Abelian splitting of division algebras of prime degrees.

Comment. Math. Helvetici **52** (1977) 519–523 Birkhäuser Verlag, Basel

Abelian splitting of division algebras of prime degrees

SHMUEL ROSSET

It is well known that division algebras of degrees 2 or 3 are cyclic, and that division algebras of degree 4 are crossed products [1]. (Here the 'degree' of a division algebra is n if its dimension over its center is n^2.) On the other hand Amitsur [2] proved that, in general, a division algebra whose degree is divisible by the square of an odd prime or by 8 is not a crossed product. Nothing seems to be known about division algebras of prime degrees (greater than 3) except for an old result of Brauer [3] that a division algebra of degree 5 has a solvable splitting field.

Using a variant of a theorem of Tate, on the compatibility between the transfer map in K-theory and the corestriction map in group cohomology, we show below that Brauer's result holds for all division algebras of prime degrees–provided the degree is not equal to the characteristic. In fact if the center contains enough roots of unity then the result is that there is always an abelian splitting. Thus from the point of view of 'solvability degree' our result even improves Brauer's for the case of degree 5.

1. The compatibility lemma

If n is an integer μ_n is the group of n-th roots of 1.

LEMMA. *Let F be a field of characteristic not dividing n. Given a positive integer m there exists an integer $e = e(m)$ such that: if $\mu_{n^e} \subset F$ and F_1 is an extension of F of dimension m then the square*

$$\begin{array}{ccc} K_2(F_1)/nK_2(F_1) & \xrightarrow{R_{n,F_1}} & \mathrm{Br}_n(F_1) \otimes \mu_n \\ {\scriptstyle \mathrm{tr}}\downarrow & & \downarrow{\scriptstyle \mathrm{cor}\otimes 1} \\ K_2(F)/nK_2(F) & \xrightarrow{R_{n,F}} & \mathrm{Br}_n(F) \otimes \mu_n \end{array} \qquad (*)$$

is commutative.

Here tr is the transfer, $R_{n,F}$ is the power norm residue map, Br_n is the group of elements of order n in Br and cor is the corestriction. We refer to the books of Milnor and Serre for these concepts.

First some notations. We suppress the μ_n and write $\mathrm{Br}_n(F)$ instead of $\mathrm{Br}_n(F)\otimes\mu_n$ and cor for $\mathrm{cor}\otimes 1$. If $\{\alpha,\beta\}$ is in $K_2(F)$ its image in $\mathrm{Br}_n(F)$ is denoted by $(\alpha,\beta)_n$ or just (α,β) if n is clear.

We only prove the lemma if n is a prime power so we write $n=p^r$. This would be (more than) enough for the application below, and, in fact, the proof for general n is the same.

Note that our assumption on the characteristic now reads: $\mathrm{char}\,(F)\neq p$.

Proof. There are three easy reduction steps.

A. Let $\{\alpha,\beta\}$ be a symbol in $K_2(F_1)$ such that $\alpha\in F$. Then $\mathrm{Tr}\,\{\alpha,\beta\}=\{\alpha,\mathrm{Norm}\,(\beta)\}$ and $\mathrm{cor}\,(\alpha,\beta)=(\alpha,\mathrm{Norm}\,\beta)$ so the commutativity is trivial in this case. Here the Norm is from F_1 to F.

B. Assuming that, for some $\gamma\in F_1$, α and β have 'linear' representations over F i.e. $\alpha=a+b\gamma$, $\beta=c+d\gamma$ one uses step A to show commutativity as follows. Change β by a 'scalar' from F so that $\alpha+\beta=u\in F^*$. Then the identity $\{u^{-1}\alpha, u^{-1}\beta\}=1$ shows that $\{\alpha,\beta\}=\{u,u\}^{-1}\cdot\{u,\beta\}\cdot\{\alpha,u\}$ and the last product is of the type dealt with above. Note that the same method 'reduces the degree' of a symbol whenever α and β are polynomials in γ of the same degree.

C. Both tr and cor are transitive, i.e. if $F\subset F_1\subset F_2$ then $\mathrm{tr}_{F_2/F}=\mathrm{tr}_{F_1/F}\circ\mathrm{tr}_{F_2/F_1}$, and a similar formula for cor. Thus, by induction on the degree $(F_1:F)$ we can assume that there are no proper subfields between F and F_1. This implies that, if $\alpha\notin F$ is arbitrary, $F_1=F(\alpha)$. In particular every symbol $\{\alpha,\beta\}$ in $K_2(F_1)$ can be written as $\{\alpha,f(\alpha)\}$ where $f(x)\in F[x]$ has degree $<(F_1:F)$. The integer $\deg f$ is called the degree of $\{\alpha,\beta\}$.

