Correction to "Cyclic Division Algebras", by Louis Halle Rowen, Israel Journal of Mathematics, Vol. 41, No. 3, 1982, pp. 213–234.

Tignol has spotted two errors in the proof of [1, Theorem 6]. The proof given below requires a more careful analysis, based on the original idea but taking into account that the number of roots of unity available at each stage changes.

Fix any power f of p, where $f \geqq p$ for p odd and $f \geqq 4$ for $p = 2$. Take $\hat{K} = \mathbf{Q}(\zeta_f)(\mu_1, \cdots, \mu_u)$ where $u = fn/p$ and let K be the fixed subfield under σ^n (where σ permutes the μ_i cyclically). Then $R = (K, \sigma, \zeta_f)$ is a division algebra by Brauer's Theorem, which we claim has exponent p. (Indeed we argue as in Example 3. Let K_1 be the fixed subfield of K under $\sigma^{n/p}$. Then $\sigma^{n/p}(x) = \zeta_f x$ for some x in $\hat{K}$ so $\sigma(x) = a_1 x$ for some a_1 in K_1; hence $\zeta_f = \sigma^{n/p-1}(a_1) \cdots a_1$ and $\zeta_f^p = N(a_1)$ proving $\exp(R) \leqq p$; equality holds since $\exp(R) \neq 1$.)

Form R' as in §1 by taking $m = p = q$. Then R' has degree n and exponent p by [1, Remark 6], and this is the example to be used for [1, Theorem 6] and [1, Theorem 8]. (Note for $f = p$ we have $u = n$, which provided the example originally considered.)

Proof of [1, Theorem 6]. Suppose R' is a crossed product with respect to the split Galois group of exponent p. By Example 2, R' has a commutative p-central set of order n. Thus, by Remark 7, R has a commutative p-central set S of order n all of whose elements are in $R_0 k^i z^j$ for various $i, j > p$, where we recall $K = K_0(k)$, and R_0 is the subalgebra of R generated by K_0 and z^p.

We need some more notation. For any given d let $c = n/p^{d+1}$ and let K_d denote the fixed subfield of K under σ^c; let R_d be the subalgebra of R generated by K_d and z^p. Then $z^c \in Z(R_d)$ and is thus identified in R_d as a primitive p^{d+1}-root of ζ_f.

Given a commutative p-central set S_{d-1} of elements $s_t = r_t z^{i_t}$ for suitable r_t in R_{d-1}, let $\zeta = z^{pc}$, a primitive p^d-root of ζ_f. Put $P = \mathbf{Q}(\zeta_f)$ and $H = P[\mu_1, \cdots, \mu_u]$. Writing $r_t = \sum_{i=0}^{c-1} x_{i,t} z^{pi}$ for suitable $x_{i,t}$ in $K_{d-1}(\zeta)$ and multiplying through by a suitable element of F we may assume all $x_{i,t} \in H$. Put $V = \sum_{j=1}^{u} P\mu_j$ and write $V = \bigoplus_{i=1}^{e} V_i$, a finite direct sum of e irreducible σ-submodules. For each $\alpha = (\alpha_1, \cdots, \alpha_e)$ write $V_\alpha = \prod_{i=1}^{e} V_i^{\alpha_i}$. Note the V_α are homogeneous in total degree in the μ_j, so an easy dimension counting argument shows $H = \bigoplus_\alpha V_\alpha$ is graded as σ-module, and we order the V_α according to the lexicographic order of α. Let V_{α_t} denote the leading component of all $x_{i,t}$ appearing in r_t, let $x'_{i,t}$ denote the V_{α_t}-component of $x_{i,t}$ (possibly 0), let $r'_t = \sum_{i=0}^{c-1} x'_{i,t} z^{pi}$ and $s'_t = r'_t z^{i_t}$. Then the s'_t form a new commutative p-central set S'_{d-1} of which we claim

$|S_{d-1}|/p$ elements have r'_t in R_d; this subset of $|S_{d-1}|/p$ elements from S'_{d-1} will be denoted as S_d. (Note that each r'_t is fixed by σ^{pc}, where σ acts naturally on H by setting $\sigma(\zeta)=\zeta$.)

