SCALAR EXTENSIONS OF ALGEBRAS WITH EXPONENT EQUAL TO INDEX[1]

SAM PERLIS

If a normal simple algebra A has a special structural property, it is of interest to inquire whether every finite scalar extension A_K also has this property. We shall make such an inquiry here where the property assumed for A is equality of exponent and index.

It suffices to consider only separable and purely inseparable fields K. Roughly stated, our result for separable extensions of finite degree is that preservation of the property in question depends only on whether it is preserved for scalar extension fields which are cyclic of prime degree. In the case of purely inseparable extensions the problem is immediately reducible to the case of such extensions of prime degree p, where p is the characteristic of the field. There remains the question whether such extensions always preserve equality of exponent and index, and we shall answer this question in the negative by means of an example.

Every p-algebra over a field of degree of imperfection[2] unity has equal index and exponent.[3] The example mentioned above, however, shows that for every integer $r>1$ there exists a modular field of degree of imperfection r such that not all the p-algebras ($p=2$) over this field have exponent equal to index.

1. **Exponent reduction factor.** If A is any normal simple algebra of exponent ρ over F, the exponent of any scalar extension A_K is a divisor σ of $\rho=\sigma\tau$. The integer τ may be called the *exponent reduction factor* of A relative to K. This concept is analogous to that of index reduction factor and gives rise to a theorem analogous to that for index reduction factors.

THEOREM 1. *Let A be a normal simple algebra over F, and K be an algebraic extension of degree q over F. Then the exponent reduction factor of A relative to K is a divisor of q.*

PROOF. The direct power A^σ has exponent τ and K as splitting field. Now τ divides the index μ of A^σ, and μ divides the degree q of the splitting field K. Hence τ divides q.

[1] Presented to the Society, April 12, 1940.

[2] For the concept of degree of imperfection see §3 of O. Teichmuller, *p-Algebren*, Deutsche Mathematik, vol. 1 (1936), pp. 362–388.

[3] Cf. O. Teichmuller, op. cit., p. 384. See also A. A. Albert, *p-algebras over a field generated by one indeterminate*, this Bulletin, vol. 43 (1937), pp. 733–736.

COROLLARY. *If the degree q of K is prime to the exponent of A, the scalar extension A_K has the same exponent and index as A.*

For purely inseparable fields K the following result is stronger than that of Theorem 1.

THEOREM 2. *The exponent reduction factor of A relative to a purely inseparable field K is a divisor of the exponent of K.*

PROOF. Now F has characteristic p, K has exponent p^a and degree p^b over F, and $A = B \times B_1$ where B has exponent p^e and B_1 has exponent prime to p. We have $\rho = p^e m = \sigma\tau$, where σ is the exponent of A_K. By Theorem 1, τ is a power of p so that $\sigma = p^f m$, B_K has exponent p^f, and $\tau = p^{e-f}$. Hence B_K has a purely inseparable splitting field L of exponent p^f over K. Now L splits B and is purely inseparable of exponent at most p^{f+a} over F, whence it follows that $p^{f+a} \geqq p^e$, and $p^a \geqq p^{e-f} = \tau$, as desired.

2. **Separable extensions.** In view of the fundamental result on the factorization of a normal division algebra corresponding to the factorization of its degree, it is completely sufficient to consider algebras of prime-power index p^e, and we shall do so. We begin with a known tool theorem[4] on fields.

LEMMA 1. *Let K be a separable field of degree $p^e g$ over a field W, with g prime to p. Then K is contained in a field L of degree $p^e h$ over W, with h prime to p, such that*

$$L = L_e > L_{e-1} > \cdots > L_0 \geqq W, \tag{1}$$

where L_i is cyclic of degree p over L_{i-1} $(i = 1, 2, \cdots, e)$ and L_0 is separable of degree h over W.

This result will now be applied to algebras.

THEOREM 3. *Let F be a field, p a prime, and W any separable finite extension of F. Every normal simple algebra A of index p^n and exponent p^n (n variable) over every such field W has the property that the index and exponent of A_K are equal, for every separable field K of finite degree over W, if and only if this is true for every field K which is cyclic of degree p over W.*

[4] Cf. the proof of Theorem 31, Chapter IV of A. A. Albert, *Structure of Algebras*, American Mathematical Society Colloquium Publications, vol. 24, 1939. A brief proof is obtainable as follows. The field K is contained in a normal field N of degree $p^r h$ over W, h prime to p. Then N is normal over K and contains a Sylow subfield L of degree hg^{-1} over K, degree $p^e h$ over W. Hence N is metacyclic over a subfield L_0, and we have (1).

