FACTORIZATION OF POLYNOMIALS OVER FINITE FIELDS

RICHARD G. SWAN

Dickson [1, Ch. V, Th. 38] has given an interesting necessary condition for a polynomial over a finite field of odd characteristic to be irreducible. In Theorem 1 below, I will give a generalization of this result which can also be applied to fields of characteristic 2. It also applies to reducible polynomials and gives the number of irreducible factors mod 2.

Applying the theorem to the polynomial $x^p - 1$ gives a simple proof of the quadratic reciprocity theorem. Since there is some interest in trinomial equations over finite fields, e.g. [2], [4], I will also apply the theorem to trinomials and so determine the parity of the number of irreducible factors.

1. The discriminant. If $f(x)$ is a polynomial over a field F, the discriminant of $f(x)$ is defined to be $D(f) = \delta(f)^2$ with

$$\delta(f) = \prod_{i<j}(a_i - \alpha_j)$$

where $\alpha_1, \cdots, \alpha_n$ are the roots of $f(x)$ (counted with multiplicity) in some extension field of F. Clearly $D(f) = 0$ if f has any repeated root. Since $D(f)$ is a symmetric function in the roots of f, $D(f) \in F$.

An alternative formula for $D(f)$ which is sometimes useful may be obtained as follows:

$$D(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = (-1)^{n(n-1)/2}\prod_{i\neq j}(\alpha_i - \alpha_j) = (-1)^{n(n-1)/2}\prod_i f'(\alpha_i)$$

where n is the degree of $f(x)$ and $f'(x)$ the derivative of $f(x)$. In § 4, I will give still another way to calculate $D(f)$.

If $f(x)$ is monic with integral coefficients in some $\mathfrak{p}$-adic or algebraic number field, all α_i are integral and so $D(f)$ is integral. Consider the expression

$$\delta_1 = \prod_{i<j}(\alpha_i + \alpha_j)\ .$$

This is integral and lies in F, being a symmetric function of the roots. Clearly $\delta(f) = \delta_1 + 2\delta_2$ where δ_2 is integral. Thus $D(f) = \delta(f)^2 \equiv \delta_1^2 \bmod 4$, so $D(f)$ is congruent to a square in F mod 4. This is a special case of a well-known theorem of Stickelberger [3, Ch. 10, Sec. 3].

Received November 15, 1961. The author is an Alfred P. Sloan Fellow.

Added in Proof. I have recently discovered that Theorem 1 of this paper is due to L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verh. 1 Internat. Math. Kongresses, Zurich 1897, Leipzig 1898, 182-193. A simplified proof, essentially the same as mine, was given by K. Dalen, *On a theorem of Stickelberger*, Math. Scand. **3** (1955), 124-126.

The applications of the theorem, however, seem to be new.

Suppose $f(x)$ is monic with integral coefficients in a $\mathfrak{p}$-adic field F. I will denote by $\bar{f}(x)$ the polynomial over the residue class field obtained by reducing all coefficients of F mod $\mathfrak{p}$. In some extension field of F we have $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$. Therefore $\bar{f}(x) = (x - \bar{\alpha}_1) \cdots (x - \bar{\alpha}_n)$ where $\bar{\alpha}_i$ is α_i reduced modulo the (unique) extension of $\mathfrak{p}$. It follows that $D(\bar{f})$ is $D(f)$ reduced mod $\mathfrak{p}$. In particular, if $\bar{f}(x)$ has no repeated root, $D(\bar{f}) \neq 0$ and so $D(f)$ is prime to $\mathfrak{p}$.

2. The main theorem. If $f(x)$ is a monic polynomial with integral coefficients in a $\mathfrak{p}$-adic field, I will again denote by $\bar{f}(x)$ the result of reducing the coefficients of $f(x)$ mod $\mathfrak{p}$.

