FACTORIZATION OF TRINOMIALS OVER GALOIS FIELDS OF CHARACTERISTIC 2

UZI VISHNE

Abstract. We study the parity of the number of irreducible factors of trinomials over Galois fields of characteristic 2. As a consequence, some sufficient conditions for a trinomial being reducible are obtained. For example, $x^n + ax^k + b \in GF(2^t)[x]$ is reducible if both n, t are even, except possibly when $n = 2k$, k odd.

The case $t = 1$ was treated by R.G.Swan [10], who showed that $x^n + x^k + 1$ is reducible over $GF(2)$ if $8|n$.

Appeared in *Finite Fields and their applications*, **3**(4), (1997).

1. Introduction

Trinomials are polynomials of the form $x^n + ax^k + b$ $(n > k)$. They have applications in the theory of finite fields (*e.g.* [1]), in coding theory (*e.g.* [2, Chap. 6]) and in cryptography (*e.g.* [6]). Many tables of factorizations of trinomials and of irreducible trinomials were published (*e.g.* [6], [12], and the recent [3]), apparently all of them over $GF(2)$.

Using an old result of Stickelberger (see 2.2 below), Swan [10] proves that all trinomials over $GF(2)$, with degree divisible by 8, have an even number of factors, and are thus reducible.

In this paper we use Swan's computation of the discriminant of a trinomial, together with some facts about local fields, to prove

Corollary 5.1. *Let K be an even-dimensional extension of $GF(2)$. Then any trinomial of even degree over K is reducible, except possibly for $x^{2d} + ax^d + b$ $(a, b \in K)$ when $t^2 + at + b$ have no roots in K.*

In particular, the only primitive trinomials over even-dimensional K are of degree 2.

This result is part of a full description of the parity of the number of irreducible factors of a trinomial over finite extension of $GF(2)$, given in 3.4, 4.1 and 4.2.

Date: November 24, 1996. *Revised version:* June 29, 1997.

The author would like to thank Ido Efrat for some very helpful remarks.

The background material is given in the next section. In section 3 we handle all but some exceptional types of trinomials, and give the exact condition for the number of factors to be even (theorem 3.4). In section 4 we reduce the treatment of the exceptional types to questions about the reducibility of certain quadratic polynomials. Some corollaries and applications are given in section 5.

2. Preliminaries

In this section we present Stickelberger's theorem about the number of irreducible factors of a polynomial. We quote the characterization of unramified extensions of the 2-adic field $\mathbb{Q}_2$ and derive one result for future use. We also give Swan's formula for the discriminant of a trinomial.

Let $\upsilon : K \to \mathbb{Z}$ be a discrete valuation, $R = R_\upsilon$ the valuation ring, and $I = I_\upsilon$ the valuation ideal. $\bar{K} = R/I$ is the *residue class field* of K. The natural projection $R \to \bar{K}$ is denoted by $a \mapsto \bar{a}$.

We assume henceforth that K is a completion of an algebraic number filed. In particular K is *local*, *i.e.* complete in the metric induced by υ and $\bar{K}$ is finite.

The recognition of squares in R can be done mod $4I$:

Lemma 2.1 (*e.g.* [10, lemma 1])**.** *Let $a \in R$, $a \notin I$. Then a is a square in K iff it is a square* mod $4I$*.*

This result holds for any local field.

Let $f(x) \in K[x]$ be a monic polynomial of degree n. If $f(x) = (x-\eta_1)...(x-\eta_n)$ is split in an extension field L of K, we define the *discriminant* of f to be $D(f) = (-1)^{\binom{n}{2}} \prod_{i \neq j} (\eta_i - \eta_j) \in K$.

Let $\Delta(f) = \prod_{i<j}(\eta_i - \eta_j) \in L$. Obviously $D(f) = \Delta(f)^2$, so $D(f)$ is a square in L. This raises a natural question, when is $D(f)$ a square in K.

Assume $f(x)$ has integral coefficients, and $\bar{f}$ has no repeated roots. Then $D(f) \in R$ and $\overline{D(f)} = D(\bar{f}) \neq 0$. Let r be the number of irreducible factors of $\bar{f}$ (over $\bar{K}$).

