DIHEDRAL CROSSED PRODUCTS OF EXPONENT 2 ARE ABELIAN

UZI VISHNE

Abstract. We prove that assuming enough roots of unity in the base field, a central simple algebra of exponent 2 which is split by a dihedral group, is also split by certain abelian groups.

Accepted to *Archiv der Math.*, 7/2001.

1. Introduction

One of the best ways to understand central simple algebras is to learn their maximal subfields. If an algebra happens to have a maximal subfield K which is Galois over the center F, it has an easy description via an element of the second cohomology group $H^2(G, K^*)$, where $G = \mathrm{Gal}(K/F)$. Such an algebra is called a *crossed product* over K/F, or a crossed product with respect to G. For example, a cyclic algebra is a crossed product over a cyclic extension.

In the early days every known division algebra was constructed as a crossed product, and by classical theorems of Wedderburn, Albert and Dickson, all division algebras of degree $2, 3, 4, 6$ or 12 are crossed products.

An interesting question concerning crossed products is to describe in what cases will every crossed product with respect to a given group be a crossed product with respect to some other group too. In particular it is interesting to know that an algebra is a crossed product with respect to an abelian maximal subfields, for then one can apply the Amitsur-Saltman techniques [4] to gather information on the algebra.

If all the Galois maximal subfields of a suitable central simple algebra have the same Galois group G, this group is termed *rigid*. Amitsur showed that the elementary abelian groups are rigid, and this was a key step in his construction of noncrossed products [2]. Since then it was shown by Saltman [8] and Tignol-Amitsur [11] that every noncyclic abelian group is rigid.

Date: May 20, 2001.

1991 *Mathematics Subject Classification.* Primary 16K20; Secondary 16S35.

The following notation was suggested in [11]. A group G *splits* a central simple algebra A, if A is similar (in the Brauer sense) to a crossed product with respect to some subgroup of G. We denote by $G \Rightarrow_k H$ the assertion that for every field $F \supseteq k$, every central simple algebra over F which is split by G, is also split by H. The following is well known.

Example 1. *Let $n = n_1 n_2$ be integers and assume k has n_2-roots of unity. Then $\mathbb{Z}_n \Rightarrow_k \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$.*

Proof. Let $F \supseteq k$. Let $A = (K/F, \sigma, b)$ be a cyclic algebra of degree n over F, with $z \in A$ inducing σ on K, such that $z^n = b \in F$. Then $K^{\sigma^{n_1}}[z^{n_1}] = K^{\sigma^{n_1}} \otimes_F F[z^{n_1}]$ is a maximal subfield of A, Galois over F with Galois group $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. □

Let D_n denote the dihedral group of order $2n$. It was shown by Rowen and Saltman [10] that if n is odd, then every crossed product with respect to D_n is cyclic (assuming $\operatorname{char} F$ is prime to n, and F has n roots of unity). Their proof is constructive; a few years later Mammone and Tignol [7] gave another proof, using the corestriction. If $\operatorname{char}(F)$ divides n, then any semidirect product of a cyclic group acting on $\mathbb{Z}_n$ is abelian. This is a result of Albert [1], proved by what is in modern language a relatively easy use of the corestriction.

Brussel [5] has shown that D_4, and more generally the dihedral-type groups of order p^3, are all rigid.

In this note we show that if the field F contains n roots of unity, then every central simple algebra of exponent 2 which is split by D_n, is also split by $\mathbb{Z}_2 \times \mathbb{Z}_n$. The same proof shows that division algebras which are crossed product with respect to D_n are also crossed product with respect to $\mathbb{Z}_2 \times \mathbb{Z}_n$. Under the weaker assumption that F contains n/m roots of unity for $m \mid n$, every algebra of exponent 2 split by D_n is also split by $\mathbb{Z}_{n/m} \times D_m$.

This note is based on part of the Author's doctoral dissertation [12, Chap. 3], done under the supervision of Prof. L. Rowen.

2. Crossed Products with Involution

Let A be a central simple algebra over a field F, with a maximal subfield K which is Galois over F. Let $G = \operatorname{Gal}(K/F)$. By Skolem-Noether Theorem [9, Theorem 7.1.10], for every $g \in G$, there exist some $z_g \in A$ such that $z_g k z_g^{-1} = g(k)$ for all $k \in K$.

Assume that A has an involution $v \mapsto v^*$ whose restriction to K is an automorphism $\tau \in G$, so that necessarily $\tau^2 = 1$.

