ADDITIVE POLYNOMIALS. II

BY

T. H. M. CRAMPTON AND G. WHAPLES

Introduction. Results. Let k be a field and $u(x)$, $u_i(x)$ elements of the polynomial ring $k[x]$. We shall call $u(x)=u_1(u_2(x))$ a *composite* of $u_1(x)$ and $u_2(x)$, and shall call $u_1(x)$ an *outer component*, $u_2(x)$ an *inner component* of $u(x)$. An identity

$$u(x) = u_1(u_2(\cdots(u_r(x))\cdots))$$

will be called a *decomposition* of $u(x)$. In the case where k has characteristic zero, the problem of finding all relations among the different decompositions of a given $u(x)$ has been solved by J. F. Ritt [7], H. T. Engstrom [2], and H. Levi [5]. When k has characteristic p this problem has been solved only for the special case of *additive polynomials* (a.p.)—i.e., the polynomials $f(x)=\sum a_r x^{p^r}$ characterized by the identity $f(x+y)=f(x)+f(y)$. O. Ore [6] worked out the general theory of these polynomials, the decomposition theory of which is contained in his result that the set of all a.p. over k forms a non-commutative left and right principal ideal ring under the operations of addition and composition. One of us has found further results on a.p. [8] for fields k satisfying one or more of the following axioms, which are also required for a few of our present results:

Axiom 1. k has characteristic p.

Axiom 2. k has no inseparable extension.

Axiom 3. For each positive integer n, k has in any algebraic closure at most one extension of degree n; and it has exactly one extension for $n=p$.

These axioms are a weakened form of those describing the residue class fields in generalized local class field theory [9]; the results of [8], and of §1 of this paper, are the main tools in proving a new existence theorem in that theory; for this theorem see [10] or [11].

In the present paper we determine, for given $u_1(x)\in k[x]$, all decompositions of the forms

$$\begin{aligned} &u_1(x) = f_1(u_2(x)), \qquad u_1(x) = f_1(u_2(x)) + f_2(x),\\ &u_1(x) = u_2(f_1(x)), \qquad u_1(x) = u_2(f_1(x)) + f_2(x),\\ &\qquad\qquad u_1(x) = f_1(u_2(f_2(x))) + f_3(x) \end{aligned} \tag{1}$$

where the $u_2(x)$ are arbitrary polynomials and the $f_i(x)$ are a.p. We show that each $u_1(x)\in k[x]$ has a maximal decomposition of each of these five types, of

Presented to the Society, December 29, 1952; received by the editors July 9, 1953 and, in revised form, November 18, 1953.

which all other decompositions of the same type are consequences. We also show that in general there is no maximal decomposition of the type $u_1(x) = f_1(u_2(f_2(x)))$, $f_i(x)$ a.p. The proofs in the cases of inner additive components (Theorems 5 and 6) are easy and involve only study of the set of zeros of $u_1(x)$. Those for outer additive components (Theorems 2, 3, 4) are harder and require use of the ring $\boldsymbol{S}$ of all linear transformations S of $k[x]$ into itself defined by equations of the form

$$S\phi(x) = \sum_{\nu} \phi(h_\nu(x))$$

where $\phi(x)$ is a generic element of $k[x]$ and $\{h_\nu(x)\}$ a finite sequence of elements of $k[x]$. Our results on $\boldsymbol{S}$ (Theorem 1 and its corollaries) may be summarized by saying that under a natural topology on the endomorphism ring of $k[x]$ the elements of $\boldsymbol{S}$ are everywhere dense in the commutator of the ring of endomorphisms induced by the a.p. (Corollary 1.1). This is the result needed for local class field theory. Theorem 7, concerned with the two-sided decomposition (1), is a consequence of the theorems that precede it.

1. **A ring of linear transformations of $k[x]$.** Let k be a field and consider a polynomial $\phi(x)$ over k. For every positive integer n let $\langle n\rangle = \{1, 2, \cdots, n\}$ and define

$$\phi_{[n]}(x_1, \cdots, x_n) = \sum_{S\subset\langle n\rangle} (-1)^{\#S}\phi\left(\sum_{\nu\in S} x_\nu\right), \tag{2}$$

where $\#S$ is the cardinal number of S and the sum over the empty set of indices is zero.

PROPOSITION 1. *For all n and all i such that $1 \leqq i \leqq n$*

$$\begin{aligned}\phi_{[n+1]}(x_1, \cdots, x_{n+1}) = {} & \phi_{[n]}(x_1, \cdots, \hat{x}_i, \cdots, x_{n+1}) \\ & + \phi_{[n]}(x_1, \cdots, \hat{x}_{i+1}, \cdots, x_{n+1}) \\ & - \phi_{[n]}(x_1, \cdots, (x_i + x_{i+1}), \cdots, x_{n+1}),\end{aligned} \tag{3}$$

where $\hat{x}_i$ indicates the argument x_i has been omitted.

Proof. The proposition is proved by using (2) and associating those terms of the sums on the right that are indexed by subsets of $\{1, \cdots, n+1\}$ containing i but not $i+1$, those by subsets which contain $i+1$ but not i, those by subsets containing both i and $i+1$, and those indexed by subsets containing neither i nor $i+1$. Note: The transformation (3) seems first to have been used by Artin [1] and Kaplansky [4]; the latter applied it to noncommutative polynomials.

PROPOSITION 2. *For every polynomial $\phi(x)$, $\phi_{[n]}(x_1, \cdots, x_n) = 0$ when any of the x_i is set equal to zero.*

Proof. $\phi_{[1]}(x_1) = -\phi(x_1)+\phi(0)$, so the proposition holds for $n=1$. It follows for all n by induction and Proposition 1.

