ON THE DECOMPOSITION OF A FIELD AS A TENSOR PRODUCT

by P. M. COHN

(Received 9 January, 1978)

1. Introduction. The following two results in the theory of division algebras are well known and easily proved, for an arbitrary commutative field k (cf. for example [**3**, Chapter 10]).

(i) *The tensor product of two central division algebras over k of coprime degrees is again a division algebra.*

(ii) *Every central division algebra over k is a tensor product of division algebras of prime power degrees.*

It is natural to ask whether corresponding results hold for commutative fields. The answers are not hard to find but (as far as I am aware) have not appeared in print before; since they throw some light on the nature of tensor products they seemed worth recording.

The analogue of (i) is easily seen to be true; this is proved in §2 where we examine in more detail the condition for a tensor product of field extensions to be a field. The tensor product of two field extensions E/k, F/k of which at least one is Galois is a field if and only if they contain no isomorphic non-trivial subextensions. It is even enough to assume that one of them is normal and the other separable, but an example is given to show that normality cannot be omitted. This is closely related to a corresponding criterion for linear disjointness due to Bourbaki [**1**], which also carries over to the case of a normal extension (Theorem 2.2, Corollary 2).

To answer the question relating to (ii) for fields we shall limit ourselves to (finite) Galois extensions. Here the analogue of (ii) holds precisely if the Galois group is soluble; this is an easy consequence of P. Hall's characterization of soluble groups (§3). This in turn raises the question whether for any given finite group G, division algebras exist which are crossed products with Galois group G. This is indeed the case, as was shown by Farkas [**4**]; it is also a simple consequence of the recent result of K. A. Brown that the group algebra of a torsion free abelian-by-finite group has no zero-divisors ([**2**]; cf. also [**5**]).

2. The tensor product of two fields. We begin by showing that a tensor product of finite field extensions of coprime degrees is again a field.

PROPOSITION 2.1. *Let k be any field and E/k, F/k finite extensions of degrees r, s where r, s are coprime. Then $E \otimes_k F$ is again a field.*

Proof. Let L be a composite of E and F, i.e. a field containing k-isomorphic copies of E and F and generated by them. Such a field L is well known to exist, e.g. as a homomorphic image of the k-algebra $E \otimes_k F$ by a maximal ideal. We have a surjective

Glasgow Math. J. **20** (1979) 141–145.

homomorphism

$$E \otimes_k F \to L. \tag{1}$$

Let $[L:k]=n$; since E, F are embedded in L, both r and s divide n, hence their least common multiple rs also divides n, and so $rs \leq n$. If we compare dimensions in (1), we see that equality must hold: $rs = n$, and so (1) is an isomorphism. Now the assertion follows.

If we restrict one of the extensions to be Galois (or even normal) we can give a more precise description of the tensor products that are fields. We shall not assume our extensions to be finite, but of course all Galois extensions are understood to be algebraic.

THEOREM 2.2. *Let k be any field and E/k, F/k any field extensions of which at least one is Galois. Then $E \otimes_k F$ is a field if and only if E and F have no isomorphic subfield properly containing k.*

Proof. Suppose that E, F each have a subfield isomorphic to a proper extension of k; we may as well take this to be simple, say $k(\alpha)$, where α, necessarily algebraic over k of degree $n>1$, has the minimal equation $\sum_0^n c_i x^{n-i} = 0$. Then

$$\Big(\sum_{i=0}^{n-1}\sum_{j=1}^{n-i} c_i \alpha^{n-i-j} \otimes \alpha^{j-1}\Big)(\alpha \otimes 1 - 1 \otimes \alpha) = \sum_0^n c_i \alpha^{n-i} \otimes 1 - 1 \otimes \sum_0^n c_i \alpha^{n-i} = 0,$$

and this shows that $E \otimes_k F$ has zero-divisors.