The parity of r was related to $D(f)$ by Stickelberger, who proved the following:

Theorem 2.2 (Stickelberger [9], also [10] or [5])**.** $r \equiv n \pmod 2$ *iff $D(f)$ is a square in K.*

Another formulation, replacing squares in K with traces over finite extensions, is given in [2].

Recall that an extension K of the 2-adic field $\mathbb{Q}_2$ is *unramified* if $[K : \mathbb{Q}_2] = [\bar{K} : \bar{\mathbb{Q}}_2]$. The following is a consequence of Hensel's lemma.

Theorem 2.3 (*e.g.* [11])**.** *For every n, there exist a unique unramified extension $K \supseteq \mathbb{Q}_2$ of dimension n. In fact, K is the splitting field of $x^{2^n} - x$, and the extension is cyclic.*

Corollary 2.4. *Suppose K is a finite dimensional unramified extension of $\mathbb{Q}_2$.*

Then $\sqrt{5} \in K$ iff $[K : \mathbb{Q}_2]$ is even.

Proof. Let K_0 denote the unique unramfieid quadratic extension of $\mathbb{Q}_2$. Then $K_0 \subseteq K$ iff $[K : \mathbb{Q}_2]$ is even.

K_0 is the splitting field of $x^4 - x = x(x-1)(x^2+x+1)$, and is thus equal to $\mathbb{Q}_2[\sqrt{-3}]$. By 2.1 $\sqrt{-15} \in \mathbb{Q}_2$, so $K_0 = \mathbb{Q}_2[\sqrt{5}]$. □

The setup in this paper is that we are given a trinomial $\bar{f}$ over a finite field $\bar{K}$, and we have to appropriately choose K and f in order to apply theorem 2.2. Fix the following notation.

Notation 2.5. *$\bar{K}$ is a finite field of characteristic 2. $g(x) = x^n + \bar{a}x^k + \bar{b} \in \bar{K}[x]$ is a trinomial, $\bar{a}, \bar{b}$ are arbitrary nonzero elements of $\bar{K}$.*

r is the number of irreducible factors of $g(x)$ over $\bar{K}$.

Let K be the (unique) unramified extension of $\mathbb{Q}_2$ of degree $[\bar{K} : GF(2)]$. $R, I, \bar{K}$ are the valuation ring, valuation ideal and the residue class field of K, respectively. 2 is a prime in the valuation ring $\mathbb{Z}_2$ of $\mathbb{Q}_2$, and it remains a prime in R. Thus $I = 2R$.

Let $f(x) = x^n + ax^k + b \in K[x]$ be a lift of $g(x)$: $\bar{f}(x) = g(x)$.

Our aim is to ascertain $r \pmod 2$. If n, k are both even then g is a square, since the homomorphism $\bar{K}^\times \mapsto \bar{K}^\times$ of exponentiation by 2 is an isomorphism. In this case r is always even, so we may ignore it.

The trinomials $g(x) = x^n + \bar{a}x^k + \bar{b}$ and $g_1(x) = x^n + \bar{a}\bar{b}^{-1}x^{n-k} + \bar{b}^{-1}$ have the same number of factors via the substitution $x \mapsto x^{-1}$. Thus, replacing k by $n-k$ if necessary, we may assume that exactly one of n, k is even.

Let $d = (n,k)$, $n = dn_1$, $k = dk_1$. Note that d is odd.

We register the four cases concerning the constants n, k.

Case (a): n is even, k is odd, $n \neq 2k$.

Case (a^*): k is odd, $n = 2k$.

Case (b): n is odd, k is even, $k \not| 2n$.

Case (b^*): n is odd, k is even, $k | 2n$.

To prove his results about trinomials, Swan computes the discriminant of a trinomial in general:

Theorem 2.6 (Swan, [10, Theorem 2])**.** *Let $n > k > 0$, $d = (n,k)$, and $n = dn_1$, $k = dk_1$. Let $a, b \in K$. Then $D(x^n + ax^k + b)$ equals*

$$(-1)^{\binom{n}{2}} b^{k-1} (n^{n_1} b^{n_1-k_1} - (-1)^{n_1} k^{k_1} (n-k)^{n_1-k_1} a^{n_1})^d.$$

Example 2.7. *$D(x^2 + ax + b) = a^2 - 4b$, so $x^2 + \bar{a}x + \bar{b}$ factors over $\bar{K}$ iff $a^2 - 4b$ is a square in K.*

3. The cases (a) and (b)

In this section we treat cases (a) and (b). Cases (a^*) and (b^*) are treated in the next section.

