Annals of Mathematics
Vol. 59, No. 2, March, 1954
Printed in U.S.A.

DIFFERENTIAL POLYNOMIALS AND DIVISION ALGEBRAS

By A. S. Amitsur

(Received March 24, 1953)

The present paper contains two parts. The object of the first part is to further develop the formal theory of linear homogeneous differential equations. This is used in the second part to construct division algebras and to study the Brauer group of division algebras over a commutative field $\mathcal{C}$ of characteristic zero.

Let F be a transcendental extension of $\mathcal{C}$. Let F possess a derivation $a \rightarrow a'$ such that $\mathcal{C}$ is the field of constants. By $F[t]$ we denote the ring of all non-commutative polynomials in t (known as differential polynomials), where multiplication is defined by: $at = ta + a'$ for every $a \in F$. The formal theory of linear homogeneous differential equations was shown by Ore [9] to be based on the properties of the ring $F[t]$. The aim of the first part is to define resultant of two differential polynomials $p(t)$ and $q(t)$ with properties analogous to the properties of the resultant of two commutative polynomials $p(x)$ and $q(x)$. The resultant defined here which we denote by $p(t) \times q(t)$ is not a constant but a new differential polynomial determined uniquely up to similarity in the sense of Ore [9]. The present definition originates from the following well known result on the resultant of commutative polynomials: If $p(x)$, $q(x)$ are characteristic polynomials of matrices A and B respectively, then the resultant of $p(x)$ and $q(x)$ is the determinant of the Kronecker sum $A \times 1_m - 1_n \times B$,[1] where n and m are the orders of A and B respectively. The main property of the resultant can now be stated as: a necessary and sufficient condition that $p(x)$ and $q(x)$ have a common divisor is that $x = 0$ is a root of the characteristic polynomial of the matrix $A \times 1_m - 1_n \times B$. Using Jacobson's theory of pseudo linear differential equations [6] we define characteristic polynomials in $F[t]$ of matrices in F. The resultant $p(t) \times q(t)$ is then defined as the analogue of the characteristic polynomial of $A \times 1_m + 1_n \times B$, and for this polynomial the analogue of the above stated property of the resultant holds (Theorem 7). In the course of developing the theory of the resultant we develop a theory of duals of differential transformations which we prove corresponds to the adjoint polynomial and equation.

In Part II we consider the problem of constructing all central division algebras over $\mathcal{C}$ which are split by F, where F is the transcendental extension over $\mathcal{C}$ dealt with in Part I.

Let $p(t)$ be a polynomial in $F[t]$. The set of all polynomials $q(t)$ satisfying $q(t)p(t) = p(t)q(t)$ taken modulo $p(t)F[t]$ form a ring $\mathfrak{R}(p)$ which is a finite dimensional algebra over $\mathcal{C}$. If $p(t)$ is irreducible, $\mathfrak{R}(p)$ is a division algebra. The construction of $\mathfrak{R}(p)$ resembles the way of constructing commutative extensions of $\mathcal{C}$. The answer to our problem is that every division algebras over $\mathcal{C}$ which is split by F is isomorphic with a ring $\mathfrak{R}(p)$. Furthermore, using the resultant of

[1] $1 = 1_n$ will denote the unit matrix of order n. The suffix n will be omitted when no confusion is involved.

Part I we are able to characterize all polynomials $p(t)$ whose ring $\mathfrak{R}(p)$ is split by F. The problem of the solutions of differential equations corresponding to these polynomials is settled in Section 8, and a relation between these solutions and the exponent of the corresponding division algebra is treated. The results are then applied to find the Brauer group of all division algebras which are split both by F and by an extension $\mathfrak{D}$ of $\mathfrak{C}$. In particular, if $\mathfrak{D}$ is normal over $\mathfrak{C}$ with a galois group $\mathfrak{G}$, this group is shown to be isomorphic to the first cohomology group of $\mathfrak{G}$ with coefficients in the additive group of all logarithmic derivatives $a^{-1}a'$ of the field $F\mathfrak{D}$, or equivalently with coefficients in the multiplicative group $(F\mathfrak{D}^*)/\mathfrak{D}^*$ where (*) indicates the multiplicative group of nonzero elements; and where $\mathfrak{G}$ is assumed to be extended to the group of automorphisms of $F\mathfrak{D}$ over F and hence acts on the respective additive and multiplicative groups. This last result is also obtained more generally by methods of cohomology theory.

The possibility of extending some of these results to p-algebras of exponent p are pointed out in Section 10.

The known method of constructing central division algebras, as cross products of normal fields with their Galois groups, uses the algebraic splitting fields of the division algebras. The method presented here seems to be a parallel one (for characteristic zero) utilizing transcendental splitting fields. It will be shown elsewhere that given a central division algebra $\mathfrak{A}$ over $\mathfrak{C}$ one can find a transcendental extension F of $\mathfrak{C}$ in which $\mathfrak{C}$ is algebraically closed and which splits $\mathfrak{A}$. By a result of Baer [3] one can define a derivation in F having $\mathfrak{C}$ as the field of constants. In view of these facts it follows that the present method of constructing central division algebras with the aid of differential polynomials yields all central division algebras over $\mathfrak{C}$.

Some of the results of the present paper were included in a doctoral dissertation presented to the Hebrew University in 1949 and carried under the instructions of Professor J. Levitzky. I wish to take this opportunity to thank Professor J. Levitzky for his many helpful suggestions and inspiration.

I. The resultant of differential polynomials

1. Differential polynomials

Let F be a commutative field of characteristic zero which possesses a derivation D. That is, a mapping $D: a \rightarrow a'$ is defined in F such that:

$$(a + b)' = a' + b', \qquad (ab)' = a'b + ab'.$$

The set of all elements with derivative $a' = 0$ constitutes a subfield $\mathfrak{C}$ of F which is known as the *field of constants*. The notation $a^{(n)} = (a^{(n-1)})'$ will be used.

Let $F[t]$ be the ring of all non-commutative polynomials in the indeterminate t with coefficient taken on the right in F and in which multiplication is defined by: $at = ta + a'$.

To each differential polynomial $p(t) = t^n a_0 + t^{n-1} a_1 + \cdots + a_n$, $a_0 \neq 0$, we ascribe a linear homogeneous differential equation of order n in F:

$$p(z) = z^{(n)} a_0 + z^{(n-1)} a_1 + \cdots + z a_n = 0.$$

It is well known that the solutions of $p(z) = 0$ in F form a $\mathcal{C}$-module of dimension $\leqq n$. If r is its dimension, we shall say that r is the *nullity* of the polynomial $p(t)$. Polynomials with degree of nullity equal to their degree will be said to be *completely solvable* in F.

An element $a \in F$ is called a left (right) *root* of $p(t)$ if $p(t) = (t - a)p_1(t)$, $(p = p_1(t)(t - a))$. In considering the right and left roots of differential polynomials one encounters the notion of the logarithmic derivation. The log-derivative of an element a is defined as $a^{-1}a'$, for $a \neq 0$. The set of all log-derivatives of the elements of F form an additive group. For $a^{-1}a' + b^{-1}b' = (ab)^{-1}(ab)'$ and $-(a^{-1}a') = (a^{-1})^{-1}(a^{-1})'$.

Let $y \in F$. One readily verifies that $yp(t) = tq(t) + p(y)$, hence y is a solution of the differential equation $p(z) = 0$ if and only if the polynomial t is a left factor of $yp(t)$. If $y \neq 0$, this is equivalent to $p(t) = y^{-1}tq(t) = (t - y^{-1}y')(yq(t))$. Hence,

LEMMA 1. *$0 \neq y \in F$ is a solution of $p(z) = 0$ if and only if the log-derivative of y is a left root of $p(t)$.*

The ring $F[t]$ is known to be a principal right- and left-ideal ring with both right and left Euclidean-algorithm. So that $F[t]$ is a ring with unique factorization up to similarity (Ore [10]). We recall that two polynomials $p(t)$, $q(t)$ are similar, denoted $p(t) \simeq q(t)$, if $p(t)a(t) = b(t)q(t)$ for some polynomials $a(t)$ and $b(t)$ such that $p(t)$ and $b(t)$ are relatively left prime and $a(t)$ with $q(t)$ are relatively right prime.[2] An equivalent definition is the existence of an isomorphism between $F[t]/q(t)F[t]$ and $F[t]/p(t)F[t]$ when both are considered as right $F[t]$-modules. In this case, similar isomorphism holds also between the quotients modulo the left ideals generated by $p(t)$ and $q(t)$. The definition of similarity is, therefore, symmetrical.

LEMMA 2. *$t - a \simeq t - b$ if and only if $a = b + c^{-1}c'$ for some $c \in F$. In particular, $t - a \simeq t$ is equivalent to $a = c^{-1}c'$ for $c \in F$.*

$t - a \simeq t - b$ is equivalent to the existence of $c, d \in F$ such that $d(t - a) = (t - b)c$ which is the same as $c = d$, $a = b + c^{-1}c'$.

For further application we shall use the notation $p(t) = [p_1(t), \cdots, p_k(t)]$ to denote the fact that $p(t)$ is *left* decomposed into the components $p_1(t), \cdots, p_k(t)$. That is, $p(t)$ is the right least common multiple of the non-constant polynomials $p_1(t), \cdots, p_k(t)$, where each $p_i(t)$ is the left prime with the least common multiple of $p_1(t), \cdots, p_{i-1}(t), p_{i+1}(t), \cdots, p_k(t)$, $i = 1, 2, \cdots, k$.

Let $p(t)$ be a polynomial of degree n and nullity r. Let $q(t)$ be the right common multiple of all left factors of $p(t)$ which are similar to the polynomial t. Then:

LEMMA 3a. *The polynomial $q(t)$ is a completely solvable polynomial of degree r. It is uniquely determined up to right multiplication by an element of F, and the equation $q(z) = 0$ is the minimal equation in F satisfied by all solutions of $p(z) = 0$ in F.*

By the preceding two lemmas it follows that there exists a one to one corre

[2] $a(t)$ and $b(t)$ can be chosen to be of degree $<$ degrees of $q(t)$ and $p(t)$ respectively.

spondence between the solutions of $p(z)$ (up to multiplication by constant elements) and the left factors of $p(t)$ which are similar to t. Each of these factors is also a left factor of $q(t)$, hence the solutions of $p(z) = 0$ and $q(z) = 0$ are identical. These solutions form a $\mathcal{C}$-module of dimension r which implies that the degree of $q(t)$ is $\geqq r$. Let $q_1(z) = 0$ be the minimal differential equation in F satisfied by all solutions of $p(z) = 0$ in F. It is known that this equation is of degree r.

Applying again the preceding lemmas to the polynomials $q(t)$, and $q_1(t)$ we observe that all linear left factors of $q(t)$ which are similar to t are also left factors of $q_1(t)$. $q(t)$ is the common multiple of these linear polynomials. Hence $q_1(t) = q(t)c$. From an argument about the degrees it follows immediately that $c \epsilon F$ and $q(t)$ is of degree r. The uniqueness is evident.

LEMMA 3b. *Let $y_1, \cdots, y_n \epsilon F$. A necessary and sufficient condition that the y_i are $\mathcal{C}$-independent is that the least right common multiple of the polynomials $t - y_i^{-1}y_i'$ is of degree n.*

Let $y_1, \cdots, y_n$ be $\mathcal{C}$-independent. The minimal differential equation $q(z) = 0$ which is satisfied by all y_i is of degree n. By the preceding proof it follows that $q(t)$ is the least common multiple of all $t - y_i^{-1}y_i'$. The same reason yields the converse.

We define a mapping: $p(t) \to p^*(t)$ in $F[t]$ in the following way: if $p(t) = t^n a_0 + t^{n-1}a_1 + \cdots + a_n$ then $p^*(t) = a_0(-t)^n + a_1(-t)^{n-1} + \cdots + a_n$. One immediately identifies the differential equation $p^*(z) = 0$ with the well known adjoint equation of $p(z) = 0$.

THEOREM 1. *The mapping $p(t) \to p^*(t)$ is an antiisomorphism of $F[t]$ onto itself* and $(p^*)^* = p$.

PROOF. Evidently $(p_1 + p_2)^* = p_1^* + p_2^*$. It follows also immediately that $(tp(t))^* = p^*(t) \cdot t^*$. The proof of $(p(t)q(t))^* = q^*(t)p^*(t)$ will follow by a double induction on the degrees of $p(t)$ and $q(t)$. Let $p(t) = a \epsilon F$. If the degree of $q(t)$ is zero, the proof is trivial. Let $q(t)$ be any polynomial of degree >0. Put $q(t) = b + tq_1(t)$, where $b \epsilon F$ and $q_1(t)$ is of degree $<$ degree of $q(t)$. Then, $q^* = b + q_1^*t^*$ and, by induction:

$$\begin{aligned}(aq)^* &= (ab)^* + (atq_1)^* = (ab)^* + (taq_1)^* + (a'q_1)^* \\ &= ab + (aq_1)^*t^* + q_1^*a' = ab + q_1^*at^* + q_1^* = ab + q_1^*(-at + a') \\ &= ab + q_1^*t^* = (b + q_1^*t^*)a = q^*a^*.\end{aligned}$$

Now let $p(t)$ be any polynomial of degree >0. Put $p(t) = tp_1 + a$, $a \epsilon F$, and $p_1(t)$ is a polynomial of degree $<$ degree of $p(t)$. Applying the induction on $p(t)$ we have:

$$(pq)^* = (tp_1q)^* + (aq)^* = (p_1q)^*t^* + q^*a = q^*p_1^*t^* + q^*a = q^*(p_1^*t^* + a) = q^*p^*.$$

It follows also that $p \to p^{**}$ is an isomorphism of $F[t]$ into $F[t]$. Since $t^{**} = t$, $a^{**} = a$, $a \epsilon F$, the last mapping is the identity. Consequently $p^{**} = p$ for every $p \epsilon F[t]$, and $p \to p^*$ maps $F[t]$ onto $F[t]$.

An immediate result of the preceding theorem is:

COROLLARY. *An element $a \in F$ is a left (right) root of $p(t)$ if and only if $-a$ is a right (left) root of $p^*(t)$. In particular, $y^{-1}y'$ is a right root of $p(t)$ if and only if y is a non zero solution of the adjoint equation $p^*(z) = 0$.*

These results follow by applying the (*)-mapping to the factorizations of $p(t)$ and $p^*(t)$ and using Lemma 1.

2. Differential transformations

The differential transformation (d.t.) appears in the theory of systems of linear homogeneous differential equations of order one. In fact, the whole theory of differential complexes introduced by A. Levy [8] is a matrix representation of the theory of the differential transformations. These transformations and their generalizations were introduced and studied by Jacobson in [6]. Some of his results and definitions will be quoted here.

Let $\mathfrak{V}$ be a vector space over F of dimension n. By F_n we shall denote the ring of all square matrices of order n over F. If $A = (a_{ik}) \in F_n$, we write $A' = (a'_{ik})$.

A differential transformation (d.t.) $\mathbf{A}$ of V is a linear mapping: $v \rightarrow v\mathbf{A}$ of $\mathfrak{V}$ into $\mathfrak{V}$ such that:

$$(v_1 + v_2)\mathbf{A} = v_1\mathbf{A} + v_2\mathbf{A}, \qquad (va)\mathbf{A} = v\mathbf{A}a + va' \qquad \text{for } v \in \mathfrak{V},\ a \in F.$$

Let $v_1, \cdots, v_n$ be a basis of $\mathfrak{V}$. The d.t. $\mathbf{A}$ is determined by the images $v_i\mathbf{A}$. Namely, by the matrix A defined by:

$$(v_1\mathbf{A}, \cdots, v_n\mathbf{A}) = (v_1, \cdots, v_n)A.$$

Changing the basis of $\mathfrak{V}$ to (w) by a matrix P, i.e. $(w) = (v)P$, we obtain another matrix B corresponding to the d.t. $\mathbf{A}$. This matrix is readily seen to be $B = P^{-1}AP + P^{-1}P'$. Two matrices A and B satisfying the last equality for some regular matrix P are called *similar matrices* and will be denoted by $A \simeq B$. Two d.t.'s $\mathbf{A}$ and $\mathbf{B}$ are called *similar* if there exists a *linear* transformation $\mathbf{P}$ in $\mathfrak{V}$ such that $\mathbf{B} = \mathbf{P}^{-1}\mathbf{A}\mathbf{P}$. A simple calculation shows that the matrices corresponding to two similar d.t.'s with respect to the same basis are similar, and conversely. We extend the notion of similarity of two d.t.'s acting on different spaces. Let $\mathfrak{V}$ be a vector space with a d.t. $\mathbf{A}$. The ring $F[\mathbf{A}]$ is then a ring of operators acting on the right of V. To denote the fact that $\mathfrak{V}$ is a vector space with the ring of operators $F[\mathbf{A}]$, we write $\mathfrak{V} = (\mathfrak{V}, \mathbf{A})$.

Let $\mathfrak{V} = (\mathfrak{V}, \mathbf{A})$ and $\mathfrak{W} = (\mathfrak{W}, \mathbf{B})$. A linear transformation $\mathbf{P}$ of $\mathfrak{V}$ into $\mathfrak{W}$ is called an operator homomorphism of $(\mathfrak{V}, \mathbf{A})$ into $(\mathfrak{W}, \mathbf{B})$ if $(v\mathbf{A})\mathbf{P} = v(\mathbf{P}\mathbf{A})$, $v \in \mathfrak{V}$. Let $(v_1, \cdots, v_n)$ be a basis of $\mathfrak{V}$ and $(w_1, \cdots, w_m)$ be a basis of $\mathfrak{W}$. The linear transformation $\mathbf{P}$ is uniquely determined by the matrix P with m rows and n columns, defined by:

$$(v_1\mathbf{P}, \cdots, v_n\mathbf{P}) = (w_1, \cdots, w_m)P,$$

and in order that $\mathbf{P}$ should be an operator homomorphism it is necessary and sufficient that $PA = BP + P'$ where A, B are the matrices of $\mathbf{A}$ and $\mathbf{B}$

corresponding to the bases (v_i) and (w_i) respectively. This justifies the following definition of similarity between a d.t. **A** acting on $\mathfrak{V}$ and a d.t. **B** acting on $\mathfrak{W}$. **A** and **B** will be said to be *similar* if there exists an operator isomorphism between $(\mathfrak{V}, \mathbf{A})$ and $(\mathfrak{W}, \mathbf{B})$ and we then write $\mathbf{A} \simeq \mathbf{B}$, We remark here that if $n = m$, then **P** is an isomorphism if and only if P is a regular matrix.

The starting point of the theory of differential transformations (and, more generally, the pseudo-linear transformations), as observed by Jacobson in [6], is a homomorphism of the Kronecker product $\mathfrak{V}_t = \mathfrak{V} \times F[t]$ onto $(\mathfrak{V}, \mathbf{A})$ where the first is considered as a group with the operator $F[t]$, and the latter with $F[\mathbf{A}]$. More precisely, this homomorphism is the mapping:

$$\sum v_i p_i(t) \rightarrow \sum v_i p_i(\mathbf{A}).$$

Let $\mathfrak{W}_t$ be the kernel of this homomorphism. The main results of [6] are corollaries of the following operator-isomorphism:

$$\text{(A)} \qquad (\mathfrak{V}, \mathbf{A}) = \mathfrak{V}_t/\mathfrak{W}_t \cong F[t]/g_1(t)F[t] \oplus \cdots \oplus F[t]/g_n(t)F[t]$$

where $g_1(t), \cdots, g_n(t)$ are the invariant factors of the matrix $A - t \cdot 1$[3] with A any matrix corresponding to the d.t. A. Although this result is not explicitly stated in [6] it is contained there in pp. 495–6.

At this point we introduce the assumption that F is of characteristic zero. In this case, by case 3 of [6] p. 499, the matrices of F_n have only *one* non unit invariant factor, consequently, $\mathfrak{V}$ is a cyclic space and the homomorphism (A) has the following form

$$\text{(B)} \qquad \varphi: F[t]/g(t)F[t] \cong (\mathfrak{V}, \mathbf{A}) \qquad \text{with } \varphi(t) = \varphi(1)\mathbf{A}$$

and $g(t)$ is a polynomial of degree n.