To prove the converse we must show that under the given condition $E \otimes F$ has no zero-divisors. Suppose that F/k is Galois say; then any zero-divisor in $E \otimes F$ is already a zero-divisor in $E \otimes F'$, where F' is a finitely generated Galois subextension of F. Thus it will be enough to assume that F/k is finite Galois, hence simple, say $F = k(\alpha)$, where α has minimal polynomial f over k. Over E we have a factorization

$$f = p_1 \ldots p_r \qquad (p_i \text{ monic irreducible over } E), \tag{2}$$

and $E \otimes F$ is a field if and only if $r = 1$. Assume that $E \otimes F$ is not a field; then $r>1$ and if E_1 is the subfield of E generated by the coefficients of the p_i, then $E_1 \neq k$. Let us enlarge E to a splitting field of f; this will contain a splitting field E_0 of f over k, and clearly $E_0 \supseteq E_1$. But F, as Galois extension of k generated by α, is also a splitting field of f over k; by uniqueness $F \cong E_0$. Now E_1 is a subfield of E and is contained in E_0, hence is isomorphic to a subfield of F. This shows the condition to be necessary and it completes the proof.

This result can be slightly extended. Let us (as usual) define a *normal* extension F/k as an algebraic extension such that any irreducible polynomial over k with a zero in F splits completely over F. For a finite normal extension we have the decomposition

$$F = F_s \otimes_k F_i, \tag{3}$$

where F_s is the separable closure (the set of separable elements over k) and F_i the perfect closure (the set of purely inseparable elements over k) (cf. e.g. [**3**, p. 226]). Here of course

F_s, being separable and normal, is Galois. Now assume that E/k is (algebraic) separable and F/k is normal. If $E \otimes F$ is not a field, it contains zero-divisors and again these will already be zero-divisors in $E \otimes F'$ for some finitely generated normal subfield F' of F. So we may assume F to be finite normal over k. By (3) we have

$$E \otimes F = E \otimes F_s \otimes F_i,$$

where all tensor products are over k. Now Theorem 2.2 shows that if E and F_s have no non-trivial isomorphic subextensions then $E \otimes F_s$ is a field. It is a separable extension of k, being generated by separable elements; hence $E \otimes F_s \otimes F_i$ is then a field (cf. [**3**, p. 227]), and this proves

COROLLARY 1. *Let E/k, F/k be any field extensions, of which one is normal and one (possibly the same) is separable algebraic. Then $E \otimes_k F$ is a field if and only if E, F have no isomorphic subfield properly containing k.*

There is another way of stating Corollary 1, possibly more familiar (cf. [**1**, §10] for the case of Galois extensions):

COROLLARY 2. *Let L/k be any field extension. Then two subextensions E/k, F/k of which one is normal and one separable algebraic, are linearly disjoint if and only if $E \cap F = k$.*

For if E, F have isomorphic subextensions E_1, F_1 say, and F is normal, then E_1 is conjugate to F_1 and hence $E_1 \subseteq F$, therefore $E \cap F \neq k$. The converse is clear.

Examples to show that normality cannot be omitted in Corollary 2 are well known. Here is an example to show that the same applies to Corollary 1. We first analyse the general situation, assuming only separability, by means of Galois theory.

Let E/k, F/k be any finite separable extensions and let L/k be any finite Galois extension in which E and F are embedded; then we have a homomorphism:

$$E \otimes_k F \to L. \tag{4}$$

Put $G = \mathrm{Gal}(L/k)$ and denote by H, K the subgroups of G corresponding to E, F respectively. Then EF has the group $H \cap K$, while $E \otimes F$ is an integral domain (and hence a field) if and only if (4) is injective. The condition for this that $[EF : k] = [E \otimes F : k]$, i.e.

