JOURNAL OF ALGEBRA 173, 518–548 (1995)

Finite Subgroups of Division Algebras over Local Fields

THOMAS HEWETT

Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

Communicated by D. A. Buchsbaum

Received June 22, 1993

1. INTRODUCTION

Amitsur [1] gave a complete classification of the finite groups that can occur as subgroups of finite dimensional division algebras. He also computed the finite subgroups of the real quaternions. In this paper, we look at groups inside division algebras over local fields of characteristic zero. We adopt the following conventions:

(1) A *local field*, F, will refer to a complete local field of characteristic zero with finite residue field.

(2) A *division algebra over* F will refer to a division algebra, finite dimensional over F.

(3) A *central division algebra over* F will be a division algebra over F with center equal to F.

(4) If $a/b \in \mathbb{Q}$ is reduced, i.e., $0 \leq a \leq b$ and $(a, b) = 1$, then $D(F, a/b)$ will denote the central division algebra over F, a local field, with Hasse invariant $a/b \bmod \mathbb{Z}$.

(5) If $(r, m) = 1$ then $o(r|m)$ will denote the multiplicative order of $r \bmod m$.

(6) $\langle K, \sigma, u\rangle$ or $\langle K/F, \sigma, u\rangle$ will denote the cyclic algebra, where $\mathrm{Gal}(K/F) = \langle\sigma\rangle$ is cyclic of order n and $\sigma^n = u \in F$.

Our purpose is to describe the finite subgroups of $D(F, a/b)^*$. This calculation falls naturally into two cases depending on whether the residue characteristic of F is 2 or an odd prime, p. An important class of groups that arises is the metacyclic groups of the form

$$G_{m,r} = \langle A, B : A^m = 1, BAB^{-1} = A^r, B^n = A^t\rangle,$$

where $n = o(r|m)$ and $t = m/(r-1, m)$. These are analyzed in Section 4. It turns out that the subgroups of $D(F, a/b)^*$ depend only on F and b. Our main results are as follows.

0021-8693/95 $6.00

THEOREM 1.1. *If F is a local field with odd residue characteristic, p, then all the nonabelian, finite subgroups of division algebras over F are isomorphic to $G_{m,r}$ for some m and r. The group $G_{m,r}$ embeds in a division algebra over F if and only if the following conditions hold*:

(1) $m = p^\alpha \ell$ *where* $\alpha \geq 1$, ℓ *is prime to* p *and* $(r-1, m) = \ell$.

(2) $o(r|m) | [F(\zeta_\ell, \zeta_p) : F(\zeta_\ell)]$,

(3) $q - 1 | r - 1$,

(4) $((q-1)/\ell, o(r|m)) = 1$.

Here q is the order of the residue field of $F(\zeta_m)$. In particular, $G_{m,r}$ embeds in $D(F, a/b)^*$ if and only if, in addition to (1) *through* (4), *the following holds*:

(5) $b = [F(\zeta_m) : F]s$ *where s is prime to $o(r|m)$.*

Proof. By Proposition 2.6, Theorem 6.8, and Corollary 6.9 below. ∎

Remark. *If $F/\hat{\mathbb{Q}}_p$ is unramified then we may replace* (2) *and* (5) *by*

(2′) $o(r|m) | p - 1$.

(5′) $b = o(p^{[F:\hat{\mathbb{Q}}_p]}|\ell)\phi(p^\alpha)s$ *where* $(s, o(r|m)) = 1$,

and $q = p^{[F:\hat{\mathbb{Q}}_p]o(p^{[F:\hat{\mathbb{Q}}_p]}|\ell)}$. ϕ is the Euler function. See Corollary 6.10.

THEOREM 1.2. *Let F be a local field with odd residue characteristic, p. The unit group, $D(F, a/b)^*$, contains nonabelian, finite subgroups if and only if the extension $F(\zeta_p)/F$ is ramified and b has the form $b = p^n[F(\zeta_p) : F]k$ for some k prime to p. For such a field, F, and exponent, b, we define*:

(1) $e_F = e(F(\zeta_p)/F)$,

(2) $\beta(F) = \text{Max}\{\beta : \zeta_{p^\beta} \in F(\zeta_p)\}$,

(3) $\gamma = \gamma(F, \alpha)$ *is the relative degree,* $f(F(\zeta_{p^\alpha})/\hat{\mathbb{Q}}_p)$.