This isomorphism φ is the relation between system of n linear differential equations of order one and one differential equation of order n.

Let A be a matrix of order n, and let $g(t)$ be the invariant factor of A. If **A** is any d.t. with the matrix A, we shall say that $g(t)$ is a *characteristic polynomial* of the matrix A, or of the d.t. **A**. We shall sometimes say that $g(t)$ is a polynomial which belongs to $(\mathfrak{V}, \mathbf{A})$. One readily observes that the isomorphism of (B) can also be taken as definition of the characteristic polynomial.

The characteristic polynomial being the invariant factor is uniquely determined up to similarity. Conversely, if $f(t)$ belongs to $(\mathfrak{V}, \mathbf{A})$ and $g(t)$ belongs to $(\mathfrak{W}, \mathbf{B})$. By (B) we have $(\mathfrak{V}, \mathbf{A}) \cong F[t]/f(t)F[t]$; $(\mathfrak{W}, \mathbf{B}) \cong F[t]/g(t)F[t]$ so that, **A** and **B** are similar if and only if:

$$F[t]/f(t)F[t] \cong (\mathfrak{V}, \mathbf{A}) \cong (\mathfrak{W}, \mathbf{B}) = F[t]/g(t)F[t],$$

which is equivalent to the fact that $f(t)$ and $g(t)$ are similar.

Let $f(t)$ be any polynomial of degree n, then $f(t)$ is a characteristic polynomial of some d.t. **A**. Indeed, put $\mathfrak{V} = F[t]/f(t)F[t]$, then $\mathfrak{V}$ is of dimension n, and the mapping $p(t) \rightarrow p(t)t$ determines a d.t. **A** in $\mathfrak{V}$ whose characteristic polynomial is readily seen to be $f(t)$.

[3] We shall omit the suffix n when this will not involve any confusion.

Combining previous remarks about the relation between similarity of matrices and of d.t.'s and the last results, we have:

THEOREM 2. *The correspondence between matrices, differential transformations, and characteristic polynomials is a one-one correspondence between classes of similarity of the respective objects.*

The following notation will be used: If $\mathfrak{W}$ is an invariant subspace of $(\mathfrak{V}, \mathbf{A})$, then $\mathbf{A}$ induces a d.t. in $\mathfrak{W}$ and in $\mathfrak{V}/\mathfrak{W}$. These d.t.'s will be denoted by $\mathbf{A}_{\mathfrak{W}}$ and $\mathbf{A}/\mathbf{A}_{\mathfrak{W}}$ respectively. We also use the notation $\mathbf{A} > \mathbf{A}_{\mathfrak{W}}$. If $\mathfrak{V} = \mathfrak{V}_1 \oplus \cdots \oplus \mathfrak{V}_r$, where $\mathfrak{V}_i$ are invariant subspaces of $(\mathfrak{V}, \mathbf{A})$, we shall write $\mathbf{A} = \mathbf{A}_1 \oplus \cdots \oplus \mathbf{A}_r$ where $\mathbf{A}_i = \mathbf{A}_{\mathfrak{V}_i}$.

LEMMA 4. *If $g(t)$ belongs to $(\mathfrak{V}, \mathbf{A})$ and $(\mathfrak{V}, \mathbf{A}) \supset (\mathfrak{W}, \mathbf{A}_{\mathfrak{W}})$ then $g(t) = g_1(t)g_2(t)$ where $g_1(t)$ is a characteristic polynomial of $\mathbf{A}/\mathbf{A}_{\mathfrak{W}}$ and $g_2(t)$ is a characteristic polynomial of $\mathbf{A}_{\mathfrak{W}}$. Conversely, if $g(t) = g_1(t)g_2(t)$ then $(\mathfrak{V}, \mathbf{A}) \supset (\mathfrak{W}, \mathbf{A}_{\mathfrak{W}})$ wıth $g_1(t)$ belonging to $\mathbf{A}/\mathbf{A}_{\mathfrak{W}}$ and $g_2(t)$ to $\mathbf{A}_{\mathfrak{W}}$.*

Indeed, since $(\mathfrak{V}, \mathbf{A}) \cong F[t]/g(t)F[t]$ and $F[t]$ is a principal ideal ring, the module $\mathfrak{W}$ will be mapped onto a quotient $g_1(t)F[t]/g(t)F[t]$. Consequently, $g(t) = g_1(t)g_2(t)$ and the isomorphism when restricted to $\mathfrak{W}$ and $\mathfrak{V}/\mathfrak{W}$ yields

$$(\mathfrak{V}/\mathfrak{W}, \mathbf{A}/\mathbf{A}_{\mathfrak{W}}) \cong F[t]/g_1(t)F[t]$$

and,

$$(\mathfrak{W}, \mathbf{A}_{\mathfrak{W}}) \cong g_1(t)F[t]/g_1(t)g_2(t)F[t] \cong F[t]/g_2(t)F[t],$$

which proves the first part of the lemma. The rest of the lemma follows from the fact that the preceding proof can be carried also in the reverse direction.

We introduce now the notion of nullity of a d.t. and a corresponding differential-nullity of a matrix.

Let $\mathfrak{V} = (\mathfrak{V}, \mathbf{A})$. Put $\mathfrak{N}(\mathbf{A}) = \{v \mid v \in \mathfrak{V}, v\mathbf{A} = 0\}$. Then:

LEMMA 5. *If $\mathfrak{V}$ is of dimension n, then $\mathfrak{N}(\mathbf{A})$ is a $\mathfrak{C}$-module of dimension $\leqq n$. Furthermore, any set of $\mathfrak{C}$-independent vectors of $\mathfrak{N}(\mathbf{A})$ are also F-independent in $\mathfrak{V}$.*

In fact, it suffices to show only the second part of the theorem. Let $v_1, \cdots, v_k \in \mathfrak{N}(\mathbf{A})$ be $\mathfrak{C}$-independent. Choose among them a maximal number $v_1, \cdots, v_r$ which are F-independent. If $r < k$, then $v_{r+1} = \sum_{i=1}^{r} v_i a_i$, $a_i \in F$. Hence:

$$0 = v_{r+1}\mathbf{A} = \sum v_i a_i \mathbf{A} = \sum v_i \mathbf{A} a_i + \sum v_i a_i' = \sum v_i a_i'.$$

Since $v_1, \cdots, v_r$ are F-independent, $a_i' = 0$. Consequently $a_i \in \mathfrak{C}$, which implies that $v_1, \cdots, v_r, v_{vr+1}$ are $\mathfrak{C}$-dependent. Contradiction. The rest is trivial.

The dimension of the module $\mathfrak{N}(\mathbf{A})$ is called the *nullity* of $\mathbf{A}$. If A is any matrix of $\mathbf{A}$ with respect to a base $v_1, \cdots, v_n$ of $\mathfrak{V}$, then one readily observes that $v = \sum v_i a_i \in \mathfrak{N}(\mathbf{A})$ if and only if the row (a_i) satisfies $A(a_i) + (a_i)' = 0$. With the aid of the preceding lemma one can verify that the nullity of $\mathbf{A}$ is equal to maximal rank of the matrix P which satisfies $AP + P' = 0$. We call this number the *differential nullity* of A. Another consequence of the preceding lemma is that if $P_1, \cdots, P_k$ are matrices satisfying $AP_i + P_i' = 0$ and which are C-independent, they are also F-independent. Another way to look at the differential nullity is the following: Since the basis of $\mathfrak{N}(\mathbf{A})$ is also F-independent, one can complete this basis to a basis of $\mathfrak{B}$. The corresponding matrix of $\mathbf{A}$ will contain, therefore, a number of zero rows equal to the nullity of $\mathbf{A}$.

The following theorem will often be used:

THEOREM 3. *The nullity of a* d.t. $\mathbf{A}$ *is equal to the nullity of the adjoint equation of the characteristic polynomial* $f(t)$ *of* $\mathbf{A}$. *In fact, there is a* $\mathfrak{C}$*-isomorphism between* $\mathfrak{N}(\mathbf{A})$ *and the space of solutions of the equation* $f^*(z) = 0$.

PROOF. Since $(\mathfrak{B}, \mathbf{A}) \cong F[t]/f(t)F[t]$, to each $v \in \mathfrak{N}(\mathbf{A})$ corresponds a polynomial $f_v(t)$, such that $f_v(t)t \in f(t)F[t]$. The degree of $f_v(t)$can be chosen to be less than n, the degree of $f(t)$. Hence $f_v(t)t = f(t)y_v$. Applying (*) we have $y_v f^*(t) = (-t)f_v^*(t)$. By the proof of Lemma 1 it follows that y_v is a solution of $f^*(z) = 0$. Conversely, if y_v is a solution of $f^*(z) = 0$ then the same methods yield that the vector v corresponding to $f_v(t)$ satisfies $v\mathbf{A} = 0$, i.e. $v \in \mathfrak{N}(\mathbf{A})$.

One readily verifies that the mapping $v \rightarrow y_v$ gives the required isomorphism and hence the equality of the dimensions.

One may start from a given differential polynomial $p(t)$ and find a space $(\mathfrak{B}, \mathbf{A})$ such that $p^*(t)$ belongs to $(\mathfrak{B}, \mathbf{A})$, then the nullity of $\mathbf{A}$ is equal to the nullity of $p(t)$. If now $q(t) \simeq p(t)$, $q^*(t) \simeq p^*(t)$ and hence $q^*(t)$ belongs also to $(\mathfrak{B}, \mathbf{A})$ and, therefore, has the same nullity. This proves that:

COROLLARY. *The nullity of a differential polynomial* (*and, therefore, of a* d.t.) *is invariant under similarity.*

3. Dual d.t.

Let $\mathfrak{B} = (\mathfrak{B}, \mathbf{A})$. Let $\mathfrak{B}^*$ be the *dual vector space* of $\mathfrak{B}$ over F, i.e. $\mathfrak{B}^*$ is the set of all linear functions r: $\mathfrak{B} \rightarrow F$. For $v \in \mathfrak{B}$, $r \in \mathfrak{B}^*$ we shall write $rv(\in F)$ for the value in F of the function r at the vector v. Thus, we have:

$$r(v_1 + v_2) = rv_1 + rv_2 \,; \qquad (ra)v = r(va) = (rv)a \text{ for every } a \in F.$$

Let $v_1, \cdots, v_n$ be a basis of $\mathfrak{B}$, the set of functions $r_1, \cdots, r_n \in \mathfrak{B}^*$ defined by: $r_i v_k = \delta_{ik}$, is a basis of $\mathfrak{B}^*$ called the *dual basis* of (v_i).

The dual d.t. $\mathbf{A}^*$ in $\mathfrak{B}^*$ of $\mathbf{A}$ is defined as follows:

For every $r \in \mathfrak{B}^*$, $(r\mathbf{A}^*)v = -r(v\mathbf{A}) + (rv)'$.[4] To justify this definition we show:

LEMMA 6. $\mathbf{A}^*$ *is a differential transformation in* $\mathfrak{B}^*$.

Evidently $r\mathbf{A}^*$ is a linear mapping. That is $(r\mathbf{A}^*)(v_1 - v_2) = (r\mathbf{A}^*)v_1 - (r\mathbf{A}^*)v_2$. For $a \in F$ we have:

$$\begin{aligned}(r\mathbf{A}^*)(va) &= -r(va\mathbf{A}) + [r(va)]' \\ &= -[r(v\mathbf{A})]a - (rv)a' + (rv)a' + (rv)'a = [(r\mathbf{A}^*)v]a.\end{aligned}$$

This proves that $r\mathbf{A}^* \in \mathfrak{B}^*$. $\mathbf{A}^*$ is a d.t., for:

$$(ra\mathbf{A}^*)v = -ra(v\mathbf{A}) + [(ra)v]' = -r(v\mathbf{A})a + (rv)'a + (rv)a' = (r\mathbf{A}^*a)v + (ra')v.$$

That is: $ra\mathbf{A}^* = r\mathbf{A}^*a + ra'$.

LEMMA 7. *Let* $g(t)$ *belong to* $(\mathfrak{B}, \mathbf{A}$ *and let* A *be a matrix corresponding to* $\mathbf{A}$ *with*

[4] This can be easily identified with well known Lagrange formula of the adjoint.

respect to a basis (v_i) *of* $\mathfrak{V}$. *Then, the polynomial* $g^*(t)$ *belongs to* $(\mathfrak{V}^*, \mathbf{A}^*)$ *and the matrix*[5] $-A^t$ *corresponds to* $\mathbf{A}^*$ *with respect to the dual basis* (v_i^*) *of* (v_i).

The second part of the theorem is readily verified by computation. To prove the first part we extend the antiisomorphism (*) of $F[t]$ to an antiisomorphism of the matrix ring $F_n[t]$ by defining:

$$P^* = (p^*_{ij}(t))^t \text{ where } P = (p_{ij}(t)) \in F_n[t].$$

One readily proves that $P \to P^*$ is an antiisomorphism of $F_n[t]$ and that $P^{**} = P$. Now, by definition $g(t)$ is the invariant factor of the matrix A, which means that there exist two invertible matrixes P, Q in $F_n[t]$ such that $A - t\cdot 1 = PGQ$, where G is a diagonal matrix with units in the diagonal except at the last place where $g(t)$ stands. Apply (*) to the last and obtain $A^t + t\cdot 1 = Q^*G^*P^*$, so that G^* is a diagonal matrix equivalent to $(-A^t) - t\cdot 1$. This is equivalent to the fact that $g^*(t)$ is the invariant factor of $-A^t$; hence $g^*(t)$ belongs to $(\mathfrak{V}^*, \mathbf{A}^*)$.

LEMMA 8. *If* $\mathbf{P}$ *is a linear transformation in* $\mathfrak{V}$, *and* $\mathbf{A}$ *is a* d.t. *in* $\mathfrak{V}$, *then* $(\mathbf{PAP}^{-1})^* = \mathbf{P}^{*-1}\mathbf{A}^*\mathbf{P}^*$, *where* $\mathbf{P}^*$ *is the ordinary dual of the linear transformation of* $\mathbf{P}$.

Indeed,

$$\begin{aligned}(r\mathbf{P}^{*-1}\mathbf{A}^*\mathbf{P}^*)v = (r\mathbf{P}^{*-1}\mathbf{A})(v\mathbf{P}) &= -(r\mathbf{P}^*)^{-1}(v\mathbf{PA}) + [(r\mathbf{P}^{*-1})(v\mathbf{P})]' \\ &= -r(v\mathbf{PAP}^{-1}) + [rv]' = r(\mathbf{PAP}^{-1})^*v.\end{aligned}$$

COROLLARY. *If* $\mathbf{A} \simeq \mathbf{B}$ *then* $\mathbf{A}^* \simeq \mathbf{B}^*$.

This corollary follows also by Lemma 7.

Let O_n be the zero matrix of order n, and let $e_n(t) = e(t)$ be a fixed characteristic polynomial of O_n in $F[t]$. Using the dual of d.t. we show:

THEOREM 4. (1) $e(t)^* \simeq e(t)$.

(2) *A polynomial* $q(t)$ *of degree* n *is completely soluble if and only if* $q(t) \simeq e_n(t)$.

(3) *Every right or left factor of degree* m *of a polynomial similar to* $e(t)$ *is similar to* $e_m(t)$.

The first follows immediately from the fact that $e^*(t)$ is a characteristic polynomial of $-O^t = 0$.

To prove (2) we consider a vector space $\mathfrak{V}$ with a d.t. $\mathbf{Z}$ which has the matrix O_n with respect to a base (v_i) of $\mathfrak{V}$. So that $e_n^*(t)$ belongs to $(\mathfrak{V}^*, \mathbf{Z}^*)$. It follows immediately that $\mathfrak{N}(\mathbf{Z}^*)$ is an n-dimensional $\mathfrak{C}$-space with the basis (v_i^*) since $v_i^*\mathbf{Z}^* = 0$. Hence, by Theorem 3 $[e_n^*(t)]^* = e_n(t)$ is a completely solvable polynomial of degree n.

Generally, if $q(t) \simeq e_n(t)$, then $q^*(t) \simeq e^*(t)$. Consequently $q^*(t)$ belongs to $(\mathfrak{V}^*, \mathbf{Z}^*)$, hence by Theorem 3, $q(t)$ is completely solvable.

Conversely, if $q(t)$ is completely solvable, let $q^*(t)$ belong to $(\mathfrak{V}, \mathbf{A})$. Since $q^{**} = q$, it follows by Theorem 3 that $\mathfrak{N}(\mathbf{A})$ is of dimension n. Let $v_1, \cdots, v_n$ be a basis of $\mathfrak{N}(\mathbf{A})$. By Lemma 5, the set (v_i) is also a basis of V. The matrix of A with respect to this basis is readily seen to be O_n. Hence $q^*(t) \simeq e_n(t)$. Consequently, $q(t) \simeq e_n^*(t) \simeq e_n(t)$. q.e.d.

[5] A^t denotes the transpose matrix of A.

Let $e_n(t) = g_1(t)g_2(t)$, and let $e_n(t)$ belong to $(\mathfrak{V}, \mathbf{Z})$. Let $v_1, \cdots, v_n$ be a basis of $\mathfrak{V}$ such that $v_i\mathbf{Z} = 0$. Then $\mathfrak{V}$ is completely reducible, in fact $(\mathfrak{V}, \mathbf{A}) = v_1F \oplus v_2F \oplus \cdots \oplus v_nF$. By Lemma 4, there exists an invariant subspace $\mathfrak{W}$ such that $g_1(t)$ belongs to $(\mathfrak{V}/\mathfrak{W}, \mathbf{Z}/\mathbf{Z}_{\mathfrak{W}})$ and $g_2(t)$ belongs to $(\mathfrak{W}, \mathbf{Z}_{\mathfrak{W}})$. By well known results on abelian groups with operators, $(\mathfrak{W}, \mathbf{Z}_{\mathfrak{W}})$ is completely reducible and is isomorphic with a sum of the form $v_1F \oplus \cdots \oplus v_rF = \mathfrak{W}'$. Evidently $e_r(t)$ belongs to $(\mathfrak{W}', \mathbf{Z}_{\mathfrak{W}'})$ so that $e_r(t)$ belongs also to $(\mathfrak{W}, \mathbf{Z}_{\mathfrak{W}})$. Hence $g_1(t) \simeq e_r(t)$. A similar fact is true for $(\mathfrak{V}/\mathfrak{W}, \mathbf{Z}/\mathbf{Z}_{\mathfrak{W}})$. Consequently, $g_2(t) \simeq e_r(t)$. q.e.d.

COROLLARY. *The fact that* $(\mathfrak{V}, \mathbf{A}) = v_1F \oplus \cdots \oplus v_nF$ *means by the results of Jacobson that* $e_n(t) \simeq [g_1(t), \cdots, g_n(t)]$, *where* $g_i(t)$ *belongs to* v_iF; *hence, trivially, similar to* t.

The polynomials $e_n(t)$ can be chosen in many ways. In particular, we choose $e_1(t) = t$, and for the rest of the paper the polynomials $e_1(t), e_2(t), \cdots$ will be assumed to be fixed polynomials in $F[t]$.

4. The resultant of differential polynomials

Let $(\mathfrak{V}, \mathbf{A})$, $(\mathfrak{W}, \mathbf{B})$ be two vector spaces of dimensions n and m respectively. In the product space $\mathfrak{V} \times \mathfrak{W}$ we define a d.t. $\mathbf{C}$ as follows:

$$\text{For } u \in \mathfrak{V} \times \mathfrak{W},\ u = \sum v_i \times w_i,\ u\mathbf{C} = \sum v_i\mathbf{A} \times w_i + \sum v_i \times w_i\mathbf{B}.$$

The definition is justified by the proof of the following lemma:

LEMMA 9. $\mathbf{C}$ *is a* d.t. *in* $\mathfrak{V} \times \mathfrak{W}$. *If* A *is the matrix of* $\mathbf{A}$ *with respect to the basis* (v_i) *of* $\mathfrak{V}$ *and* B *is the matrix of* $\mathbf{B}$ *with respect to the basis* (w_i) *of* $\mathfrak{W}$ *then*[1] $A \times 1_m + 1_n \times B$ *is the matrix of* C *with respect to the basis* $(v_i \times w_j)$ *of* $\mathfrak{V} \times \mathfrak{W}$.

