Reprinted from ILLINOIS JOURNAL OF MATHEMATICS
Vol. 13, No. 1, March 1969
Printed in U.S.A.

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*

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

$$\text{and} \quad [M_1M_2:K] = \operatorname{lcm}([M_1:K], [M_2:K]).$$

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.

$x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where $P \mid a_j, j = 0, \cdots, n-1$ but $P^2 \nmid a_0$. This follows as in the case of complete fields by considering the coefficients a_j as elementary symmetric functions in the conjugates of P'. Let K_T be the inertial subfield over which $\bar{L}$ is assumed to be cyclic. By construction, P generates the maximal ideal of any of the local rings over the integral closure R_T of R in K_T. Thus the equation for P' remains irreducible over K_T. Now $\bar{L}$ is generated over K_T by the conjugates of P', but $K_T(P')$ is normal over K_T since $\bar{L}$ over K_T is abelian. Thus $K_T(P') = \bar{L}$. Let now $f_K(x)$ be the minimal polynomial of P' over K. If M is an intermediate field between K and L, the minimal polynomial for P' over M is some polynomial $f_M(x)$ which divides $f_K(x)$ and M is generated over K by the coefficients of $f_M(x)$. For any such M let M' be the field intermediate between K_T and $\bar{L}$ generated by the coefficients of $f_M(x)$. We see that $[M:K] = [M':K_T]$. If M_1 and M_2 are a pair of fields intermediate between K and L then one verifies that

$$f_{M_1 \cap M_2}(x) = \operatorname{lcm}(f_{M_1}(x), f_{M_2}(x)) \quad \text{and} \quad f_{M_1 M_2}(x) = \gcd(f_{M_1}(x), f_{M_2}(x)).$$

Consequently, $(M_1 \cap M_2)' = M_1' \cap M_2'$ and $(M_1 M_2)' = M_1' M_2'$. Thus there is a monomorphism of the lattice of subfields intermediate between K and L into that between K_T and $\bar{L}$. Now apply the "Fundamental Theorem of Galois Theory" and the hypothesis that $\bar{L}$ is cyclic over K_T in order to yield the conclusion of the theorem.

We are now in a position to prove a kind of "Zassenhaus Lemma" for intermediate fields.

THEOREM 2.2. *Let the hypotheses be as in Theorem* 2.1. *Let* $K < M_1 < M_2 < L$ *and* $K < N_1 < N_2 < L$ *be intermediate fields. Then*

$$[M_2 \cap (M_1 N_2) : M_2 \cap (M_1 N_1)] = [N_2 \cap (N_1 M_2) : N_2 \cap (N_1 M_1)].$$

Proof. By Theorem 2.1 it suffices to show

$$\frac{\gcd(m_2, \operatorname{lcm}(m_1, n_2))}{\gcd(m_2, \operatorname{lcm}(m_1, n_1))} = \frac{\gcd(n_2, \operatorname{lcm}(n_1, m_2))}{\gcd(n_2, \operatorname{lcm}(n_1, m_1))},$$

where $m_i = [M_i:K]$ and $n_i = [N_i:K]$ for $i = 1, 2$. This fact is, however, readily verified.

Our final result in this section is the Jordan-Hölder theorem for intermediate fields.

THEOREM 2.3. *Let the hypotheses be as in Theorem* 2.1. *Then any two maximal chains of intermediate fields have the same length and the relative degrees of the terms in one chain equal the relative degrees of the terms in another such chain in a possibly permuted order.*

Proof. This result follows from Theorem 2.2 exactly as in the analogous case of groups. Indeed let

$$K = M_0 < M_1 < \cdots < M_r = L \quad \text{and} \quad K = N_0 < N_1 < \cdots < N_s = L$$

be two maximal chains. Consider the two chains given by

$$M_{ij} = M_{i+1} \cap (M_i N_j) \quad \text{and} \quad N_{ij} = N_{i+1} \cap (N_i M_j).$$

Since these two chains refine the original chains which were assumed maximal they give, in fact, the original chains. One now applies Theorem 2.2 in order to compare degrees and obtain the conclusion of Theorem 2.3.

It is worthwhile to remark at this point that if one is interested only in Theorem 2.3, the hypotheses of Theorem 2.1 may be weakened to the extent of assuming that $\bar{L}$ is merely abelian over K_T. The proof presents no special difficulty and we leave it to the reader. We stress, however, that the rather strong property of Theorem 2.2 is no longer valid.

3. An application to polynomial decomposition

We wish to give here a proof of a generalization of a theorem of Ritt [1].