For $\beta(F) \leq \alpha < \beta(F) + n$, we have $\gamma(F, \alpha + 1) = \gamma(F, \alpha)p^{\epsilon(F,\alpha)}$ where $\epsilon(F, \alpha)$ is 0 or 1. We set $\epsilon(F, \beta(F) + n) = 0$. The isomorphism classes of nonabelian, maximal, finite subgroups of $D(F, a/b)^*$ are in one to one correspondence with the integers, α, such that $\beta(F) \leq \alpha \leq \beta(F) + n$ and $\epsilon(F, \alpha) = 0$. This correspondence associates to each α a metacyclic group, G_{m_α, r_α}, where

(4) $m_\alpha = p^\alpha(p^{k\gamma p^{n+\beta(F)-\alpha}} - 1)$

and r_α is a unit modulo m_α satisfying the conditions:

(5) $r_\alpha \equiv 1 \bmod m_\alpha/p^\alpha$,

(6) $o(r_\alpha|p^\alpha) = e_F$.

The isomorphism class of G_{m_α, r_α} is independent of the choice of r_α subject to (5) *and* (6).

Proof. Theorems 6.12 and 6.17 below. ∎

A special case of this gives the following:

THEOREM 1.3. *If p is odd then $D(\hat{\mathbb{Q}}_p, a/b)^*$ has noncyclic subgroups if and only if $b = p^n(p-1)k$, for some k prime to p. There are $n+1$ isomorphism classes of nonabelian, maximal, finite subgroups. These are represented by the metacyclic groups, G_{m_α, r_α} where*

(1) $1 \leq \alpha \leq n+1$,

(2) $m_\alpha = p^\alpha(p^{kp^{n+1-\alpha}} - 1)$,

(3) $r_\alpha \equiv 1 \bmod m_\alpha/p^\alpha$,

(4) $o(r_\alpha | p^\alpha) = p - 1$.

Proof. Corollary 6.18 below. ∎

At 2 the main results are as follows.

THEOREM 1.4. *If F is a local field with residue characteristic 2 then $D(F, a/b)^*$ has nonabelian, finite subgroups if and only if $[F : \hat{\mathbb{Q}}_2]$ and $b/2 = k$ are odd integers. In this case there is one isomorphism class of maximal, nonabelian, finite subgroups, namely $T \times \mathbb{Z}/q^k - 1$ where T is the binary tetrahedral group and q is the cardinality of the residue field of F.*

Proof. Theorem 7.7 below.

Again, taking $F = \hat{\mathbb{Q}}_2$ we get:

COROLLARY 1.5. *The noncyclic, maximal, finite subgroups of $D(\hat{\mathbb{Q}}_2, a/b)^*$, where $b = 2k$ and k is odd, are isomorphic to $T \times \mathbb{Z}/2^k - 1$.*

Proof. Corollary 7.8 below. ∎

These results and Theorem 4.12 allow us to find a characterization of the local fields that satisfy Herstein's conjecture. A field, F, satisfies Herstein's conjecture if every central division algebra over F contains no nonabelian, finite subgroups of odd order.

THEOREM 1.6. *If F is a local field with odd residue characteristic, p, then F satisfies Herstein's conjecture if and only if the ramification index,*

$e(F(\zeta_p)/F)$, is a power of 2. If the residue characteristic is 2 then F always satisfies Herstein's conjecture.

Proof. Theorem 6.19 and Proposition 7.9 below. ∎

We extend a result by Fein and Schacher [5] to conclude:

THEOREM 1.7. *If F has residue characteristic a Fermat prime then F satisfies the Herstein conjecture. For p odd, $\hat{\mathbb{Q}}_p$ satisfies the Herstein conjecture if and only if p is a Fermat prime.*

Proof. Corollary 6.20 and 6.21 below. ∎

This investigation was undertaken so as to understand the finite subgroups of $D(\hat{\mathbb{Q}}_p, 1/n)^*$. These are of interest in homotopy theory for the following reason: complex cobordism gives rise to a host of cohomology theories which measure different aspects of homotopy theory. Among the best studied of these is the Johnson–Wilson–Morava theory $E(n)$, with coefficient ring

$$E(n)_* = \mathbb{Z}_{(p)}[v_1, \ldots, v_n^{\pm 1}], \quad |v_k| = 2(p^n - 1).$$

It turns out that a certain completion of this theory has better properties; its homotopy is precisely the coordinate ring of the Lubin–Tate moduli space for deformations of formal groups of height n,

$$E_n = W_n[[u_1, \ldots, u_{n-1}]][u^{\pm 1}].$$

Here W_n is the ring of Witt vectors of $\mathbb{F}_{p^n}$. This cohomology theory has the property that the group of automorphisms of the formal group of height n over $\mathbb{F}_{p^n}$ acts by operations on it, in a way compatible with a certain Galois action.