The space $\mathfrak{U} = \mathfrak{V} \times \mathfrak{W}$ is defined as the quotient of the free module $\bar{\mathfrak{U}}$ generated by the couples (v, w), $v \in \mathfrak{V}$, $w \in \mathfrak{W}$ modulo the submodule $\bar{\mathfrak{U}}_0$ generated by the elements $(v_1 + v_2, w) - (v_1, w) - (v_2, w)$; $(v, w_1 + w_2) - (v, w_1) - (v, w_2)$; $(va, w) - (v, w)a$, $(v, wa) - (v, w)a$, for every $v, v_i \in \mathfrak{V}$; $w, w_i \in \mathfrak{W}$ and $a \in F$.

Define a d.t. $\bar{\mathbf{C}}$ in $\bar{\mathfrak{U}}$ by:

$$(\textstyle\sum(v_i, w_i)a_i)\bar{\mathbf{C}} = \sum(v_i\mathbf{A}, w_i)a_i + \sum(v_i, w_i\mathbf{B})a_i + \sum (v_i, w_i)a_i'.$$

One readily verifies that $\bar{\mathbf{C}}$ is a d.t. and $\bar{\mathfrak{U}}_0$ is an invariant subspace. Denote by $\bar{\mathbf{C}}_0$ the effect of $\bar{\mathbf{C}}$ on $\bar{\mathfrak{U}}_0$, then $\mathbf{C} = \bar{\mathbf{C}}/\bar{\mathbf{C}}_0$ is a d.t. in $\bar{\mathfrak{U}}/\mathfrak{U}_0 = \mathfrak{V} \times \mathfrak{W}$. The rest of the proof follows now immediately by computation.

NOTATIONS: We write $\mathbf{C} = \mathbf{A} \boldsymbol{\times} \mathbf{B}$ and the matrix $A \boldsymbol{\times} B = A \times 1_m + 1_n \times B$.[6]

THEOREM 5. (1) *If* $\mathbf{A} \simeq \mathbf{A}_1$, $\mathbf{B} \simeq \mathbf{B}_1$, *then* $\mathbf{A} \boldsymbol{\times} \mathbf{B} \simeq \mathbf{A}_1 \boldsymbol{\times} \mathbf{B}_1$.

(2) $\mathbf{A} \boldsymbol{\times} \mathbf{B} \simeq \mathbf{B} \boldsymbol{\times} \mathbf{A}$.

(3) $\mathbf{A} \boldsymbol{\times} (\mathbf{B} \boldsymbol{\times} \mathbf{C}) \simeq (\mathbf{A} \boldsymbol{\times} \mathbf{B}) \boldsymbol{\times} \mathbf{C}$.

(4) *If* $\mathbf{A} = \mathbf{A}_1 \oplus \cdots \oplus \mathbf{A}_r$ *then* $\mathbf{A} \boldsymbol{\times} \mathbf{B} = (\mathbf{A}_1 \boldsymbol{\times} \mathbf{B}) \oplus \cdots \oplus (\mathbf{A}_r \boldsymbol{\times} \mathbf{B})$.

(5) *If* $\mathbf{A} > \mathbf{A}_1$, *then* $\mathbf{A} \boldsymbol{\times} \mathbf{B} > \mathbf{A}_1 \boldsymbol{\times} \mathbf{B}$ and $(\mathbf{A} \boldsymbol{\times} \mathbf{B})/(\mathbf{A}_1 \boldsymbol{\times} \mathbf{B}) \simeq (\mathbf{A}/\mathbf{A}_1) \boldsymbol{\times} \mathbf{B}$.

(6) $(\mathbf{A} \boldsymbol{\times} \mathbf{B})^* \simeq \mathbf{A}^* \boldsymbol{\times} \mathbf{B}^*$.

[6] The notation for the matrix is due to C. Chevalley [4].

Proof. If φ is the operator isomorphism of $(\mathfrak{V}, \mathbf{A}) \cong (\mathfrak{V}_1, \mathbf{A}_1)$ and ψ is the operator isomorphism of $(\mathfrak{W}, \mathbf{B}) = (\mathfrak{W}_1, \mathbf{B}_1)$, then $\varphi \times \psi$ will define an operator isomorphism $(\mathfrak{V} \times \mathfrak{W}, \mathbf{A} \boldsymbol{\times} \mathbf{B}) \cong (\mathfrak{V}_1 \times \mathfrak{W}_1, \mathbf{A}_1 \boldsymbol{\times} \mathbf{B}_1)$. Indeed, for every $v \in \mathfrak{V}$, $w \in \mathfrak{W}$,

$$(v \times w)(\mathbf{A} \boldsymbol{\times} \mathbf{B})(\varphi \times \psi) = (v\mathbf{A} \times w + v \times w\mathbf{B})(\varphi \times \psi) = v\mathbf{A}\varphi \times w\psi$$
$$+ v\varphi \times w\mathbf{B}\psi = v\varphi\mathbf{A}_1 \times w\psi + v\varphi \times w\psi\mathbf{B}_1 = (v \times w)(\varphi \times \psi)(\mathbf{A}_1 \boldsymbol{\times} \mathbf{B}_1).$$

Thus $(\mathbf{A} \boldsymbol{\times} \mathbf{B})(\varphi \times \psi) = (\varphi \times \psi)(\mathbf{A}_1 \boldsymbol{\times} \mathbf{B}_1)$ which proves (1).

(2) and (3) follow by showing that the canonical isomorphism between $\mathfrak{V} \times \mathfrak{W}$ and $\mathfrak{W} \times \mathfrak{V}$, and so between $(\mathfrak{V} \times (\mathfrak{W} \times \mathfrak{U}))$ and $(\mathfrak{V} \times \mathfrak{W}) \times \mathfrak{U}$ is also operator isomorphism.

To prove (4) we note that if $\mathfrak{V} = \mathfrak{V}_1 \oplus \cdots \oplus \mathfrak{V}_r$, where $\mathbf{A}_i = \mathbf{A}_{\mathfrak{V}_i}$, then $\mathfrak{V} \times \mathfrak{W} = \mathfrak{V}_1 \times \mathfrak{W} \oplus \cdots \oplus \mathfrak{V}_r \times \mathfrak{W}$, and one can readily show that $(\mathbf{A} \boldsymbol{\times} \mathbf{B})_{\mathfrak{V}_i \times \mathfrak{W}} = \mathbf{A}_i \boldsymbol{\times} \mathbf{B}$. The same is true for (5). Here if $\mathfrak{V} \supset \mathfrak{V}_1$, then $\mathfrak{V} \times \mathfrak{W} \supset \mathfrak{V}_1 \times \mathfrak{W}$ and $(\mathbf{A} \boldsymbol{\times} \mathbf{B})_{\mathfrak{V}_i \times \mathfrak{W}} = \mathbf{A}_1 \boldsymbol{\times} \mathbf{B}$ and the isomorphism $(\mathfrak{V} \times \mathfrak{W})/(\mathfrak{V}_2 \times \mathfrak{W}) = (\mathfrak{V}/\mathfrak{V}_1) \times \mathfrak{W}$ yields the second part of (5).

To prove (6) we identify $(\mathfrak{V} \times \mathfrak{W})^*$ with $\mathfrak{V}^* \times \mathfrak{W}^*$ by defining for every $r \times s \in \mathfrak{V}^* \times \mathfrak{W}^*$, and $v \times w \in \mathfrak{V} \times \mathfrak{W}$: $(r \times s)\ (v \times w) = (rv)(sw)$, and extending this by linearity to the space $\mathfrak{V}^* \times \mathfrak{W}^*$, it is easily verified that the latter space yields the whole space $(\mathfrak{V} \times \mathfrak{W})^*$. Then:

$$\begin{aligned}
[(r \times s)(\mathbf{A}^* \boldsymbol{\times} \mathbf{B}^*)](v \times w) &= (r\mathbf{A}^* \times s + r \times s\mathbf{B}^*)(v \times w) \\
&= (r\mathbf{A}^* \times s)(v \times w) + (r \times s\mathbf{B}^*)(v \times w) \\
&= -(r\mathbf{A}^*v)(sw) + (rv)(s\mathbf{B}^*w) \\
&= -(rv\mathbf{A})(rw) + (rv)'(sw) - (rv)(sw\mathbf{B}) + (rv)(sw)' \\
&= -(r \times s)(v\mathbf{A} \times w + v \times w\mathbf{B}) + [(rv)(sw)]' \\
&= [(r \times s)(\mathbf{A} \boldsymbol{\times} \mathbf{B})^*](v \times w).
\end{aligned}$$

After these preparations we define the resultant:

Definition. Let $f(t)$, $g(t)$ be two polynomials of degrees n and m respectively. Choose spaces $(\mathfrak{V}, \mathbf{A})$ and $(\mathfrak{W}, \mathbf{B})$ such that $f(t)$ and $g(t)$ are characteristic polynomials of $\mathbf{A}$ and $\mathbf{B}$ respectively. Then the *resultant* $f(t) \times g(t)$ of $f(t)$ and $g(t)$ is defined as a characteristic polynomial of $\mathbf{A} \boldsymbol{\times} \mathbf{B}$.[7]

The definition will be shown to be independent of $\mathbf{A}$ and $\mathbf{B}$.

Theorem 6. (1) *$f(t) \times g(t)$ is a polynomial of degree nm uniquely determined up to similarity.*

(2) *If $f(t) \simeq f_1(t)$, $g(t) \simeq g_1(t)$, then $f(t) \times g(t) \simeq f_1(t) \times g_1(t)$.*

(3) *$f(t) \times g(t) \simeq g(t) \times f(t)$.*

(4) *$f(t) \times (g(t) \times h(t)) \simeq (f(t) \times g(t)) \times h(t)$.*

[7] One can choose as resultant any characteristic polynomial, namely any representative of the class of similarity of the characteristic polynomials of $\mathbf{A} \boldsymbol{\times} \mathbf{B}$.

(5) *If* $g(t) = g_1(t) \cdots g_r(t)$, *then* $f(t) \times g(t) = h_1(t) \cdots h_r(t)$ *where* $h_i(t) \simeq f(t) \times g_i(t)$; *and, if* $g(t) = [g_1(t), \cdots, g_r(t)]$ *then* $f(t) \times g(t) = [h_1(t), \cdots, h_r(t)]$ *where* $h_i(t) = f(t) \times g_i(t)$.

(6) $(f(t) \times g(t))^* \simeq f^*(t) \times g^*(t)$.

(7) $f(t) \times (t - a) \simeq f(t - a)$.

Or more generally,

(8) *If* B *is any matrix whose characteristic polynomial is* $g(t)$ *then* $f(t) \times g(t)$ *is the invariant factor of the matrix* $f(t - B) = (t \cdot 1 - B)^n + (t \cdot 1 - B)^{n-1} a_1 + \cdots + 1 \cdot a_n$ *where* $f(t) = t^n a_0 + \cdots + a_n$, $a_0 \neq 0$.

Proof. Both the uniqueness of $f(t) \times g(t)$ and (2) follow immediately from (1) of the preceding theorem. Evidently $f(t) \times g(t)$ is of degree nm. The proof of (3), (4), the second part of (5), and (6) follow respectively by (2), (3), (4) and (6) of Theorem 5. The first part of (5) is a consequence of applying (5) of the preceding theorem repeatedly. Indeed, put $g = g_1 \bar{g}_1$, then by (5) of Theorem 5 and by Lemma 4, $f \times g = h_1 \times \bar{h}_1$, where $h_1 \simeq f_1 \times g_1$, and $\bar{h}_1 \simeq f \times \bar{g}_1$. Since $f \times g$ belongs to $(\mathfrak{V} \times \mathfrak{W}, \mathbf{A} \times \mathbf{B})$, $f\, g_1$ belongs to $(\mathfrak{V} \times (\mathfrak{W}/\mathfrak{W}_1), \mathbf{A} \times (\mathbf{B}/\mathbf{B}_1))$ and $f \times \bar{g}_1$ belongs to $(\mathfrak{V} \times \mathfrak{W}_1, \mathbf{A} \times \mathbf{B}_1)$.

(7) is the special case of (8) where $B = (a)$. The proof of (8) is carried out as follows: We may assume that $a_0 = 1$, and we can take the matrix

$$A = \begin{pmatrix} 0 & \cdots & 0 & -a_n \\ 1 & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ 0 & & 1 & -a_1 \end{pmatrix}$$

to be one which has $f(t)$ as an invariant factor (Jacobson [6]). $f(t) \times g(t)$ is by definition an invariant factor of

$$-t \cdot 1_{nm} + (A \times 1_m + 1_n \times B) = \begin{pmatrix} B - t \cdot 1 & 0 & \cdots & -a_n \cdot 1 \\ 1 & B - t \cdot 1 & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 0 & & 1 & B - t \cdot 1 - a_1 \cdot 1 \end{pmatrix} = M$$

Multiplying the n^{th} row of M (i.e. the last m-rows) on the left by $t \cdot 1 - B$ and adding to the $n - 1^{\text{th}}$ row, then multiply the $n - 1$ row on the left by $t \cdot 1 - B$ and add to the $n - 2$ row and so on $\cdots$. Then one obtains a matrix M_1 which is equivalent to M of the form:

$$M_1 = \begin{pmatrix} 0 & & \cdots & B_n(t) \\ 1 & 0 & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot\cdot 0 & \cdot \\ 0 & \cdot & \cdot\cdot 1 & B_1(t) \end{pmatrix}$$

where $B_1(t) = B - t \cdot 1 - a_1 \cdot 1$, $B_\nu(t) = (t \cdot 1 - B)B_{\nu-1} - a \cdot 1$. Hence $B_\nu(t) = -[(t \cdot 1 - B)^\nu + (t - B)^{\nu-1} a_1 + \cdots]$. In particular, $B_n = -f(t \cdot 1 - B)$.

The matrix M_1 can be readily transferred to a matrix of the type

$$\begin{pmatrix} 0 & & 0 \\ & \ddots & \\ 1 & & B_n(t) \end{pmatrix}$$

By known results (Fitting [5]), we know that the invariant factors of this matrix are the same as those of $B_n(t)$. Hence $f(t) \times g(t)$ is the invariant factor of $B_n(t)$ and, therefore, also of $-B_n(t) = f(t \cdot 1 - B)$.

An immediate consequence of the preceding theorem is:

Corollary 1. $f(t) \times t \simeq t \times f(t) \simeq f(t)$.

Corollary 2. *If* $f(t) = [t - a_1, \cdots, t - a_n]$, $g(t) = [t - b_1, \cdots, t - b_m]$ *then* $f(t) \times g(t) = [t - c_{11}, t - c_{12}, \cdots, t - c_{nm}]$ *where* $c_{ik} = a_i + b_k + d_{ik}^{-1}d'_{ik}$ *for some* $d_{ik} \epsilon F$, $i = 1, \cdots, n$, $k = 1, 2, \cdots, m$.

Indeed, by (5) of Theorem 6 $f(t) \times g(t) = [h_{ik}(t)]$, where $h_{ik}(t) \simeq t - a_i \times t - b_k$, and by (7) it follows that $h_{ik} \simeq t - (a_i + b_k)$. Since $h_{ik}(t)$ can be chosen to be with the highest coefficient 1, $h_{ik}(t) = t - c_{ik}$. The rest follows by Lemma 2.

Lemma 10. *If the nullity of* $f(t)$ *is* μ *and the nullity of* $g(t)$ *is* ν *then the nullity of* $f(t) \times g(t)$ *is* $\geq \mu\nu$.

Proof. Let $f^*(t)$ belong to $(\mathfrak{V}, \mathbf{A})$ and $g^*(t)$ belong to $(\mathfrak{W}, \mathbf{B})$. If $v_1, \cdots, v_\nu$ is a base of $\mathfrak{N}(\mathbf{A})$ and $w_1, \cdots, w\mu$ is a base of $\mathfrak{N}(\mathbf{B})$, then since

$$(v_i \times w_j)(\mathbf{A} \times \mathbf{B}) = v_i\mathbf{A} \times w_j + v_i \times w_j\mathbf{B} = 0$$

$\mathfrak{N}(\mathbf{A} \times \mathbf{B})$ contains at least $\nu\mu$ independent elements $(v_i \times w_j)$. The lemma is now an immediate consequence of Theorem 3 and (6) of Theorem 6.

In particular if $f(t)$, $g(t)$ are completely solvable, i.e. $f(t) \simeq e_n(t)$, $g(t) \simeq e_m(t)$, we have:

Corollary. $e_n \times e_m \simeq e_{nm}$.

Let $\mathfrak{V}$ and $\mathfrak{W}$ be two vector spaces over F of dimension n and m respectively. By Hom $(\mathfrak{W}, \mathfrak{V})$ we denote the set of all linear transformations of $\mathfrak{W}$ into $\mathfrak{V}$. The set is again an F-space.

Lemma 11. *The vector space* $\mathfrak{V} \times \mathfrak{W}^*$ *is canonically isomorphic with* Hom $(\mathfrak{W}, \mathfrak{V})$.

The isomorphism is readily seen to be obtained by corresponding to $v \times r \epsilon \mathfrak{V} \times \mathfrak{W}^*$ the linear transformation $\varphi \epsilon$ Hom $(\mathfrak{W}, \mathfrak{V})$ defined by $\varphi: w \rightarrow v(rw)$ for every $w \epsilon \mathfrak{W}$.

We identify henceforth the two spaces and write $w(v \times r) = v(rw)$ for every $v \epsilon \mathfrak{V}$, $r \epsilon \mathfrak{W}^*$, $w \epsilon \mathfrak{W}$.

Lemma 12. *Let* $\mathfrak{V} = (\mathfrak{V}, A)$, $\mathfrak{W} = (\mathfrak{W}, B)$. *The set of all vectors* $(\mathfrak{V} \times \mathfrak{W}^*)(\mathbf{A} \times \mathbf{B}^*)$ *is identical with the set of all linear transformations of* Hom $(\mathfrak{W}, \mathfrak{V})$, *of the form* $u\mathbf{A} - \mathbf{B}u$, $u \epsilon$ Hom $(\mathfrak{W}, \mathfrak{V})$.

For, let $u = \sum v_i \times r_i$, $v_i \epsilon \mathfrak{V}$, $r_i \epsilon \mathfrak{W}^*$, then $u(\mathbf{A} \times \mathbf{B}^*) = \sum (v_i\mathbf{A} \times r_i + v_i \times r_i\mathbf{B}^*)$. Hence the effect of this element on $w \epsilon W$ is

$$\begin{aligned} w[u(\mathbf{A} \times \mathbf{B}^*)] &= \sum(v_i\mathbf{A})(r_iw) + \sum v_i(r_i\mathbf{B}^*w) = \sum (v_iA)(r_iw) \\ &\quad - \sum v_i(r_iw\mathbf{B}) + \sum v_i(r_i\mathbf{w})' = \sum [v_i(r_iw)]\mathbf{A} - \sum v_i(r_iw)' \\ &\quad + \sum v_i(r_iw\mathbf{B}) + \sum v_i(r_iw)' = w(\sum v_i \times r_i)\mathbf{A} - wB(\sum v_i \times r_i) = w(u\mathbf{A} - \mathbf{B}u). \end{aligned}$$

The same proof gives the converse,

COROLLARY 1. *The module of all operator homomorphisms of* $(\mathfrak{W}, \mathbf{B})$ *into* $(\mathfrak{V}, \mathbf{A})$ *is* $\mathfrak{C}$*-isomorphic with the modules of vectors of* $\mathfrak{V} \times \mathfrak{W}^*$ *which annihilate* $\mathbf{A} \times \mathbf{B}^*$, i.e. *with* $\mathfrak{N}(\mathbf{A} \times \mathbf{B}^*)$.