PROOF. We simply apply Lemma 1 and Theorem 1. Since the degree of L over K is prime to p, the index and exponent of A_K are the same, respectively, as those of A_L. Now $A_L=(A_{L_0})L$ and A_{L_0} has index and exponent both equal to p^n since L_0 has degree h over W. By assumption A_{L_1} has equal index and exponent. But L_1 is a separable finite extension of F and L_2 is cyclic of degree p over L_1 so that A_{L_2} has equal index and exponent. A finite number of steps of this sort completes the proof.

Every finite extension of a field W has the form

$$Q = Q_t > Q_{t-1} > \cdots > Q_0 = K \geqq W, \tag{2}$$

where each Q_i is purely inseparable of prime degree q over Q_{i-1}, q the characteristic of F, and Q_0 is separable over W. If $q \neq p$, the index and exponent of A_Q are the same as those of A_K, the type of scalar extension considered in Theorem 3. If $q=p$, we obtain an analogue of Theorem 3, applying to all finite extension fields Q, by allowing W to vary over all finite extensions of F, and assuming that A_Q has equal index and exponent not only for all fields Q which are cyclic of degree p over W but also for all fields Q which are purely inseparable of degree p. It follows that every A_Q has index equal to exponent, Q any finite extension of F.

3. **Purely inseparable extensions.** Let P be either the prime field of characteristic two or a field obtained from this prime field by adjunction of a finite number of independent indeterminates. Let x_0 and x be independent indeterminates over P, and $F=P(x_0, x)$. We shall construct an example of a cyclic algebra

$$D = (Z, S, x_0x) \tag{3}$$

over F with the properties described in Theorem 4 below.

To select the cyclic extension Z we first consider $F_0=P(x_0)$. The equation $\lambda^2=\lambda+x_0$ is irreducible over F_0, hence defines[5] a cyclic field $Y_0=F_0(\xi)$ of degree two over F_0, and Y_0 is contained in a field Z_0 which is cyclic of degree four over F_0. Now $Z=Z_0(x)$ is cyclic of degree four over $F=F_0(x)$ and Z contains $Y=Y_0(x)$. Any generating automorphism S of Z_0 over F_0 may be regarded as a generating automorphism of Z over F.

If the exponent of $D=(Z, S, x_0x)$ were less than four, we should[6] have $D^2 \sim (Y, S, x_0x) \sim 1$ so that x_0x would be a norm in Y over F,

[5] For the theory of cyclic fields used in this section see Chapter IX of A. A. Albert, *Modern Higher Algebra*, Chicago, 1937.

[6] Albert, *Structure of Algebras*, chap. 7, Theorem 14.

contrary to the fact that x is an indeterminate over F_0. Hence D has exponent and index four and D is a division algebra.

The field $K=F(j), j^2=x$, is purely inseparable of degree two over F and

$$D_K = (Z_K, S, x_0 x). \tag{4}$$

Now $Y=F(\xi)$, $\xi^2=\xi+x_0$ and, letting $Y_1=Y\times K$, we have $x_0=N_{Y|F}(\xi)=N_{Y_1|K}(\xi)$, $x_0x=N_{Y_1|K}(\xi j)$. The exponent of D_K is thus at most two while by Theorem 1 it is at least two; hence it is equal to two. However, when the extension Z_0 is appropriately chosen we may show by a matric representation of D that D_K has index four. To make the required proof we need only show that K is not equivalent over F to a subfield of D.

In order to select Z_0 we prove

LEMMA 2. *The extension Z_0 over Y_0 may be chosen so that x_0 is not a norm with respect to Z_0 over Y_0.*