THEOREM 3.1. *Let k be an arbitrary field and let $f(x)$ be a polynomial in $k[x]$. Moreover, we will assume that either* char $(k) = 0$ *or* char $(k) >$ deg $(f(x))$. *If*

$$f(x) = g_1(g_2(\cdots(g_r(x))\cdots) = h_1(h_2(\cdots(h_s(x))\cdots)$$

where the polynomials g_i and h_i have coefficients in k and cannot be further decomposed over k, then $r = s$ and there exists a permutation π of the symbols $1, \cdots, r$ such that deg $(g_i(x))$ = deg $(h_{\pi(i)}(x))$.

We defer the proof of Theorem 3.1 until we verify several preliminary propositions.

PROPOSITION 3.2. *Let k be a field and let z be an element of $k(x)$. Then z is in $k[x]$ if and only if the prime at infinity in $k(x)$ is the only prime which lies over the prime at infinity in $k(z)$. Under these circumstances the prime at infinity is totally ramified.*

Proof. Given the truth of the if and only if portion of the proposition we note that the prime at infinity must be totally ramified since the residue class degree of the prime at infinity is always unity. Let us suppose first that z is a polynomial in x, but that there is a valuation ring R such that $k \leq R$, $k(x)$ is the quotient field of R, $x \in R$ and R contracts in $k(z)$ to the local ring at infinity (whose maximal ideal is, of course, generated by $1/z$). Thus z is not in R since $1/z$ is certainly not a unit in R. However, z must be in R since $z \in k[x] \leq R$. Thus we have a contradiction. Conversely the hypothesis clearly implies that z in an element of every valuation ring of $k(x)$ which contains $k[x]$. But the intersection of these rings is exactly $k[x]$.

Using Proposition 3.2 we can tie up the decomposition of a polynomial with the lattice of subfields of $k(x)$. First we need a definition.

DEFINITION 3.3. Let k be any field and let $f(x)$ and $g(x)$ be two poly-

nomials in $k[x]$. We say the $f(x)$ and $g(x)$ are *linearly equivalent* if there exist constants a and b in k such that $f(x) = ag(x) + b$.

We now construct a correspondence between polynomials in $k[x]$ and subfields of $k(x)$ as follows. Let $f(x)$ be an element of $k[x]$. By S we will denote the set of all polynomials $h(x)$ in $k[x]$ such that $f(x) = g(h(x))$ for some polynomial $g(x)$ in $k[x]$. By T we will denote the set of all intermediate fields between $k(f(x))$ and $k(x)$. Given $h(x)$ in S we assign to it the intermediate field $M_h = k(h(x))$.

PROPOSITION 3.4. *The mapping $h \to M_h$ sends S onto T and $M_h = M_w$ if and only if h and are linearly equivalent.*

Proof. We note first that $M_h = M_w$ if and only if h and w are related by a linear fractional transformation as a result of the general theory of function fields. Thus, if h and w are linearly equivalent, we see that $M_h = M_w$. Conversely, if $M_h = M_w$, we make use of the hypothesis that $m(w(x)) = f(x) = g(h(x))$ for suitably selected polynomials m and g. This, together with Proposition 3.2, shows that the prime at infinity is the same in both M_h and M_w. In other words, h and w are linearly equivalent. Finally, in order to show that every intermediate field is of the form M_h we appeal to Lüroth's theorem together with Proposition 3.2. Indeed, for an intermediate field M, we have $M = k(a(x)/b(x))$. We may assume that the prime at infinity in $k(a(x)/b(x))$ lies over the prime at infinity in $k(f(x))$. Use a linear fractional transformation if necessary. Thus the hypotheses for Proposition 3.2 are satisfied for $k(x)$ over M and M over $k(f(x))$. Hence $a(x)/b(x) = h(x)$ and $f(x) = g(a(x)/b(x)) = g(h(x))$.

We can now give the following:

Proof of Theorem 3.1. First we see that $k(x)$ is separable over $k(f(x))$ since $f'(x) \neq 0$. Let R be the local ring at infinity in $k(f(x))$. Its integral closure in $k(x)$ is again a discrete valuation ring by Proposition 3.2. Moreover, the assumption char $(k) = 0$ or char $(k) >$ deg $(f(x))$ guarantees that *all* ramification is tame and thus $\bar{L}$ over K_T is cycle where $\bar{L}$ is the Galois closure of $k(x)$ over $k(f(x))$ and K_T is the inertial subfield of some extension of the prime in R to $\bar{L}$. The hypotheses of Theorem 2.3 are thus satisfied and interpretation of its conclusion in terms of Proposition 3.4 finishes our work.