Note that an element z_g inducing g on K can be replaced by another element kz_g, $k \in K$. In [3, Theorem 2.1] it is shown that if G has exponent 2, then z_g can be chosen such that $z_g^* = \pm z_g$. Slightly altering their proof, we have

Proposition 2. *If $g \in G$, $g \neq \tau$, satisfies $(g\tau)^2 = 1$, then we can choose z_g to satisfy $z_g^* = z_g$.*

Proof. Let $r = z_g^* z_g^{-1}$. For every $k \in K$ we have that

$$\begin{aligned} rkr^{-1} &= z_g^* z_g^{-1} k z_g (z_g^*)^{-1} \\ &= z_g^* g^{-1}(k)(z_g^*)^{-1} \\ &= z_g^* (\tau g^{-1}(k))^* (z_g^*)^{-1} \\ &= (z_g^{-1} \tau g^{-1}(k) z_g)^* \\ &= (g^{-1}\tau g^{-1}(k))^* \\ &= \tau g^{-1} \tau g^{-1}(k) = k, \end{aligned}$$

where the last equality follows from the assumption $(g\tau)^2 = 1$. Thus r commutes with K, and since $\mathrm{Cent}_A(K) = K$ by the double centralizer theorem [9, Theorem 7.1.9], we have that $r \in K$. Compute the norm of r with respect to $g\tau$:

$$\begin{aligned} r \cdot g\tau(r) &= z_g^* z_g^{-1} \cdot z_g r^* z_g^{-1} \\ &= z_g^* (z_g^* z_g^{-1})^* z_g^{-1} \\ &= z_g^* (z_g^*)^{-1} z_g z_g^{-1} = 1 \end{aligned}$$

By Hilbert's theorem 90, there is some $t \in K$ such that $r = g\tau(t)^{-1} t$. The element tz_g satisfies

$$(tz_g)^* = z_g^* t^* = r z_g \tau(t) = r g\tau(t) t^{-1} \cdot (tz_g) = tz_g,$$

so that tz_g is a symmetric element inducing g on K. □

3. Dihedral crossed products of exponent 2

Let $m \,|\, n$, and let k be any field containing a primitive (n/m)th root of unity. We show that for algebras of exponent 2, we have that $D_n \Rightarrow_k \mathbb{Z}_{n/m} \times D_m$. In particular, for $m = 1$ we get $D_n \Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_n$, and (if n is even), for $m = 2$ we get $D_n \Rightarrow \mathbb{Z}_2^2 \times \mathbb{Z}_{n/2}$.

Theorem 3. *Let F be a field containing n/m roots of unity. Every central simple F-algebra A of exponent 2 which is split by the dihedral group D_n, is also split by $\mathbb{Z}_{n/m} \times D_m$.*

Proof. Since the subgroups of D_n are either cyclic or dihedral, and the cyclic case is treated in Example 1, we may assume A is a crossed product with respect to D_n. Let K be a maximal subfield of A, with Galois group generated by σ, τ, such that

$$\sigma^n = \tau^2 = 1, \quad \tau\sigma\tau^{-1} = \sigma^{-1}.$$

Since $\exp A = 2$, A has an involution of the first kind [1, Theorem X.17]. Moreover, by [9, Prop. 7.2.45], we may assume the restriction of the involution to K is τ.

By Proposition 2 there is a symmetric element $z \in A$ that induces σ on K. Observe that $K \cap F[z] = F$: indeed, elements of $F[z]$ commute with z and are symmetric, so $K \cap F[z] \subseteq K^{\sigma} \cap K^{\tau} = F$. Let $b = z^n$, then $b \in \mathrm{Cent}_A(K) = K$ since z^n acts trivially on K, so that $b \in K \cap F[z] = F$.

Let u be a maximal divisor of n/m such that $b = z^n \in F^{*u}$. If $u = 1$, then $F[z^m]$ is a field, cyclic over F. Since conjugation by z^m induces σ^m, we have that $F[z^m]$ commutes with K^{σ^m}, which has Galois group $D_n/\langle\sigma^m\rangle \cong D_m$ over F. Moreover, $K^{\sigma^m} \cap F[z^m] \subseteq K \cap F[z] = F$, so that $K^{\sigma^m}[z^m]$ is a maximal subfield of A, Galois over F, with Galois group $\mathbb{Z}_{n/m} \times D_m$.