A recent theorem of M. Hopkins and H. Miller shows that this action can be "rigidified," so that one may form homotopy fixed point sets with respect to closed subgroups. In case $n = 1$, one has a subgroup of order 2; E_1 is essentially p-adic K-theory, and the homotopy fixed point subspectrum is p-adic real K-theory. One now has a wide extension of "real K-theory."

The automorphism group in question is precisely the group of units in the maximal order of the division algebra $D(\hat{\mathbb{Q}}_p, 1/n)$. Finite subgroups of this each give rise to "real" versions of higher K-theory.

2. Finite Groups in $D(F, a/b)$.

We define some groups as follows.

Definition 2.1. (1) $G_{m,r} = \langle A, B : A^m = 1, B^n = A^t, BAB^{-1} = A^r \rangle$ where r is a residue class mod m, $(m, r) = 1, n = o(r|m)$ and $t = m/(r-1, m)$.

(2) $T = \langle P, Q, R : P^4 = 1, P^2 = Q^2, PQP^{-1} = Q^{-1}, RPR^{-1} = Q, RQR^{-1} = PQ, R^3 = 1 \rangle$. T is the binary tetrahedral group.

(3) O is the binary octahedral group.

(4) I is the binary icosahedral group.

The following result is a weak version of Amitsur's theorem [1, Thm. 7].

Theorem 2.2. *If G is a finite subgroup of a division ring then G is one of the following types*:

(1) *A metacyclic group, $G_{m,r}$,*

(2) *A product $T \times G_{m,r}$,*

(3) *O or I.*

A central part of Amitsur's classification is the analysis of the following algebras:

Definition 2.3. Let $\phi: G \hookrightarrow D^*$ be an embedding of a finite group, G, into a division algebra with center F. If K is a subfield of F then we define

$$K\phi G = \left\{ \sum_{g \in G} z_g \phi(g) : z_g \in K \right\}.$$

$K\phi G$ is a K-algebra and there is a unique K algebra map from the group ring, $K[G]$, to $K\phi G$ that extends ϕ.

$$K[G] \xrightarrow{\hat{\phi}} K\phi G.$$

Amitsur proves the following ([1], Lemma's 4, 12, 13, and 14):

Theorem 2.4. *If $\phi: G \to D^*$ is an embedding of a finite group in a division algebra then*:

(1) *If G is cyclic, then $\mathbb{Q}\phi G$ is a cyclotomic extension of $\mathbb{Q}$.*

(2) *If $G \cong G_{m,r}$, then $\mathbb{Q}\phi G$ is isomorphic to the cyclic algebra $\langle \mathbb{Q}(\zeta_m), \sigma_r, \zeta_m^t \rangle$ where $\sigma_r(\zeta_m) = \zeta_m^r$ and $t = m/(m, r-1)$ via $A \to \zeta_m$, $B \to \sigma_r$.*

(3) *If* $G \cong T$, *then* $\mathbb{Q}\phi T$ *is isomorphic to the quaternion algebra* $\left(\begin{smallmatrix} -1,-1 \\ \mathbb{Q} \end{smallmatrix}\right)$ *via the identification* $P \to i, Q \to j, R \to -(1+i+j+k)/2$.

(4) *If* $G \cong O$, *then* $\mathbb{Q}\phi O \cong \left(\begin{smallmatrix} -1,-1 \\ \mathbb{Q}(\sqrt{2}) \end{smallmatrix}\right)$.

(5) *If* $G \cong I$, *then* $\mathbb{Q}\phi I \cong \left(\begin{smallmatrix} -1,-1 \\ \mathbb{Q}(\sqrt{5}) \end{smallmatrix}\right)$.

PROPOSITION 2.5. *Let* $D(F, a/b)$ *and* $D(F, c/d)$ *be central division algebras over a local field* F. $D(F, c/d)$ *embeds as an* F*-subalgebra of* $D(F, a/b)$ *if and only if*

(1) $b = df$ *where* $(d, f) = 1$,

(2) $c \equiv af^{-1} \bmod d$.

Proof. If $D(F, c/d) \subseteq D(F, a/b)$ then, by the double centralizer theorem [8], $D(F, a/b) \cong D(F, c/d) \underset{F}{\otimes} C(D(F, c/d))$ and so the exponents of $D(F, c/d)$ and $C(D(F, c/d))$ are relatively prime which proves (1). $C(D(F, c/d)) \cong D(F, g/f)$ for some g and f. Now, $a/b \equiv c/d + g/f \bmod \mathbb{Z}$ implies $c \equiv af^{-1} \bmod d$.