It is possible to give an alternate proof of Theorem 3.1. Since the techniques are somewhat different, we include the proof. Let us begin with a result which, while special, is surprising. We do not know how much the hypotheses can be weakened.

THEOREM 3.5. *Let k be an arbitrary field and let $f(x)$ be a polynomial in $k[x]$ such that* gcd $(\deg (f(x)), \text{char } (k)) = 1$ *or* char $(k) = 0$. *Let $\bar{k}$ be the algebraic closure of k. Then the correspondence $M \to \bar{k} \otimes_k M$ establishes a relative degree-*

preserving isomorphism of the lattice of fields intermediate between $k(x)$ *and* $k(f(x))$ *onto the lattice of fields intermediate between* $\bar{k}(x)$ *and* $\bar{k}(f(x))$.

Proof. Since $k(x)$ and $\bar{k}$ are linearly disjoint over k, the given correspondence is a lattice monomorphism. To show the surjective nature of it let $\bar{M}$ be a field between $\bar{k}(x)$ and $\bar{k}(f(x))$. By Proposition 3.4 there are polynomials $g(x)$ and $h(x)$ with coefficients in $\bar{k}$ such that $f(x) = g(h(x))$ and $\bar{M} = \bar{k}(h(x))$. It is easy to arrange matters so that both the leading and constant term coefficients of $h(x)$ are in k. Indeed, take a polynomial linearly equivalent to $h(x)$ if necessary. Let

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \qquad g(x) = b_0 + b_1 x + \cdots + b_r x^r$$

and

$$h(x) = c_0 + c_1 x + \cdots + c_s x^s.$$

We note that $a_n = b_r c_s^r$. Thus b_r is in k. We continue by induction. For $0 < t < s$ we see that $a_{n-t} = rb_r c_s^{r-1} c_{s-t} + w$. But w is a universal polynomial involving only $b_r, c_s, \cdots, c_{s-t+1}$ and thus is in k by inductive hypothesis. Since r and char (k) are relatively prime we may therefore assume that c_{s-t} is in k. Hence, $h(x)$ is in $k[x]$. Now $a_{n-s} = b_{r-1} c_s^{r-1} + u$ where u is a universal polynomial involving only b_r and the coefficients of $h(x)$. Thus b_{r-1} is in k. Continuing in this way we see finally that $g(x)$ has coefficients in k. Finally let $M = k(h(x))$. Clearly $\bar{M} = \bar{k} \otimes_k M$.

Our next result is quite similar to Theorem 2.1. The methods used in the two cases are, however, very different. Neither result exactly contains the other.

THEOREM 3.6. *Let* k *be an arbitrary field and let* $z = f(x)$ *be a polynomial in* $k[x]$ *such that* gcd (char (k), deg $(f(x))) = 1$ *or* char $(k) = 0$. *If* M_1 *and* M_2 *are fields intermediate between* $L = k(x)$ *and* $K = k(f(x))$, *then*

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

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

Proof. By virtue of Theorem 3.5 we may assume from the start that k is algebraically closed. Let K_∞ and L_∞ be the completions of K and L at their respective infinite primes. By Hensel's lemma there is an element w in L_∞ such that $w^n = 1/z$ where $n = \deg(f(x))$. Moreover $L_\infty = k((w))$ and $K_\infty = k((w^n))$. Thus L_∞ is a cyclic extension of K_∞ and the fields intermediate between them are given exactly by $k((w^r))$ where r ranges over the divisors of n. Now let $M_j = k(z_j)$ where $z_j = f_j(x)$ in $k[x]$, $j = 1, 2$. Moreover, let deg $(f_j(x)) = n_t t$ where gcd $(n_1, n_2) = 1$. We wish to show first that there exist polynomials $g_j(x)$ with degrees n_j such that $g_1(z_1) = g_2(z_2)$. Indeed, let $w_j = w^{n/n_j t}$. By replacing each z_j with a linearly equivalent polynomial if

necessary we may assume that

$$z_j = w_j^{-1} + a_{j0} + a_{j1} w_j + \cdots + a_{jm} w_j^m + \cdots$$

are the respective power series expansions of z_1 and z_2 in $k((w_1))$ and $k((w_2))$. Since, for an arbitrary natural integer r, $z_j^r = w_j^{-r}$ + terms of higher order in w_j, there are, clearly, polynomials $g_j(x)$ of degrees n_j, respectively, such that

$$g_j(z_j) = w_j^{n_j} + b_{j0} + b_{j1} w_j + \cdots .$$

Now $w_1^{n_1} = w_2^{n_2}$ so $g_1(z_1) - g_2(z_2)$ has non-negative order at infinity. But this element has non-negative order at all of the finite primes as well. Hence it must be an element of k. By adding the appropriate constant to one or the other of the two polynomials we may assume that $g_1(z_1) = g_2(z_2)$. Thus $k(g_j(z_j)) \leq M_1 \cap M_2$. From this it follows that