In the general case, $F[z^m]$ is still a Galois extension of rings over F, but no longer a field. Instead, consider $F[z^{n/u}] = F[\sqrt[u]{b}]$, which is isomorphic to a direct product of u copies of F. Let $e_1, \dots, e_u \in F[z^{n/u}]$ be pairwise orthogonal idempotents such that $\sum e_i = 1$. Set $C = \mathrm{Cent}_A(F[z^{n/u}])$, then $C = Ce_1 \oplus \cdots \oplus Ce_u$, and Ce_1 is a central simple algebra over $F_1 = Fe_1 \cong F$. Moreover, $A \cong M_u(Ce_1)$, so that $A \sim Ce_1$ in the Brauer group [6, Chap. 2]. Note that $K \cap C = K^{\sigma^{n/u}}$, so that $K^{\sigma^{n/u}}e_1$ is a maximal subfield of Ce_1, with Galois group $D_{n/u}$.

By the maximality of u, we have that $F_1[z^m]$ is a cyclic field extension (of dimension $\frac{n}{um}$) over F, and the same argument as in the case $u = 1$, applied to $F_1[z^m]$, shows that $K^{\sigma^m}F_1[z^m]$ is a maximal subfield of Ce_1 with Galois group $\mathbb{Z}_{n/um} \times D_m$ over F_1. $\square$

Here are the first few instances of the theorem for algebras of exponent 2 (assuming enough roots of unity):

$$\begin{array}{rcl}
D_4 & \Rightarrow & \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2^3 \\
D_6 & \Rightarrow & \mathbb{Z}_2 \times \mathbb{Z}_6 \\
D_8 & \Rightarrow & \mathbb{Z}_2 \times D_4, \quad \mathbb{Z}_2^2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_8 \\
D_{10} & \Rightarrow & \mathbb{Z}_2 \times \mathbb{Z}_{10} \\
D_{12} & \Rightarrow & \mathbb{Z}_2^2 \times S_3, \quad \mathbb{Z}_3 \times D_4, \quad \mathbb{Z}_4 \times S_3, \quad \mathbb{Z}_2^2 \times \mathbb{Z}_6, \quad \mathbb{Z}_2 \times \mathbb{Z}_{12}
\end{array}$$

It would be interesting to know the relations among the other groups. For example, does $\mathbb{Z}_2 \times D_4 \Rightarrow \mathbb{Z}_2^2 \times \mathbb{Z}_4$ for algebras of exponent 2?

References

[1] A. A. Albert, Structure of Algebras, Amer. Math. Soc. Coll. Publ., Vol. XXIV, Providence, 1961.

[2] S. A. Amitsur, *On Central Division Algebras*, Israel J. Math. **24**, 408–420, (1972).

[3] S. A. Amitsur, L. H. Rowen and J.-P. Tignol, *Division Algebras of Degree* 4 *and* 8 *with Involution*, Israel J. Math. **33**(2), 133–148, (1979).

[4] S. Amitsur and D. Saltman, *Generic Abelian Crossed Products and p-Algebras*, J. Algebra **51**(1), 76–87, (1978).

[5] E. Brussel, *Noncrossed Products and Nonabelian crossed products over* $\mathbb{Q}(t)$ *and* $\mathbb{Q}((t))$, Amer. J. Math. **117**(2), 377–393, (1995).

[6] N. Jacobson, Finite Dimensional Division Algebras over Fields, Springer, 1996.

[7] P. Mammone and J.-P. Tignol, *Dihedral Algebras are Cyclic*, Proc. Amer. Math. Soc. **101**(2), 217–218, (1987).

[8] D. J. Saltman, *Noncrossed product p-algebras and Galois p-extensions*, J. Algebra **52**, 302–314, (1978).

[9] L. H. Rowen, Ring Theory, Academic Press, 1988.

[10] L. H. Rowen and D. J. Saltman, *Dihedral Algebras are Cyclic*, Proc. Amer. Math. Soc. **84**(2), 162–164, (1982).

[11] J.-P. Tignol and S. A. Amitsur, *Kummer subfields of Malcev-Neumann division algebras*, Israel J. Math. **50**, 114–144, (1985).

[12] U. Vishne, Central Simple Algebras, Doctoral Dissertation, Bar-Ilan Univ., Israel, July 2000.

Department of Mathematics, Bar-Ilan University, Ramat-Gan 52900, ISRAEL

E-mail address: `vishne@macs.biu.ac.il`