We have

$$Z_0 = Y_0(\eta), \qquad \eta^2 = \eta + x_0\xi + w, \tag{5}$$

where w in F_0 is at our choice. We shall choose $w=1$. Suppose $x_0=N_{Z_0|Y_0}(z)$, z in Z_0. Then z cannot be in Y_0 for, if so, $z^2=x_0$ whereas Y_0 contains no quantities inseparable over F_0. Hence $z=a_1(b+\eta)$ with $a_1\neq 0$, a_1 and b in Y_0, $x_0=N_{Z_0|Y_0}(z)=a_1^2(b^2+b+x_0\xi+1)$ and, if $a=a_1^{-1}$,

$$b^2 + b + x_0\xi + 1 = x_0 a^2. \tag{6}$$

Letting $a=\alpha_1\xi+\alpha_2$, $b=\beta_1\xi+\beta_2$ with α_i and β_i in F_0 we find that (6) is equivalent to the pair of equations

$$\begin{aligned} \beta_1^2 + \beta_1 + x_0 &= \alpha_1^2 x_0, \\ \beta_2^2 + \beta_2 + 1 &= x_0(\alpha_2^2 + \beta_1 + x_0). \end{aligned} \tag{7}$$

Let

$$\alpha_i = \mu_i/\delta_i, \qquad \beta_i = \nu_i/\delta_i', \qquad i = 1, 2, \tag{8}$$

be expressions for the α_i and β_i as quotients of relatively prime polynomials in $P[x_0]$ with denominators δ_i and δ_i' all monic (i.e., having leading coefficients unity). Substituting in (7_1) we find that $\delta_1'=\delta_1$ so that (7_1) is equivalent to

$$\nu_1^2 + \nu_1\delta_1 + x_0\delta_1^2 = x_0\mu_1^2.$$

This equation shows that δ_1 is prime to x_0.

Now substituting from (8) in (7_2) we are led to the equation

$$\nu_2^2 + \nu_2\delta_2' + \delta_2'^2 = x_0\delta_2'^2(\mu_2^2\delta_1 + \nu_1\delta_2^2 + x_0\delta_1\delta_2^2)/\delta_2^2\delta_1. \tag{9}$$

We observe from (9) that δ_2^2 divides $x_0\delta_1\delta_2'^2$, and since δ_1 is prime to x_0, it follows that if δ_2 has a factor x_0 so does δ_2'. Thus in any case the right side of (9) is a polynomial divisible by x_0. If the constant terms of ν_2 and δ_2' are ν and δ, respectively, we see then that the left side of (9) has constant term $\nu^2+\nu\delta+\delta^2=0$. Further, ν and δ cannot both be zero since ν_2 and δ_2' are relatively prime. The equation $\lambda^2+\lambda+1=0$ thus has a solution $\lambda=\nu\delta^{-1}$ or $\lambda=\delta\nu^{-1}$ in P. On the other hand this equation has no solution in the field P, and this contradiction establishes the lemma.

THEOREM 4. *There exists a cyclic algebra D of index and exponent four over an appropriate field F of characteristic two, and a purely inseparable extension K of degree two over F, such that D_K has index four and exponent two.*

To make the proof we first represent $D=(Z, S, x_0x)$ by a set of four-rowed matrices with elements in Z. We have $D=Z+uZ+u^2Z+u^3Z$, $u^4=x_0x$, and $zu=uz^S$ for every z of Z. If

$$v = z_0 + uz_1 + u^2z_2 + u^3z_3, \qquad z_i \text{ in } Z, \tag{10}$$

is any quantity of D and U is the vector $(1, u, u^2, u^3)$, then $vU=U\bar{v}$ where $\bar{v}$ is the matrix

$$\bar{v} = \begin{pmatrix} z_0 & xx_0z_3^S & xx_0z_2^{S^2} & xx_0z_1^{S^3} \\ z_1 & z_0^S & xx_0z_3^{S^2} & xx_0z_2^{S^3} \\ z_2 & z_1^S & z_0^{S^2} & xx_0z_3^{S^3} \\ z_3 & z_2^S & z_1^{S^2} & z_0^{S^3} \end{pmatrix}. \tag{11}$$

The correspondence $v\to\bar{v}$ is an equivalence over F (when we identify F with the field of four-rowed scalar matrices over F) of D with the set of matrices $\bar{v}$. Note that the quantities $v=z_0$ in z correspond to diagonal matrices, diag $\{z_0, z_0^S, z_0^{S^2}, z_0^{S^3}\}$, such that $|\bar{v}|=N_{Z|Y}(z_0)$. For this norm we shall use the simpler symbol $N(z_0)$.

Suppose that D contains a subfield equivalent over F to K, that is, D contains a quantity v such that $v^2=x$. Then $\bar{v}^2=x$, $|\bar{v}^2|=x^4$, and $|\bar{v}|=x^2$. Every z_i in (10) has the form $z_i=s_it_i^{-1}$ where s_i and t_i are in the polynomial domain $Z_0[x]$ and are relatively prime. Also, $N(s_i)$ and $N(t_i)$ are in $F_0[x]$.