The passage from S_{d-1} to S_d will be called *Brauer's degree reduction argument*, based on Jacobson's exposition of Brauer, and the above claim can be proved by proving the following stronger assertion:

$$z^c r'_t z^{-c} = \zeta(t) r'_t \qquad \text{where } \zeta(t) \text{ is a suitable } p\text{th-root of } 1.$$

To see this, first note σ^c induces a transformation on V_i whose order divides p^{d+1}, so $\sigma^c(w_i)=\zeta^{(i)}w_i$ for some nonzero $w_i \in V_i$ and some power $\zeta^{(i)}$ of ζ. The characteristic subspace of $\zeta^{(i)}$ under σ^c is a nonzero σ-submodule of V_i (since $\sigma^c(w)=\zeta^{(i)}w$ implies $\sigma^c(\sigma w)=\sigma(\sigma^c w)=\sigma(\zeta^{(i)}w)=\zeta^{(i)}\sigma(w)$) and is thus all of V_i, i.e. $\sigma^c(w)=\zeta^{(i)}w$ for all w in V_i. Hence for each $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_e)$ there is some power $\zeta^{(\alpha)}$ of ζ with $\sigma^c(w)=\zeta^{(\alpha)}w$ for each w in V_α. Writing $\zeta(t)$ for $\zeta^{(\alpha)}$ note that $\zeta(t)^p=1$ (since $\sigma^{pc}(x_{i,t})=x_{i,t}$ by hypothesis), and

$$z^c r'_t z^{-c} = z^c\left(\sum_{i=0}^{c-1} x'_{i,t} z^{pi}\right) z^{-c} = \sum_{i=0}^{c-1} z^c x'_{i,t} z^{-c} z^{pi} = \sum \zeta(t) x'_{i,t} z^{pi} = \zeta(t) r'_t,$$

proving the claim.

For example, we see from the first paragraph that we could take $|S_0|=n/p$ yielding $|S_d|=c$ for each d. We need some more observations about this reduction argument.

REMARK. If $s \in S_{d-1}$ and $s' \in Fz^{n/p}$ then $s \in Fz^{n/p}$. (Indeed $s=(\alpha z^{n/p}+r)z^j$ where $\alpha \in H\cap F$ is the leading component, $r \in H \cap R_{d-1}$, and $j<p$. Hence $j=0$; since r commutes with $z^{n/p}$ we get $s^p=\alpha^p z^n + p\alpha^{p-1}z^{(p-1)n/p}r+\cdots \in F$. Hence the leading component of $p\alpha^{p-1}z^{(p-1)n/p}r$ is in F, so the leading component of r is in $Fz^{n/p}$; working inductively yields $r \in Fz^{n/p}$.)

REMARK. If $s \in S_{d-1}$ and $s' \in Fk''z^{in/p}$ where k'' is any element of K such that $\sigma(k'')=\zeta_p k''$, then $s \in Fk''z^{in/p}$. (Indeed k'' commutes with z^p so the argument of the previous remark applies.)

Iterating each remark over all d, we may assume that if $z^{n/p}$ or $k''z^{in/p}$ appears in any S_d then it already appears in S_0 (and thus in S). *For the remainder of the proof* fix $d=\log_p n-2$, i.e., $p^{d+2}=n$. Then $c=p$ and $R_d=K_d(z^p)$ is a field in which z^p is identified with ζ_u; hence R_d cannot have a p-central set of more than p^2 elements. Also $K_d=F(k_d)$ for suitable k_d where $\sigma(k_d)=\zeta_p k_d$, and R_{d-2} is a division ring of degree p^2 whose center contains z^{p^3} (u/p^2-root of 1).

CLAIM 1. *If* $s \in S_{d-2} \cap R_{d-2}$ *then* $s' \in R_{d-1}$ *(notation as before); in particular if* $S_{d-2} \subseteq R_{d-2}$ *then* $S'_{d-2} \subseteq R_{d-1}$ *and we may take* S_{d-1} *to be all of* S'_{d-2}.

PROOF OF CLAIM 1. Otherwise $\sigma^{p^2}(s') = \zeta_p s'$ for some p-th root ζ_p of 1. Hence z^{p^2} and s' generate a cyclic central subalgebra of R_{d-2} having degree p, whose centralizer thus also has degree p. Conclude as in Claim 1 of the original proof.

REMARK. $S_d \subseteq R_d$. Indeed otherwise we have rz^j in S_d with $r \in R_d$ and $j \neq 0$. Then $r\sigma(r)\cdots\sigma^{p-1}(r)z^{pj} \in F$ contrary to Proposition 6, where the notation L_1, L, and h of Proposition 6 are replaced here respectively by $R_d = K_d(z^p) = K_d(\zeta_u)$, K_d and r (i.e. $e = u$ in Proposition 6).