The proof follows from the fact that $u \in \text{Hom}(\mathfrak{W}, \mathfrak{V})$ is an operator homomorphism means that $u\mathbf{A} = \mathbf{B}u$, i.e. $u\mathbf{A} - \mathbf{B}u = 0$, and in view of the preceding lemma this is identical with $u(\mathbf{A} \times \mathbf{B}^*) = 0$. The proof of the $\mathfrak{C}$-isomorphism is now evident.

It is worth determining this set of linear transformations in the language of matrices.

Let $(v_1, \cdots, v_n)$ be a basis of $\mathfrak{V}$ and $(w_1, \cdots, w_m)$ a basis of W. Let A, B be the matrices of $\mathbf{A}$ and $\mathbf{B}$ corresponding to basis (v_i) and (w_i) respectively. As we have seen in Section 2, the $m \times n$ matrices U which correspond to the operator homomorphism of W into V are those which satisfy $BU = UA + U'$. Hence in view of the last corollary and theorem we obtain the results:

COROLLARY 2. *The set of all matrices* U *of order* $n \times m$ *which satisfy* $BU - UA = U'$ *is a* $\mathfrak{C}$*-module of dimension* $\leqq nm$. *Furthermore, if a set of matrices which satisfy this equation are* $\mathfrak{C}$*-independent then they are also* F*-independent.* (Levy [8]).

Let $u \in \mathfrak{V} \times \mathfrak{W}^*$ be an operator homomorphism of $\mathfrak{W}$ into $\mathfrak{V}$. Let $\mathfrak{W}_u$ be the kernel of this homomorphism and $\mathfrak{W}u$ be its image, then $\mathfrak{W}/\mathfrak{W}_u = \mathfrak{W}u$. Denote by $\mathbf{B}_u$ the induced d.t. of $\mathbf{B}$ in $\mathfrak{W}_u$ and $\mathbf{A}_u$ the induced d.t. of $\mathbf{A}$ in $\mathfrak{W}u$. Thus, the preceding isomorphism, which is an operator isomorphism means that $\mathbf{B}/\mathbf{B}_u$ and $\mathbf{A}_u$ are similar. With the aid of this fact we shall prove the following theorem which justifies the name "resultant."

THEOREM 7. *Let* $f(t)$, $g(t)$ *be two polynomials of degree* > 0. *A necessary and sufficient condition for the existence of factorizations* $f(t) = f_1(t)f_2(t)$, $g(t) = g_1(t)g_2(t)$ *such that* $f_2(t)$ *is of degree* >0 *and* $f_2(t) \simeq g_1(t)$ *is that the nullity of the resultant* $f^*(t) \times g(t)$ *is* > 0.

PROOF. By the proof of Theorem 2 one can find $\mathfrak{V} = (\mathfrak{V}, \mathbf{A})$, $\mathfrak{W} = (\mathfrak{W}, \mathbf{B})$ such that $f(t)$ and $g(t)$ belong to $\mathbf{A}$ and $\mathbf{B}$ respectively. Since $(f^*(t) \times g(t))^* \simeq f(t) \times g^*(t)$, it follows by definition of the resultant and by Theorem 3 that the nullity of the $\mathbf{A} \times \mathbf{B}^*$ is greater than zero. Hence by Corollary 1 of Lemma 12 there exists a non zero operator homomorphism $u: \mathfrak{W} \to \mathfrak{V}$. Hence $\mathbf{B}/\mathbf{B}_u$ and $\mathbf{A}_u$ are similar. The proof follows now immediately from Lemma 4.

Conversely, applying the converse of Lemma 4 and the fact that $f_2(t) \simeq g_1(t)$ we obtain the result that $\mathbf{B}/\mathbf{B}_u$ and $\mathbf{A}_u$ are similar and hence the existence of an operator homomorphism $u: \mathfrak{W} \to \mathfrak{V}$ with kernel $\mathfrak{W}_u$ and image $\mathfrak{W}_u$. Evidently $u \neq 0$. Thus by Corollary 1 of Lemma 12, the nullity of $\mathbf{A} \times \mathbf{B}^*$ is > 0 and as in the first part of the proof the result will follow immediately from Theorem 3.

In particular,

COROLLARY. *If* $p(t)$, $q(t)$ *are irreducible polynomials then a necessary and sufficient condition that* $p(t) \simeq q(t)$ *is that the nullity of* $p(t) \times q^*(t)$ *is* > 0.

Since $b(t + a) = (t + a) + b'$; one can readily verify that the mapping φ_a: $\sum t^{\nu}a_{\nu} \to \sum (t + a)^{\nu}a_{\nu}$ is an automorphism of $F[t]$. The following lemma will be very useful:

LEMMA 13. $\varphi_a[f(t) \times g(t)] \simeq \varphi_a[f(t)] \times g(t) \simeq f(t + a) \times g(t) \simeq f(t) \times g(t + a)$.

PROOF. Indeed, $f(t) \times g(t)$ is the invariant factor of the matrix $-t \times 1 + (A \times 1 + 1 \times B)$ (Lemma 9). Extend φ_a in the natural way to $F_n[t]$. One readily obtains that $\varphi_a(f(t) \times g(t))$ is the invariant factor of $\varphi_a[-t\cdot 1 + (A \times 1 + 1 \times B)] = -t\cdot 1_{nm} - a\cdot 1_{nm} + (A \times 1_m + 1_n \times B) = -t\cdot 1_{nm} + (A - a\cdot 1_n) \times 1_m + 1_n \times B$, since $1_{nm} = 1_n \times 1_m$. Now since $f(t)$ is the invariant factor of the matrix $-t\cdot 1 + A$, $\varphi_a(f(t)) = f(t + a)$ is the invariant factor of $-t\cdot 1 + (A - a\cdot 1)$. Consequently, by Lemma 9 and by definition of the resultant it follows that the $f(t + a) \times g(t)$ is the invariant factor of $-t\cdot 1_{nm} + (A - a\cdot 1_n) \times 1_m + 1_n \times B$ is similar to $\varphi_a(f(t) \times g(t))$. The other part of the theorem follows by symmetry.

COROLLARY. *Let $f(t)$, $g(t)$ be two non constant polynomials. A necessary and sufficient condition for the existence of a factorization $f(t) = f_1(t)f_2(t)$, $g(t) = g_1(t)g_2(t)$ and the existence of $a \in F$ such that $f_2(t) \simeq g_1(t + a)$ is that a be a left root of $f^*(t) \times g(t)$.*[8]

Let $f^*(t) \times g(t) = (t - a)h(t)$, so that $\varphi_a(f^*(t) \times g(t)) \simeq th(t + a)$. Hence, since $\varphi_a(f^*(t) \times g(t)) \simeq f^*(t) \times g(t + a)$ it follows that: a is a left root of $f^*(t) \times g(t)$ is equivalent to the fact that $f^*(t) \times g(t + a)$ is similar to a polynomial of the type $th(t)$.[9] Consequently, this is equivalent to the fact that the nullity of $f^*(t) \times g(t + a)$ is >0. The rest follows now by Theorem 7.

REMARK. The resultant behaves in a different form under the following type of automorphism. Let F, F_0 be two fields with a derivation. Let ϑ be an isomorphism between F and F_0 such that $(a')^{\vartheta} = (a^{\vartheta})'$. Then ϑ can be extended in a natural way to $F[t]$ and $F_n[t]$. It follows almost immediately that:

(1) If $f(t) \simeq g(t)$ then $f^{\vartheta}(t) \simeq g^{\vartheta}(t)$.

(2) $(f(t)^*)^{\vartheta} = (f^{\vartheta}(t))^*$.

(3) $(f(t) \times g(t))^{\vartheta} \simeq f^{\vartheta}(t) \times g^{\vartheta}(t)$.

The order of the nullity of $f^*(t) \times g(t)$ is interpreted in the following theorem:

THEOREM 8. *The set of all classes of polynomials modulo $f(t)F[t]$ which have representative polynomial $h(t)$ such that $h(t)g(t) \equiv 0 \pmod{f(t)F[t]}$ constitute a $\mathfrak{C}$-module of dimension equal to the nullity of $f^*(t) \times g(t)$.*

In the proof of Theorem 2, it was pointed out that one can choose $(\mathfrak{V}, \mathbf{A})$ to be the $F[t]$ module $F[t]/f(t)F[t]$. Namely, the right multiplication by t induces the d.t. $\mathbf{A}$. Similarly let $(\mathfrak{W}, \mathbf{B})$ be the module $F[t]/g(t)F[t]$. Now the set of all $F[t]$-homomorphisms of $F[t]/g(t)F[t]$ into $F[t]/f(t)F[t]$ is the determined by the mapping $1 \to h(t)$, and a necessary and sufficient condition that such a mapping is a $F[t]$-homomorphism is that $g(t) \to h(t)g(t) \equiv 0 \pmod{f(t)F[t]}$. Hence, one readily identifies the module of these homomorphisms with the classes of the

[8] This means that a is a left root of at least one polynomial of the class of the similarity of polynomials $f^*(t) \times g(t)$.

[9] Then $th(t)$ can be taken as $f^*(t) \times g(t + a)$.

polynomials of the theorem. The proof follows now by Corollary 1 of Lemma 12 and by Theorem 3.

The finiteness of this module was proved by Ore in [9].

5. The invariant ring of a differential polynomial and a d.t.

The set of all operator automorphisms of $(\mathfrak{B}, \mathbf{A})$, that is: the set of all linear transformations $\mathbf{P}$ of $\mathfrak{B}$ such that $\mathbf{PA} = \mathbf{AP}$ form a ring. We shall call this ring the *invariant ring*[10] of $\mathbf{A}$ and denote it by $\mathfrak{R}(\mathbf{A})$. This ring is in fact a finite $\mathfrak{C}$-algebra whose dimension will be determined later.

Let $f(t)$ belong to $(\mathfrak{B}, \mathbf{A})$, then $(\mathfrak{B}, \mathbf{A}) = F[t]/f(t)F[t]$. This implies that that ring $\mathfrak{R}(\mathbf{A})$ is isomorphic with the ring of all $F[t]$-endomorphisms of $F[t]/f(t)F[t]$. Similar to the proof of Theorem 8 this ring is isomorphic to the ring of all classes $p(t) + f(t)F[t]$ which have a representative $p(t)$ satisfying $p(t)f(t) = f(t)p_1(t)$, where addition and multiplication are the ordinary addition and multiplication of representatives. We call this ring the invariant ring $\mathfrak{R}(f)$ of $f(t)$. We remark here that if $t = x$ is a commutative variable and $f(x)$ is irreducible, the constructing of the invariant ring of $f(x)$ is the Steinitz method of constructing algebraic extensions which has a solution of the equation $f(x) = 0$.

Another form of representing the isomorphic rings $\mathfrak{R}(\mathbf{A})$, $\mathfrak{R}(f)$ is the matrix representation. Let A be any matrix corresponding to $\mathbf{A}$, as we have already shown in the beginning of Section 2 the matrices P corresponding to the operator endomorphisms of $(\mathfrak{B}, \mathbf{A})$ with the respect to the same basis, are those and only those matrices which satisfy $PA - AP = P'$. Thus the set of all these matrices form also a $\mathfrak{C}$-algebra isomorphic with $\mathfrak{R}(\mathbf{A})$ and $\mathfrak{R}(f)$. We call this ring the *invariant ring* of A and denote it by $\mathfrak{R}(A)$.

The ring $\mathfrak{R}(\mathbf{A})$, is a finite $\mathfrak{C}$-module. In fact it is $\mathfrak{C}$-isomorphic with the $N(\mathbf{A} \times \mathbf{A}^*)$ of $V \times V^*$. The dimension of the latter is equal, by Theorem 3, to the nullity of $f(t)^* \times f(t)$. Thus:

THEOREM 9. *The ring $\mathfrak{R}(f)$ (hence $\mathfrak{R}(\mathbf{A})$, $\mathfrak{R}(A)$) is a finite $\mathfrak{C}$-algebra of dimension equal to the nullity of $f(t) \times f(t)^*$.*

The finiteness of $\mathfrak{R}(f)$ was proved by Ore [9] and by a result of Jacobson [6] we have:

THEOREM 10. *If $f(t)$ is irreducible (equivalently, $\mathbf{A}$ is irreducible) then $\mathfrak{R}(f)$ (and $\mathfrak{R}(A)$) is a finite division algebra over C.*

6. Extensions of F

A field K will be said, in the present paper, to be an extension of F if $K \supseteqq F$ and a derivation is defined in K which is an extension of the derivation of F. In particular, we have in this case $K[t] \supseteqq F[t]$. Every d.t. $\mathbf{A}$ in $\mathfrak{B}$ over F can be extended to a d.t., also denoted by $\mathbf{A}$, in $\mathfrak{B} \times K$ in a unique way. Namely, if $v_1, \cdots, v_n$ is a basis of $\mathfrak{B}$ over F, then $(\sum v_i a_i)\mathbf{A} = \sum (v_i\mathbf{A})a_i + \sum v_i a_i'$ for every $a_i \in K$, one readily observes that this extension is independent on the base and it is unique. Note that the matrix of $\mathbf{A}$ with respect to (v_i) is the same in $\mathfrak{B} \times K$ as in $\mathfrak{B}$.

[10] See Jacobson [6], section 10, p. 502–3.

If $\mathfrak{D}$ is the constant field of K, and $\mathfrak{C}$ the constant field of F then $\mathfrak{D} \supseteqq \mathfrak{C}$. K is said to be a constant extension of F if $K = F\mathfrak{D}$, where $F\mathfrak{D}$ denotes the composite field of F and $\mathfrak{D}$.

It is well known that the derivation in F can be extended to a derivation in any field K containing F, and if K is algebraic over F the extension is unique. We shall denote by $\mathfrak{V}_K$ the vector space $\mathfrak{V} \times K$ which is a space over K. Vector spaces without a subscript will always be over F.

If $f(t) \in F[t]$, then $f(t) \in K[t]$, and the invariant ring of $f(t)$ in $K[t]$ will, of course, contain the invariant ring of $f(t)$ in $F[t]$, we denote the first by $\mathfrak{N}_K(f)$ and the latter by $\mathfrak{N}(f)$. A similar notation will be used for the invariant ring of matrices and of d.t.

The purpose of the present section is to study the behavior of relations and operations defined in the preceding sections under an extension of the field F.

THEOREM 11. (1) *If $f(t)$ is a characteristic polynomial of $A \in F_n$, then $f(t)$ is also a characteristic polynomial of A when considered as a matrix in K_n.*

(2) *If $f(t)$ belongs to $(\mathfrak{V}, \mathbf{A})$, it also belongs to $(\mathfrak{V}_K, \mathbf{A})$.*

(3) *The relation of similarity is invariant under field extensions, i.e. if $f(t) \simeq g(t)$ in $F[t]$; or $\mathbf{A} \simeq \mathbf{B}$ as* d.t. *over F; or $A \simeq B$ in F_n then $f(t) \simeq g(t)$ in $K[t]$; $\mathbf{A} \simeq \mathbf{B}$ as* d.t. *over K and $A \simeq B$ in K_n.*

(4) *If $f(t)$, $g(t) \in F[t]$, then the definition of $f(t) \times g(t)$ is independent of the field F.*

(5) *$f^*(t)$ in $F[t]$ is the same in $K[t]$.*

PROOF. Since $f(t)$ is the invariant factor of the matrix $-t\cdot 1 + A$ in $F_n[t]$, one immediately observes that since the relation of equivalence of matrices is not touched by extension of the field F, $f(t)$ will also be the invariant factor of $-t\cdot 1 + A$ in $K_n[t]$. This proves (1).

To prove (2), note that to $\mathbf{A}$ in $\mathfrak{V}$ and $\mathfrak{V}_K$ correspond the same matrix A in F_n with respect to a given basis (v_i) of V over F (and over K). Thus (2) follows now immediately from (1).

If $f(t) \simeq g(t)$, they belong to $(\mathfrak{V}, \mathbf{A})$ for some d.t. $\mathbf{A}$. Hence by (2) they belong also to $(\mathfrak{V}_K, \mathbf{A})$ with the same $\mathbf{A}$, consequently $f(t) \simeq g(t)$ in $K[t]$. The proof follows also immediately from definition of similarity of polynomials (see remarks after Lemma 1). The proof of the rest of (2) follows by reducing it to similarity of polynomials or straightforward. The proof of (5) is trivial.

To prove (4), let $f(t)$, $g(t)$ be characteristic polynomials of the matrices A and B respectively; then $f(t) \times g(t)$ is defined as the invariant factor of $-t\cdot 1 + (A \times 1 + 1 \times B)$. The same relations hold also in $K_n[t]$ which means that the definition of $f(t) \times g(t)$ is independent of the field F.

LEMMA 14. (1) *Let $\mathfrak{V} = (\mathfrak{V}, \mathbf{A})$; then $\mathfrak{N}_k(\mathbf{A})$ contains $\mathfrak{N}(\mathbf{A})$, the K-module of all vectors annihilating $\mathbf{A}$ in $\mathfrak{V}_K$. Furthermore, a set of $\mathfrak{C}$-independent vectors in $\mathfrak{N}(\mathbf{A})$ will also be $\mathfrak{D}$-independent in $\mathfrak{N}_K(\mathbf{A})$, even K-independent in $\mathfrak{V}_K$.*

Respectively:

(2) *The $\mathfrak{C}$-module of the solutions of $g(z) = 0$, $g(t) \in F[t]$, in F is contained in the $\mathfrak{D}$-module of solutions of $g(z) = 0$ in K, and solutions in F which are $\mathfrak{C}$-independent are also $\mathfrak{D}$-independent in K.*

PROOF. Evidently $\mathfrak{N}(\mathbf{A}) \subset \mathfrak{N}_K(\mathbf{A})$. If $v_1, \cdots, v_r$ are r $\mathfrak{C}$-independent vectors in $\mathfrak{N}(\mathbf{A})$ then by Lemma 5, they are also F-independent. Hence, also K-independent in $\mathfrak{V}_K = \mathfrak{V} \times K$. Consequently, (v_i) are $\mathfrak{D}$-independent which proves (1). The proof of the second part follows by using the isomorphism between the the space of solutions of a differential equation and the space of vectors annihilating a d.t. (proof of Theorem 3).

The converse of Theorem 11 is also true:

THEOREM 12: *If $f(t)$, $g(t) \in F[t]$ and $f(t) \simeq g(t)$ in $K[t]$, then $f(t) \simeq g(t)$ in $F[t]$. Similarly, if $\mathfrak{V} = (\mathfrak{V}, \mathbf{A})$, $\mathfrak{W} = (\mathfrak{W}, \mathbf{B})$ and A, B are similar over K then they are similar also over F.*

PROOF. In fact, it suffices to prove only the second part. Since then one can choose $\mathfrak{V} = (\mathfrak{V}, \mathbf{A})$ and $\mathfrak{W} = (\mathfrak{W}, \mathbf{B})$ such that $f(t)$ and $g(t)$ belong to $(\mathfrak{V}, \mathbf{A})$ and $(\mathfrak{W}, \mathbf{B})$ respectively. These polynomials will still belong to $(\mathfrak{V}_K, \mathbf{A})$ and $(\mathfrak{W}_K, \mathbf{B})$ and, therefore, $\mathbf{A}$ and $\mathbf{B}$ will be similar over K. By the second part of the theorem $\mathbf{A}$ and $\mathbf{B}$ are also similar over F; hence $f(t) \simeq g(t)$ in $F[t]$.