THEOREM 1. *Let $f(x)$ be a monic polynomial of degree n with integral coefficients in a $\mathfrak{p}$-adic field F. Assume that $\bar{f}(x)$ has no repeated roots. Let r be the number of irreducible factors of $\bar{f}(x)$ over the residue class field. Then $r \equiv n \bmod 2$ if and only if $D(f)$ is a square in F.*

Proof. Over the residue class field K we can factor $\bar{f}(x) = \bar{f}_1(x) \cdots \bar{f}_r(x)$. Since the $\bar{f}_i(x)$ are relatively prime, Hensel's lemma shows that there is a corresponding factorization $f(x) = f_1(x) \cdots f_r(r)$ over F where $\bar{f}_i(x)$ is $f_i(x)$ mod $\mathfrak{p}$. Since $\bar{f}_i(x)$ is irreducible over K, $f_i(x)$ is irreducible over F. Since $\bar{f}_i(x)$ has no repeated root, $D(f_i)$ is prime to $\mathfrak{p}$. Therefore the field E_i obtained by adjoining a root of $f_i(x)$ to F is unramified over F. Since there is only one unramified extension of F of any given degree and that extension is cyclic, E_i is cyclic over F and thus is the splitting field of f_i. The splitting field E of $f(x)$ is the composite of all the E_i and therefore is unramified over F. Thus E/F is a cyclic extension. (A more elementary proof of this was pointed out by W. Feit. Let m be the least common multiple of the degrees of the $f_i(x)$. It is easy to construct a cyclic unramified extension E_1/F of degree m by adjoining a root of unity to F. Now $\bar{f}(x)$ splits completely over the residue class field K_1 of E_1 since the degree n_i of every irreducible factor of $\bar{f}(x)$ divides $m = [E_1 : F]$. By Hensel's lemma, $f(x)$ splits completely over E_1 so $E \subset E_1$.)

Let σ generate the galois group of E/F. Let β_j be a root of $f_j(x)$. Then the roots to $f_j(x)$ are given by $\sigma^i(\beta_j)$ for $0 \leqq i \leqq n_j - 1$ where n_j is the degree of $f_j(x)$. Thus the roots of $f(x)$ are $\sigma^i(\beta_j)$ for $j = 1, \cdots, n$, $i = 0, \cdots, n_j - 1$. These can be ordered by defining $(i_1, j_1) < (i_2, j_2)$ if $j_1 < j_2$ or if $j_1 = j_2$ and $i_1 < i_2$. For any i, the symbol (i, j) will be interpreted to mean (i', j) where $i' \equiv i \bmod n_j$, $0 \leqq i' \leqq n_j - 1$.

Now $D(f) = \delta(f)^2$ where

$$\delta(f) = \prod_{(i_1, j_1) < (i_2, j_2)} (\sigma^{i_1}\beta_{j_1} - \sigma^{i_2}\beta_{j_2}).$$

If we apply σ to $\delta(f)$, we get

$$\sigma\delta(f) = \prod_{(i_1\ j_1)<(i_2, j_2)} (\sigma^{i_1+1}\beta_{j_1} - \sigma^{i_2+1}\beta_{j_2}) .$$

The terms occurring in this product are the same as those in $\delta(f)$ except for sign. The term $\sigma^{i_1+1}\beta_{j_1} - \sigma^{i_2+1}\beta_{j_2}$ occurs in $\delta(f)$ and $\sigma\delta(f)$ with the same sign if and only if $(i_1 + 1, j_1) < (i_2 + 1, j_2)$. This is certainly the case if $j_1 < j_2$ or if $j_1 = j_2 = j$ and $i_2 < n_j - 1$. However, if $j_1 = j_2 = j$ and $i_2 = n_j - 1$, then $(i_2 + 1, j) = (0, j) < (i_1 + 1, j)$. Therefore the total number of terms which occur with different signs in $\delta(f)$ and $\sigma\delta(f)$ is equal to the number of pairs $((i_1, j), (n_j - 1, j))$ where $0 \leqq i_1 \leqq n_j - 2$. There are $n_j - 1$ such pairs for each j. The total number is given by

$$\sum_j (n_j - 1) = n - r .$$

This shows that $\sigma\delta(f) = (-1)^{n-r}\delta(f)$. Now $D(f)$ is a square in F if and only if $\delta(f) \in F$, which is the case if and only if $\sigma\delta(f) = \delta(f)$. Therefore $D(f)$ is a square in F if and only if $n \equiv r \bmod 2$.

