SOME TOPICS IN THE ARITHMETIC OF POLYNOMIALS

L. CARLITZ

1. **Introduction.** Let $GF(p^n)$ denote a fixed Galois (finite) field, and x an indeterminate. The arithmetic of polynomials in x with coefficients in $GF(p^n)$ is in many ways similar to ordinary arithmetic, and was discussed in some detail by Dedekind.[1] As a matter of fact it appears that in many instances the arithmetic of polynomials is the simpler. Thus, for example, in the case of the analogues of the familiar arithmetic functions, in place of asymptotic formulas there are exact formulas for the polynomial domain. This is perhaps due to the possibility of grouping polynomials according to degree. Again it is familiar that in the problem of representing a rational integer as a sum of an even number of squares there is a considerable difference between the case $2t \leqq 8$ and $2t > 8$; in the former case the number of representations can be expressed in terms of divisor functions, while in the latter case this is in general impossible. For the polynomial case however the number of representations by an even number of squares can always be expressed in terms of divisor functions. Similar remarks apply to the case of an odd number of squares.

In the present paper we rather arbitrarily select three or four topics in the arithmetic of polynomials in a Galois field. In §2 we consider the simplest arithmetic functions. In §3 we discuss the problem of representing a given polynomial as a sum of squares. In §4 we define various special polynomials and functions that are rather intimately connected with the arithmetic of polynomials in $GF(p^n)$; application to power sums are given in §5. Finally in §6 we define analogues of the ordinary Bernoulli numbers; the principal result here is the Staudt-Clausen theorem. We remark that for the most part the extension of theorems from the coefficient field[2] $GF(p)$ to $GF(p^n)$ is quite trivial; however, in at least the last topic mentioned there appears to be some difference between the special and the general case.

It is evident from the above that we are ignoring such questions as construction and distribution of irreducible polynomials, the existence of irreducibles in an arithmetic progression, theorems of reciproc-

An address delivered before the meeting of the Society in Hanover, N. H., on September 12, 1940, by invitation of the Program Committee under the title *Arithmetic of polynomials in a Galois field*; received by the editors January 22, 1942.

[1] Journal für die reine und angewandte Mathematik, vol. 54 (1857), pp. 1–26.

[2] The field $GF(p)$ may be defined as the set of residues (mod p).