To prove the second part we note that since $(\mathfrak{W}_K, \mathbf{B}) \cong (\mathfrak{V}_K, \mathbf{A})$ it follows that to this isomorphism belongs an element $u \in \mathfrak{V}_K \times \mathfrak{W}_K^*$ such that $u(\mathbf{A} \times \mathbf{B}^*) = 0$ (proof of Corollary 1 of Lemma 12). Now $\mathfrak{V}_K \times \mathfrak{W}_K^* = (\mathfrak{V} \times \mathfrak{W}^*)_K$; consider K as a vector space over F and (k_i) a basis of K over F (not necessarily finite). Then $u = \sum_{i=1}^n u_i k_i$, $u_i \in \mathfrak{V} \times \mathfrak{W}^*$. Since $\mathbf{A} \times \mathbf{B}^*$ acts on $\mathfrak{V} \times \mathfrak{W}^*$, we have that $u(\mathbf{A} \times \mathbf{B}^*) = \sum [u_i(\mathbf{A} \times \mathbf{B}^*)]k_i = 0$ implies that $u_i(\mathbf{A} \times \mathbf{B}^*) = 0$ for all u_i. Hence, for any chosen element $c_i \in C$, $(\sum u_i c_i)(\mathbf{A} \times \mathbf{B}^*) = 0$, i.e. $\sum u_i c_i \in \mathfrak{N}(\mathbf{A} \times \mathbf{B}^*)$. Fixing basis of $\mathfrak{V}$ and $\mathfrak{W}$, there corresponds to each $u_i \in \mathfrak{V} \times \mathfrak{W}^*$ an $n \times n$ matrix U_i in F_n. With respect to some couple of bases, the same matrix will correspond to u_i's in K_n. Hence, to $\sum u_i k_i$ will correspond the matrix $\sum U_i k_i$. Let (x_i) be a set of variables over K; then the determinant $| \sum U_i x_i | \neq 0$, since for $x_i = k_i$ the matrix $\sum U_i k_i$ is regular. Noting that the field C is infinite we can find also $x_i = c_i$ such that $| \sum U_i c_i | \neq 0$. Consequently, the matrix $\sum U_i c_i$ is regular and, therefore, the homomorphism determined by $\sum u_i c_i \in \mathfrak{V} \times \mathfrak{W}^*$ is an isomorphism, which completes the proof.

II. CENTRAL SIMPLE ALGEBRAS AND DIFFERENTIAL POLYNOMIALS

7. The semi group of A-polynomials

Part of Theorem 6 can be stated as follows:

THEOREM 13. *The set of differential polynomials of degree >0 form a commutative, associative, multiplicative system with a unit (the polynomial t), with respect to the relation of similarity, and the operation $\times$.*

Our first aim is to distinguish in this semi group, a subsystem which is a multiplicative system with cancellation.

We say that a polynomial $f(t)$ is uniformly reducible with the factor $p(t)$ if $f(t) = [p_1(t), \cdots, p_r(t)]$, where $p_i(t) \simeq p(t)$, $i = 1, \cdots, r$.

LEMMA 15. *$f(t)$ is uniformly reducible with the factor $p(t)$ if and only if $f(t) \simeq p(t) \times e_k(t)$.*

By the corollary of Theorem 4, $e_k(t) = [g_1(t), \cdots, g_k(t)]$ where $g_i(t) \simeq t$.

Hence, Theorem 6, part (5), yields that $e_k(t) \times p(t) = [p_1, \cdots, p_k]$ where $p_i(t) \simeq p(t) \times g_i(t) \simeq p(t) \times t \simeq p(t)$, which proves that $e_k(t) \times p(t)$ is uniformly reducible.

Conversely, if $f(t) = [p_1(t), \cdots, p_k(t)]$ with $p_i(t) \simeq p(t)$, let $f(t)$ belong to $(\mathfrak{B}, \mathbf{A})$ and let $p(t)$ belong to $(\mathfrak{U}, \mathbf{B})$. By [6] (p. 498) $A = A_1 \oplus \cdots \oplus A_k$, with $\mathbf{A}_i \simeq \mathbf{B}$. On the other hand $e_k(t)$ belongs to $(\mathfrak{W}, \mathbf{Z})$ (in the notation of Theorem 4) and $\mathfrak{W} = v_1F \oplus \cdots \oplus v_kF$ with $v_i\mathbf{Z} = 0$. Hence $(\mathfrak{W} \times \mathfrak{U}, \mathbf{A} \times \mathbf{B}) = (v_1F \times \mathfrak{U}) \oplus \cdots \oplus (v_kF \times \mathfrak{U})$. Evidently $(v_iF \times \mathfrak{U}, \mathbf{Z}_i \times \mathbf{B}) = (\mathfrak{U}, B)$ by mapping $v_i \times u \rightarrow u$, $u \in \mathfrak{U}$. Consequently $\mathbf{Z} \times \mathbf{B} = \mathbf{Z}_1 \times \mathbf{B} \oplus \cdots \oplus \mathbf{Z}_k \times \mathbf{B}$. Since $\mathbf{Z}_i \times \mathbf{B} \simeq \mathbf{B} \simeq \mathbf{A}_i$, it follows immediately that also $\mathbf{A} \simeq \mathbf{Z} \times \mathbf{B}$. Hence

$$f(t) \simeq e_k(t) \times p(t).$$

LEMMA 16. (The cancellation law) *$e_n(t) \times f(t) \simeq e_n(t) \times g(t)$ if and only if $f(t) \simeq g(t)$.*

Decompose $f(t) = [f_1, \cdots, f_r]$, $g(t) = [g_1, \cdots, g_s]$ in indecomposable factors f_i, g_i. By Theorem 6 and by the preceding lemma:

$$e_n(t) \times f(t) = [f_{11}, \cdots, f_{1n}, f_{21}, \cdots, f_{2n}, \cdots, f_{r1}, \cdots, f_{rn}] \text{ where } f_{ij} \simeq f_i,$$

$$i = 1, \cdots, r, j = 1, \cdots, n.$$

Similarly

$$e_n(t) \times g(t) = [g_{11}, \cdots, g_{1n}, \cdots, g_{s1}, \cdots, g_{sn}], \ g_{ij.} \simeq g_i, \ i = 1, \cdots, s,$$

$$j = 1, \cdots, n.$$

Since $e_n(t) \times f(t) \simeq e_n(t) \times g(t)$, the preceding two decompositions must be identical up to similarity. Thus, $rn = sn$, hence $r = s$.

The nr factors f_{ij} are similar in pairs with the nr factors g_{ij}, and each of these sets of factors is divided into r sets of elements $(f_{1j}), \cdots, (f_{rj}), \cdots, (g_{wj})$ each containing n elements and all isomorphic to $f_1, \cdots, f_r, g_1, \cdots, g_s$ respectively. Hence one readily proves that also the sets $(f_1, \cdots, f_r)$ and $(g_1, \cdots, g_s)$ must be similar in pairs. Consequently, the decompositions $[f_1, \cdots, f_r]$, $[g_1, \cdots, g_r]$ must be similar (Ore [10]). Q.E.D.

The proof in the other direction follows from Theorem 6.

One can also obtain the proof, and essentially the same proof, by considering vector spaces and d.t. belonging to $f(t)$ and $g(t)$.

DEFINITION. A polynomial $g(t)$ of degree n is called an *A-polynomial* if there exists a polynomial $\bar{g}(t)$ of some degree m such that $g(t) \times \bar{g}(t) \simeq e_{nm}(t)$.[11]

THEOREM 14. (1) *If g is an A-polynomial, and $h \simeq g$ then h is also an A-polynomial.*

(2) *If g, h are A-polynomials, then so is $g \times h$.*

(3) *If g_1, g_2 are two similar A-polynomials, and $g_1 \times h_1 \simeq g_2 \times h_2$, then $h_1 \simeq h_2$.*

[11] We can use the short notation $g \times \bar{g} \simeq e$, for the degree of the right hand side must evidently be nm.

(4) *Every A-polynomial $g(t)$ is similar to $p(t) \times e_r(t)$, where $p(t)$ is an irreducible A-polynomial uniquely determined up to similarity.*

(5) *g is an A-polynomial if and only if $g \times g^* \simeq e$. Hence g^* is also an A-polynomial.*

(6) *If $g(t)$ is an A-polynomial, then so is $g(t + a)$ for every $a \in F$.*

Proof. The proof of (1) follows from the fact that if $g \simeq h$, $g \times \bar{g} \simeq h \times \bar{g} \simeq e$. Let $g \times \bar{g} \simeq e^{(1)}$, $h \times \bar{h} \simeq e^{(2)}$. By the associative law and by the corollary of Lemma 10, $(g \times h) \times (\bar{g} \times \bar{h}) \simeq (g \times \bar{g}) \times (h \times \bar{h}) \simeq e^{(1)} \times e^{(2)} \simeq e$ which proves (2).

To prove (3), note that if $g_1 \simeq g_2$, then $g_1 \times \bar{g} \simeq g_2 \times \bar{g} \simeq e$. Hence, if $g_1 \times h_1 \simeq g_2 \times h_2$, then $e \times h_1 \simeq \bar{g} \times g_1 \times h_1 \simeq \bar{g} \times g_2 \times h_2 \simeq e \times h_2$, and the proof follows by the preceding lemma.

Let g be an A-polynomial and $g \times \bar{g} \simeq e$. Among all polynomials $\bar{g}$ the polynomials $\bar{p}$ of minimal degree are irreducible. For if $\bar{p} = p_1 \cdot p_2$ then by (5) of Theorem 6, $e \simeq g \times \bar{p} = g_1 \cdot g_2$, where $g_1 \simeq g \times \bar{p}_1$, $g_2 \simeq g \times \bar{p}_2$. By Theorem 4, $g_1 \simeq e$ so that p_1 is also of the same type, which contradicts the minimality of $\bar{p}$. Now let p be a polynomial of minimum degree such that $p \times \bar{p} \simeq e$; hence p is irreducible. Let g be of degree n, p of degree m and $\bar{p}$ be of degree r.

$$e_m \times g \times g \times \bar{p} \simeq g \times e_m \times e_{nr} \simeq g \times e_{nmr} \simeq g \times e_r \times e_{nm} \simeq g \times e_r \times p \times \bar{p}.$$

Applying (3) for $g \times \bar{p}$ we have $e_m \times g \simeq e_r \times p$. It follows now by Lemma 15 that $[g_1, \cdots, g_m] \simeq [p_1, \cdots, p_r]$ where $g_i \simeq g$ and $p_i \simeq p$. Since p_i are irreducible and hence also indecomposable, one readily verifies by the uniqueness of decomposition (Ore [9]) that g_i and hence also g are similar to $[p_1, \cdots, p_s]$ for some s. Again by Lemma 15, $g \simeq p \times e_s$ which proves (4). In a similar way one proves the uniqueness of p.

The following argument proves (5). If $g \times h \simeq e$, then $g \times (h^*)^* \simeq e$. In case g and h are irreducible it follows, by the main property of the resultant, (corollary of Theorem 7) $g \simeq h^*$. Equivalently $g^* \simeq h$. If g is any A-polynomial, $g \simeq p \times e$, where p is an irreducible A-polynomial, then $g \times g^* \simeq (p \times e) \times (p^* \times e^*) \simeq (p \times p^*) \times (e \times e^*) \simeq e$. (Corollary of Lemma 10).

Let φ_a denote the automorphism of Lemma 13. Then, let $g \times h \simeq e$. $e \simeq g(t) \times h(t) = (\varphi_{-a}\varphi_a)[g(t) \times h(t)] \simeq \varphi_{-a}[g(t + a) \times h(t)] \simeq g(t + a) \times h(t - a)$ which proves that $g(t + a)$ is also an A-polynomial, i.e. (6) is proved.

By the proof of (4) and (5) it follows immediately that

Corollary 1. *If g is an A-polynomial, and $g \simeq p \times e$, where p is an irreducible A-polynomial, then $g \times \bar{g} \simeq e$ if and only if $\bar{g} \simeq p^* \times e$.*

Another result which follows immediately by definition and by Lemma 4 combined with Theorem 6 is:

Corollary 2. *If g is an A-polynomial and $g \simeq g_1 \times g_2$, or $g = g_1 g_2$ then each g_i is also an A-polynomial.*

Denoting the set of all A-polynomials of $F[t]$ by $\mathfrak{A}(\mathfrak{C}, F)$, we can summarize the results (1) and (3) of the preceding theorem as follows:

Theorem 15. *The set $\mathfrak{A}(\mathfrak{C}, F)$ is a multiplicative (associative and commutative)* *system with cancellation with the polynomial t as a unit under the operation* $\times$ *and the relation* $\simeq$.

$\mathfrak{A}(\mathfrak{C}, F)$ will henceforth be considered always as a semi-group with the above relation and operation.

We turn now to division algebras. The set of all central simple algebras over $\mathfrak{C}$ form a semi-group under the relation of isomorphism and the Kronecker product. The subset of these algebras which are split by F is a sub-semi-group which we shall denote by $\mathfrak{C}\mathfrak{S}(\mathfrak{C}, F)$.

The first main theorem of this part is:

THEOREM 16. *The mapping $g(t) \rightarrow \mathfrak{R}(g)$ determines a homomorphism of $\mathfrak{A}(\mathfrak{C}, F)$ onto $\mathfrak{C}\mathfrak{S}(\mathfrak{C}, F)$. In particular, the homomorphism is such that to polynomials of degree n correspond division algebras of degree n^2.*

The homomorphism of the theorem will be shown to be obtained by mapping $g(t) \rightarrow \mathfrak{R}(g)$ where $\mathfrak{R}(g)$ is the invariant ring of the polynomial $g(t)$.

This will follow from a sequence of lemmas to be proved. In the following lemmas and henceforth we shall use the following notation: Let $\mathfrak{V}$ be a vector space of dimension n over F. The set Hom $(\mathfrak{V}, \mathfrak{V})$ which was identified with the space $\mathfrak{V} \times \mathfrak{V}^*$ is readily seen to be isomorphic (over F) with the matrix ring F_n. The multiplication in Hom $(\mathfrak{V}, \mathfrak{V})$ is the natural multiplication of homomorphisms, and in the notation of $\mathfrak{V} \times \mathfrak{V}^*$ we have: $(v_1 \times r_1)(v_2 \times r_2) = v_1(r_1 v_2) \times r_2$ for every $v_i \in V$, $r_i \in W^*$. We turn now to the lemmas:

LEMMA 17. *Let $g(t)$ be a polynomial of degree n (>0). The ring $\mathfrak{R}(g)$ is a finite algebra of dimension n^2 if and only if $g(t)$ is an A-polynomial.*

The proof is an immediate consequence of Theorem 9 and (5) of Theorem 14.

LEMMA 18. *If $g(t)$ is an A-polynomial of degree n, then $\mathfrak{R}(g)$ is a central simple algebra of order n^2 over $\mathfrak{C}$ which is split by F.*

PROOF. Let $g(t)$ belong to $(\mathfrak{V}, \mathbf{A})$ then $\mathfrak{R}(g) \cong \mathfrak{R}(\mathbf{A})$. Since $g(t)$ is an A-polynomial $g(t) \times g^*(t)$ is a completely solvable polynomial of degree n^2. Hence $\mathfrak{R}(\mathbf{A} \times \mathbf{A}^*)$ contains n^2 $\mathfrak{C}$-independent vectors $u_i \in \mathfrak{V} \times \mathfrak{V}^*$ such that $u_i(\mathbf{A} \times \mathbf{A}^*) = 0$. Equivalently $u\mathbf{A} = \mathbf{A}u$. The set $\mathfrak{R}(\mathbf{A} \times \mathbf{A}^*)$ is the ring $\mathfrak{R}(\mathbf{A})$ under the ordinary multiplication, in $\mathfrak{V} \times \mathfrak{V}^*$, recalled above. Since the set (u_i) are also F-independent (Lemma 5), it follows that the space $\{\sum u_i a_i \mid a_i \in F\}$ is of degree n^2, hence the whole space $\mathfrak{V} \times \mathfrak{V}^*$. The set $\{\sum u_i a_i \mid a_i \in F\}$ is evidently isomorphic with $\mathfrak{R}(\mathbf{A}) \times F$, hence $\mathfrak{R}(g) \times F \cong \mathfrak{R}(\mathbf{A}) \times F \cong F_n$. This shows that F splits $\mathfrak{R}(g)$, and therefore $\mathfrak{R}(g)$ is also central simple.

LEMMA 19. *If $g(t)$ and $h(t)$ are A-polynomials, then $g \times h$ is also an A-polynomial and $\mathfrak{R}(g \times h) \cong \mathfrak{R}(g) \times \mathfrak{R}(h)$.*

The first part is (2) of Theorem 14. To prove the second part, let $g(t)$ belong to $(\mathfrak{V}, \mathbf{A})$ and $h(t)$ belong to $(\mathfrak{W}, \mathbf{B})$, then $g \times h$ belongs to $(\mathfrak{V} \times \mathfrak{W}, \mathbf{A} \times \mathbf{B})$.

$\mathfrak{R}(A)$ is a subring of $\mathfrak{V} \times \mathfrak{V}^*$ and contains a basis $x_1, \cdots, x_{n^2}$ over $\mathfrak{C}$ (and F) and so is $\mathfrak{R}(\mathbf{B})$ a subring of $\mathfrak{W} \times \mathfrak{W}^*$ and contains a basis $y_1, \cdots, y_{m^2}$ over $\mathfrak{C}$ (and F). By the proof of (6) of Theorem 5, $(\mathbf{A} \times \mathbf{B})^* \simeq \mathbf{A}^* \times \mathbf{B}^*$. Thus $(\mathbf{A} \times \mathbf{B}) \times (\mathbf{A} \times \mathbf{B})^* \simeq (\mathbf{A} \times \mathbf{A}^*) \times (\mathbf{B} \times \mathbf{B}^*)$. This similarity is obtained by considering $\mathfrak{V} \times \mathfrak{V}^* = (\mathfrak{V} \times \mathfrak{V}^*, \mathbf{A} \times \mathbf{A}^*)$, $\mathfrak{W} \times \mathfrak{W}^* = (\mathfrak{W} \times \mathfrak{W}^*, \mathbf{B} \times \mathbf{B}^*)$ and $(\mathfrak{V} \times \mathfrak{W}) \times (\mathfrak{V} \times \mathfrak{W})^* = [(\mathfrak{V} \times \mathfrak{W}) \times (\mathfrak{V} \times \mathfrak{W})^*, (\mathbf{A} \times \mathbf{B}) \times (\mathbf{A} \times \mathbf{B})^*]$.

The isomorphism between $(\mathfrak{B} \times \mathfrak{W}^*) \times (\mathfrak{W} \times \mathfrak{W}^*)$ and $(\mathfrak{B} \times \mathfrak{W}) \times (\mathfrak{B} \times \mathfrak{W})^*$ is readily seen to be also ring isomorphism, and therefore $\mathfrak{R}(\mathbf{A} \times \mathbf{B})$ is isomorphic with the ring formed by all annihilators of $(\mathbf{A} \times \mathbf{A}^*) \times (\mathbf{B} \times \mathbf{B}^*)$. The latter contains all vectors $x_i \times y_k$ for $(x_i \times y_k)[(\mathbf{A} \times \mathbf{A}^*) \times (\mathbf{B} \times \mathbf{B}^*)] = x_i(\mathbf{A} \times \mathbf{A}^*) \times y_k + x_i \times y_k(\mathbf{B} \times \mathbf{B}^*) = 0 + 0 = 0$.

Since the x_i are $\mathfrak{C}$-independent and so are the y_k, the set $(x_i \times y_k)$ contains $(nm)^2$ $\mathfrak{C}$-independent elements, which is the maximal number of independent elements in $\mathfrak{R}[(\mathbf{A} \times \mathbf{A}^*) \times (\mathbf{B} \times \mathbf{B}^*)]$. Consequently, they form a basis of this ring (= module). Which means that the ring $\mathfrak{R}(\mathbf{A} \times \mathbf{B})$ is isomorphic with the ring of elements of the form $\sum (x_i \times y_k)\alpha_{ik}$, $\alpha_{ik} \in \mathfrak{C}$. The latter is evidently $\mathfrak{R}(\mathbf{A}) \times \mathfrak{R}(\mathbf{B})$. Q.E.D.

