ALGEBRAS SPLIT BY A GIVEN PURELY INSEPARABLE FIELD

KLAUS HOECHSMANN

1. Let K be a field of characteristic $p \neq 0$. By a *p-algebra* we mean a central simple algebra over K whose dimension is a power of p. Although it is known that such an algebra always has a purely inseparable (over K) splitting field E, the role played by E in the structure of the algebra has not been clear. In this paper, we intend to show that essentially all p-algebras split by E are obtained by a natural composition of two constituents: a certain purely inseparable field $\hat{E}$ containing E and any abelian normal extension N of K whose Galois group is related, in a manner to be described, to the structure of $\hat{E}$. We must dwell a little on the nature of these ingredients.

Consider a subgroup X of the multiplicative group E^* of E such that X contains the multiplicative group K^* of K. Such a group will be called *regular*, if any system of representatives of X modulo K^* is linearly independent over K. E itself is called *regular* if it is additively generated by some regular subgroup of E^*, which in this case will be called a *maximal regular* subgroup. Just below the corollary for Theorem 2 in [2], it was shown that every finite purely inseparable extension E can be further extended to a regular one $\hat{E}$ with the same exponent over K and also finite. In what follows, we require E to be regular. The field originally given may have to be enlarged to fulfill this condition, just as a separable field is extended to a normal one in the theory of crossed products. We assume, therefore that $\hat{E}=E$.

It follows at once from Theorem 1 of [2] that the group $G(X)=X/K^*$ associated with a maximal regular subgroup X of E^* is independent of X. There is thus a unique p-group G attached to E. The group X is an extension of K^* by G. Hence with the selection of a maximal regular group X we obtain a cohomology class $\tilde{X} \in H^2(G, K^*)$. For the sequel let X be fixed.

As for N, it will be a normal extension of F with Galois group $\Gamma \simeq G$. However, N need not be a field; in general it may be a direct sum of fields

$$N = N_1 \oplus \cdots \oplus N_n,$$

with a "T-group" Γ of automorphisms, as defined in [1], i.e., a group of automorphisms satisfying the following three conditions.

Received by the editors July 6, 1962.

I. If $\sigma \in \Gamma$ and σ keeps the elements of N_i fixed (for any i), then $\sigma = 1$.

II. Γ is transitive on the set of fields $N_1, \cdots, N_n$.

III. If $a \in N$ and a is fixed under all elements of Γ, then $a \in K$.
Teichmüller [3] proved that for $\alpha \in H^2(\Gamma, N^*)$ the crossed product (N, Γ, α) defined in the usual way is central simple over K and has all the usual properties. The pair (N, Γ) will be called a *normal ring.*[1]

We can now state our main theorem.

THEOREM 1. *Let A be a simple algebra of dimension $(E:K)^2$ over its center K. Then E splits A if and only if $A \simeq (N, \Gamma, \bar{X})$ for some normal ring (N, Γ) with $\Gamma \simeq G$.*

Here X is interpreted as an element of $H^2(\Gamma, K^*)$ as it can be because of the isomorphism between G and Γ.

Before attempting to prove Theorem 1, we shall reformulate it to bring it into better accord with the crude version given at the outset. Given a normal ring (N, Γ), consider an injection $\phi: \Gamma \rightarrow E^*/K^*$ such that $\bigcup_{\sigma \in \Gamma} \phi(\sigma)$ is a regular subgroup of E^* (it is automatically maximal). The regularity of E guarantees the existence of such injections, since $\Gamma \simeq G$.

On the vector space $E \otimes_K N$, a multiplication is defined by demanding that

$$(x \otimes u)(y \otimes v) = (xy \otimes u^\sigma v) \qquad \text{if } y \in \phi(\sigma). \tag{1}$$

The resulting algebra will be denoted by $E \otimes_\phi N$.

THEOREM 1'. *The class of algebras of the form $E \otimes_\phi N$ (for fixed regular E) coincides with that of p-algebras containing E as a maximal commutative subring.*

It is easily verified that the definition of $E \otimes_\phi N$ makes it isomorphic to $(N, \Gamma, \bar{X})$ for suitable X. Indeed, suppose $\phi: \sigma \rightarrow x_\sigma K^*$. The nature of ϕ is such that the set $\{x_\sigma | \sigma \in \Gamma\}$ is a basis of E over K, and hence a basis of $E \otimes_\phi N$ over N. If we write x and u instead of $(x \otimes 1)$ and $(1 \otimes u)$, respectively, the elements of $E \otimes_\phi N$ are of the form

$$\sum_{\sigma \in \Gamma} x_\sigma u_\sigma,$$

where the u_σ are arbitrary coefficients from N. The commuting rule (1) appears as:

$$x_\sigma u = u^\sigma x_\sigma.$$

[1] Often called "Galois algebra" and extensively studied in [5].