COROLLARY 1. *Let K be a finite field of odd characteristic. Let $g(x)$ be a polynomial over K of degree n with no repeated root. Let r be the number of irreducible factors of $g(x)$ over K. Then $r \equiv n \bmod 2$ if and only if $D(g)$ is a square in K.*

Proof. We can assume that $g(x)$ is monic. Let F be a $\mathfrak{p}$-adic field with residue class field K. Let $f(x)$ be a monic polynomial over F with integral coefficients such that $\bar{f}(x) = g(x)$. Then $D(g)$ is $D(f)$ reduced mod $\mathfrak{p}$. Since $D(g) \neq 0$, $D(f)$ is a square in F if and only if $D(g)$ is a square in K. This follows immediately from Hensel's lemma applied to the polynomial $x^2 - D(f)$.

A more elementary proof of Corollary 1 can be obtained by repeating the proof of Theorem 1 using K in place of F.

If $f(x)$ is irreducible over K, $r = 1$ and so n is odd if and only if $D(f)$ is a square in K. This is the theorem of Dickson mentioned above.

If K has characteristic 2, the proof of Corollary 1 breaks down because $D(g)$ may be a square mod $\mathfrak{p}$ even though $D(f)$ is not a square. For example, 3 is a square mod 2 but not mod 8. In this case we need the following well-known result.

LEMMA 1. *Let a be a $\mathfrak{p}$-adic integer prime to $\mathfrak{p}$. Then a is a $\mathfrak{p}$-adic square if and only if a is a square* mod $4\mathfrak{p}$.

Proof. Suppose $a \equiv b_i^2 \bmod 4\mathfrak{p}^i$. Then $a = b_i^2 + 4c_i$ where $c_i \equiv 0$

mod $\mathfrak{p}^i$. Let $d_i = b_i^{-1}c_i$. Then $d_i \equiv 0 \mod \mathfrak{p}^i$ since b_i is prime to $\mathfrak{p}$, and $a = (b_i + 2d_i)^2 - 4d_i^2$. Let $b_{i+1} = b_i + 2d_i$. Then $a \equiv b_{i+1}^2 \mod 4\mathfrak{p}^{i+1}$ (in fact mod $4\mathfrak{p}^{2i}$). The b_i form a Cauchy sequence and $a = b^2$ where $b = \lim b_i$.

COROLLARY 2. *Let $f(x)$ be a monic polynomial of degree n with integral coefficients over a $\mathfrak{p}$-adic field F. Assume that $\bar{f}(x)$ has no repeated root. Let r be the number of irreducible factors of $\bar{f}(x)$ over the residue class field K of F. Then $r \equiv n \mod 2$ if and only if $D(f)$ is a square* mod $4\mathfrak{p}$.

This follows immediately from Theorem 1 and Lemma 1. In applying Corollary 2 we are usually given K and $\bar{f}(x)$ and choose any convenient F and $f(x)$. For example, in case $K = GF(2)$, we get

COROLLARY 3. *Let $g(x)$ be a polynomial of degree n over $GF(2)$ with no repeated root. Let r be the number of irreducible factors of $g(x)$ over $GF(2)$. Let $f(x)$ be any monic polynomial over the 2-adic integers such that $\bar{f}(x) = g(x)$. Then $r \equiv n \mod 2$ if and only if $D(f) \equiv 1 \mod 8$.*

This follows immediately from Corollary 2 and the fact that 1 is the only odd square mod 8. Note that $D(f) \equiv 1$ or $5 \mod 8$ by Stickelberger's theorem.