The proof of Theorem 16 will be completed if we show:

LEMMA 20. *Every central simple algebra $\mathfrak{A}$ of order n^2 over $\mathfrak{C}$ and split by F is isomorphic with some invariant ring $\mathfrak{R}(g)$ of an A-polynomial $g(t)$ of degree n.*

The proof of this lemma was given already in [1] and [2]. We give here an alternative proof. This proof is based on the following version of a well known property of the representation of simple algebras:

Let $\mathfrak{A}$ be a central simple algebra (of finite degree) over $\mathfrak{C}$ and let F be *any*[12] field containing $\mathfrak{C}$, then any two representations of $\mathfrak{A}$ by finite matrices in F_m in which 1 is mapped on the unit matrix, are similar (in F_m).

The case F is finite over $\mathfrak{C}$, is a special case of [11], Theorem 11, (Ch. 5, p. 100). The proof given there really does not assume finiteness over $\mathfrak{C}$. The proof can also be reduced to the case $\mathfrak{C} = F$, which is well known. Indeed, let $a \to A$, $a \in \mathfrak{A}$, $A \in F_m$, be any representation. Then the mapping $\sum a_i\alpha_i \to \sum A_i\alpha_i$ where (a_i) is a base of $\mathfrak{A}$ over $\mathfrak{C}$ is evidently also a homomorphism of $\mathfrak{A} \times F$ into F_m. Since $\mathfrak{A} \times F$ is simple this is really a representation of $\mathfrak{A} \times F$. Thus, any two representations of $\mathfrak{A}$ induce two representations of $\mathfrak{A} \times F$, and these two are known to be similar.

Now, if $\mathfrak{A}$ is a central division algebra of order n^2 over $\mathfrak{C}$, and $\mathfrak{A} \times F = F_n$, $\mathfrak{A}$ has a representation in F_n: $a \to P_a$, $a \in \mathfrak{A}$, $P_a \in F_n$. This induces two representations

$$a \to \begin{pmatrix} P_a & 0 \\ 0 & P_a \end{pmatrix}, \qquad a \to \begin{pmatrix} P_a & P'_a \\ 0 & P_a \end{pmatrix}$$

in F_{2n}. Thus, there exists a regular matrix

$$Q = \begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix}$$

in F_{2n} such that:

$$\begin{pmatrix} P_a & 0 \\ 0 & P_a \end{pmatrix}\begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix} = \begin{pmatrix} Q_1 & Q_2 \\ Q_3 & Q_4 \end{pmatrix}\begin{pmatrix} P_a & P'_a \\ 0 & P_a \end{pmatrix}$$

for all P_a, $a \in \mathfrak{A}$. This implies $P_aQ_1 = Q_1P_a$, $P_aQ_3 = Q_3P_a$. The set of all matrices P_a contain n^2 independent elements over F since this representation was obtained

[12] Not necessarily finite over $\mathfrak{C}$.

as a representation induced by $A \times F$ which is isomorphic with F_n. Hence Q_1, Q_2 commute with F_n which shows that $Q_i = \alpha_i 1$, Q is regular, and therefore, not both $\alpha_1 = \alpha_3 = 0$. If $\alpha_1 \neq 0$, we may assume, by multiplying Q by α_1^{-1}, that $\alpha_1 = 1$. In this case, we have $P_a Q_2 = P_a' + Q_2 P_a$, for the set of matrices P_a. (If $\alpha_2 \neq 0$, and $\alpha_1 = 0$, the same holds for Q_4.) By Section 5 it follows that the invariant ring $\mathfrak{N}(Q_2)$ contains the representation (P_a) of A, which contain a basis (P_i) over $\mathcal{C}$ and F. On the other hand, by Theorem 9 the dimension of $\mathfrak{N}(Q_2)$ is at most, and therefore equal, to n^2. Consequently $\mathfrak{N}(Q_2) = \{\sum P_i c_i, c_i \in C\}$. But the latter is exactly the set of all matrices (P_a) which is the representation of $\mathfrak{A}$. Consequently $\mathfrak{N}(Q_2) \cong \mathfrak{A}$. Let $g(t)$ be a characteristic polynomial of Q_2, then $\mathfrak{N}(Q_2) \cong \mathfrak{N}(g) \cong \mathfrak{A}$. The fact that $g(t)$ is an A-polynomial follows now from Lemma 17.

The polynomial $g(t)$ will be said to *represent* the algebra $\mathfrak{A}$ if $\mathfrak{A}$ is isomorphic with $\mathfrak{N}(g)$. In other words, if $g(t) \to \mathfrak{A}$ in the homomorphism of Theorem 16.

In order to turn the homomorphism of Theorem into an isomorphism, we prove:

THEOREM 17. *If $g(t)$ and $h(t)$ are two A-polynomials, then $\mathfrak{N}(g) \cong \mathfrak{N}(h)$ if and only if $g(t) \simeq h(t + a) \simeq h(t) \times t + a$, for some $a \in F$.*

Evidently $t + a$ is an A-polynomial, and $\mathfrak{N}(t + a) = \mathcal{C}$. It follows now by Lemma 19 that $\mathfrak{N}(g) \cong \mathfrak{N}(h) \times \mathfrak{N}(t + a) \cong \mathfrak{N}(h)$.

Conversely, let $\mathfrak{N}(g) \cong \mathfrak{N}(h)$. Let $g(t)$ belong to $(\mathfrak{V}, \mathbf{A})$. Since the dimensions of $\mathfrak{N}(g)$ and $\mathfrak{N}(h)$ are the same, and g, h are A-polynomials, the degrees of g and h are equal. We may assume, therefore, that $h(t)$ belongs to $(\mathfrak{V}, \mathbf{B})$ (the same vector space $\mathfrak{V}$). Thus $\mathfrak{N}(\mathbf{A}) = \mathfrak{N}(\mathbf{B})$ will constitute two representations of $\mathfrak{N}(g)$ or $\mathfrak{N}(h)$ in $V \times V^*$ $(\cong F_n)$, which implies that the isomorphism between $\mathfrak{N}(\mathbf{A})$ and $\mathfrak{N}(\mathbf{B})$ is induced by an inner automorphism in $\mathfrak{V} \times \mathfrak{V}^*$, i.e. $\mathfrak{N}(\mathbf{A}) = u_0 \mathfrak{N}(\mathbf{B}) u_0^{-1}$, for some $u_0 \in \mathfrak{V} \times \mathfrak{V}^*$. Evidently, $u_0 \mathfrak{N}(\mathbf{B}) u_0^{-1} = \mathfrak{N}(u_0 \mathbf{B} u_0^{-1})$. Thus we have obtained two d.t. $\mathbf{A}$ and $\mathbf{A}_1 = u\mathbf{B}u^{-1}$ with the same invariant ring $\mathfrak{N}(\mathbf{A})$. The mapping $v \to v(\mathbf{A} - \mathbf{A}_1)$ for every $v \in \mathfrak{V}$ is a linear transformation in $\mathfrak{V}$, hence belongs to $\mathfrak{V} \times \mathfrak{V}^*$. For, $(va)(\mathbf{A} - \mathbf{A}_1) = v(\mathbf{A} - \mathbf{A}_1)a + va' - va' = v(\mathbf{A} - \mathbf{A}_1)a$. On the other hand, for every $u \in \mathfrak{N}(\mathbf{A})$, $u(\mathbf{A} - \mathbf{A}_1) = (\mathbf{A} - \mathbf{A}_1)u$, which shows that $\mathbf{A} - \mathbf{A}_1$ is a linear transformation in $\mathfrak{V} \times \mathfrak{V}^*$ commuting with $\mathfrak{N}(\mathbf{A})$. The latter contains a basis of $\mathfrak{V} \times \mathfrak{V}^*$; hence $\mathbf{A} - \mathbf{A}_1$ must belong to the center of $\mathfrak{V} \times \mathfrak{V}^*$. Thus $\mathbf{A} - \mathbf{A}_1 = b\mathbf{1}$ for some $b \in F$. $\mathbf{1}$ denotes here the identity linear transformation of F. One readily verifies that this implies that $\mathbf{A} = \mathbf{A}_1 + b\mathbf{1}$. If (v) is a base of $\mathfrak{V}$ then the matrices of $\mathbf{A}$ with respect to (v) is $A_1 + b1$ where A_1 is the matrix of $\mathbf{A}_1$ with respect to (v). The d.t. $\mathbf{A}_1 = u_0 \mathbf{B} u_0^{-1}$ is similar to $\mathbf{B}$, hence $h(t)$ belongs also to $\mathbf{A}_1$. By the proof of Lemma 13, it follows that $h(t - b)$ belongs to $\mathbf{A}$ and since $g(t)$ also belongs to $\mathbf{A}$, $g(t) \simeq h(t + a)$, where $a = -b$. By (7) of Theorem 6, it follows now that $g(t) \simeq h(t) \times t + a$.

Evidently $e_n(t)$ is an A-polynomial.

LEMMA 21. $\mathfrak{N}(e_n) \cong \mathcal{C}_n$.

Indeed $e_n(t)$ is a characteristic polynomial of the zero 0_n and a matrix $P \in F_n$ belongs to $\mathfrak{N}(0_n)$ if and only if $0 = P \cdot 0 - 0 \cdot P = P'$, i.e. $P \in \mathcal{C}_n$. Thus $\mathfrak{N}(e_n) \cong \mathfrak{N}(0_n) \cong \mathcal{C}_n$.

It follows therefore by Theorem 17 and this lemma that:

COROLLARY. *If g is an A-polynomial, $\mathfrak{R}(g) \cong \mathfrak{C}_n$ if and only if $g \simeq e_n \times t + a$, for some $a \in F$.*

Another criterion for $\mathfrak{R}(g)$ to be a matrix ring is the following:

LEMMA 22. *If g is an A-polynomial, then $\mathfrak{R}(g) \simeq \mathfrak{C}_n$ if and only if in the decomposition of g as a multiple of prime polynomials at least one of the factors is linear, and then $g \simeq e_n \times t + c$, where $t + c$ is the linear factor.*

If $\mathfrak{R}(g) = \mathfrak{C}_n$, $g \simeq e_n \times t + a$, which implies by Lemma 15 that $g(t)$ is completely reducible with each factor being similar to $t + a$.

Conversely, $g(t) \simeq p \times e$ where p is an irreducible polynomial. By Lemma 15 it follows that $g(t)$ is uniformly reducible with factors similar to $p(t)$. In particular this yields that $g(t)$ can be written as a multiple of prime polynomials similar to $p(t)$ (Ore [10]). If $g(t)$ has a representation as a multiple of prime factor with one of them of the first degree, it follows by the uniqueness of decomposition that this linear factor is also similar to $p(t)$. Hence $p(t)$ is linear and can be taken as $t + a$. The theorem follows now from the preceding corollary.

We are able now to determine an isomorphism between the central simple algebras $\mathfrak{CS}(\mathfrak{C}, F)$ and a semi-group generated by $\mathfrak{A}(\mathfrak{C}, F)$ by introducing a new relation in $\mathfrak{A}(\mathfrak{C}, F)$. Namely, we write $f(t) \cong g(t)$ if $f(t) \simeq g(t + a)$ for some $a \in F$. Then we have:

THEOREM 18. *The set $\mathfrak{A}(\mathfrak{C}, F)$ form a semi-group under the operation $\times$ and the relation $\cong$ which is isomorphic with $\mathfrak{CS}(\mathfrak{C}, F)$.*

This theorem is an immediate consequence of Theorems 16 and 17, if we show that the A-polynomials form a multiplicative system with respect to $\cong$ and $\times$. Evidently $f(t) \cong f(t)$. If $f(t) \cong g(t + a)$, applying the automorphism φ_{-a} of Lemma 13 we have $f(t - a) = \varphi_{-a}(f) \simeq \varphi_{-a}(g(t + a)) = g(t)$. i.e. $g \cong f$.

If $f(t) \simeq g(t + a)$ and $g(t) \simeq h(t + b)$, then applying φ_b on the second similarity and using the transitivity of $\simeq$, we have $f(t) \simeq h(t + a + b)$, i.e. $f \cong h$. And if $f(t) \simeq f_1(t + a)$, $g(t) \simeq g_1(t + b)$, then $f(t) \times g(t) \simeq f_1(t + a) \times g_1(t + b)$. By Lemma 13 the latter equals $\varphi_a\varphi_b(f_1 \times g_1) = \varphi_{a+b}(f_1 \times g_1)$. Consequently $f \times g \cong f_1 \times g_1$ which completes the proof.

It is well known that the relation of similarity between central simple algebras together with Kronecker product of algebras turn the set of all central simple algebras over $\mathfrak{C}$ into a group, known as the Brauer group. Evidently the set $\mathfrak{CS}(\mathfrak{C}, F)$ is then turned into a subgroup. We shall denote the latter by $\mathfrak{B}(\mathfrak{C}, F)$.

The definition of similarity of algebras leads us to the following definition of weak-similarity between A-polynomials: Two A-polynomials $f(t)$, $g(t)$ will be said to be *weakly similar* and we write $f(t) \sim g(t)$ if there exist two polynomials $e_n(t)$ and $e_m(t)$ such that $f(t) \times e_n \simeq g(t) \times e_m$. e_n and e_m must be chosen, of course, so that the degrees of the polynomials on both sides will be equal. The A-polynomial $f(t)$ is similar to $p(t) \times e'(t)$ and $g(t) \simeq q(t) \times e''(t)$, where $p(t)$ and $q(t)$ are irreducible A-polynomials. By Lemma 15 and by the unique decomposition of polynomials one readily observes that $f(t) \sim g(t)$ is equivalent to the fact that $p(t) \simeq q(t)$. This shows immediately that the weak-similarity is an equivalence relation. Furthermore, it follows that weak-similarity for irreducible polynomials is the same as similarity.

THEOREM 19. *The set of all A-polynomials $\mathfrak{A}(C; F)$ form a group under the weak-similarity relation and the operation $\times$. This group is homomorphic with $\mathfrak{B}(C, F)$. The kernel of this homomorphism is the group of all linear polynomials.*

PROOF. The mapping is again $g(t) \to \mathfrak{R}(g)$. By Lemma 20, the images run over all elements of the Brauer group.

$g(t) \sim f(t)$ is equivalent to $q(t) \simeq p(t)$. $\mathfrak{R}(g) \cong \mathfrak{R}(q) \times \mathfrak{C}_\nu$, $\mathfrak{R}(f) \cong \mathfrak{R}(p) \times \mathfrak{C}_\mu$, and since $q(t)$, $p(t)$ are irreducible, $\mathfrak{R}(q)$ and $\mathfrak{R}(p)$ are division algebras. Thus if $g \sim f$, $\mathfrak{R}(q) \cong \mathfrak{R}(p)$ which means that $\mathfrak{R}(g)$ and $\mathfrak{R}(f)$ are similar, hence represent the same class in the Brauer group.

Theorems 6 and 14 immediately show that the set of A-polynomials form a group with the relation $\sim$ and the operation $\times$. The homomorphism follows now by Lemma 19, and the structure of the kernel is a consequence of the corollary of Theorem 17.

REMARK. Here again we can pick out in each class of weakly similar A-polynomials a unique prime polynomial and one may consider the group of all A-polynomials as a group of all irreducible A-polynomials with the relation of similarity but with an operation $\otimes$ defined: $p(t) \otimes q(t) \simeq r(t)$ where $r(t)$ is the irreducible A-polynomial which satisfies $p(t) \times q(t) \simeq r(t) \times e(t)$.

8. Solutions of A-equations

The aim of the present part is to find the structure of the solutions of the differential equations corresponding to A-polynomials and to determine the relation between their properties and the properties of the algebras determined by the corresponding polynomial.

As in Section 6, we consider an extension K of F with the constant field $\mathfrak{D}$ of K containing $\mathfrak{C}$.

Let $g(t)$ be a polynomial belonging to $(\mathfrak{B}, \mathbf{A})$; it was shown in Theorem 11 that $g(t)$ belongs also to $(\mathfrak{B}_K, \mathbf{A})$. The polynomial $g(t)$ determines an invariant ring $\mathfrak{R}(g)$ in $F[t]$ and $\mathfrak{R}_K(g)$ in $K[t]$. Similarly, $\mathbf{A}$ determines $\mathfrak{R}(\mathbf{A})$ in the Hom $(\mathfrak{B}, \mathfrak{B})$, i.e. in $\mathfrak{B} \times \mathfrak{B}^*$, and an invariant ring $\mathfrak{R}_K(\mathbf{A})$ in $\mathfrak{B}_K \times \mathfrak{B}_K^*$. Generally we can only prove that:

LEMMA 23. *The ring $\mathfrak{R}_K(\mathbf{A})\,(\mathfrak{R}_K(g))$ contains a ring isomorphic with*

$$\mathfrak{R}(\mathbf{A}) \times \mathfrak{D}(\mathfrak{R}_K(g) \times \mathfrak{D}).$$

In view of the fact that $g(t)$ belongs also to $(\mathfrak{B}_K, \mathbf{A})$, $\mathfrak{R}_K(\mathbf{A}) \cong \mathfrak{R}_K(g)$, and it suffices therefore to prove the Lemma for $\mathfrak{R}_K(\mathbf{A})$ only.

Consider $\mathfrak{R}(\mathbf{A})$ as a subring of $\mathfrak{B} \times \mathfrak{B}^*$ containing the vectors of $\mathfrak{R}(\mathbf{A} \times \mathbf{A}^*)$ since $\mathfrak{B}_K \times \mathfrak{B}_K^* = (\mathfrak{B} \times \mathfrak{B}^*)_K$, it follows by Lemma 14 that $\mathfrak{R}_K(\mathbf{A} \times \mathbf{A}^*)$ contains $\mathfrak{R}(\mathbf{A} \times \mathbf{A}^*)$ which is equal to $\mathfrak{R}_K(\mathbf{A})$. Let $u_1, \cdots, u_m$ be a basis of $\mathfrak{R}(\mathbf{A} \times \mathbf{A}^*)$. By the same lemma they are also $\mathfrak{D}$-independent in $\mathfrak{R}_K(\mathbf{A} \times \mathbf{A}^*)$, consequently the latter which is the ring $\mathfrak{R}_K(\mathbf{A})$ contains $\mathfrak{R}(\mathbf{A}) \times \mathfrak{D} = \{\sum u_i d_i , d_i \in \mathfrak{D}\}$. In particular if $g(t)$ is an A-polynomial of degree n, $\mathfrak{R}(g)$ contains n^2 independent elements over C, and therefore the dimension of $\mathfrak{R}(g) \times \mathfrak{D}$ over $\mathfrak{D}$ is n^2. On the other hand, $\mathfrak{R}_K(g)$ can contain at most n^2 elements independent over $\mathfrak{D}$. Hence:

THEOREM 20: *If $g(t)$ is an A-polynomial in $F[t]$, then $g(t)$ is also an A-polynomial in $K[t]$ and $\mathfrak{R}_K(g) = \mathfrak{R}(g) \times \mathfrak{D}$.*

We recall that the exponent of a central simple algebra $\mathfrak{A}$ is the minimal integer ρ such that $\mathfrak{A}^\rho = \mathfrak{A} \times \cdots \times \mathfrak{A}(\rho$ times) is a total matrix ring over $\mathfrak{C}$.

An immediate consequence of this theorem and of the corollary of Theorem 17 is:

COROLLARY. *Let $g(t)$ represent an algebra $\mathfrak{A}$. Then a necessary and sufficient condition that $\mathfrak{D}$ splits $\mathfrak{A}$ is that $g(t)$ has a left or a right root in K.*

The notation $g^{[\rho]}$ will be used for $g \times \cdots \times g(\rho$ times).

THEOREM 21. *Let $g(t)$ be an A-polynomial of degree n, and let $\mathfrak{R}(g)$ be of exponent ρ. One can find an algebraic extension $\mathfrak{D}$ of $\mathfrak{C}$ of degree $\leqq n$, a finite algebraic extension K of degree $\leqq \rho$ of the composite field $F\mathfrak{D}$ and an element $a \in F$ such that the equation belonging to $g(t - a)$ has n independent solutions in K.*

PROOF. By Lemma 19, Corollary of Theorem 17 and the fact that $\mathfrak{R}(g)$ is a matrix ring over $\mathfrak{C}$, it follows that $g^{[\rho]} \simeq t + b \times e(t)$.