In the following two lemmas we study $D(f)$ mod $4I$, *i.e.* mod $8R$.

Lemma 3.1. *$D(f)$ satisfies:*

- *In case (a): $D(f) \equiv (-1)^{\binom{n+1}{2}+1} k^k (n-k)^{n-k} b^{k-1} a^n \pmod{8R}$.*
- *In case (b): $D(f) \equiv (-1)^{\binom{n}{2}} b^{n-1} n^n \pmod{8R}$.*

In particular $D(\bar{f}) \neq 0$.

Proof. $D(f)$ is given in theorem 2.6.

Assume case (a) holds. $n_1 > k_1$ so $n_1 \geq 2$, but $n_1 \neq 2$ for $n \neq 2k$. Now $n \equiv 0 \pmod{2R}$, so we have $n^3 \equiv 0 \pmod{8R}$, and $n^{n_1} \equiv 0 \pmod{8R}$ too.

Assume case (b) holds. $k_1 \neq 1$ since k does not divide n, and also $k_1 \neq 2$ by the assumption. Thus $k_1 \geq 3$ and the previous argument shows that $k^{k_1} \equiv 0 \pmod{8R}$. The result follows. □

Next, we show that for $D(f)$ to be a square in K depends on n and k only.

Lemma 3.2. *$D(f)$ is a square in K iff:*

- *In case (a): $(-1)^{\frac{n}{2}+1} k(n-k)$ is a square.*
- *In case (b): $(-1)^{\frac{n-1}{2}} n$ is a square.*

Proof. By 2.1 it is enough to compute mod $8R$. Using the formulas of 3.1 we have in case (a),

$D(f) \equiv (-1)^{\binom{n+1}{2}+1} k^k (n-k)^{n-k} b^{k-1} a^n = (-1)^{\binom{n+1}{2}+1} k(n-k) u^2$ for some $u \in R$ since $k-1, n$ are even. In case (b), $D(f) \equiv (-1)^{\binom{n}{2}} b^{n-1} n^n = (-1)^{\binom{n}{2}} n u^2$ for $n-1$ is even. □

Note that by a theorem of Stickelberger [11, 4-8-19], $D(f)$ is always a square mod $4R$.

The following is a generalization of [10, corollary 5] (for the cases (a) and (b)).

Theorem 3.3. *Assume one of* (a),(b) *holds.*
Then $r \equiv n \pmod 2$ *if and only if*
1. $[\bar{K} : GF(2)]$ *is even,* **or**
2. $n \equiv 0, 1, -1 \pmod 8$*,* **or**
3. $n \equiv 2, 6 \pmod 8$ *and* $2k \equiv n \pmod 8$*.*

Proof. We use 3.2 to test if $D(f)$ is a square in K. Note that the test value given in 3.2 is always 1 or 5 mod $8R$. When it is 1 $D(f)$ is a square, and when it is 5 $D(f)$ is a square iff $[\bar{K} : GF(2)]$ is even, by 2.4. The result follows from 2.2. □

Note that $n - r \pmod{2}$ is independent of $\bar{a}$ and $\bar{b}$. Furthermore, extending the field $\bar{K}$, as long as the dimension *was* even or *remains* odd, does not change the parity of r. If $n \equiv \pm 3 \pmod 8$ and $[\bar{K} : GF(2)]$ is odd then r is even, so there is some irreducible factor of even degree. Such factors are made reducible by an even-dimensional extension of $\bar{K}$, and r becomes odd.