We now make a second inductive assumption: for *all* finite field extensions $k\subset K$ and all symbols of degree $<\deg\{\alpha,\beta\}$ commutativity has been proved. There are now two cases to consider: $\deg\{\alpha,\beta\}$ prime to p(*I*) and $\deg\{\alpha,\beta\}$ a power of p(II). (We leave the mixed case for the reader.)

Case I. Here $\beta=f(\alpha)$ with $f\in F[x]$. If f is reducible we are covered by the inductive hypothesis, so assume f is irreducible. As $\deg f$ is prime to p not all irreducible factors of f over F_1 have degrees divisible by p. Adding a root of such a factor to F and F_1 we get fields F' and $F_2=F_1\circ F'$. Thus $(F_2:F_1)$ is prime to p and $(F':F)<(F_1:F)$ since $(F':F)=\deg f$.

Using the formulas $\mathrm{tr}_{F_2/F_1}\{\alpha,\beta\}_{F_2}=(F_2:F_1)\cdot\{\alpha,\beta\}_{F_1}$ and $\mathrm{cor}_{F_2/F_1}(\alpha,\beta)_{F_2}=(F_2:F_1)\cdot(\alpha,\beta)_{F_1}$ it is easy to see that it suffices to show the commutativity for $\{\alpha,\beta\}_{F_2}$ i.e. with F_2 replacing F_1. As β splits over F' into factors of smaller degrees and as $(F':F)<(F_1:F)$ the transitivity of tr and cor coupled with the two inductive hypotheses conclude the proof in this case.

Case II. Suppose $\deg f = p^m$. There is an embedding of Br_{p^r} in $\mathrm{Br}_{p^{r+m}}$, simply sending an algebra class to itself. On the symbols this map can be described by $(\alpha, \beta)_{p^r} \mapsto (\alpha^{p^m}, \beta)_{p^{r+m}}$. The analogous map on K_2 is a map $K_2(F)/p^rK_2(F) \to K_2(F)/p^{r+m}K_2(F)$ obtained from the map

$$\frac{1}{p^r} Z/Z \to \frac{1}{p^{r+m}} Z/Z.$$

This map, too, can be described on the symbols by

$$\{\alpha, \beta\} \bmod p^rK_2(F) \mapsto \{\alpha^{p^m}, \beta\} \bmod p^{r+m}K_2(F).$$

Now let F' (resp. F_2) be the field obtained by adding to F (resp. F_1) a root of $f(x)$. We will assume that $(F':F) = (F_2:F_1) = \deg f = p^m$. The case where $(F_2:F_1) < (F':F)$ is treated similarly. In the square

$$\begin{tikzcd}
K_2(F_2)/p^{r+m}K_2(F_2) \arrow[r] \arrow[d, "\mathrm{tr}"'] & \mathrm{Br}_{p^{r+m}}(F_2) \arrow[d, "\mathrm{cor}"] \\
K_2(F)/p^{r+m}K_2(F) \arrow[r] & \mathrm{Br}_{p^{r+m}}(F)
\end{tikzcd}$$

The element $\{\alpha, \beta\}$ – considered to be in the upper left corner – is mapped to the same thing by $\mathrm{cor} \circ R$ as by $R \circ \mathrm{tr}$. This follows from the fact that β splits over F' and breaking the square into two, the first from F_2 to F' and the second from F' to F, one uses the transitivity of tr and cor as in case I. Now

$$\mathrm{tr}_{F_2/F_1}(\{\alpha, \beta\}_{F_2} \bmod p^{r+m}K_2(F_2)) = \{\alpha^{p^m}, \beta\}_{F_1} \bmod p^{r+m}K_2(F_1)$$

which is precisely the image of $\{\alpha, \beta\}_{F_1} \bmod p^rK_2(F_1)$ under the map $K_2/p^rK_2 \to K_2/p^{r+m}K_2$ described above.

It follows from all the above that

$$\mathrm{cor}_{F_1/F}(R_{p^{r+m}}\{\alpha^{p^m}, \beta\}_{F_1}) = R_{p^{r+m}}(\mathrm{tr}_{F_1/F}(\{\alpha^{p^m}, \beta\} \bmod p^{r+m})).$$

The proof now follows easily by chasing around the diagram (where $p^r = q$, $p^{r+m} = q'$)

$$\begin{tikzcd}
K_2/q'K_2(F_1) \arrow[rr] \arrow[dd] & & \mathrm{Br}_{q'}(F_1) \arrow[dd] & \\
& K_2/qK_2(F_1) \arrow[ul] \arrow[rr] \arrow[dd] & & \mathrm{Br}_q(F_1) \arrow[ul] \arrow[dd] \\
K_2/q'K_2(F) \arrow[rr] & & \mathrm{Br}_{q'}(F) & \\
& K_2/qK_2(F) \arrow[ul] \arrow[rr] & & \mathrm{Br}_q(F) \arrow[ul]
\end{tikzcd}$$

Remark. In the statement e is left unspecified. It is clear from the proof how to estimate it.