CLAIM 2. *We may assume* S *contains* $z^{n/p}$ *and* k_d.

PROOF OF CLAIM 2. We showed $|S_d| \geqq p$ and $S_d \subseteq R_d \approx K_d(\zeta_u)$, so we may assume S_d contains $z^{n/p}$ or $k_d z^{in/p}$ for some i. By the above remarks we may assume S contains one of these elements; we need to prove S contains both of them or, equivalently, $|S_d| = p^2$.

If $z^{n/p} \in S$ then each s_t in S commutes with $z^{n/p}$ and thus has suitable form $r_t z^{i_t}$ for r_t in R_0, i.e., $|S_0| = n$; then the Brauer reduction argument yields $|S_d| = p^2$ and we are done. If $k_d z^{in/p} \in S$ then each $s_t \in R_0(kz^i)^{i_t}$ for some i_t, so we could find $S_0 \subseteq R_0$. Then $S_{d-2} \subset R_{d-2}$ so by Claim 1 we may take $|S_{d-1}| = p^3$ and so $|S_d| = p^2$, proving Claim 2.

But now we know S is centralized by $z^{n/p}$ and k_d, implying $S \subseteq R_0$. Hence we may take $S_0 = S$ and $|S_0| = n$, so $|S_{d-2}| = p^4$ and $S_{d-2} \subset R_{d-2}$, implying $|S_{d-1}| = p^4$ by Claim 1 and $|S_d| = p^3$, contrary to $S_d \subset R_d$. Q.E.D.

Added in proof

Unfortunately this argument opens up another gap, namely, letting T_d denote the subalgebra of R generated by K_d and z (so that R_d is the centralizer of z^p in T_d) and $F_d = Z(T_d) = F(z^c)$, we do not necessarily have the s'_t independent over F_d (although each $(s'_t)^p \in Z(R_d)$). To assure this we must make a further modification. Write $S_{d-1} = s_1, \cdots, s_u$ and $K_{d-1} = K_d(k_{d-1})$ with $\sigma^c(k_{d-1}) = \zeta_p k_{d-1}$. Taking leading components (denoted as ') we may assume k_{d-1} is homogeneous. We note the following for all t:

(i) If $s_t \notin F_{d-1}$ then $s'_t \notin F_{d-1}$ (for if $s_t r = \zeta_p r s_t$ then $s'_t r' \neq r' s'_t$).

(ii) $(s'_t)^p \in F_{d-1}$ (for $s_t^p k_{d-1} = k_{d-1} s_t^p$, implying $(s'_t)^p k_{d-1} = k_{d-1}(s'_t)^p$).

(iii) If $s_t \in F_m$ for any $m \geqq d$ then $s_t \in F_{d-1} z^{cj}$ for some j (since $s_t^p \in F_{d-1}$ and F_m is cyclic over F_{d-1}). Likewise by (ii), if $s'_t \in F_m$ then $s'_t \in F_{d-1} z^{cj}$ for some j.

(iv) If $s'_t \in F_{d+1}$ then $s_t \in F_d$. Indeed $s'_t = \alpha z^{cj}$ for some $\alpha \in F_{d-1}$ by (iii), so $s_t = \alpha z^{cj} + r$ for $r \in H \cap R_{d-1}$ of lower order. As in the Remark above, we get $r \in F_{d-1} z^{cj}$ so $s_t \in F_{d-1} z^{cj} \subset F_d$.

(v) Analogously, if $s'_t \in F_{d+1} k''$ where $\sigma k'' = \zeta_p k''$ then $s_t \in F_d k''$.

Now as in the argument in the original correction $z^{n/p} \in S$. Thus $|S_0| = n$ so we can replace S_0 by a set of n/p elements which are $F(z^{n/p})$-independent. *Now* we finally can claim S_d is p-central in T_d. This is clear by induction unless say $F_d(s'_1) = F_d(s'_2)$, so $s'_2 \in F_d s'^j_1$ for some j implying $s^j_1 s_2^{-1} \in F_d$ by (iv) which implies S_0 has two elements x_1, x_2 with $x^j_1 x_2^{-1} \in F_0 = F(z^{n/p})$, contrary to assumption.

Reference

1. L. H. Rowen, *Cyclic division algebras*, Isr. J. Math. **41** (1982), 213–234.

Department of Mathematics
Bar Ilan University
Ramat Gan, Israel