Finally, let $X = \bigcup_{\sigma\in\Gamma} x_\sigma K^*$. X is a maximal regular subgroup of E^*, which can be thought of as an extension of K^* by either G or Γ. Taking the latter point of view, we may regard the factor set

$$\alpha(\sigma, \tau) = \frac{x_\sigma x_\tau}{x_{\sigma\tau}}, \qquad (\sigma, \tau \in \Gamma),$$

as a representative of the cohomology class $\tilde{X}$.

We have exhibited the structure of a crossed product $(N, \Gamma, \tilde{X})$ in $E \otimes_\phi N$. For reasons of dimension and the simplicity of crossed products,

$$E \underset{\phi}{\otimes} N \simeq (N, \Gamma, \tilde{X}).$$

Since E is obviously contained in $E \otimes_\phi N$ (as the subring $E \otimes K$), we have also proved the "if" part of Theorem 1.

2. For proving the second and more important part of Theorem 1, the theory of differential extensions, as worked out in [1], is needed. We recall briefly what it is about. Let Z be a finite extension field of K such that $Z^p \subseteq K$, d be a derivation of Z into Z, whose kernel is precisely K, and $f(x)$ be the minimal polynomial of d over K. Given a central simple Z-algebra A, we can extend d to a derivation $\bar{d}$ of A into A and find an element c in the kernel of $\bar{d}$ such that $ca - ac = f(\bar{d})(a)$ for all $a \in A$. The K-algebra $(A, \bar{d}, c)$, generated by A and a symbol u such that

$$ua - au = \bar{d}a, \qquad \text{for all } a \in A, \tag{2}$$

and

$$f(u) = c \tag{3}$$

is called a *differential extension* of A by $\bar{d}$. It turns out that $(A, \bar{d}, c)$ is central simple over K and contains A as the centralizer of Z and that, conversely, every such K-algebra is of the form $(A, \bar{d}, c+\gamma)$ with $\gamma \in K$. It is emphasized that d and $\bar{d}$ can be chosen in various ways; in particular, d can always be chosen to be *regular*, i.e., such that its proper vectors form a maximal regular subgroup of Z^*. (Note that Z, being of exponent p, is automatically regular.)

Now let A be a crossed product of the normal ring (M, Δ) over Z: $M = M_1 \oplus \cdots \oplus M_m$, each M_i being a separable extension field of Z and Δ being a T-group of automorphisms relative to Z. Let $\alpha \in Z^2(\Delta, M^*)$ be a 2-cocycle defining A. We now impose a rather severe condition, namely, *that the values* $\alpha(\sigma, \tau)$ *lie in some maximal* *regular subgroup of* Z^*. It is well known that a derivation d of Z into Z can be constructed whose group of proper vectors coincides with any given maximal subgroup of Z^*, in particular the one containing the values $\alpha(\sigma, \tau)$ (see, for example, [1, Proposition 1.3]). This derivation d will be extended to A as follows.

Since all elements of M are separable over Z, d has a unique extension to M. If $\{y_\sigma | \sigma \in \Delta\}$ is the usual M-basis for the crossed product A, the extensions $\bar{d}$ such that $\bar{d}(M) \subseteq M$ are defined by $dy_\sigma = y_\sigma \delta(\sigma)$, with $\delta: \Delta \rightarrow M$ satisfying

$$d(\alpha(\sigma, \tau))/\alpha(\sigma, \tau) = \delta(\sigma)^\tau - \delta(\sigma\tau) + \delta(\tau).\text{[2]} \tag{4}$$

The function β: $(\sigma, \tau) \rightarrow d(\alpha(\sigma, \tau))/\alpha(\sigma, \tau)$, as the "logarithmic derivative" of the multiplicative cocycle α, is an additive cocycle, and (4) can be satisfied by setting

$$\delta(\sigma) = \sum_{\rho \in \Delta} \beta(\rho, \sigma) a^{\rho\sigma} \tag{5}$$

with any $a \in M$ for which $\sum_{\rho \in \Delta} a^\rho = 1$. If M were a field, the existence of such an element a would be well known; in our case it can be found as follows. Let Δ_1 be the subgroup of Δ leaving M invariant. Clearly, $\Delta = \sigma_1\Delta_1 \cup \sigma_2\Delta_1 \cup \cdots \cup \sigma_m\Delta_1$, where $M_1^{\sigma_i} = M_i$. Furthermore, Δ_1 induces on each subfield M_i its Galois group over Z. We take an a_1 from M_1 whose trace is 1. Then $a_1^{\sigma_i}$ has trace 1 in M_i; more precisely, if the elements of M are represented in the form $(x_1, \cdots, x_m)$ with $x_i \in M_i$, we have

$$\sum_{\rho \in \Delta} (a_1, 0, \cdots 0)^{\sigma_i \rho} = (0, \cdots, 1, 0 \cdots)$$

with the 1 in the ith place. Hence

$$\sum_{\rho \in \Delta} (a_1, 0, \cdots 0)^\rho = \sum_{i=1}^{m} (0, \cdots, 1, 0 \cdots) = 1.$$