Since $R(g)$ is a central simple algebra of degree n^2, it possesses a splitting field $\mathfrak{D}$ of degree at most n over $\mathfrak{C}$. Extend the derivation F to $F\mathfrak{D}$, the constant field will then be $\mathfrak{D}$. Since $\mathfrak{R}(g) \times \mathfrak{D}$ is a matrix ring it follows by the preceding theorem and by corollary of Theorem 17 that $g(t) \simeq t + c \times e(t)$ in $F\mathfrak{D}[t]$.

Now in $F\mathfrak{D}[t]$, $g(t)^{[\rho]} \simeq (t + c)^{[\rho]} \times e(t)^{[\rho]} \simeq t + \rho c \times e'(t)$ (part (7) of Theorem 6 and the corollary of Lemma 10), which implies by Theorem 11 that

$$t + \rho c \times e'(t) \simeq t + b \times e(t).$$

Consequently, Lemma 16 yields $t + \rho c \simeq t + b$ in $F\mathfrak{D}[t]$. This means that there exists an element $d \neq 0$ in $F\mathfrak{D}$ such that $\rho c = b + d^{-1} d'$ (Lemma 2). Put $a = (1/\rho)b$ and $K = F\mathfrak{D}(\sqrt[\rho]{d})$. Extending the derivation of $F\mathfrak{D}$ to K, we have $y^{-1}y' = (1/\rho)d^{-1} d'$, where $y = \sqrt[\rho]{d}$, which in particular means that $t + \rho^{-1}d^{-1} d' \simeq t + y^{-1}y' \simeq t$ in K.

On the other hand, since $g(t) \simeq t + c \times e(t)$, it follows by Lemma 13, $g(t - \rho^{-1}b) \simeq t + c - \rho^{-1}b \times e(t) = t + \rho^{-1}d^{-1} d' \times e(t) \simeq t \times e(t) \simeq e(t)$. The result follows now from part (2) of Theorem 4.

REMARK. Note that by Theorem 17, $g(t - a)$ is also a polynomial whose invariant ring is isomorphic with $\mathfrak{R}(g)$. This means that if one starts from a central simple algebra $\mathfrak{A}$ one can find a polynomial $g(t)$ such that $\mathfrak{A} \cong R(g)$ and $g(t)$ has all solutions in the field K of the preceding lemma.

We remark also that if for the polynomial $g(t)$ of the preceding lemma $g(t)^{[\rho]} \simeq t + b \times e(t)$ holds, then by part (7) of Theorem 6, $g(t - \rho^{-1}b)^{[\rho]} \simeq t + b - b \times e(t) \simeq e(t)$ which we can state in view of the previous remark that:

COROLLARY. *If $\mathfrak{A}$ is a central simple algebra of exponent ρ then one can find an*

A-polynomial $g(t)$ representing $\mathfrak{A}$ such that $g^{[\rho]}$ is completely solvable and $g(t)$ has all its solutions in the field K of the preceding lemma.

Let K be any extension of F with the constant field $\mathfrak{D}$.

THEOREM 22. *Let $g(t)$ be an A-polynomial of the type of the preceding corollary representing an algebra $\mathfrak{A}$ of exponent ρ. If the equation $g(z) = 0$ has a solution in K, then K contains a subfield $K' \supseteqq F\mathfrak{D}$ such that K' contains n independent solutions of $g(z) = 0$ and $K' = F\mathfrak{D}(\sqrt[\rho]{c})$ for some $c \in F\mathfrak{D}$. Furthermore, every solution of $g(z) = 0$ in K satisfies an equation $x^\rho - d = 0$, $d \in F\mathfrak{D}$.*

PROOF. Since $g(z) = 0$ has a solution in K it follows by the corollary of Lemma 23 and by Lemma 1 that the field $\mathfrak{D}$ splits $\mathfrak{R}(g)$. Considering the extension $F\mathfrak{D}$ of F, we have $\mathfrak{R}(g) \times \mathfrak{D} \cong \mathfrak{R}_{FD}(g)$ and the latter is a total matrix ring over $\mathfrak{C}$. It follows, therefore, by corollary of Theorem 17 that $g(t) \simeq t - a \times e(t)$ in $F\mathfrak{D}[t]$ for some $a \in F\mathfrak{D}$.

Let y be any solution of $g(z) = 0$ in the field $F\mathfrak{D}(y) = K_0 \subseteqq K$. It follows by Lemma 1 and Lemma 22 that $g(t) \simeq t - y^{-1}y' \times e(t)$ in $K_0[t]$. Thus $t - a \times e(t) \simeq t - y^{-1}y' \times e(t)$ in $K_0[t]$, which yields, by the cancellation law (Lemma 16), that $t - a \simeq t - y^{-1}y'$. The right polynomial is similar to t, hence by Lemma 2 $a = x^{-1}x'$ for some $x \in K_0$. We remark, that the factor $t - a$ could be chosen as a left factor of $g(t)$ (since they are all similar) which will yield by Lemma 1 that x is also a solution. Now $g(t)$ was assumed to be of the type of the preceding corollary, that is: $g^{[\rho]}(t) \simeq e'(t)$. Applying Lemma 13 we have $(t - a \times e(t))^{[\rho]} \simeq t - \rho a \times e'(t) \simeq e'(t)$, and again by the cancellation law $t - \rho a \simeq t$, which implies that $\rho a = m^{-1}m'$ for some $m \in F\mathfrak{D}$. The result that $m \in F\mathfrak{D}$ is a consequence of the fact that the last similarity holds in $F\mathfrak{D}[t]$. Passing now to K_0 we have: $\rho(x^{-1}x') = m^{-1}m'$; hence $(x^\rho m^{-1})^{-1}(x^\rho m^{-1})' = 0$. This implies that $x^\rho = dm$, where $d \in \mathfrak{D}$. Put $K' = FD(x)$, x satisfies the equation $x^\rho = c$, $c = dm \in F\mathfrak{D}$. In K' the equation $g(z) = 0$ has at least one solution $z = x$. By the same argument as in the beginning of this proof, $g(t) \simeq t - a \times e(t)$ in $F\mathfrak{D}$. It follows therefore by Lemma 15 that $g(t)$ is uniform reducible in $F\mathfrak{D}$ with factors similar to $t - a$, i.e. $g(t) = [t - q_i, \cdots, t - q_n]$, with $t - q_i \simeq t - a$. This yields that $q_i = a_i^{-1}a_i' + a$, $a_i \in F\mathfrak{D}$. Since $a = x^{-1}x'$, we have $q_i = (a_ix)^{-1}(a_ix)'$. Put $y_i = a_ix$. Then by Lemma 3 $y_1, \cdots, y_n$ is a complete set of independent solutions in K'.

As a result of part (2) of Lemma 14, (y_i) form also a base of their solutions of $g(z) = 0$ in K. Thus, every solution $y = \sum y_i d_i$, $d_i \in \mathfrak{D}$. Hence $y_i = \sum x_i a_i d_i = xa$, $a = \sum a_i d_i \in F\mathfrak{D}$. But then $y^\rho = x^\rho a = ca \in F\mathfrak{D}$. Q.E.D.

9. The Brauer group of algebras which are split by two fields

Let $\mathfrak{D}'$ be any extension field of $\mathfrak{C}$. Form a composition $F\mathfrak{D}$ of F, where $\mathfrak{D} \cong \mathfrak{D}'$ and such that F and $\mathfrak{D}$ are linearly disjoint over $\mathfrak{C}$. This is always possible since the constant field is algebraically closed in F and F has characteristic zero.[13]

[13] For definition of linear disjointness, and the proof of the construction of $F\mathfrak{D}$ in the case F, $\mathfrak{D}$ are of finite transcendence degree over $\mathfrak{C}$ see A. Weil [12], Ch. I. The proof of the case of infinite transcendence degree is readily obtained from there.

The derivation in F can be canonically extended to a derivation in $F\mathfrak{D}$ possessing $\mathfrak{D}$ as a constant field. For, a derivation in $F\mathfrak{D}$ is determined by the mapping of the transcendence base over $\mathfrak{C}$. Choose a transcendence base by picking transcendence bases of F over $\mathfrak{C}$ and of $\mathfrak{D}$ over $\mathfrak{C}$, map the latter on zeros, and the first on their derivatives already defined in F. One readily shows that this is the required extension.

Denote by $F\mathfrak{D}^+$, F^+ the additive group of the elements of $F\mathfrak{D}$ and F respectively. The set $a^{-1}a'$, $a \in F\mathfrak{D}$ of all logarithmic derivatives form a sub-group $\mathfrak{L}(F\mathfrak{D})$ of $F\mathfrak{D}^+$. We shall be interested in the quotient group $F\mathfrak{D}^+/[F^+ + \mathfrak{L}(F\mathfrak{D})]$. We prove:

THEOREM 23: *The Brauer group of central simple algebras over* $\mathfrak{C}$ *which are split both by* F *and by* $\mathfrak{D}$ *is isomorphic with a subgroup of* $F\mathfrak{D}^+/[F^+ + \mathfrak{L}(F\mathfrak{D})]$.

PROOF. By Theorem 19 it follows that it suffices to prove the isomorphism of the subgroup of all A-polynomials of that theorem, whose division algebras are split both by F and $\mathfrak{D}$.

Let $g(t)$ be an A-polynomial. If $\mathfrak{N}(g)$ is assumed to be split also by $\mathfrak{D}$, then it follows by Theorem 20 and the corollary of Theorem 17 that $g(t) \simeq t + a_g \times e(t)$, equivalently $g(t) \sim t + a_g$ in $F\mathfrak{D}[t]$. We define now the correspondence: $g(t) \to \bar{a}_g$ where $\bar{a}_g$ is the class of $F\mathfrak{D}^+/[F^+ + \mathfrak{L}(F\mathfrak{D})]$ represented by a_g. If $g(t) \sim f(t)$ in $F[t]$, one shows readily that this holds also in $F\mathfrak{D}[t]$ (Theorem 11). Hence $t + a_g \sim t + a_f$. But, as was pointed out in the preceding section, weak-similarity for irreducible polynomials is similarity; hence, by Lemma 2, $a_g = a_f + b^{-1}b'$, i.e. $\bar{a}_g = \bar{a}_f$. If $g(t) \sim t + a_g$ and $f(t) \sim t + a_f$ then $g(t) \times f(t) \sim t + a_g \times t + a_f \sim t + (a_g + a_f)$ by (7) of Theorem 6. Thus $g \times f \to \bar{a}_g + \bar{a}_f$. This proves that this group of all A-polynomials is homomorphic with a subgroup of $F\mathfrak{D}^+/[F^+ + L(F\mathfrak{D})]$. To find the kernel of this homomorphism, we consider a polynomial $g(t)$ such that $a_g = k + b^{-1}b'$, $b \in F\mathfrak{D}$. Lemma 2 shows that $t + a_g \simeq t + k$ in $F\mathfrak{D}[t]$, hence $g(t) \simeq t + a_g \times e(t) \simeq t + k \times e(t)$ in $F\mathfrak{D}[t]$. $g(t) \in F[t]$ and $t + k \times e(t)$ can be chosen to be a polynomial in $F[t]$. It follows, therefore, by Theorem 12 that $g(t) \simeq t + k \times e(t)$ in $F[t]$ which implies that $g(t) \sim t + k$ in $F[t]$. This means that the kernal is exactly the set of these polynomials which are also the kernel of the homomorphism of Theorem 19. Namely, the polynomials whose algebra is the matrix algebra, and this completes the proof.

In particular, one can choose $\mathfrak{D}$ to be an isomorphic copy F_0 of F, or $\mathfrak{D} = \bar{\mathfrak{C}}$, the algebraic closure of $\mathfrak{C}$. In both cases, the preceding theorem states:

COROLLARY. *The Brauer group* $\mathfrak{B}(\mathfrak{C}, F)$ *is isomorphic with a subgroup of:* (1) $FF_0^+/[F^+ + \mathfrak{L}(FF_0)]$, (2) $F\bar{\mathfrak{C}}^+/[F^+ + \mathfrak{L}(F\bar{\mathfrak{C}})]$.

Theorem 23 gives a representation of the Brauer group as a homomorphic image of a subgroup of the additive group of elements of F. When considering only algebras of exponent dividing a fixed number ρ, we are able to obtain a representation of the subgroup on the multiplicative group of elements of F. Denote by $F\mathfrak{D}^*$, F^* and $\mathfrak{D}^*$ the multiplicative group of the elements of $F\mathfrak{D}$, F and $\mathfrak{D}$ respectively. The set of all elements $y \in F\mathfrak{D}^*$ which satisfy a differential equation $y' - yk = 0$ for some $k \epsilon F$, form a multiplicative group. For, if $y_1' = y_1k_1$ and $y_2' = y_2k$ then $(y_1y_2)' = (k_1 + k_2)(y_1y_2)$ and $(y^{-1})' = -ky^{-1}$. Denote this group by $\mathfrak{F}$. Evidently $\mathfrak{F} \supseteqq F^*\mathfrak{D}^*$. We wish to show that $\mathfrak{F} = F^*\mathfrak{D}^*$. For let $y \epsilon F\mathfrak{D}^*$ such that $y' = yk$ with $k \epsilon F$. Consider $F\mathfrak{D}$ as a vector space over F and let $(d_i) \epsilon \mathfrak{D}$ be a basis of $F\mathfrak{D}$ over F then $y = \sum d_ik_i$, $k_i \epsilon F$. Hence: $y' = \sum d_ik_i' = \sum d_ikk_i$. Since (d_i) is a basis, $k_i' = kk_i$. Note that since $y \neq 0$, at least one $k_i \neq 0$. The solutions of an equation $z' - kz = 0$ are all of the form dk_i, where d ranges over all elements of the constant field $\mathfrak{D}$. Thus $y = dk_i$ which proves that $\mathfrak{F} \subsetneqq F^*D^*$. Let $g(t)$ be an A-polynomial whose invariant ring $\mathfrak{R}(g)$ is of exponent ρ and is split both by F and $\mathfrak{D}$; then as we have seen in the proof of the preceding theorem, $g(t) \sim t + a_g$ in $F\mathfrak{D}[t]$, which implies that $g(t)^{[\rho]} \sim (t + a_g)^{[\rho]} \simeq t + \rho a_g$. On the other hand, since $\mathfrak{R}(g)$ is of exponent ρ it follows by Theorem 19 that $g(t)^{[\rho]} \sim t + k$ for some $k \epsilon F$. Consequently $t + k \sim t + a_g$ in $F\mathfrak{D}[t]$ and thus $t + k \simeq t + a_g$, which by Lemma 2 yields that $a_g = k + b_g^{-1}b_g'$ for some $b_g \epsilon F\mathfrak{D}$. In the notation of the proof of the preceding theorem we have $\bar{a}_g = \overline{\rho^{-1}b_g^{-1}b_g'}$.

THEOREM 24. *The mapping $g(t) \rightarrow b_g$ induces an isomorphism between the Brauer subgroup of all division algebras of exponent ρ which are split both by F and $\mathfrak{D}$ and a subgroup of $F\mathfrak{D}^*/F^*\mathfrak{D}^*(F\mathfrak{D}^*)^\rho$, where $(F\mathfrak{D}^*)^\rho$ denotes the group of all ρ^{th} powers of the elements of $F\mathfrak{D}^*$.*

Denote by $\tilde{b}_g$ the class of $(F\mathfrak{D})^*/F^*\mathfrak{D}^*(F\mathfrak{D}^*)^\rho$ represented by b_g. If $\tilde{b}_g = \tilde{b}_h$, then $b_h = b_g \cdot k\alpha \cdot c^\rho$ where $c \epsilon F\mathfrak{D}$, $\alpha \epsilon \mathfrak{D}^*$, $k \epsilon F^*$. Taking the log derivative on both sides we have $b_h^{-1}b_h' = b_g^{-1}b_g' + k^{-1}k' + \rho c^{-1}c'$;. hence $\rho^{-1}(b_h^{-1}b_h') = \rho^{-1}(b_g^{-1}b_g') + c^{-1}c' + h$ where $h = \rho^{-1}k^{-1}k' \epsilon F$. Now $g(t) \sim t + a_g$, $h(t) \sim t + a_h$ where $\bar{a}_g = \overline{\rho^{-1}b_g^{-1}b_g'}$ (in the notation of the proof of the preceding theorem) and $\bar{a}_g = \overline{\rho^{-1}b_h^{-1}b_h'}$. Consequently $\bar{a}_g = \bar{a}_h$, which implies by the preceding theorem that $g(t) \sim h(t)$.

Conversely, if $g(t) \sim h(t)$ it follows by the proof of the preceding theorem that $\bar{a}_g = \bar{a}_h$. Hence $\overline{\rho^{-1}b_g^{-1}b_g'} = \overline{\rho^{-1}b_h^{-1}b_h'}$, which yields $b_h^{-1}b_h' = b_g^{-1}b_g' + k + \rho c^{-1}c'$ for some $c \epsilon FD$, $k \epsilon F$. Since $\rho c^{-1}c' = (c^\rho)^{-1}(c^\rho)'$ we have $k = (b_hb_g^{-1}c^\rho)(b_hb_g^{-1}c^\rho)$. As already shown this implies that $b_hb_g^{-1}c^\rho = l \cdot d$, $l \epsilon F$, $d \epsilon \mathfrak{D}$. i.e. $\tilde{b}_h = \tilde{b}_g$.

If $g(t) \sim t + a_g$ and $h(t) \sim t + a_h$, then by the proof of the preceding theorem $g(t) \times h(t) \sim t + (a_g + a_h)$. Hence if $\bar{a}_g = \overline{\rho^{-1}b_g^{-1}b_g'}$ and $\bar{a}_h = \overline{\rho^{-1}b_h^{-1}b_h'}$ then $\bar{a}_g + \bar{a}_h = \overline{\rho^{-1}(b_g^{-1}b_g' + b_h^{-1}b_h')} = \overline{\rho^{-1}(b_gb_h)^{-1}(b_gb_h)'}$. Which proves that to $g \times h$ corresponds the class b_gb_h. The proof follows now by the fact that the Brauer subgroup of the algebras considered in this theorem is isomorphic, by the isomorphism induced by that of Theorem 19, with the subgroup of all A-polynomials which were just considered.

As in the preceding corollary we have:

COROLLARY. *The Brauer subgroup of all division algebras split by F and of exponent ρ is isomorphic with a subgroup of*:

$$(1)\ FF_0^*/F^*F^*(FF_0^*)^\rho, \qquad (2)\ F\mathfrak{C}^*/F^*\mathfrak{C}^*(F\mathfrak{C}^*)^\rho.$$

The problem is now to characterize the elements of $F\mathfrak{D}^+/[F^+ + \mathfrak{L}(F\mathfrak{D})]$ in the first case and $F\mathfrak{D}^*/F^*D^*(F\mathfrak{D}^*)^\rho$ in the second case which are images of the algebras of the Brauer group in the isomorphisms of Theorems 23 and 24. One characterization which is not satisfactory is just their definition, namely: in the first case, $\bar{a}$ is an image of a division algebra if and only if there exists an A-polynomial $g(t)$ in $F[t]$ such that $g(t) \sim t + a$ which means $g(t) \simeq t + a \times e_n(t)$; in the second case, b is an image of a division algebra if and only if there exists an A-polynomial $g(t)$ such that $g(t) \sim t + b^{-1}b'/\rho$. A more satisfactory answer we can give only in the case that $\mathfrak{D}$ is an algebraic normal extension of $\mathfrak{C}$ (finite or infinite).