PROPOSITION 3. *Let k have characteristic p and let $\phi(x)=x^n$. Denote by $s=s(n)$ the sum of the digits of n written to the base p. Then*

$$\phi_{[s]}(x_1, \cdots, x_s) = c_n \sum_{P(1)+\cdots+P(s)=n} x_1^{P(1)} \cdots x_s^{P(s)}, \quad P(i) = p^{\nu(i)}, \quad c_n \neq 0, \tag{4}$$

$$\phi_{[t]}(x_1, \cdots, x_t) = 0, \qquad t > s, \tag{5}$$

and for $1 \leqq i \leqq s$

$$\phi_{[s]}(x_1, \cdots, x_i + x_i', \cdots, x_s) = \phi_{[s]}(x_1, \cdots, x_i, \cdots, x_s) + \phi_{[s]}(x_1, \cdots, x_i', \cdots, x_s). \tag{6}$$

Proof. By Proposition 2, the only possible nonzero terms of $\phi_{[s]}$ are those which contain all the arguments $x_1, \cdots, x_s$. Hence by (2) and the multinomial theorem

$$\phi_{[s]}(x_1, \cdots, x_s) = (-1)^s \sum \frac{n!}{i_1! \cdots i_s!} x_1^{i_1} \cdots x_s^{i_s}, \tag{7}$$

where the sum is taken over all sets of positive integers $i_1 \cdots i_s$ with $i_1+\cdots+i_s=n$. Now it is well known [3, p. 111] that $m!$ is exactly divisible by p raised to the power $(m-s(m))/(p-1)$, so the coefficient of a term of (7) is exactly divisible by p raised to the power

$$\left(n - s - \sum_{\nu=1}^{s} (i_\nu - s(i_\nu))\right) \Big/ (p-1) = \left(\sum_{\nu=1}^{s} s(i_\nu) - s\right) \Big/ (p-1),$$

which is a positive integer unless $s(i_\nu)=1$ for each ν, i.e., unless each i_ν is a power of p, in which case the i_ν are uniquely determined up to order. Hence all nonzero terms of (7) have the same coefficient and are of the form asserted. Proposition 1 (with $i=s$) and (6) imply (5); (6) is obvious from (4).

We call a polynomial that has the property (6) *multiadditive* for the field k. Proposition 3 shows that for any polynomial $\phi(x)$ over a field k with characteristic p there is a unique integer s such that $\phi_{[s]}(x_1, \cdots, x_s)$ is multiadditive. We call a term

$$m(x_1, \cdots, x_n) = \alpha x_1^{P(1)} \cdots x_n^{P(n)}, \quad P(i) = p^{\nu(i)}, \quad \alpha \in k, \tag{8}$$

a *multiadditive monomial* (m.a.m.) in $x_1, \cdots, x_n$ over k. If $\{\beta_{ij}\}$, $i=1, \cdots, q$, $j=1, \cdots, n$, are elements of k then the equation

$$L(m(x_1, \cdots, x_n)) = \sum_{\mu=1}^{q} m(\beta_{\mu 1}x_1, \cdots, \beta_{\mu n}x_n) \tag{9}$$

defines a function L on the set of all m.a.m. (in $x_1, \cdots, x_n$) into itself. Call such functions Σ-functions. If $m \to L_i(m)$ are Σ-functions, then their composite, i.e. the mapping $m \to L_1(L_2(m))$, is again a Σ-function. A set of m.a.m. shall be called *independent* if none of them is equal to a constant times a p^ith power of another.

PROPOSITION 4. *If k is an infinite field with characteristic p and has no inseparable extensions, if $\{m_i\}$, $i=1, \cdots, r$, is an independent set of m.a.m. in $x_1, \cdots, x_n$ over k and $\alpha \in k$, then there is a Σ-function L such that $L(m_1)=\alpha m_1$ and $L(m_i)=0$ for $i \neq 1$.*

Proof. If m is given by (8) and L by (9), then $L(m)=\lambda m$, where

$$\lambda = \sum_{\mu=1}^{q} \left(\prod_{\nu=1}^{n} \beta_{\mu\nu}^{P(\nu)} \right) \in k.$$

If

$$m' = \beta m^P, \qquad P = p^e, \qquad \beta \in k, \tag{10}$$

then $L(m')=\lambda^P m'$. This shows: (a) If $\{m_i\}$ is an independent set of m.a.m., then the set of nonzero m.a.m. in $\{L(m_i)\}$ is also independent; and (b) in proving Proposition 4 we may without loss of generality replace a given independent set $\{m_i\}$ by a set $\{m_i'\}$ where the m_i' are related to the m_i by transformations of form (10). From (a) and the fact that the composite of two Σ-functions is again a Σ-function it is easy to see that our proposition will follow if we show: (c) If m_1 and m_2 are independent m.a.m., then there is a Σ-function L with $L(m_1)=\alpha m_1$, $L(m_2)=0$.

Case 1. $n=1$. Then no two m.a.m. are independent and our proposition is trivial.

Case 2. $n=2$. By (b) we may assume

$$m_1 = x_1^P x_2^Q, \qquad m_2 = x_1^P x_2^R,$$

where P, Q, R are powers of p and $Q \neq R$. Since k has infinitely many elements it contains a β such that

$$\beta^R - \beta^Q = \gamma \neq 0.$$

Let

$$L(m(x_1, x_2)) = m(\gamma^{-1}\delta\beta^R x_1, x_2) + (p-1)m(\gamma^{-1}\delta x_1, \beta^P x_2),$$

where $\delta^P=\alpha$; then (c) holds for this L.