The preceding paragraph is entirely independent of the condition imposed on α, whose only purpose is to insure that certain things are separable over K. For, if a_1 is not K-separable, a_1^p will surely be, and

$$\sum_{\rho \in \Delta} (a_1^p)^\rho = \left(\sum_{\rho \in \Delta} a_1^\rho \right)^p = 1.$$

In any case, a_1 can be chosen separable over K. Since each $\alpha(\sigma, \tau)$

[2] This observation was made by G. Hochschild (Trans. Amer. Math. Soc. **80** (1955), 146).

is a proper vector of the regular derivation d, each of the quotients $\beta(\sigma, \tau)$ is an element of K. Therefore, the function δ defined by (5) maps Δ into the maximal K-separable subring M' of M. Now we can state

THEOREM 2. *In the notation introduced above, let* $B=(A, \bar{d}, c)$ *be any differential extension of the crossed product* A. *Then* B *is again a crossed product. More precisely, for suitable choice of* $\bar{d}$, *the ring* N *generated in* B *by* M' *and an element* u *satisfying* (2), *is a direct sum of fields; the inner automorphisms induced in* B *by certain proper vectors of* $\bar{d}$ ($\bar{d}$ *being regarded as a linear transformation of* A *over* M') *define a* T-*group of automorphisms on* N. N *is a maximal commutative subring of* B.

PROOF. Let $\bar{d}$ be defined as an extension of the regular derivation d of Z, exactly as above. B is generated by A and the element u mentioned in the theorem, the latter satisfying the polynomial equation (3). Our first aim is to modify our choice of $\bar{d}$ so as to make c lie in M'.

Note that $c\in M$, because $ca-ac=f(\bar{d})(a)=0$, for $a\in M$, and because M is maximal commutative in A. If c is not separable over K, replace $\bar{d}$ by $\bar{d}^p$ and u by u^p. It is easily checked that this change leaves all our conventions concerning d intact. Now $f(u^p)=c^p$, which is K-separable.

Assume $c=c_1+\cdots+c_m$, $c_i\in M_i'$. Then

$$N = M'[u] \simeq M'[x]/f(x) - c \simeq \bigoplus_{i=1}^{m} M_i'[x]/f(x) - c_i.$$

Let $f(x)-c_i=\phi_{i1}(x)\cdots\phi_{ir}(x)$ be a factorization into irreducible polynomials (it will become apparent that the number r is the same for each i). Setting

$$N_{ij} = M_i'[x]/\phi_{ij}(x),$$

we have, since $\phi_{i1}(x), \cdots, \phi_{ir}(x)$ are all distinct because of the separability of $f(x)$,

$$N \simeq \bigoplus_{i=1}^{m} N(_{i1} \oplus \cdots \oplus N_{ir}),$$

as claimed.

For an element $a\in A$, let Ia denote the map induced on N by the inner automorphism $b\to a^{-1}ba$ of B.

Let $\{y_\sigma | \sigma\in\Delta\}$ be an M-basis of A such that $xy_\sigma=y_\sigma x^\sigma$ for all $x\in M$. Finally denote by W the group of proper vectors of d in Z^*.

We shall prove that the maps $I(y_\sigma z)$ with $z\in W$ form a T-group of automorphisms of N. In fact

$$u(y_\sigma z) - (y_\sigma z)u = \bar{d}(y_\sigma z) = y_\sigma z(\delta(\sigma) + \lambda),$$

where λ is the proper value belonging to z, so that

$$I(y_\sigma z): u \to u + \delta(\sigma) + \lambda.$$

For $x\in M$, $I(y_\sigma z): x\to x^\sigma$. $I(y_\sigma z)$ is therefore an automorphism of N.

Before verifying conditions I, II, and III for a T-group, we make an observation:

$M_i = Z\otimes_K M_i'$, and the restriction of $\bar{d}$ to M_i is a regular derivation of M_i over M_i' with the same proper values and vectors as d. Therefore we can use Theorem 6.1 of [1] to conclude that the maps $\{Iz \mid z\in W\}$ form a T-group of automorphisms on $M_i'[u]$.

