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

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

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.