Checking all possible values of $n \mod 8$, we get another formulation, with emphasis on the property $r \equiv 0 \pmod 2$:

Theorem 3.4. *Assume* $n \neq 2k$ *and (if* n *is odd)* $k \not| 2n$*.*
$r \equiv 0 \pmod 2$ *if and only if*
1. $n \equiv 0 \pmod 8$ **or**
2. $n \equiv 2, 4, 6 \pmod 8$ *and* $[\bar{K} : GF(2)]$ *is even,* **or**
3. $n \equiv 3, 5 \pmod 8$ *and* $[\bar{K} : GF(2)]$ *is odd,* **or**
4. $n \equiv 2, 6 \pmod 8$ *and* $2k \equiv n \pmod 8$*.*

In all the above cases the polynomial is reducible.

4. The cases (a^*) and (b^*)

This section handles the special cases (a^*),(b^*). We reduce the determination of $r \bmod 2$ in these cases to questions about quadratic polynomials over $\bar{K}$.

Lemma 4.1 (case (a^*))**.** *Let* d *be odd.* $x^{2d} + \bar{a}x^d + \bar{b}$ *has an even number of irreducible factors iff* $t^2 + \bar{a}t + \bar{b}$ *factors over* $\bar{K}$*.*

Proof. By Swan's formula $D(x^{2d} + ax^d + b) = -b^{d-1}d^{2d}(4b - a^2)^d$, which is a square in K iff $a^2 - 4b$ is.

By 2.7, $a^2 - 4b$ is a square iff $t^2 + \bar{a}t + \bar{b}$ factors. □

Assume n is odd, k even, $k|2n$. Denote $h(t) = t^2+t+a^{\frac{2n}{k}}b^{2-\frac{2n}{k}} \in K[t]$.

Lemma 4.2 (case (b^*))**.** *The number r of irreducible factors of $g(x) = x^n + \bar{a}x^k + \bar{b}$ over $\bar{K}$ is odd iff*

1. $[\bar{K} : GF(2)]$ is even or $n \equiv 1, 7 \pmod 8$, and $\bar{h}(t)$ factors over $\bar{K}$, **or**

2. $[\bar{K} : GF(2)]$ is odd, $n \equiv 3, 5 \pmod 8$, and $\bar{h}(t)$ does not factor over $\bar{K}$.

Proof. The discriminant of $h(t)$ is $D(h) = 1 - 4a^{\frac{2n}{k}}b^{2-\frac{2n}{k}}$. By Swan's formula $D(x^n+ax^k+b) \equiv (-1)^{\frac{n-1}{2}}nD(h)u^2 \pmod{8R}$ for some $u \in R$.

In the first case $(-1)^{\frac{n-1}{2}}n$ is a square in K (use 2.4), so $D(f)$ is a square iff $D(h)$ is.

In the second case $(-1)^{\frac{n-1}{2}}n \equiv 5 \pmod 8$ is not a square. If $h(t)$ factors than $D(h)$ is a square so $D(f)$ is not. If $h(t)$ does not factor then $K[\sqrt{D(h)}] \cong K[t]/ < h(t) >$ is an unramified extension of K (since $\bar{h}$ has two different roots over $\bar{K}$) so it equals $K[\sqrt{5}]$ by uniqueness (2.4), and we see that $D(f)$ is a square. □

5. Summary and applications

We collect the data from the previous sections to formulate some corollaries about trinomials over even-dimensional extensions of $GF(2)$. For the sake of notational simplicity, we omit the bars from the field letter K and the constants.

Let K be a Galois field over $GF(2)$. Let $0 \neq a, b \in K$, and assume $g(x) = x^n + ax^k + b$ is not a square (*i.e.* n and k are not both even).

From theorem 3.4 and lemma 4.1 we get

Corollary 5.1. *If $[K : GF(2)]$ and n are both even, then $g(x)$ has an odd number of factors in only one case, namely, when $g(x) = x^{2d} + ax^d + b$ and $t^2 + at + b$ has no roots in K.*

Especially, $g(x)$ is reducible except possibly in this case.

