# ON FACTORABLE POLYNOMIALS IN SEVERAL INDETERMINATES

By Leonard Carlitz

1. **Introduction.** In this paper we consider a class of polynomials in several indeterminates with coefficients in a Galois field $GF(p^n)$, such that each polynomial may be completely factored into a product of linear factors in *some* Galois field $GF(p^{nn'})$, say. For the case of a single indeterminate a body of theorems[1] exists, and the purpose of this paper is to extend these theorems, whenever possible, to the case of several indeterminates. As will be seen in several cases, certain theorems are capable of extension, but the proof for the case of a single indeterminate is no longer applicable, and new methods become necessary. This is true in particular of the formula for the product of all (factorable) polynomials of fixed degree. Again, in the case of a single indeterminate, the form of a polynomial is known explicitly; in the case of several indeterminates, the definition is in terms of an intrinsic property, and thus it seems necessary to deal first with irreducible polynomials and from them go on to arbitrary polynomials.

In the case of polynomials in a single indeterminate $x$, as is well known, the quantity

$$x^{p^{ns}} - x \tag{1.1}$$

is fundamental.[2] In the extended case this is replaced by a certain determinant. Thus for example, for two and three indeterminates, we have

$$\begin{vmatrix} 1 & x & y \\ 1 & x^{p^{ns}} & y^{p^{ns}} \\ 1 & x^{p^{2ns}} & y^{p^{2ns}} \end{vmatrix}, \qquad \begin{vmatrix} 1 & x & y & z \\ 1 & x^{p^{ns}} & y^{p^{ns}} & z^{p^{ns}} \\ 1 & x^{p^{2ns}} & y^{p^{2ns}} & z^{p^{2ns}} \\ 1 & x^{p^{3ns}} & y^{p^{3ns}} & z^{p^{3ns}} \end{vmatrix}, \tag{1.2}$$

respectively. Certain formulas in the case of a single indeterminate carry over to the extended case by merely substituting the proper expression (1.2) for (1.1). In particular this is true for the product of irreducible polynomials and the product of all polynomials of fixed degree.

The number of (primary) irreducible polynomials of degree $s$ in a single indeterminate, with coefficients in the $GF(p^n)$, is determined by the familiar expression

$$\psi(s, p^n) = \sum_{s=d\delta} \mu(\delta)\, p^{nd},$$

Received October 12, 1936.

[1] For the classic theorems, see L. E. Dickson, *Linear Groups*, 1901, pp. 3–54.

[2] Dickson, loc. cit.