Case 3. $n>2$. Assume that (c) has been shown for all $n'<n$, and suppose

$$m_1 = x_1^P x_2^{P(2)} \cdots x_n^{P(n)}, \qquad m_2 = x_1^P x_2^{Q(2)} \cdots x_n^{Q(n)}.$$

Let

$$m_1^* = x_2^{P(2)} \cdots x_n^{P(n)}, \qquad m_2^* = x_2^{Q(2)} \cdots x_n^{Q(n)}.$$

If m_1^* and m_2^* are independent, then by our assumption there is an L^* with $L^*(m_1^*) = \alpha m_1^*$, $L^*(m_2^*) = 0$ and (c) follows easily for m_1 and m_2. If m_1^* and m_2^* and not independent then

$$m_1 = x_1^P (m^*)^Q, \qquad m_2 = x_1^P (m^*)^R$$

for some m.a.m. m^* in $x_2, \cdots, x_n$ and (c) follows by an argument similar to that used in Case 2.

Let $\boldsymbol{S}$ be the set of all mappings

$$S: S(\phi(x)) = \sum_\nu \phi(h_\nu(x)) \tag{11}$$

of $k[x]$ into itself, each $S \in \boldsymbol{S}$ being defined by a finite sequence $\{h_\nu(x)\}$ of polynomials $h_\nu(x) \in k[x]$. It is easy to see that $\boldsymbol{S}$ is a ring under the operations of addition, subtraction, and composition. ($-S$ is the operator obtained by repeating the sum on the right of (11) $p-1$ times because k has characteristic p. For characteristic 0 we could get a similar ring by taking $\boldsymbol{S}$ to be the ring of all S defined by a sequence $\{h_\nu(x)\}$ and a sequence $\epsilon_\nu = \pm 1$ with $S\phi(x) = \sum_\nu \epsilon_\nu \phi(h_\nu(x))$.) The elements $S \in \boldsymbol{S}$ are k-linear transformations of $k[x]^+$, considered as vector space over k; indeed they have by (11) the somewhat stronger property that for every $\phi(x) \in k[x]$, every a.p. $f(x)$, every $S \in \boldsymbol{S}$

$$Sf(\phi(x)) = f(S\phi(x)). \tag{12}$$

Let $\boldsymbol{L}$ be the subring of $\boldsymbol{S}$ consisting of all mappings L with

$$L\phi(x) = \sum_\nu \phi(\alpha_\nu x + \beta_\nu), \qquad \alpha_\nu, \beta_\nu \in k, \tag{13}$$

and $\boldsymbol{H}$ the subring of all mappings H with

$$H\phi(x) = \sum_\nu \phi(\gamma_\nu x), \qquad \gamma_\nu \in k. \tag{14}$$

It is easily verified that they are rings under $+$, $-$, and composition and that $\boldsymbol{H} \subset \boldsymbol{L} \subset \boldsymbol{S}$.

THEOREM 1. *Let k be as in Proposition 4 and let T be a finite set of integers prime to p. Then* (A) *for each $n \in T$ there is an $H_n \in \boldsymbol{H}$ with*

$$H_n x^t = 0 \quad \textit{for} \quad t \in T - \{n\}, \qquad H_n x^n = x^n, \tag{15}$$

and (B) *there is an $L_n \in \boldsymbol{L}$ with*

$$L_n x^t = 0 \quad \textit{for} \quad t \in T - \{n\}, \qquad L_n x^n = x. \tag{16}$$

Proof. Assume (A) for all sets with fewer than $\#T$ elements since it is obvious for sets with but one. Let a be an element of T with $s(a)$ maximal ($s(a)$

as in Proposition 3), let $s=s(a)$, let $\phi_t(x)=x^t$ for each $t\in T$, and consider the polynomials $\phi_{t[s]}(x_1, x_2, \cdots, x_s)$ for all $t\in T$. Each of these polynomials is either identically zero or of the form (4). The set of all the m.a.m. which occur in any of the nonzero $\phi_{t[s]}(x_1, x_2, \cdots, x_s)$ for $t\in T$ is independent because each such term is of total degree t which is prime to p, hence can't be a p^νth power of another term; this same fact shows that any given m.a.m. can't appear in the right side of (4) for more than one t. Let $m_0=x_1^{P(1)}x_2^{P(2)}\cdots x_s^{P(s)}$ be one term of $\phi_{a[s]}(x_1, \cdots, x_s)$ with $P(1)=1$; since a is prime to p we may assume this. (It is needed only for proof of (B).) By Proposition 4 there is a sequence $\{\beta_{\lambda i}\}$, $\beta_{\lambda i}\in k$, $i=1\cdots s$, λ on some finite set, with

$$(17)\quad \sum_{\lambda}\phi_{[s]}(\beta_{\lambda 1}x_1, \beta_{\lambda 2}x_2, \cdots \beta_{\lambda s}x_s) = \begin{cases} 0 & \text{when } \phi(x)=x^t,\ t\in T-\{a\},\\ m_0 & \text{when } \phi(x)=x^a.\end{cases}$$

Set $x_1=x_2=\cdots=x_s=x$ and we find, using (2),

$$\sum_{\lambda, S\subset\{1\cdots s\}}(-1)^{\#S}\phi\Big(\sum_{\mu\in S}\beta_{\lambda\mu}x\Big) = \begin{cases} 0 & \text{when } \phi(x)=x^t,\ t\in T-\{a\},\\ x^a & \text{when } \phi(x)=x^a.\end{cases}$$

The mapping of polynomials $\phi(x)$into the left side of this equation is an element of $\boldsymbol{H}$ which satisfies (15) for $n=a$. Call it H_a. Let H^* be the mapping $H^*\phi(x)=\phi(x)-H_a\phi(x)$; H^* takes x^a into 0, x^t into itself for all $t\in T-\{a\}$ and $H^*\in\boldsymbol{H}$. By the induction assumption there exists for each $n\in T-\{a\}$ an H_n' satisfying (15) on $T-\{a\}$. Then $H_n=H_n'H^*$ satisfies (15) on T.