$$(G : H \cap K) = (G : H)(G : K). \tag{5}$$

Now $(G : H \cap K) = (G : H)(H : H \cap K) = (G : H)(HK : K)$, hence (5) holds if and only if $(HK : K) = (G : K)$, i.e. $HK = G$. The condition that E, F have non-trivial isomorphic subextensions is that H, K be contained in proper conjugate subgroups of G. Thus we must find a finite group G and subgroups H, K such that $HK \neq G$ but there is no proper subgroup M of G such that $H \subseteq M$, $K \subseteq xMx^{-1}$ for some $x \in G$. Equivalently, H and $x^{-1}Kx$ generate G, for all $x \in G$. Such an example is of course easily constructed. Let $G = S_4$ be the symmetric group of degree 4 and take H, K to be the subgroups generated by a 3-cycle and a 4-cycle respectively; then $|HK| = 12$, hence $HK \neq G$, but if the subgroup generated by H, K were proper, it would be of order 12, i.e. the alternating

group, which is not the case because it contains a 4-cycle. Thus H, K generate G and likewise for any conjugates. On retracing our steps we find, by taking a Galois extension with group S_4, two subextensions which have no non-trivial isomorphic subextensions but whose tensor product has zero-divisors.

3. The tensor product decomposition of a Galois extension. Let E/k be a finite Galois extension of degree

$$m = p_1^{\alpha_1} \dots p_r^{\alpha_r} \qquad (p_i \text{ distinct primes}). \tag{1}$$

We shall keep this notation throughout the section and in particular write

$$q_i = p_i^{\alpha_i} \qquad (i = 1, \dots, r).$$

If for $i = 1, \dots, r$, E contains a subfield E_i of degree q_i over k, then

$$E \cong E_1 \otimes \dots \otimes E_r, \quad \text{where} \quad [E_i : k] = q_i. \tag{2}$$

For the right-hand side is a field, by an easy induction using Proposition 2.1, and the inclusions $E_i \to E$ combine to produce a homomorphism of the right-hand side into the left-hand side which must be injective; by counting dimension we find that it is an isomorphism. Conversely, if we have an isomorphism (2), E must contain a subfield isomorphic to E_i, hence of degree q_i. In terms of the group $G = \mathrm{Gal}(E/k)$ we can say that (2) holds if and only if for $i = 1, \dots, r$, G has a subgroup H_i of index q_i, i.e. a p_i-complement. By P. Hall's theorem (cf. e.g. [7, VI.2.3]) this holds if and only if G is soluble. Moreover, any two decompositions into Sylow complements are conjugate ([7, VI.2.4]). Thus we have proved

THEOREM 3.1. *A finite Galois extension E/k of degree m given by* (1) *has a decomposition* (2) *if and only if its Galois group G is soluble, and any two such decompositions are conjugate by an automorphism of G.*

In (2) the E_i need not be Galois over k; they are so if and only if each p_i-complement H_i is normal in G. As is well known, this is the case precisely when G is nilpotent (for G then has normal Sylow subgroups cf. [6, p. 155]).

Theorem 3.1 is in sharp contrast with the behaviour of division algebras, which we know always have such a decomposition. If we are given a finite Galois extension E/k we can always construct a crossed product over E/k, but this need not be a division algebra; in fact there may be no division algebra which is a crossed product over E/k (e.g. if k is finite). However, given any finite group G, there exists a Galois extension E/k with group G and a crossed product over E/k which is a division algebra (cf. [4]).

REFERENCES

1. N. Bourbaki, *Algèbre* Ch.V (Hermann, Paris 1950).
2. K. A. Brown, Zero-divisors in group rings, *Bull. London Math. Soc.* **8** (1976), 251–256.
3. P. M. Cohn, *Algebra* II (J. Wiley, Chichester 1977).

4. D. R. Farkas, Miscellany on Bieberbach group algebras, *Pacific J. Math.* **59** (1975), 427–435.

5. D. R. Farkas and R. L. Snider, K_0 and Noetherian group rings, *J. Algebra* **42** (1976), 192–198.

6. M. Hall, Jr., *The theory of groups* (Macmillan, New York 1959).

7. B. Huppert, *Endliche Gruppen* I (Springer, Berlin 1967).

BEDFORD COLLEGE
REGENT'S PARK
LONDON NW1 4NS