EXAMPLE. Let $f(x)$ be a polynomial of degree k over a finite field of characteristic 2 such that $f(0) \neq 0$. Let $g(x) = f(x)^8 + x^m$ where m is odd. Then $n = \deg g(x) = \max(8k, m)$. Choose an appropriate $\mathfrak{p}$-adic field and a polynomial $F(x)$ of degree k such that $f(x) = \bar{F}(x)$. Then $g(x) = \bar{G}(x)$ where $G(x) = F(x)^8 + x^m$. Now $G'(x) \equiv mx^{m-1} \mod 8$ so

$$D(G) \equiv (-1)^{n(n-1)/2} \prod m\alpha_i^{m-1} \pmod 8 .$$

Since $\Pi\alpha_i = (-1)^n G(0) \equiv f(0)^8 \not\equiv 0 \mod \mathfrak{p}$, $D(G) \not\equiv 0 \mod \mathfrak{p}$ so $g(x)$ has no repeated root. Since m is odd, $\Pi\alpha_i^{m-1}$ is a square. Thus $D(G)$ differs by a square factor from

$$D' = (-1)^{n(n-1)/2} m^n .$$

If $n = 8k$, D' is a square. Thus $r \equiv n \equiv 0 \mod 2$. Therefore $g(x)$ has an even number of factors and so is reducible. If $n = m$, D' differs by a square factor from $(-1)^{(m-1)/2}m$. If $m \equiv \pm 3 \mod 8$, $(-1)^{(m-1)/2}m \equiv 5$

mod 8 and so $r \not\equiv n \equiv 1 \bmod 2$. Therefore $g(x)$ is reducible if $m \equiv \pm 3 \bmod 8$.

In particular, $x^{8k} + x^m + 1$ is reducible mod 2 if $m < 8k$. If $m > 8k$ it is reducible if $m \equiv \pm 3 \bmod 8$.

3. Quadratic reciprocity. The discriminant of the polynomial $x^n + a$ over any field is given by

$$D(x^n + a) = (-1)^{n(n-1)/2} \prod n\alpha_i^{n-1} = (-1)^{n(n-1)/2} n^n a^{n-1}$$

because $\Pi\alpha_i = (-1)^n a$.

Consider in particular the polynomial $x^p - 1 = (x - 1)\Phi_p(x)$ where p is an odd prime. Its discriminant differs by a square factor from $(-1)^{(p-1)/2}p$. Therefore $x^p - 1$ has an odd number of factors over $GF(2)$ if and only if $p \equiv \pm 1 \bmod 8$. If $q \neq p$ is an odd prime, $x^p - 1$ has an odd number of factors over $GF(q)$ if and only if $(-1)^{(p-1)/2}p$ is a square mod q.

Now, if α is any root of $\Phi_p(x)$ over $GF(q)$, $q \neq p$, α is a primitive pth root of unity. Therefore $\alpha \in GF(q^n)$ if and only if $p \mid q^n - 1$. Thus the degree of α (and hence of any irreducible factor of $\Phi_p(x)$) over $GF(q)$ is the order n of q mod p. It follows that $x^p - 1$ has $1 + \varphi(p)/n$ factors over $GF(q)$.

Since the multiplicative group Z_p^* of integers mod p is cyclic, Z_p^* has a unique subgroup of index 2 which consists of all squares. Thus q is a square mod p if and only if it generates a subgroup of Z_p^* of even index. This index, however, is just $\varphi(p)/n$, so q is a square mod p if and only if $x^p - 1$ has an odd number of factors over $GF(q)$. Comparing this with the results obtained from Theorem 1, we get

$$\left(\frac{q}{p}\right) = \left(\frac{(-1)^{(p-1)/2}p}{q}\right) \text{ if } q \text{ is odd}$$

$$\left(\frac{2}{p}\right) = 1 \text{ if and only if } p \equiv \pm 1 \bmod 8 .$$

These equations, together with the trivial formula

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

constitute the quadratic reciprocity theorem.

4. Calculations. For the calculations made above, the discriminant could easily be found using the formula given in § 1. However, for more complicated polynomials this method of finding the discriminant is very inefficient. In this section I will give a simpler method based on

the Euclidean algorithm and use it to calculate the discriminant of any trinomial.