If $g(x)$ is irreducible over K, the order of a root α in the multiplicative group of the splitting field $K[\alpha]$ of $g(x)$ is called the *exponent* of g. A polynomial with maximal possible exponent, *i.e.* $|K|^{deg(g)} - 1$, is called *primitive.*

Corollary 5.2. *If $[K : GF(2)]$ is even, the only primitive trinomials of even degree over K are of the form $x^2 + ax + b$.*

Proof. By 5.1, the only candidate is $g(x) = x^{2d}+ax^d+b$. Assume $d > 1$. Let β be a root of $g(x)$, and $\alpha = \beta^d$. Then α is a root of $t^2 + at + b$, α

belongs to the extension of degree 2 of K. Thus the order of α in $K[\alpha]^{\times}$ divides $|K|^2-1$, and the order of β divides $d(|K|^2-1) < |K|^{2d}-1$. □

Primitive trinomials of the form x^2+ax+b *do* exist: let K' be the extension of degree 2 of K, and let $u \in K'$ be a generator of $K'^{\times}$. Then $g(x) = x^2 + (u+u^{|K|})x + u^{1+|K|} \in K[x]$ is primitive. This is the only way to get a primitive quadratic polynomial.

From 3.4 and 4.2 we get another corollary:

Corollary 5.3. *Suppose $[K : GF(2)]$ is even. Only two types of odd-degree trinomials have an even number of factors, namely:*

1. $g(x) = x^n + ax^k + b$, $2|k|2n$, if $t^2+t+a^{\frac{2n}{k}}b^{2-\frac{2n}{k}}$ has no roots in K.

2. $g(x) = x^n + ax^k + b$, $(n-k)|n$, if $t^2+t+a^{\frac{2n}{k}}b^{-2}$ has no roots in K.

Since there has been some interest in the number of solutions of trinomials of small degree, we demonstrate how our results can refine old results on these questions.

Cazacu and Simovici [4] discuss the number of solutions of x^4+ax+a over a finite extension K of $GF(2)$. They give exact criterion for the number of solutions to be 1 or 2. Combined with their results, we can formulate

Corollary 5.4. *Let A be the multiset of degrees of the irreducible factors of $g(x) = x^4+ax+a$ over K.*
1. Assume $[K : GF(2)]$ is even. If $a^{\frac{|K|-1}{3}} = 1$, g splits or $A = \{2,2\}$; otherwise, $A = \{3,1\}$.
2. Assume $[K : GF(2)]$ is odd. Then g is irreducible or $A = \{2,1,1\}$. (See [4, Theorem 2] *for details).*

References

[1] A.A. Albert, On Certain Trinomial Equations in Finite Fields, *Ann. of Math.* **66**, (1957), 170-178.

[2] E. Berlekamp, "Algebraic Coding Theory", McGraw-Hill, New-York, 1968.

[3] I.F.Blake, S.Gao and R.L.Lambert, Constructive Problems for Irreducible Polynomials Over Finite Fields, *Information Theory and Applications* (A.Gulliver and N.Secord, eds.) LNCS **793**, Springer-Verlag, (1994), 1-23.

[4] C. Cazacu and D. Simovici, A New Approach of some Problems Concerning Polynomials Over Finite Fields, *Information and Control* **22**, (1973), 503-511.

[5] K. Dalen, On a theorem of Stickelberger, *Math. Scand.* **3**, (1955), 124-126.

[6] S.W. Golomb, “Shift Register Sequences”, Holden-Day Inc., San Francisco, 1967.

[7] R. Lidl and H. Niederreiter, “Finite Fields”, Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge Univ. Press, 1983.

[8] E. Selmer, On the Irreducibility of Certain Trinomials, *Math. Scandinavica,* **4**, (1956), 287-302.

[9] L. Stickelberger, Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, *Verh.* **1** *Internat. Math. Kongresses,* Zurich 1897, Leipzig (1898), 182-193.

[10] R.G. Swan, Factorization of Polynomials Over Finite Fields, *Pacific J. of Math,* **12**(2), (1962), 1099-1106.

[11] E. Weiss, “Algebraic Number Theory”, McGraw-Hill, New-York, 1963.

[12] N. Zierler and J. Brillhart, On Primitive Trinomials (mod 2) II, *Information and Control* **14**, (1969), 566-569.

Department of Mathematics, Bar-Ilan University, 52900 Ramat-Gan, ISRAEL

E-mail address: vishne@macs.biu.ac.il