To prove (B) proceed in exactly the same way through (17) and this time let $x_1=x$, $x_2=\cdots=x_s=1$. Then (17) gives $L_ax^t=0$ for $t\in T-\{a\}$, $L_ax^a=x$ for an $L_a\in\boldsymbol{L}$. We may assume (B) true for all sets with less than $\#T$ elements, hence may assume that for each $n\in T-\{a\}$ there is an L_n' satisfying (16) on $T-\{a\}$. Then $L_n=L_n'H^*$ (for H^* as before) satisfies (16) on T.

COROLLARY 1.1. *Let $u(x)\in k[x]$, $u(0)=0$: Then* A. *If $u(x)\neq 0$ there is an $L\in\boldsymbol{L}$ with $Lu(x)$ a nonzero a.p.* B. *There is an $H\in\boldsymbol{H}$ with $Hu(x)$ an a.p. (perhaps unavoidably 0) and $Hx=x$.*

Proof. Write each exponent in a nonzero term of $u(x)$ in the form τp^ν where τ is prime to p. Collecting terms with the same τ gives

$$(18)\qquad u(x)=\sum_{\tau\in T}f_\tau(x^\tau)$$

where T is a finite set of positive integers prime to p and $f_\tau(y)$ is an a.p. for each $\tau\in T$. Clearly we may if we wish assume that $1\in T$, taking $f_1(y)=0$ if necessary, and we shall do this.

If $u(x)\neq 0$ then $f_n(x)\neq 0$ for some $n\in T$. Let $L=L_n$ satisfy (16). Then $Lu(x)=\sum_{\tau\in T}Lf_\tau(x^\tau)=\sum_{\tau\in T}f_\tau(Lx^\tau)=f_n(x)$. This proves A. To prove B, let H be the operator defined by (15) with $n=1$ and use a similar argument.

If one topologizes the ring of all linear transformations of $k[x]^+$ into itself by taking as neighborhoods of 0 the sets of transformations which are 0 on some finite-dimensional subspace it is easy to show:

COROLLARY 1.2. *S is everywhere dense in the ring E' of all linear transformations of $k[x]^+$ into itself which commute with the linear transformations induced by the a.p.*

2. **Outer additive components of arbitrary polynomials.** The following is easily verified.

PROPOSITION 5. *If $g(x)$, $d(x)$ are a.p. over k and*

$$g(x) = d(w(x))$$

for $w(x) \in k[x]$, then $w(x) = h(x) + \gamma$ where $h(x)$ is an a.p. and $d(\gamma) = 0$, so that

$$g(x) = d(h(x)).$$

If $f(x)$, $g(x)$, and $h(x)$ are a.p. and $f(x) = g(h(x))$, we shall call $f(x)$ an *inner composite* of $g(x)$ and an *outer composite* of $h(x)$. In the ring of a.p. under addition and composition, *inner composite* is the exact analogue of "right multiple," and *outer composite* the exact analogue of "left multiple." In this ring of a.p., every two a.p. have a *least common inner composite* (l.c.i. composite)—the analogue of least common right multiple; a *least common outer composite* (l.c.o. composite)—the analogue of least common left multiple; and *greatest common inner* and *outer components* (g.c.i. component and g.c.o. component)—the analogues of greatest common right and left divisors. For proofs see [6].

Now let $u(x) \in k[x]$, $u(0) = 0$, write it in the form (18), and let

$$d(x) = \text{g.c.o. component} \quad \{f_\tau(x) \mid \tau \in T\}. \tag{19}$$

For every $u(x)$, (19) characterizes $d(x)$ up to a transformation $d^*(x) = d(\alpha x)$, $\alpha \in k$.

THEOREM 2. *Let k be an infinite field of characteristic p with no inseparable extensions. Let $u(x) \in k[x]$, $u(x) \neq 0$, and $u(0) = 0$. Then the polynomial $d(x)$ defined by* (19) *is also uniquely characterized (up to the transformation already mentioned) by any one of the following four properties:*

A1. *$d(x)$ is an a.p. of greatest degree among all a.p. $h(x)$ for which $u(x)$ has a decomposition*

$$u(x) = h(v(x)), \qquad v(x) \in k[x]. \tag{20}$$

A2. *$d(x)$ is a l.c.i. composite of all a.p. $h(x)$ for which $u(x)$ has a decomposition* (20).

B1. *$d(x)$ is an a.p. of least degree among all a.p. $g(x)$ which have a represen-*

tation

$$g(x) = Su(x), \qquad S \in \mathbf{S}. \tag{21}$$

B2. *$d(x)$ is a g.c.o. component of all a.p. $g(x)$ which have a representation* (21).

The polynomial $d(x)$ also has the property

C. *For all finite algebraic extensions K of k, $d(K^+) = \langle u(K^+)\rangle$ = the smallest additive subgroup containing all values of $u(x)$ over K.*

If k satisfies Axiom 3 of the introduction and if the exponents of the nonzero terms of $u(x)$ are not all divisible by p, then $d(x)$ is a simple a.p. (i.e. has nonzero coefficient of the power x) and is characterized by the property C.

Proof. It is evident from (19) that $u(x) = d(w(x))$ for some $w(x) \in k[x]$. On the other hand, Theorem 1B shows that for each $\tau \in T$ there is an $L_\tau \in \mathbf{S}$ with $L_\tau u(x) = f_\tau(x)$. If $u(x) = h(v(x))$ for any a.p. $h(x)$, then $f_\tau(x) = L_\tau(h(v(x))) = h(L_\tau v(x))$ so $h(x)$ is an outer component of $f_\tau(x)$ by Proposition 5. So (20) implies that $h(x)$ is an outer component of $d(x)$. This proves that $d(x)$ is characterized by either of the properties A1 and A2.