We assume henceforth that $\mathfrak{D}$ is algebraic normal extension of $\mathfrak{C}$ with the Galois group $\mathfrak{G}$. Since F and $\mathfrak{D}$ are linearly disjoint over $\mathfrak{C}$, the automorphisms of $\mathfrak{D}$ over $\mathfrak{C}$ can be extended in a unique way to automorphisms of $F\mathfrak{D}$ over F and we may assume that $\mathfrak{G}$ is in fact the Galois group of $F\mathfrak{D}$ over F. We note that for every $a \in F\mathfrak{D}$ and for every $\vartheta \in G$, we have $(a')^\vartheta = (a^\vartheta)'$. Indeed, a is algebraic over F since $\mathfrak{D}$ is algebraic over $\mathfrak{C}$. Let $f(x) = x^n + b_1x^{n-1} + \cdots + b_n$ be the minimal equation of a over F. Taking the derivative of $f(a) = 0$, we obtain $\partial f/\partial a \cdot a' + f'(a) = 0$ where $f'(a) = b_1'a^{n-1} + \cdots + b_n'$. This shows that $a' = g(a)$, where $g(x)$ is a polynomial in F. Thus $(a')^\vartheta = g(a^\vartheta)$. On the other hand a satisfies the same equation as $f(x)$ over F, hence $(a^\vartheta)' = g(a^\vartheta)$ which proves $(a')^\vartheta = (a^\vartheta)'$.

By the remark of the preceding Lemma 13 we may assume that the automorphisms of $\mathfrak{G}$ were extended in a natural way to $F\mathfrak{D}[t]$.

A consequence of the fact that $(a')^\vartheta = (a^\vartheta)'$ is that the restriction of ϑ to $\mathfrak{L}(F\mathfrak{D})$ is also an isomorphism, so that ϑ induces an automorphism of $F\mathfrak{D}^+/\mathfrak{L}(F\mathfrak{D})$. Let $M/\mathfrak{L}(F\mathfrak{D})$ the maximal subgroup of $FD^+/\mathfrak{L}(F\mathfrak{D})$ whose elements are left invariant under $\mathfrak{G}$. This group contains the group $\bar{F} = (F^+ + \mathfrak{L}(F\mathfrak{D}))/\mathfrak{L}(F\mathfrak{D})$. Then:

THEOREM 25. *The Brauer group of all division algebras over $\mathfrak{C}$ which are split both by F and $\mathfrak{D}$ is isomorphic with $M/[F^+ + \mathfrak{L}(F\mathfrak{D})]$.*

PROOF. The previous characterization of the classes $\bar{a}$ of $F\mathfrak{D}^+/[F^+ + \mathfrak{L}(F\mathfrak{D})]$ which correspond to division algebras was that $g(t) \simeq t + a \times e_n(t)$ for some A-polynomial $g(t) \in F[t]$. If this holds, then by the remark preceding Lemma 13, $g^\vartheta(t) \simeq t + a^\vartheta \times e_n(t)$. But $g^\vartheta(t) = g(t)$ and $e_n(t)$ is chosen to belong to $F[t]$, hence $g(t) \simeq t + a \times e_n(t) \simeq t + a^\vartheta \times e_n(t)$. By the cancellation law $t + a \simeq t + a^\vartheta$ in $F\mathfrak{D}[t]$, which by Lemma 2 shows that $a^\vartheta = a + b_\vartheta^{-1}b_\vartheta'$, i.e. $a \in M$.

Conversely if $a \in M$ then $a^\vartheta = a + b_\vartheta^{-1}b_\vartheta'$ for $\vartheta \in G$ and for some $b_\vartheta \in F\mathfrak{D}$. Only a finite number of the elements of a^ϑ is different from a; hence the least common right multiple $g(t) = [t - a^\vartheta]$ for all $\vartheta \in G$ is a polynomial in $F\mathfrak{D}[t]$. If $g(t)$ is a monic polynomial then $g(t) \in F[t]$. Indeed, for every $\vartheta \in \mathfrak{G}$ $g^\vartheta(t)$ is the least common right multiple of all $t - a^\vartheta$ and again it is a monic polynomial which yields $g^\vartheta(t) = g(t)$ and proves that $g(t) \in F[t]$. Another consequence of the fact that $a^\vartheta = a + b_\vartheta^{-1}b_\vartheta'$ is that $t + a^\vartheta \simeq t + a$. It follows, therefore, by Lemma

15 that $g(t) \simeq t + a \times e_\nu(t)$ in $F\mathfrak{D}[t]$. Applying (6) and (7) of Theorem 14 and corollary of Lemma 10 we obtain

$$g(t) \times g^*(t) \simeq t + a \times e_\nu(t) \times t - a \times e^*_\nu(t) \simeq t + a - a \times e_{\nu^2}(t) \simeq e_{\nu^2}(t).$$

Since $g(t) \times g^*(t)$ can be chosen in $F[t]$ and so can $e_{\nu^2}(t)$, it follows by Theorem 12 that $g(t) \times g^*(t) \simeq e_{\nu^2}(t)$ in $F[t]$, i.e. $g(t)$ is an A-polynomial.

The proof is now completed since $g(t) \simeq t + a \times e_\nu(t)$ so that $g(t)$ corresponds to a.

Remark. The degree of $g(t)$ can be also determined. For if $g(t) = [t + a^\vartheta]$ then $g(t - a) = [t - a + a^\vartheta] = [t + b_\vartheta^{-1}b'_\vartheta]$. Put $c_\vartheta = b_\vartheta^{-1}$, then $g(t - a) = [t - c_\vartheta^{-1}c'_\vartheta]$. In view of the proof of Lemma 3b, $g(t - a)$ determines the minimal equation satisfied by all c_ϑ . Hence the degree of $g(t - a)$ and, therefore, also of $g(t)$ equals the maximal number of $\mathfrak{D}$-independent elements among the c_ϑ .

To give the characterization of the classes $\tilde{b}$ of $F\mathfrak{D}^*/F^*\mathfrak{D}^*(F\mathfrak{D}^*)^\rho$ which represent division algebras, we first consider the group $N/\mathfrak{D}^*(F\mathfrak{D}^*)^\rho$ which contains classes $\tilde{b}$ left invariant by $\mathfrak{G}$. Then $N \supset F^*\mathfrak{D}^*(F\mathfrak{D}^*)^\rho$ and we show:

Theorem 26. *The Brauer subgroup of all division algebras over* $\mathfrak{C}$ *which are split both by* F *and* $\mathfrak{D}$ *and of exponent* ρ *is isomorphic with* $N/F^*\mathfrak{D}^*(F\mathfrak{D}^*)^\rho$.

The characterization of the classes $\tilde{b}$ of $F\mathfrak{D}^*/F^*\mathfrak{D}^*(F\mathfrak{D}^*)^\rho$ which represented division algebras is that the classes of $\overline{\rho^{-1}b^{-1}b'}$ of $F\mathfrak{D}^+/[F^+ + \mathfrak{L}(F\mathfrak{D})]$. By the preceding theorem this means that $(\rho^{-1}b^{-1}b')^\vartheta = \rho^{-1}b^{-1}b' + c_\vartheta^{-1}c_\vartheta$. Hence it is equivalent to $(b^\vartheta)^{-1}(b^\vartheta)' = b^{-1}b' + (c^\rho)^{-1}(c^\rho)'$ so that $b^\vartheta = bc_\vartheta^\rho \cdot d_\vartheta$, $d_\vartheta \in \mathfrak{D}$ which proves that these classes $\tilde{b}$ are exactly those determined by N.

Theorems 25 and 26 can be formulated in another way:

Theorem 27. *The Brauer group of all division algebras over* $\mathfrak{C}$ *which are split both by* F *and* $\mathfrak{D}$ *is isomorphic with the first cohomology group of* $\mathfrak{G}$ *with coefficient in the additive group* $\mathfrak{L}(F\mathfrak{D})$, *or equivalently with coefficient in the multiplicative group* $(F\mathfrak{D})^*/\mathfrak{D}^*$.

It suffices to show only the first statement since the mapping $a \rightarrow a^{-1}a'$ determines an isomorphism between $(F\mathfrak{D})^*/\mathfrak{D}^*$ and $\mathfrak{L}(F\mathfrak{D})$ which commutes with the action of the group of automorphisms $\mathfrak{G}$. This evidently implies that the first cohomology groups $H^1(\mathfrak{L}(F\mathfrak{D}); \mathfrak{G})$, $H^1((F\mathfrak{D})^*/\mathfrak{D}^*; \mathfrak{G})$ are isomorphic.

To prove the first statement we observe that $\bar{a} \in M/\mathfrak{L}(F\mathfrak{D})$ if and only if $a^\vartheta = a + b_\vartheta^{-1}b'_\vartheta$, (Theorem 25). To this element $\bar{a}$ we shall make correspond the cochain f of $\mathfrak{G}$ defined as: $f(\vartheta) = b_\vartheta^{-1}b'_\vartheta$. Since $f(\vartheta) = a^\vartheta - a$ it is a cocycle in $F\mathfrak{D}^+$, hence also a cocycle in $H^1(\mathfrak{L}F\mathfrak{D}), \mathfrak{G})$. Conversely, if f is a cocycle in $H^1(\mathfrak{L}(F\mathfrak{D}), \mathfrak{G})$, it bounds when considered in $H^1(F\mathfrak{D}^+, \mathfrak{G})$ hence $f(\vartheta) = a^\vartheta - a$ for some $a \in F\mathfrak{D}$ and for all $\vartheta \in \mathfrak{G}$. Thus the corresponding class $\bar{a} \in M/\mathfrak{L}(F\mathfrak{D})$. Now $\bar{a} \in [F^+ + \mathfrak{L}(F\mathfrak{D})]/\mathfrak{L}(F\mathfrak{D})$ if and only if $a = k + b^{-1}b'$ for some $k \in F$ which implies that $a^\vartheta - a = (b^\vartheta)^{-1}(b^\vartheta)' - b^{-1}b' = c^\vartheta - c, c \in \mathfrak{L}(F\mathfrak{D})$. So that the cocycle f determined by a, i.e. $f(\vartheta) = a^\vartheta - a$ bound in $\mathfrak{L}(F\mathfrak{D})$. Conversely, if $f(\vartheta)$ bounds in $\mathfrak{L}(F\mathfrak{D}), f(\vartheta) = c^\vartheta - c$ with $c = b^{-1}b' \in \mathfrak{L}(F\mathfrak{D})$; but $f(\vartheta) = a^\vartheta - a$ hence $(a - c)^\vartheta = a - c$ for all $\vartheta \in \mathfrak{G}$, which implies that $a - c = k \in F$. Consequently, $a \in F^+ + L(FD)$. It follows now easily that $M/(F^+ + \mathfrak{L}(F\mathfrak{D}))$ is isomorphic with H^1 $(\mathfrak{L}(F\mathfrak{D}), \mathfrak{G})$ and the rest follows by Theorem 25.

The last result can also be obtained straightforward, in a more general case, by cohomology theory methods.

Let $\mathfrak{D}$ be a normal algebraic extension of a field $\mathfrak{C}$ of *any* characteristic. Let F be a field containing $\mathfrak{C}$ and which is linearly disjoint from $\mathfrak{D}$ over $\mathfrak{C}$ (F need not be a transcendental extension of $\mathfrak{C}$). In this case the composite field $F\mathfrak{D}$ is normal over F and its Galois group $\mathfrak{G}$ contains the natural extensions of the automorphisms of the Galois group of $\mathfrak{D}$ over $\mathfrak{C}$. Thus $\mathfrak{G}$ induces also automorphisms of the group $(F\mathfrak{D})^*/\mathfrak{D}^*$.

Under these circumstances we can show:

THEOREM 28. *The Brauer group of the division algebras which are split both by F and $\mathfrak{D}$ is isomorphic with $H^1((F\mathfrak{D})^*/\mathfrak{D}^*, \mathfrak{G})$.*

Indeed, consider the exact sequence $0 \to \mathfrak{D}^* \xrightarrow{i} (F\mathfrak{D})^* \xrightarrow{j} (F\mathfrak{D})^*/\mathfrak{D}^* \to 0$ where i is the injection of $\mathfrak{D}^*$ into $(F\mathfrak{D})^*$ and j is the projection. This gives rise to the exact sequence $H^1((F\mathfrak{D}^*: \mathfrak{G}) \xrightarrow{j^*} H^1((F\mathfrak{D})^*/\mathfrak{D}^*: \mathfrak{G}) \xrightarrow{\delta^*} H^2(\mathfrak{D}^*; \mathfrak{G})) \xrightarrow{i^*} H^2((F\mathfrak{D})^*; \mathfrak{G})$. It is well known that $H^1((FD)^*; \mathfrak{G}) = 0$ which means that δ^* is an isomorphic mapping of $H^1((F\mathfrak{D})^*/\mathfrak{D}^*; \mathfrak{G})$ into $H^2(\mathfrak{D}^*; \mathfrak{G})$. The exactness of the sequence means that $H^1((F\mathfrak{D})^*/\mathfrak{D}^*; \mathfrak{G})$ is isomorphic with the subgroup of $H^2(\mathfrak{D}^*; \mathfrak{G})$ which are mapped onto zero by i^*. From the nature of the mapping i^* one immediately observes that the latter coincides with the set of all 2-cocycles of $H^2(\mathfrak{D}^*; \mathfrak{G})$ which are split when the basic field is extended to F, namely, isomorphic with that group of the division algebras over $\mathfrak{C}$ split by $\mathfrak{D}$ $(\subseteq H^2(\mathfrak{D}^*; \mathfrak{G}))$ which become matrix algebras when the base field is extended to F, i.e. which are split also by F.

10. Characteristic p

In the arguments of the two preceding parts the fact that the characteristic of F is zero enters in three phases. The first phase is the possibility of dividing by any integer; the second phase is the possibility of defining a derivation in F with constant field $\mathfrak{C}$, where F is any transcendental extension over $\mathfrak{C}$ in which $\mathfrak{C}$ is algebraically closed; and third and most important is the result of Jacobson that every d.t. in a vector space $\mathfrak{V}$ over F is cyclic.[14] We shall point out here briefly in which cases these phases do not interfere in the general proofs. The first phase did not enter up to Section 8, proof of Theorem 21 and in Section 9 in representing the Brauer group by multiplicative subgroups of the fields. The second phase is avoided by assuming that F *has* a derivation with $\mathfrak{C}$ as a constant field which means that if F is of characteristic zero, F is any transcendental extension of $\mathfrak{C}$ such that $\mathfrak{C}$ is algebraically closed in F and if F is of characteristic $p \neq 0$, this means that F is a totally inseparable extension of $\mathfrak{C}$ of exponent 1; that is $F^p \subseteqq \mathfrak{C} \subset F$. Then the whole theory of d.t. and their duals can be carried out also for characteristic p, but as regards the theory of the differential polynomials this can be carried out only to those cases where the differential trans-

[14] Jacobson [6], p. 499, Special case no. 3.

formations considered are cyclic. It was shown in [13] that if $(F\colon \mathfrak{C}) = p^{\nu}$ then there exists a finite polynomial (in the sense of [6], i.e. the right ideal generated by it is two sided) $q(t) = \sum_1^{\nu} t^{p^{\mu}}\alpha_{\mu}$, $\alpha_{\mu} \in \mathfrak{C}$ and all other finite polynomials of $F[t]$ are polynomials in $q(t)$ with coefficients of $\mathfrak{C}$, and if $\nu = \infty$ the only finite polynomials are constants. Applying the same methods of [6] one obtains that if $\nu = \infty$ all d.t.'s in the finite vector spaces over F are cyclic and if $\nu < \infty$ all d.t. in the vector spaces over F whose dimension is $\leqq p^{\nu}$ are cyclic. In view of this fact, the whole theory of Part I will hold for characteristic p in case $(F\colon \mathrm{C}) = \infty$, and if $(F\colon C) = p^{\nu} < \infty$ the results will hold as long as the polynomial involved will be of degree $\leqq p^{\nu}$.

It is well known that division algebras over $\mathfrak{C}$ split by an inseparable extension F of exponent 1 (i.e. $C \supseteqq F^{p}$) are of exponent p. Conversely, division algebras of exponent p have a splitting field F which is totally inseparable extension of exponent 1 of $\mathfrak{C}$. By [3], we know that one can define a derivation in this field F so that $\mathfrak{C}$ is the field of constants. Hence in view of the preceding remarks Lemma 20 yields:

LEMMA 20′: *Every central simple algebra $\mathfrak{A}$ of order n^2 which is split by F (hence of exponent p) and where $n \leqq (F\colon \mathfrak{C})$ is isomorphic with some invariant ring $\mathfrak{R}(g)$ of an A-polynomial $g(t)$ of degree n.*

Here one has to define an A-polynomial as a polynomial for which the order of its invariant ring is the square of its degree.

Since it is known that every division algebra $\mathfrak{A}$ which is split by F is of order n^2, where $n \leqq (F\colon \mathfrak{C})$, the preceding lemma holds for all division algebras split by F. The case of Lemma 20′, where $n = (F\colon \mathfrak{C})$, can be shown to be contained in the results of [7].

The results of sections 8 and 9 cannot be carried over to an arbitrary extension $\mathfrak{D}$, of C. The main reason for this is the fact that the derivation of F over $\mathfrak{C}$ cannot be extended to $F\mathfrak{D}$ over $\mathfrak{D}$. Nevertheless this can be done if $\mathfrak{D}$ is separable. But even if we restrict ourselves to the case that $\mathfrak{D}$ is separable over $\mathfrak{C}$ Theorems 21 and 22 cannot be extended. Yet the rest of Section 8 and Theorems 23, 25 and 27 which give the representation of the Brauer group by additive groups formed from $F\mathfrak{D}^{+}$ will hold, without any modification in the proof, if $(F\colon \mathfrak{C}) = \infty$[15]. Using Lemma 20′ which holds for division algebras and modifying the part of the proof which is related to the product of differential polynomials, one obtains the same results also for the case $(F\colon \mathfrak{C}) < \infty$.

HEBREW UNIVERSITY and
THE INSTITUTE FOR ADVANCED STUDY

BIBLIOGRAPHY

[1] A. S. AMITSUR, *La representation d'algèbres centrales simples*, C. R. Acad. Sci. Paris, t. 230 (1950), pp. 902–904.

[2] A. S. AMITSUR, *Construction d'algèbres centrales simples*, C. R. Acad. Sci. Paris, t. 230 (1950), pp. 1026–1028.

[15] For the sake of theorem 12, we have to assume that $\mathfrak{C}$ is infinite. This is evident if $(F\colon \mathfrak{C}) = \infty$.

[3] R. BAER, *Algebraische Theorie der differentierbaren Funktionkörper* I, Sitz. Heid. Akad., (1927), pp. 15–32.

[4] C. CHEVALLEY, *A new kind of relationship between matrices*, Amer. J. Math., v. 65 (1943), pp. 521–531.

[5] F. FITTING, *Gleichartigkeit b. Idealen und Aquivalenzbegriff der Elementarteilertheorie*, Math. Ann., v. 112 (1935), pp. 572–582.

[6] N. JACOBSON, *Pseudo-linear transformations*, Ann. of Math., v. 38 (1937), pp. 484–507.

[7] N. JACOBSON, *p-algebras of exponent p*, Bull. Amer. Math. Soc., v. 43 (1937), pp. 667–670.

[8] A. LEVY, *Uber Matrizen und Differentialkomplexe, I, II, and III*, Math. Zeit., v. 78 (1916), pp. 1–51, 343–358, 359–368.

[9] O. ORE, *Formale Theorie der linear Differentialgleichungen II*, J. Reine Angew. Math. v. 168 (1932), pp. 233–252.

[10] O. ORE, *Theory of non commutative polynomials*, Ann. of Math., v. 34 (1933), pp. 480–508.

[11] N. JACOBSON, Theory of rings, Math. Surveys, No. II, Amer. Math. Soc. 1943.

[12] A. WEIL, Foundations of algebraic geometry, Amer. Math. Soc. Colloquium Publications XXIX, 1946.

[13] A. S. AMITSUR, *Finite differential polynomials* (Hebrew). Riveon Lemathematica, v. 5 (1950) pp. 1–8. See also Math. Review, v. 13 (1952), p. 202.