Let f and g be any polynomials over any field F. Let g have roots $\beta_1, \cdots, \beta_m$, (counted with multiplicity), and leading coefficient b. Let n be the degree of $f(x)$. Then the resultant of f and g is defined to be

$$R(f, g) = b^n \prod_{j=1}^{m} f(\beta_j) .$$

Clearly $R(f, g) \in F$ since it is a symmetric function in the roots of g. Comparing this definition with the formula for $D(f)$ given in § 1 shows that if f is monic

$$D(f) = (-1)^{n(n-1)/2} R(f', f) .$$

The following properties of $R(f, g)$ are presumably well known, but I will include them for completeness.

LEMMA 2. (1) $R(g, f) = (-1)^{\deg f \cdot \deg g} R(f, g)$

(2) *If* $f = gq + r$,

$$R(f, g) = b^{\deg f - \deg r} R(r, g)$$

where b *is the leading coefficient of* g.

(3) *If* a *and* b *are constants not both* 0, $R(a, b) = 1$.

(4) $R(f_1 f_2, g) = R(f_1, g) R(f_2, g)$.

The proof is trivial.

COROLLARY 4. (5) $R(f, g_1 g_2) = R(f, g_1) R(f, g_2)$

(6) *If* a *is contant,* $R(f, a) = a^{\deg f} = R(a, f)$

(7) $R(f, x^m) = R(f, x)^m = f(0)^m$.

It follows from properties (1), (2), and (3) of Lemma 2 that we can compute $R(f, g)$ by applying the Euclidean algorithm to f and g. This method of computation seems much easier in practice than the rather cumbersome determinant formula [5, Ch. 11, § 71, 72.].

In order to compute the discriminant of a trinomial, it is first necessary to compute the resultant of two binomials.

LEMMA 3. *Let* $d = (r, s)$ *be the greatest common divisor of* r *and* s. *Let* $r = dr_1$, $s = ds_1$. *Then* $R(x^r - \alpha, x^s - \beta) = (-1)^s [\alpha^{s_1} - \beta^{r_1}]^d$.

Proof. We first observe that if the result holds for a given pair (r, s) it holds for (s, r). This follows easily from Lemma 2 (1) using the fact $rs + s + d \equiv r \bmod 2$.

Since the result is trivial for $s = 0$, we can prove it by induction on $r + s$, assuming also $r \geqq s$ by the previous remark.

Now, dividing $x^r - \alpha$ by $x^s - \beta$ gives the remainder $\beta x^{r-s} - \alpha$. Thus we can apply Lemma 2 (2) and the result follows easily by induction.

It is now easy to find the discriminant of a trinomial over any field.

THEOREM 2. *Let $n > k > 0$. Let $d = (n, k)$ and $n = n_1 d$, $k = k_1 d$. Then*

$$D(x^n + ax^k + b) = (-1)^{n(n-1)/2} b^{k-1} [n^{n_1} b^{n_1 - k_1} + (-1)^{n_1+1} (n-k)^{n_1-k_1} k^{k_1} a^{n_1}]^d .$$

Proof. Consider the generic polynomial f of degree n, multiply out

$$D(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

and express the resulting symmetric functions as integral polynomials in the coefficients of f. This gives an expression for $D(f)$ as a specific integral polynomial in the coefficients of f and this expression is independent of the characteristic. In order to find the form of this polynomial, it is sufficient to do it in characteristic 0. For any polynomial f of degree n,

$$D(f) = (-1)^{n(n-1)/2} R(f', f) .$$

Therefore

$$\begin{aligned} D(x^n + ax^k + b) &= (-1)^{n(n-1)/2} R(nx^{n-1} + kax^{k-1}, x^n + ax^k + b) \\ &= (-1)^{n(n-1)/2} n^n b^{k-1} R(x^n + ax^k + b, x^{n-k} + n^{-1}ka) \end{aligned}$$

using Lemma 2 (1), (4) and Corollary 4 (7)

Now, dividing $x^n + ax^k + b$ by $x^{n-k} + n^{-1}ka$ leaves the remainder $a(1 - n^{-1}k)x^k + b$. Therefore the result follows from Lemma 2 (2) and Lemma 3.