From Theorem 1B and the decomposition theory of a.p. [6; 8] it follows that $d(x) = Su(x)$ for some $S \in \mathbf{S}$; namely $d(x) = \sum_{\tau \in T} f_\tau(g_\tau(x))$ by [6; 8] and if G_τ denote elements of $\mathbf{S}$ defined by $G_\tau \phi(x) = \phi(g_\tau(x))$ and $S = \sum_{\tau \in T} G_\tau L_\tau$ then $d(x) = Su(x)$. Since $u(x) = d(w(x))$, (21) and Proposition 5 imply that $d(x)$ is outer component of $g(x)$; this shows that $d(x)$ is characterized by either B1 or B2. Finally, $u(x) = d(w(x))$ implies $d(K^+) \supset \langle u(K^+)\rangle$ and $d(x) = Su(x)$ implies $d(K^+) \subset \langle u(K^+)\rangle$ for all K; under the extra assumptions Corollary 8.2 of [8] shows that $d(x)$ is characterized by property C.

REMARK. If k is finite it is still true that $d(x)$ satisfies A; to see this embed k in an infinite field (inseparable algebraic closure of $k(t)$, for example) and apply Theorem 1. But $d(x)$ may not satisfy B and C; suppose for example that $k = GF(q^m)$, $k' = GF(q)$, let $n = (q^m - 1)/(q - 1)$ and let $u(x) = x^n$. Then $u(\xi) = N_{k/k'}\xi$ for every $\xi \in k$ so $\langle u(k^+)\rangle = k'^+$, while $d(x) = x$; so B and C are not satisfied.

Now let $T' = T - \{1\}$ and

$$d'(x) = \text{g.c.o. component } \{f_\tau(x) \mid \tau \in T'\}, \tag{22}$$

interpreting the g.c.o. component of the empty set to be 0. Clearly $d(x)$ is an outer component of $d'(x)$.

THEOREM 3. *For k, $u(x)$ as in Theorem* 2, *the $d'(x)$ defined by* (22) *is also characterized (up to the previously mentioned transformation) by any one of the following four properties*:

A1. *$d'(x)$ is an a.p. of maximal degree among all a.p. $h'(x)$ for which $u(x)$ has a decomposition.*

$$u(x) = h'(v(x)) + l(x), \qquad v(x) \in k[x], \qquad l(x) \text{ an a.p.} \tag{23}$$

A2. *$d'(x)$ is a l.c.i. composite of all $h'(x)$ satisfying* (23).

B1. *$d'(x)$ is an a.p. of minimal degree among all a.p. $h'(x)$ which are expressible in the form*

$$h'(x) = Su(x), \text{ where } S \in \mathbf{S} \text{ and } Sx = 0. \tag{24}$$

B2. *$d'(x)$ is a g.c.o. component of all the $h'(x)$ satisfying* (24).

Proof. If $u(x)$ is an a.p., then $d'(x)=0$ and the theorem is trivially true. Assume $u(x)$ is not an a.p. and express it in form (18). Assume $1\in T$, taking $f_1(x)=0$ if necessary. It is evident from (22) that there is a decomposition

$$u(x) = d'(w(x)) + f_1(x), \qquad w(x) \in k[x]. \tag{25}$$

By Theorem 1B there is for each $\tau\in T'$ an $L_\tau\in S$ with $L_\tau x^t=0$ for $t\in T$ and $t\neq\tau$ (in particular, $L_\tau x=0$) and $L_\tau x^\tau=x$. If $h'(x)$ satisfies (23) then $L_\tau u(x) = f_\tau(x)=h'(L_\tau v(x))$. So (23) implies that $h'(x)$ is outer component of $f_\tau(x)$ for each $\tau\in T'$, hence that $h'(x)$ is outer component of $d'(x)$. This verifies characterizations A1 and A2.

Now $d'(x)$ is expressible [6; 8] in the form $d'(x)=\sum_{\tau\in T'} f_\tau(g_\tau(x))$ where the $g_\tau(x)$ are a.p. Let G_τ be the elements of $\mathbf{S}$ defined by $G_\tau\phi(x)=\phi(g_\tau(x))$, and let $S=\sum_{\tau\in T'} G_\tau L_\tau$, L_τ as above. Evidently $d'(x)=Su(x)$ and $Sx=0$; so $d'(x)$ has a representation of form (24). If $h'(x)$ is any polynomial satisfying (24) then (25) gives $h'(x)=S(d'(w(x))+f_1(x))=d'(Sw(x))$ so, by Proposition 5, $d'(x)$ is outer component of $h'(x)$. This verifies characterizations B1 and B2.

Our $d'(x)$ has a deeper characterization which we shall use to derive an analogue of the C of Theorem 2 and to determine all relations (1). We need first:

PROPOSITION 6. *Let $u(x)$, $v(x)\in k[x]$, $u(0)=v(0)=0$, and*

$$u(x) = v(e(x)) + h(x) \tag{26}$$

where $e(x)$ is a simple a.p. and $h(x)$ an a.p. Let $u(x)$ be given by (18), *let*

$$v(x) = \sum_{\rho\in R} g_\rho(x^\rho)$$

be a similar decomposition of $v(x)$, and let $d_u'(x)=$ g.c.o. component $\{f_\tau(x)\,|\,\tau\in T-\{1\}\}$ and $d_v'(x)=$ g.c.o. component $\{g_\rho(x)\,|\,\rho\in R-\{1\}\}$. Then $d_u'(x)=d_v'(x)$ (or $d_u'(x)=d_v'(\alpha x)$).

Proof. If either $u(x)$ or $v(x)$ is an a.p. they both are, and $d_u'(x)=d_v'(x)=0$. Exclude this trivial case. Theorem 3A and (26) give at once that $d_v'(x)$ is outer component of $d_u'(x)$. So by Theorem 3B (applied to $u(x)$) we see that it suffices to prove that $d_v'(x)$ is expressible in the form $Su(x)$, $S\in\mathbf{S}$, $Sx=0$.