(II) To map N_{11} onto N_{ij} we use $I(y_\sigma z)$ where $\sigma: M_1\to M_i$, and hence $M_1'\to M_i'$. Then Iy_σ maps $M_1'[u]$ onto $M_i'[u]$, and hence N_{11} onto some N_{ik}. Since $I(W)=\{Iz \mid z\in W\}$ is transitive on the fields $N_{i1}, \cdots, N_{ir}$ in $M_i'[u]$, the desired $z\in W$ can be found.

(I) Suppose $\tau = I(y_\sigma z)$ leaves N_{11} elementwise fixed. There exist $z_i\in W$ $(i=1\cdots r)$ such that $\zeta_i = Iz_i$ maps N_{11} onto N_{1i}. Since W is in the center of A and $y_\sigma\in A$, each ζ_i commutes with τ. Let $x\in M_1'[u]$, $x=x_1+\cdots+x_r$ with $x_i\in N_{1i}$.

$$x^\tau = \sum_{i=1}^{r} x_i^\tau = \sum_{i=1}^{r} \left(x_i^{\zeta_i^{-1}}\right)^{\tau\zeta} = x.$$

Thus τ is identity on $M_1'[u]$, in particular on M_1'. Since z commutes with M_1', σ itself is identity on M_1', hence on M_1, hence on all of M: $\sigma=1$ and $\tau=Iz$. Finally $\tau=1$, because the automorphisms $I(W)$ form a T-group on $M_1'[u]$ over M_1'.

(III) If $x\in N$ is fixed under $I(W)$, it must be in M'. If it is fixed under Δ as well, it must be in K, since Δ is a T-group on M over Z, hence on M' over K.

We have already observed that the elements $\{y_\sigma z \mid \sigma\in\Delta,\ z\in W\}$ are proper vectors of $\bar{d}$:

$$\bar{d}(y_\sigma z) = y_\sigma z(\delta(\sigma) + \lambda).$$

Finally, we recall that the degree of $f(x)$ equals $(Z:K)$. Hence $(N:K)=(M'[u]:K)=(M':K)(Z:K)$. This is precisely the dimension $(M:Z)(Z:K)$ of a maximal commutative subring of the differential extension B. Theorem 2 is now established.

Remark. It is easy to describe the algebra B of Theorem 2 without referring to the structure of a differential extension. Given

$A=(M, \Delta, \alpha)$ and having chosen $\bar{d}$ and c in such a way that $c \in M'$ and $dy_\sigma = y_\sigma \delta(\sigma)$, as before, we can define a normal ring (N, Γ). $N = M'[u]$, where u is an indeterminate commuting with elements of M' and satisfying the single condition $f(u)=c$. Γ is an extension of the factor group W/K^* by Δ: elements of Γ will be written in the form $[\sigma, \zeta]$ with $\sigma \in \Delta$, $\zeta \in W/K^*$. Multiplication is then defined by

$$[\sigma, \zeta][\sigma', \zeta'] = [\sigma\sigma', \zeta\zeta'\alpha(\sigma\sigma')^-],$$

where the bar over an element of W denotes the coset modulo K^* to which it belongs. The action of Γ on N is given as follows:

$$a^{[\sigma,\zeta]} = a^\sigma \qquad \text{for } a \in M',$$
$$u^{[\sigma,\zeta]} = u + \delta(\sigma) + \lambda(\zeta),$$

where $\lambda(\zeta)$ is the one proper value of d common to all representatives of ζ. Finally, $B=(N, \Gamma, \beta)$ with β easily computed as

$$\beta([\sigma, \zeta], [\sigma', \zeta']) = \gamma(\zeta, \zeta')\gamma(\zeta\zeta', \alpha(\sigma, \sigma')^-) \frac{\alpha(\sigma, \sigma')}{z_{\alpha(\sigma,\sigma')^-}},$$

where $\{z_\zeta \mid \zeta \in W/K^*\}$ is some fixed system of representatives of W modulo K^*, and

$$\gamma(\zeta, \zeta') = \frac{z_\zeta z_{\zeta'}}{z_{\zeta\zeta'}}.$$

We note especially that the range of β is in K.

3. **Back to the proof of Theorem 1.** E is again a regular purely inseparable extension of K, X a maximal regular subgroup of E^*. We consider the subgroup W of those members of X whose pth power lies in K^* and set $Z=K(W)$.

LEMMA. *In E over Z, the group XZ^* is a maximal regular subgroup of E^*.*

PROOF. X generates E additively, as before; hence regularity of XZ^* over Z is all that must be proved.