2. The splitting theorem

Assume again that F is a field of characteristic $\neq p$ and $\mu_p \subset F$. Let D be a central division algebra over F of degree p (i.e. $(D:F)=p^2$). Suppose the class of D, $[D] \in \mathrm{Br}_p(F)$, is in the image of $R_{p,F}: K_2/qK_2(F) \to \mathrm{Br}_p(F)$. This means that $[D]$ is a linear combination of symbols $(\alpha, \beta)_p$ where α and β are in F. From the explicit description of $(\alpha, \beta)_p$ and the Kummer theory it is then easily deduced that D has an abelian splitting i.e. there exists a normal extension K/F with $\mathrm{Gal}\,(K/F)$ abelian and $D_K = D \otimes_F K$ trivial.

Let E be a subfield of D such that $(E:F)=p$. Then E is a separable extension F. Let L be its normal closure. The group $\mathrm{Gal}\,(L/F)$ is a (transitive) group of permutations on p letters, hence, if H is a Sylow p-subgroup, $L^H = F_1$ is an extension of F of order prime to p and let L/F_1 a cyclic extension of order p. It follows that D_{F_1} is a cyclic algebra, i.e. $[D_{F_1}] = (\alpha, \beta)_{F_1}$ for some $\alpha, \beta \in F_1$.

As $[D_{F_1}] = \mathrm{res}_{F/F_1}[D]$ we get $\mathrm{cor}\,[D_{F_1}] = (F_1:F) \circ [D]$, that is

$$(F_1:F) \cdot [D] = \mathrm{cor}_{F_1/F} \circ R_{p,F_1}(\{\alpha, \beta\} \bmod p).$$

As $((F_1:F), p) = 1$ we see that $[D]$ is in the image of $\mathrm{cor}_{F_1/F} \circ R_{p,F_1}$.

Thus if the diagram (*) commutes for F, F_1 it clearly follows that $[D]$ is in the image of $R_{p,F}$. To ensure the commutativity we may have to add a p^e-th root of 1 to F for some e. (In fact scanning the proof above one sees that $e \leq [\log_p((p-1)!)]$.) This gives an abelian extension of F of degree a power of p, since μ_p is already in F by assumption.

Using the Kummer theory again it is clear that we have proved the

THEOREM. *If F is a field of* char $\neq p$, *$\mu_p \subset F$ and D is a division algebra of degree p over F then D has a solvable splitting field. If F has "enough" roots of* 1 *(cf. above) D has a splitting field with elementary abelian galois group (of* exponent *p).*

If F does not contain μ_p then we get an abelian splitting after adding μ_p to F. This gives an extension $F(\mu_p)$ such that $(F(\mu_p):F) < p$. Thus we get

COROLLARY. *If D is a division algebra of degree p (no assumption on F except* char $\neq p$*) then D has a solvable splitting of solvability degree* ≤ 2, *i.e. D has a splitting field K such that* $\mathrm{Gal}\,(K/F)$ *has normal abelian p-subgroup with quotient cyclic of order $<p$.*

We end with some remarks. (1) Essentially our result is that an algebra of prime degree is a combination of symbols. Apparently the question of whether division algebras of prime degrees are cyclic, i.e. whether such an algebra *is* a symbol, is still open.

(2) The questions of the injectivity and surjectivity of R_n are, in general, open and have important applications in the geometry of cycles of codimension 2. See Bloch's paper [4].

(3) The proof of the compatibility lemma should probably be simpler. Perhaps a more conceptual proof can be given which covers all K_n-*s* simultaneously and does not depend on the interpretation of elements as symbols.

REFERENCES

[1] Albert, A. A., Structure of Algebras, Amer. Math. Soc. Coll. Publ. *24* (1939).
[2] Amitsur, S. A., The generic division rings, Israel J. Math. *18* (1974).
[3] Brauer, R., On normal division algebras of index 5, Proc. Nat. Ac. Sci. USA. *24* (1938) 243–246.
[4] Bloch, S., Torsion algebraic cycles, K_2 and Brauer groups of function fields, preprint.
[5] Milnor, J., Introduction to algebraic K-theory, Ann. Math. Studies 72, Princeton 1971.
[6] Serre, J. P., Corps locaux, Hermann, Paris (1962).

Forschungsinstitut für Mathematik,
ETH, Zurich
and
Tel Aviv University

Received February 4, 1977