Let $e(x)=\alpha_0 x+\alpha_1 x^p+\cdots+\alpha_m x^{p^m}$, $\alpha_0\alpha_m\neq 0$. Exclude the trivial case $m=0$. Then

$$v(e(x)) = \sum_{\rho \in R} g_\rho((e(x))^\rho), \tag{27}$$

and differs from $u(x)$ only by an a.p. Applying the multinomial theorem to $(e(x))^\rho$, $\rho \in R$, we see that T is contained in the set of all integers τ such that

$$\begin{aligned} p \nmid \tau,\ p^n\tau &= \nu_0 + \nu_1 p + \cdots + \nu_m p^m \qquad \text{for some } n \geqq 0, \\ \nu_0 + \nu_1 + \cdots + \nu_m &= \rho \in R. \end{aligned} \tag{28}$$

In particular, if a is the greatest integer in R, then $(e(x))^a$ contains the term $a\alpha_m^{a-1}\alpha_0 x^b$ where $b = (a-1)p^m + 1$. It is easy to see that this b is the largest integer τ satisfying (28), does appear in T, and hence is the largest integer in T, and that the exponent b does not appear in $(e(x))^\rho$ for $\rho \neq a$. So from (27) and (26) we see that (18) contains a term $f_b(x^b) = g_a(a\alpha_m^{a-1}\alpha_0 x^b)$. From Theorem 1B it follows that $g_a(x) = Lu(x)$ for an $L \in \boldsymbol{S}$ with $Lx = 0$. If G is the element of $\boldsymbol{S}$ with $G\phi(x) = \phi((e(x))^a)$ then $u(x) - GLu(x) = \sum_{\rho \in R^*} g_\rho((e(x))^\rho) +$an a.p., where $R^* = R - \{a\}$; that is, the sum over R^* is of form ($S^*u(x) +$an a.p.) where $S^* \in \boldsymbol{S}$ and $S^*x = x$. From this and an easy induction we conclude that all the $g_\rho(x)$, $\rho \in R$, are expressible in form $S_\rho u(x)$ with $S_\rho \in \boldsymbol{S}$ and $S_\rho x = 0$, hence (see end of proof of Theorem 3) that $d_v'(x) = Su(x)$, $Sx = 0$.

THEOREM 4. *For $u(x)$, $d'(x)$ as above, $d'(x)$ is also characterized by*:

B3. *$d'(x)$ is an a.p. of minimum degree in the set of all a.p. $h''(x)$ which have the property that for every simple a.p. $e(x)$ there is an $S \in \boldsymbol{S}$ with*

$$h''(x) = Su(e(x)), \qquad Sx = 0. \tag{29}$$

B4. *$d'(x)$ is the g.c.o. component of the set of $h''(x)$ described in* B1.

Also, $d'(x)$ has the property

C. *For every finite extension K of k, $d'(K^+)$ equals the intersection of all groups $\langle u(e(K^+))\rangle$ for all a.p. $e(x)$ over K. Under the same extra assumptions as in Theorem 2, $d'(x)$ is characterized by* C.

Proof. Let $d'(x)$ be defined by (22) and let $e(x)$ be any simple a.p. Write $u(e(x)) = \sum_{\omega \in W} g_\omega(x^\omega)$. By Proposition 6 (applied to $u(e(x))$ and $u(x)$ instead of to $u(x)$ and $v(x)$), $d'(x)$ is g.c.o. component of the $g_\omega(x)$, $\omega \in W - \{1\}$, hence by Theorem 3B, $d'(x)$ is expressible in form $Su(e(x))$ with $S \in \boldsymbol{S}$, $Sx = 0$, and is g.c.o. component of the set of all $h''(x)$ which are so expressible. This verifies characterizations B3 and B4. For the statement about C, let $u(x) = d'(v(x)) + l(x)$. For properly chosen $e(x)$, $d'(x)$ is outer component of $l(e(x))$, hence $\langle u(e(K^+))\rangle \subset d'(K^+)$; and (29) implies $d'(K^+) \subset \langle u(e(K^+))\rangle$. In C we can drop the restriction that $e(x)$ be simple, since we assumed $k^p = k$.

3. **Inner additive components of arbitrary polynomials.** In the following k is a field and k^c an algebraic closure of k. The set of all zeros of a polynomial in k^c will be called the *k^c-kernel* of the polynomial.

PROPOSITION 7. *Let $u(x)$ be any nonadditive polynomial over k with $u(0) = 0$,*

degree $u(x)=n$. *The set* $\mathfrak{C}_u$ *of* $\Gamma\in k^c$ *for which*

$$u(x+\Gamma) = u(x) + u(\Gamma) \tag{30}$$

forms an additive group and $\#\mathfrak{C}_u<n$. *If the characteristic of* k *is* 0, *then* $\mathfrak{C}_u=\{0\}$.

Proof. Let $\Gamma_1, \Gamma_2\in\mathfrak{C}_u$. Then from (30)

$$\begin{aligned} u(x+(\Gamma_1+\Gamma_2)) &= u(x+\Gamma_1)+u(\Gamma_2) = u(x)+u(\Gamma_1)+u(\Gamma_2) \\ &= u(x)+u(\Gamma_1+\Gamma_2), \end{aligned}$$

i.e., $\mathfrak{C}_u$ is closed under addition. Now

$$u(x+y)-u(x)-u(y) = \sum_{i=1}^{n-1} p_i(y)x^i,$$

where the $p_i(y)$ are polynomials of degree at most $n-1$ and are not all zero. Since $\mathfrak{C}_u$ is the set of common zeros of the $p_i(y)$, we have $\#\mathfrak{C}_u<n$. Being closed and finite, $\mathfrak{C}_u$ is a group.

