ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 12, Number 1, Winter 1982

SEPARABILITY AND FACTORING POLYNOMIALS

RAY MINES AND FRED RICHMAN

ABSTRACT. The basic facts about separable extensions of discrete fields and factoring polynomials are developed in the constructive spirit of Errett Bishop. The ability to factor polynomials is shown to be preserved under finite separable extensions, while the ability to factor separable polynomials is preserved under arbitrary finite extensions. A method is given for converting any procedure that finds roots into one which finds arbitrary factors. Thus the rational root test gives rise to an effective procedure for factoring polynomials over the rational numbers, providing a new proof of a well known theorem of Kronecker.

0. Introduction. This paper contains a constructive development of the basic facts about separability and factoring of polynomials over discrete fields. The point of view is that of [1] and we build on the results of that paper. We summarize the main results in [1] upon which we shall draw.

Every set comes equipped with an equality relation $=$ and an inequality relation $\neq$ with the usual properties. A set is *discrete* if for every pair x and y, either $x = y$ or $x \neq y$. A *field* is a set with distinguished elements 0 and 1, and binary functions $+$ and $\times$ satisfying the usual axioms of a field. In addition we require that $0 \neq 1$ and the peculiarly constructive axioms:

1) For each positive integer n, if $a^n = 0$, then $a = 0$;
2) If $a + b \neq 0$, then $a \neq 0$ or $b \neq 0$; and
3) If $ab \neq 0$, then $a \neq 0$.

The *characteristic* of a discrete field is the infimum, in the one point compactification of the positive integers, of the set $\{n: n \times 1 = 0\}$. The field of rational numbers has characteristic infinity. A *prime field* is a field in which every element is equal to an element of the form $(n \times 1)/(m \times 1)$ where n and m are integers and $m \times 1 \neq 0$. Every discrete field contains a unique prime field. A discrete field k is *factorial* if every polynomial with coefficients in k is equal to a product of irreducible polynomials. We will have occasion to use the following characterization of integral elements, whose statement is similar, and proof is identical, to that of [1; Theorem 3.1].

Received by the editors on March 11, 1980, and in revised form on September 2, 1980.