ON THE INVARIANCE OF CHAINS OF FIELDS

BY

Michael D. Fried and R. E. MacRae[1]

1. Introduction

Let K be a field and let $L = K(a)$ be a primitive algebraic extension of K. It is well known that there are only finitely many fields intermediate between K and L. We ask whether maximal chains of such intermediate fields have the same length and whether the relative degrees of the terms in such chains form a set of invariants for the pair L over K. The exact statement is given in Theorem 2.3. Theorem 2.1 and Theorem 3.6 give two contexts in which the conclusion of Theorem 2.3 (invariance of chains) is true. The methods used in these two cases are quite different. By making use of either of these two theorems we are able to give a new proof of a theorem of Ritt [1] concerning composition of polynomials. See Theorem 3.1 for an exact statement. The paper concludes with Theorem 4.2 which gives a criterion for a polynomial of the form $f(x) - g(z)$ to have a proper divisor of the same form.

2. A Jordan-Hölder theorem for fields

Let K and L be fields such that $K < L$. We wish to consider maximal chains of subfields between K and L and to ask the following questions: (i) do any two such chains have the same length and (ii) are the relative degrees of the terms in any two such chains the same in some possibly permuted order? As we will show, the answer is in the affirmative if suitable assumptions are made on K and L. We begin with:

Theorem 2.1. *Let R be a discrete valuation ring with quotient field K and let L be a finite separable extension of K with R' equal to the integral closure of R in L. Moreover, let $\bar{L}$ be Galois closure of L over K, and let R'' be the integral closure of R in $\bar{L}$. If* (i) *R' is again a discrete valuation ring,* (ii) *the residue class degree of R over R' equals unity and* (iii) *$\bar{L}$ is cyclic over the inertial field with respect to some prime of R'', then for any pair of fields M_1 and M_2 intermediate between K and L we have*

$$[M_1 \cap M_2 : K] = \gcd([M_1 : K], [M_2 : K])$$

$$\textit{and} \quad [M_1 M_2 : K] = \operatorname{lcm}([M_1 : K], [M_2 : K]).$$

Proof. Let P' be a generator of the (unique) prime ideal of R' and let P be a generator of the prime ideal of R. By hypothesis we have $PR' = (P'R')^n$ where $n = [L:K]$. Thus $L = K(P')$. Now P' satisfies an Eisenstein equation over K. That is to say, the minimal polynomial of P' over K is of the form

Received June 16, 1967.

[1] This work was partly supported by a National Science Foundation grant.