PROPOSITION 8. *Let* $\mathfrak{C}$ *be a finite subset of* k^c. *If* $h(x)$ *is a polynomial over* k^c, *if degree* $h(x)<\#\mathfrak{C}$, *and if for all* $\Gamma\in\mathfrak{C}$, *all* σ *in the Galois group* G *of* k^c/k,

$$h(\Gamma^\sigma) = (h(\Gamma))^\sigma,$$

then $h(x)$ *has coefficients in* k.

Proof. For $\sigma\in G$ define

$$g_\sigma(x) = h(x) - h^\sigma(x),$$

where $h^\sigma(x)$ is the polynomial whose coefficients are the σ-images of the corresponding coefficients of $h(x)$. Then degree $g_\sigma(x)<\#\mathfrak{C}$ and $g_\sigma(\mathfrak{C}^\sigma)=\{0\}$, so $g_\sigma(x)=0$. Hence for all $\sigma\in G$ we have $h(x)=h^\sigma(x)$, and the proposition is proved.

THEOREM 5. *Let* k *be a field of characteristic* p *with no inseparable extensions, let* $u(x)$ *be a nonadditive polynomial over* k *with* $u(0)=0$, *and let* $e'(x)$ *be a simple a.p. over* k *whose* k^c*-kernel is precisely* $\mathfrak{C}_u$ (*Proposition 7 and* [8, *Theorem 2*]). *This characterizes* $e'(x)$ *up to transformation* $e'^*(x)=\alpha e'(x)$. *This* $e'(x)$ *is also characterized by*

A1. $e'(x)$ *is of maximal degree in the set of all simple a.p.* $g'(x)$ *for which* $u(x)$ *has a decomposition*

$$u(x) = v'(g'(x)) + l(x), \qquad l(x) \text{ an a.p.}, \qquad v'(x)\in k[x]. \tag{31}$$

A2. $e'(x)$ *is a l.c.o composite of all a.p.* $g'(x)$ *which satisfy* (31).

Proof. Let $\bar{r}=$ prime field of k. By Proposition 7, $\mathfrak{C}_u$ is a finite $\bar{r}$-modul and $u(x)$ induces an $\bar{r}$-linear transformation of $\mathfrak{C}_u$ onto some finite subgroup of k^c. Hence [8, Theorem 3], there is a unique simple a.p. $h(x)$ over k^c that is either

zero or has degree less than $\#\mathfrak{C}_u$ = degree $e'(x)$ with the property $u(\Gamma)=h(\Gamma)$, $\Gamma\in\mathfrak{C}_u$. It follows by Proposition 8 that $h(x)$ has coefficients in k. Let

$$w(x) = u(x) - h(x).$$

From (30) we see that $\mathfrak{C}_w=\mathfrak{C}_u$; and

$$w(\mathfrak{C}_w) = \{0\}. \tag{32}$$

Let $e'(x)$ be as described in the theorem. Then by (32), $w(x)=w_1(x)\cdot e'(x)$, where $w_1(x)$ is a polynomial over k. Suppose we have shown

$$w(x) = \alpha_1 e'(x) + \alpha_2(e'(x))^2 + \cdots + \alpha_{m-1}(e'(x))^{m-1} + w_m(x)\cdot(e'(x))^m,$$

where $\alpha_i\in k$ and $w_m(x)$ is a polynomial over k. We see from the fact $e'(x+\Gamma)=e'(x)$, $\Gamma\in\mathfrak{C}_u$, that

$$0 = w(x+\Gamma) - w(x) - w(\Gamma) = (e'(x))^m(w_m(x+\Gamma) - w_m(x)),$$

$$w_m(x+\Gamma) - w_m(x) = 0 \tag{33}$$

for each $\Gamma\in\mathfrak{C}_u$. Setting $x=0$ in (33), we find that the polynomial

$$w_m(x) - w_m(0)$$

vanishes on $\mathfrak{C}_u$ so that

$$w_m(x) = w_m(0) + w_{m+1}(x)\cdot e'(x),$$

where $w_{m+1}(x)$ is a polynomial over k and degree $w_{m+1}(x)<$ degree $w_m(x)$. Hence

$$w(x) = \alpha_1 e'(x) + \cdots + \alpha_m(e'(x))^m + w_{m+1}(x)\cdot(e'(x))^{m+1},$$

and the descent in degree shows $w(x)=v(e'(x))$ for a uniquely determined polynomial $v(x)$ over k. This proves that $g'(x)=e'(x)$ satisfies (31). Suppose $g'(x)$ and $l(x)$ are as in (31). (By application of the appropriate "division" algorithm we can always make (31) into an expression where degree of $l(x)$ is less than degree of $g'(x)$, although this is of no importance here.) Let $\mathfrak{C}'$ be the k^c-kernel of $g'(x)$, which is assumed simple. If $\Gamma'\in\mathfrak{C}'$, then Γ' satisfies (30). Hence $\mathfrak{C}'\subset\mathfrak{C}_u$, and by [8, Theorem 5] $g'(x)$ is an inner component of $e'(x)$, i.e.,

$$e'(x) = f(g'(x))$$

for some additive $f(x)$. Theorem 5 follows.

THEOREM 6. *For k and $u(x)$ as in Theorem 5, let $\mathfrak{D}_u$ be the set of all $\Delta\in k^c$ with*

$$u(x+\Delta) = u(x). \tag{34}$$

Let $e(x)$ be a simple a.p. over k whose kernel is exactly $\mathfrak{D}_u$. Then $e(x)$ is also characterized by:

A1. *$e(x)$ is of maximal degree in the set of all simple a.p. $g(x)$ for which $u(x)$ has a decomposition.*

$$u(x) = v(g(x)), \qquad g(x) \text{ an a.p.}, \qquad v(x) \in k[x]. \tag{35}$$

A2. *$e(x)$ is a l.c.o. composite of all $g(x)$ satisfying* (35).