Let x^m be the highest power of x occurring as a factor in the denominators t_i. Then $w=vx^m=z_0'+uz_1'+u^2z_2'+u^3z_3'$, $z_i'=z_ix^m=s_i'(t_i')^{-1}$, t_i' prime to x $(i=0, 1, 2, 3)$, and w corresponds to a matrix $\bar{w}=\bar{v}x^m$ all of whose elements have denominators prime to x. Further, $|\bar{w}|=|\bar{v}|x^{4m}=x^{2+4m}$, and $N(t_i')$ is in $F_0[x]$ and is prime to x.

We shall prove $m=0$. Assuming $m>0$ we have

$$|\bar{w}| = x^{2+4m} = N(z_0') + xx_0Q = \frac{N(s_0')}{N(t_0')} + xx_0Q, \tag{12}$$

where Q may be written as a quotient of polynomials in x with denominator prime to x. From the equation,

$$N(t_0')x^{2+4m} = N(s_0') + xx_0Q\cdot N(t_0'), \tag{13}$$

we see that x is a factor of $N(s_0')$, hence of s_0'. This result implies that x^m is not a factor of t_0. Using $s_0'=xs_0''$ in the matrix $\bar{w}$ we find

$$|\bar{w}| = x^{2+4m} = \frac{N(s_1')}{N(t_1')}xx_0 + x^2Q_1, \tag{14}$$

and as above we deduce that $s_1'=xs_1''$ with s_1'' in $F_0[x]$.

We may continue this process until we have shown that every s_i' is divisible by x. But this means that no t_i has the factor x^m, contrary to the definition of m. This contradiction proves that $m=0$ so that the denominators t_i of all the z_i are prime to x. Now $w=v$, and by repeating the argument above we find that s_0 and s_1 are divisible by x.

Computing $v^2=a_0+ua_1+u^2a_2+u^3a_3=x$ (a_i in Z), we must obtain $a_1=a_2=a_3=0$, $a_0=x$. For a_0 we find

$$a_0 = z_0^2 + x_0x(z_1\overset{S^3}{\cdot}z_3 + z_2\overset{S^2}{\cdot}z_2 + z_3\overset{S}{\cdot}z_1) = x, \tag{15}$$

whence we have

$$z_0^2 + x_0x(z_1\overset{S^3}{\cdot}z_3 + z_1\overset{S}{\cdot}z_3) = x(1 - x_0z_2\overset{S^2}{\cdot}z_2). \tag{16}$$

Since the numerators of the terms on the left are all divisible by x^2, the numerator, $t_2t_2^{S^2}-x_0s_2s_2^{S^2}=N_{Z|Y}(t_2)-x_0N_{Z|Y}(s_2)$, of the quantity in parentheses on the right must have a factor x. If the polynomials t_2 and s_2 of $Z_0[x]$ have constant terms τ_2 and σ_2, respectively, the constant term of $N_{Z|Y}(t_2)-x_0N_{Z|Y}(s_2)$ is, then,

$$N_{Z|Y}(\tau_2) - x_0N_{Z|Y}(\sigma_2) = 0. \tag{17}$$

Since t_2 is prime to x, we have $\tau_2\neq 0$, hence $\sigma_2\neq 0$ by (17). Also, τ_2 and σ_2 are in Z_0. Thus (17) may be written as

$$x_0 = N_{Z_0|Y_0}(\tau_2\sigma_2^{-1}), \tag{18}$$

contrary to the result stated in Lemma 2. This contradiction completes the proof.

Let r be any integer greater than unity, and let P be obtained from its prime subfield P_0 by adjunction of $r-2$ independent indeterminates. Then F is obtained from the perfect field P_0 by adjunction of r indeterminates, F and K are said to be fields of degree of imperfection r, and we have the following result.

THEOREM 5. *For every integer $r>1$ there exists a modular field K of degree of imperfection r such that not all the p-algebras over K have exponent equal to index.*

This is in contrast to the case $r=1$ for which every p-algebra is known to be cyclic with equal index and exponent. One may note, finally, that much of the work above is valid when the characteristic is any prime p, and it seems likely that the remaining details can be carried through for this generalized case.

ILLINOIS INSTITUTE OF TECHNOLOGY