As an application of Theorem 3, I will determine the parity of the number of factors of $x^n + x^k + 1$ over $GF(2)$.

COROLLARY 5. *Let $n > k > 0$. Assume exactly one of n, k is odd. Then $x^n + x^k + 1$ has an even number of factors (and hence is reducible) over $GF(2)$ in the following cases.*

(a) *n is even, k is odd, $n \neq 2k$ and $nk/2 \equiv 0$ or $1 \bmod 4$*

(b) *n is odd, k is even, $k \nmid 2n$, and $n \equiv \pm 3 \bmod 8$*

(c) *n is odd, k is even, $k \mid 2n$, and $n \equiv \pm 1 \bmod 8$*

In all other cases $x^n + x + 1$ has an odd number of factors over $GF(2)$.

The case where n and k are both odd can be reduced to the case k even by considering $x^n + x^{n-k} + 1$ which has the same number of irreducible factors as $x^n + x^k + 1$.

To prove Corollary 5 we regard $x^n + x^k + 1$ as a polynomial over the 2-adic integers, compute its discriminant by Theorem 2, and apply Corollary 3.

Note that the fact that some trinomial $x^n + x^k + 1$ has an odd number of factors does not imply that it is irreducible. For example, we may consider the trinomial $x^{2k} + x^k + 1$ with k odd. In a number of cases, including this one, the reducibility or irreducibility of $x^n + x^k + 1$ can be decided by using the results of [1, Ch. V, § 9]. Recall that an irreducible polynomial $f(x)$ over a finite field is said to belong to the exponent e if e is the least integer such that $f(x) \mid x^e - 1$. In other words, e is the order of a root of $f(x)$.

If $f(x)$ is irreducible of degree n and exponent e over $GF(q)$, it follows from [1, Ch. V, Th. 18] that $f(x^s)$ is irreducible over $GF(q)$ if and only if every prime p dividing s also divides e but does not divide $(q^n - 1)/e$ and, in addition, $4 \nmid s$ if $q^n \equiv -1 \bmod 4$.

In particular $x^{2k} + x^k + 1$ is irreducible over $GF(2)$ if and only if k is a power of 3 and $x^{4k} + x^k + 1$ is irreducible over $GF(2)$ if and only if $k = 3^r5^s$.

Some other cases can be disposed of by observing that if $x^r + x^s + 1$ divides $x^e + 1$ then $x^r + x^s + 1$ divides $x^n + x^k + 1$ if $n \equiv r$, $k \equiv s \bmod e$. For emample, $x^2 + x + 1$ divides $x^n + x^k + 1$ if $n \equiv 2$, $k \equiv 1 \bmod 3$ or if $n \equiv 1$, $k \equiv 2 \bmod 3$.

REMARK. I. Kaplansky points out that Theorem 1 can be reformulated so as to avoid the use of $\mathfrak{p}$-adic numbers by considering the positive and negative terms in $\Pi(\alpha_i - \alpha_j)$. These are polynomials in the α_i which also make sense in characteristic 2. This yields an elementary form of the theorem but one which is hard to apply because of the difficulty in computation.

REFERENCES

1. A. A. Albert, *Fundamental Concepts of Higher Algebra*, University of Chicago Press, 1956.

2. ———, *On certain trinomial equations in finite fields*, Ann. of Math., **66** (1957), (1957), 170-178.

3. E. Artin, *Theory of Algebraic Numbers*, Gottingen, 1959.

4. H. S. Vandiver, *On trinomial equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. **40** (1954), 1008-1010.

5. B. L. van der Waerden, *Moderne Algebra*, Julius Springer, Berlin, 1931.

THE UNIVERSITY OF CHICAGO