Proof. It is obvious from (30) and (34) that $\mathfrak{D}_u$ is the intersection of $\mathfrak{C}_u$ and the kernel of any a.p. $l'(x)$ for which $u(x)=v'(e'(x))+l'(x)$, so $\mathfrak{D}_u$ is a finite subgroup of k^{c+} and the $e(x)$ as described exists [8, Theorem 2]; since it satisfies an equation $l'(x)=l''(e(x))$, $u(x)=v''(e(x))+l''(e(x))=v(e(x))$. If $g(x)$ satisfies (35) then $\mathfrak{D}_u$ contains the kernel of $g(x)$, hence $g(x)$ is inner component of $e(x)$.

REMARK. Once all *simple* a.p. satisfying (31) or (35) are known, it is a trivial matter to determine *all* a.p.

4. **Two-sided decompositions.**

THEOREM 7. *Let k, $u(x)$, $d'(x)$, $e'(x)$ be as in Theorems 3, 4, and 5. Let $h(x)$ be any a.p. and $g(x)$ any simple a.p. over k. Then $u(x)$ has a decomposition*

$$u(x) = h(v(g(x))) + l(x) \tag{36}$$

(for some a.p. $l(x)$ and some $v(x)\in k[x]$) if and only if $h(x)$ is an outer component of $d'(x)$ and $g(x)$ is an inner component of $e'(x)$.

Proof. By Theorem 5, $u(x)=v_1(e'(x))+l_1(x)$. By assumption, $d'(x)$ is defined by (18) and (22) for the polynomial $u(x)$. Let $d_1'(x)$ be defined in the same way for the polynomial $v_1(x)$. By Proposition 6 we may assume $d'(x)=d_1'(x)$. By Theorem 3 we find $v_1(x)=d'(v(x))+l_2(x)$; so we get

$$u(x) = d'(v(e'(x))) + l(x), \tag{37}$$

which proves that our condition on $h(x)$ and $g(x)$ implies that $u(x)$ has a decomposition (36).

Conversely, if (36) is satisfied, then Theorems 3 and 5 imply that $h(x)$ is an outer component of $d'(x)$ and $g(x)$ is an inner component of $e'(x)$. Theorem 7 follows.

REMARK. Omitting the restriction that $g(x)$ be simple would have required a tedious but trivial discussion of decompositions

$$u(x) = d''(x^{p^\nu}) \circ v(x^{p^\mu}) \circ e''(x^{p^\lambda})$$

(where we use $\phi(x) \circ \psi(x)$ to denote $\phi(\psi(x))$). We have chosen to study (36) under the restriction that $g(x)$ be simple. We could also have done it under the restriction that $h(x)$ be simple, with similar results.

We conclude with an example to show that an analogue of Theorem 7 cannot be expected for decompositions

$$u(x) = g(v(h(x))). \tag{38}$$

Let k be any field of characteristic 3, let $\varphi(x)=x^3-x$, and let $u(x)=\varphi((\varphi(x))^2)+\varphi(x)=x^3-x+x^{18}-x^2+x^{12}-x^4$. One finds that $d(x)=d'(x)=\varphi(x)$ and (since $u(x+\Gamma)-u(x)-u(\Gamma)=\varphi((\varphi(x)+\varphi(\Gamma))^2-(\varphi(x))^2-(\varphi(\Gamma))^2)=\varphi(2\varphi(x)\cdot\varphi(\Gamma))$), that $e(x)=e'(x)=\varphi(x)$. The decomposition

$$u(x) = (\varphi(x) \circ x^2 \circ \varphi(x)) + \varphi(x)$$

illustrates Theorem 7; but the decompositions $u(x)=\varphi(x)\circ((\varphi(x))^2+x)\circ x=\varphi(x)\circ(x+x^2+x^6+x^4)\circ x=x\circ(\varphi(x^2)+x)\circ\varphi(x)=x\circ(x^6-x^2+x)\circ\varphi(x)$, none of which can be further refined, illustrate the complications that can arise with decompositions (38). It is easy to see that further examples of a $u(x)$ with more than one maximal decomposition (38) could be constructed by choosing the $l(x)$ in (37) properly, and that—in a certain sense—all such examples arise in this way.

References

1. E. Artin, *Linear mappings and existence of a normal basis*, Studies and Essays presented to R. Courant, New York, 1948, pp. 1–5.

2. H. T. Engstrom, *Polynomial substitutions*, Amer. J. Math. vol. 63 (1941) pp. 249–255.

3. K. Hensel, *Zahlentheorie*, Berlin and Leipzig, Goeschen, 1913.

4. I. Kaplansky, *Rings with a polynomial identity*, Bull. Amer. Math. Soc. vol. 54 (1948) pp. 575–580.

5. H. Levi, *Composite polynomials with coefficients in an arbitrary field of characteristic zero*, Amer. J. Math. vol. 64 (1942) pp. 389–400.

6. O. Ore, *On a special class of polynomials*, Trans. Amer. Math. Soc. vol. 35 (1933) pp. 559–584.

7. J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. vol. 23 (1922) pp. 51–66.

8. G. Whaples, *Additive polynomials*, Duke Math. J. vol. 21 (1954) pp. 55–65.

9. ———, *Generalized local class field theory*. I. *Reciprocity law*, Duke Math. J. vol. 19 (1952) pp. 505–517.

10. ———, *Generalized local class field theory*. II. *Existence theorem*, Duke Math. J. vol. 21 (1954) pp. 247–255.

11. ———, *Existence of generalized local class fields*, Proc. Nat. Acad. Sci. U.S.A. vol. 39 (1953) pp. 1100–1103.

Indiana University,
Bloomington, Ind.