$$t = [k(g_j(z_j)):K]|[M_1 \cap M_2:K]| \gcd(n_1 t, n_2 t) = t.$$

Hence the first conclusion of the theorem is verified. For the second conclusion let $M_1 M_2 = k(z_3)$, where z_3 is in $k[x]$. Moreover let $[M_1 M_2:K] = tn_1 n_2 u$. Let $w_3 = w^{n/s}$ where $s = tn_1 n_2 u$. We have

$$z_3 = w_3^{-1} + a_0 + a_1 w_3 + \cdots .$$

As before we can find a polynomial of degree u, say $h(x)$, such that $h(z_3) = w_3^{-u} + b_0 + b_1 w_3 + \cdots$. Moreover we can find by the same process polynomials $g_1(x)$ and $g_2(x)$ of degrees n_1 and n_2, respectively, such that

$$g_1(h(z_3)) = w_3^{-r} + c_0 + c_1 w_3 + \cdots \quad \text{and} \quad g_2(h(z_3)) = w_3^{-s} + d_0 + d_1 w_3 + \cdots$$

where $r = un_2$ and $s = un_1$. As in the first part of the proof we find that each of the elements $z_j - g_j(h(z_3))$ has a non-negative order at infinity as well as at all the finite primes. Thus we may assume (by a linear change, if necessary) that $z_j = g_j(h(z_3))$. Now $M_1 M_2 \leq k(h(z_3))$. Hence

$$tn_1 n_2 u = [M_1 M_2:K]|[k(h(z_3)):K] = tn_1 n_2 .$$

Thus $u = 1$ and we are done.

From this point on the proof of Theorem 3.1 is exactly the same as in the first part of this section. As a matter of fact we may even weaken the assumption concerning the degree of $f(x)$ in Theorem 3.1 to the hypothesis that it is relatively prime to the characteristic of k.

4. Composite pairs

In this final section we consider the problem of factorization of polynomials of the form $f(x) - g(z)$ where $f(x)$ and $g(z)$ are themselves polynomials.

DEFINITION 4.1. Let $f(x)$ and $g(x)$ be elements of $k[x]$ where k is an arbitrary ring. We say that *f and g are a composite pair over k* if there exists a polynomial $F(x)$ of degree greater than one and polynomials $f_1(x)$ and $g_1(x)$, all in $k[x]$, such that $f(x) = F(f_1(x))$ and $g(x) = F(g_1(x))$.

The main result is the following:

THEOREM 4.2. *Let k be a field and let $f(x)$ and $g(x)$ be elements of $k[x]$. Then $f(x)$ and $g(x)$ are a composite pair if and only if the polynomial $f(x) - g(z)$ has a proper divisor of the form $f_1(x) - g_1(z)$ in $k[x, z]$.*

Proof. If $f(x)$ and $g(x)$ are a composite pair then we have $f(x) = F(f_1(x))$ and $g(x) = F(g_1(x))$ with $\deg(F) > 1$. Clearly $f_1(x) - g_1(z)$ is a proper divisor of $f(x) - g(z)$. Conversely, suppose that $f_1(x) - g_1(z)$ is a proper divisor for $f(x) - g(z)$. Let $q(x, z)$ be an irreducible factor of $f_1(x) - g_1(z)$. Moreover let $L = k(u, v)$ be the field of algebraic functions on the curve $q(u, v) = 0$. Consider the subfields $k(u)$ and $k(v)$. Let M be their intersection. We have, for $w = f(u) = g(v)$ and $w_1 = f_1(u) = g_1(v)$, that $k(w) < M$ and $k(w_1) \leq M$. The first containment is proper since $f_1(x) - g_1(z)$ is a proper divisor of $f(x) - g(z)$ by hypothesis. Now by Proposition 3.4, $M = k(w_3)$ where $w_3 = f_3(u) = g_3(v)$ and $w = F(w_3)$ where $\deg(F) > 1$. Hence $f(x) = F(f_3(x))$ and $g(x) = F(g_3(x))$ as was to be shown.

REFERENCES

1. J. F. RITT, *Prime and composite polynomials*, Trans. Amer. Math. Soc., vol. 23 (1922), pp. 51–66.
2. O. F. G. SCHILLING, *The theory of valuations*, New York, 1950.

INSTITUTE FOR ADVANCED STUDY
PRINCETON, NEW JERSEY
UNIVERSITY OF COLORADO
BOULDER, COLORADO