Let $\{x_1, \cdots, x_s\}$ and $\{w_1, \cdots, w_t\}$ be systems of representatives of X modulo W and of W modulo K^*, respectively. The K-space spanned by the latter is clearly a ring and must coincide with Z. Since $\{x_iw_j \mid i=1, \cdots, s; j=1 \cdots t\}$ is a system of representatives of X modulo K^*, it is linearly independent over K. Hence $\{x_1, \cdots, x_s\}$ is linearly independent over Z. This completes the proof because $\{x_1, \cdots, x_s\}$ is also a system of representatives of XZ^* modulo Z^*.

We are given a p-algebra A over K containing the field E as a maximal commutative subring. It is required to show that A also contains a direct sum of fields N with a T-group Γ of automorphisms which is isomorphic to G and induced by the inner automorphisms of A belonging to a system of representatives of X modulo K^*. (Here X is an arbitrary preselected maximal regular subgroup of E^*.) The proof is by induction on the dimension of E over K, the assertion being trivial if the latter is 1.

Let A' be the centralizer of Z in A. A' is central simple over Z, contains E as a maximal commutative subring, and has a smaller dimension than A. We choose the maximal regular subgroup XZ^* of E^* for the application of the induction hypothesis. A' has the structure of a crossed product (M, Δ, α), where (M, Δ) is a normal ring with $\Delta \simeq XZ^*/Z^*$. Δ is induced by the inner automorphisms of A' belonging to a system of representatives of XZ^* modulo Z^* which could certainly be chosen to coincide with the system $\{x_1 \cdots x_s\}$ occurring in the proof of the lemma. This set was previously denoted by $\{y_\sigma | \sigma \in \Delta\}$, and $\alpha(\sigma, \tau)$ defined as $y_{\sigma\tau}^{-1} y_\sigma y_\tau$. Let the elements of Δ be numbered $\sigma_1, \cdots, \sigma_s$ in such a way that $y_{\sigma_i} = x_i$. We note that $\alpha(\sigma_i, \sigma_k) \in W$. W being a maximal regular subgroup of Z^*, and A (a central simple algebra containing A' as the centralizer of Z) being a differential extension of A', we apply Theorem 2 to find a normal ring (N, Γ) from which A is produced as a crossed product. The elements of A' whose corresponding inner automorphisms induce Γ are $\{y_\sigma z | \sigma \in \Delta, z \in W\}$ according to the proof of Theorem 2.

Since K is the center of A, the elements z might as well be restricted to the set $\{w_1, \cdots, w_t\}$ of representatives of W modulo K^*. Thus $\Gamma = I(S)$, where $S = \{x_i w_j\}$ is a system of representatives of X modulo K^*. Finally, the map $xK^* \to Ix$ is a homomorphism from X/K^* onto Γ; that it is an isomorphism, hence $G \simeq \Gamma$, is most easily seen by noting that $(A:K) = (G:1)^2$.

Theorem 1 is a generalization of one of the central results of [**4**] (Satz 32), which treats the case where E is a simple extension and G therefore cyclic. Its second formulation, Theorem 1′, is intended to give more equal weight to E and N, the former appearing only implicitly in the formula of Theorem 1. It is reminiscent of the simplest p-algebras $(\alpha, \beta]$ studied by H. L. Schmid, Witt, and others, which were generated over K by two symbols u, v with the relations:

$$u^p = \alpha \in K, \qquad v^p - v = \beta \in K, \qquad u^{-1}vu = v - 1.$$

We would set $K(u) = E$, $K(v) = N$, and define ϕ by $\phi(\sigma) = uK^*$, σ being the automorphism $v \to v - 1$ of N. Then $(\alpha, \beta] = E \otimes_\phi N$. Whereas criteria for isomorphism and rules about Kronecker products are known for the algebras $(\alpha, \beta]$, they remain an open question in the general case.

References

1. K. Hoechsmann, *Simple algebras and derivations*, Trans. Amer. Math. Soc. (to appear).

2. K. Hoechsmann and H. Zassenhaus, *On purely inseparable extensions*, Illinois J. Math. (to appear).

3. O. Teichmüller, *Verschränkte Produkte mit Normalringen*, Deutsche Math. 1 (1936), 92–102.

4. ———, *p-Algebren*, Deutsche Math. 1 (1936), 362–388.

5. P. Wolf, *Algebraische Theorie der galoisschen Algebren*, Mathematische Forschungsberichte, III. VEB Deutscher Verlag der Wissenschaften, Berlin, 1956.

University of Notre Dame and
Universität Hamburg