, 1970, 520 pp.
43. J. Szarski, Differential inequalities, 2nd ed., 1967, 256 pp.
44. K. Borsuk, Theory of retracts, 1967, 251 pp.
45. K. Maurin, Methods of Hilbert spaces, 2nd ed., 1972, 552 pp.
50. K. Borsuk, Multidimensional analytic geometry, 1969, 443 pp.
51. R. Sikorski, Advanced calculus. Functions of several variables, 1969, 460 pp.
52. W. Ślebodziński, Exterior forms and their applications, 1970, 427 pp.
53. M. Krzyżański, Partial differential equations of second order I, 1971, 562 pp.
54. M. Krzyżański, Partial differential equations of second order II, 1971, 407 pp.
57. W. Narkiewicz, Elementary and analytic theory of algebraic numbers, 1974, 630 pp.
58. C. Bessaga and A. Pełczyński, Selected topics in infinite-dimensional topology, 1975, 353 pp.
59. K. Borsuk, Theory of shape, 1975, 379 pp.
60. R. Engelking, General topology, in print.

**New series**

### BANACH CENTER PUBLICATIONS

Vol. 1. Mathematical control theory, 1976, p. 166.
Vol. 2. Mathematical foundations of computer science, in print.
Vol. 3. Mathematical models and numerical methods, in preparation.
Vol. 4. Approximation theory, in preparation.