Conversely, if (1) and (2) hold, let $g \equiv ad^{-1} \bmod f$. $a \equiv cf + gd \bmod df$, as $(d, f) = 1$. This gives $a/b \equiv c/d + g/f \bmod \mathbb{Z}$ and hence $D(F, c/d) \subseteq D(F, a/b)$. ∎

Now we wish to consider which of the groups T, O and I of Theorem 2.2 can appear as subgroups of $D(F, a/b)^*$. If $\phi: G \to D(F, a/b)$ is an embedding then there is an algebra surjection

$$F \underset{\mathbb{Q}}{\otimes} \mathbb{Q}\phi G \twoheadrightarrow F\phi G.$$

$F\phi G$ is a division algebra.

Case 1. If $G = T$ then $F \underset{\mathbb{Q}}{\otimes} \mathbb{Q}\phi G \cong \left(\begin{smallmatrix} -1,-1 \\ F \end{smallmatrix}\right)$ by Theorem 2.4. Thus, $F \underset{\mathbb{Q}}{\otimes} \mathbb{Q}\phi G \cong M_2(F)$ if p is odd or if $p = 2$ and $[F : \hat{\mathbb{Q}}_2]$ is even. It is a division algebra otherwise, with invariant $1/2 \bmod \mathbb{Z}$. It follows that T embeds in $D(F, a/b)^*$ if and only if $p = 2$, $[F : \hat{\mathbb{Q}}_2]$ is odd and $b = 2f$ for f odd.

*Case*2. If $G = O$ or $G = I$ then G contains a subgroup isomorphic to the binary tetrahedral group T and so, by the case above, if G embeds in $D(F, a/b)^*$ it follows that $p = 2$. $D(F, a/b)$ would also contain a division algebra quotient of

$$\hat{\mathbb{Q}}_2 \underset{\mathbb{Q}}{\otimes} \left(\begin{smallmatrix} -1,-1 \\ \mathbb{Q}(\sqrt{2}) \end{smallmatrix}\right) \quad \text{or} \quad \hat{\mathbb{Q}}_2 \underset{\mathbb{Q}}{\otimes} \left(\begin{smallmatrix} -1,-1 \\ \mathbb{Q}(\sqrt{5}) \end{smallmatrix}\right).$$

These algebras are $M_2(\hat{\mathbb{Q}}_2(\sqrt{2}))$ and $M_2(\hat{\mathbb{Q}}_2(\sqrt{5}))$, respectively, and so, in fact, O and I do not embed in $D(F, a/b)^*$. In short, $\sqrt{2} \notin \hat{\mathbb{Q}}_2$ so

$$\hat{\mathbb{Q}}_2 \underset{\mathbb{Q}}{\otimes} \left(\frac{-1,-1}{\mathbb{Q}(\sqrt{2})} \right) \cong \hat{\mathbb{Q}}_2 \underset{\mathbb{Q}}{\otimes} \mathbb{Q}(\sqrt{2}) \underset{\mathbb{Q}(\sqrt{2})}{\otimes} \left(\frac{-1,-1}{\mathbb{Q}(\sqrt{2})} \right)$$

$$\cong \hat{\mathbb{Q}}_2(\sqrt{2}) \underset{\mathbb{Q}(\sqrt{2})}{\otimes} \left(\frac{-1,-1}{\mathbb{Q}(\sqrt{2})} \right)$$

$$\cong \left(\frac{-1,-1}{\hat{\mathbb{Q}}_2(\sqrt{2})} \right) \cong M_2\big(\hat{\mathbb{Q}}_2(\sqrt{2})\big).$$

Similarly,

$$\sqrt{5} \notin \hat{\mathbb{Q}}_2 \text{ so } \hat{\mathbb{Q}}_2 \underset{\mathbb{Q}}{\otimes} \left(\frac{-1,-1}{\mathbb{Q}(\sqrt{5})} \right) \cong M_2\big(\hat{\mathbb{Q}}_2(\sqrt{5})\big).$$

These considerations give the following:

PROPOSITION 2.6. *If a finite group, G, embeds in $D(F, a/b)^*$, then G is of one of the following types*:

(1) *Metacyclic*, $G_{m,r}$,

(2) *A product*, $T \times G_{m,r}$.

Case (2) *occurs if and only if* $p = 2$, $[F : \hat{\mathbb{Q}}_2]$ *is odd and* $b = 2f$ *where* f *is odd.*

DEFINITION 2.7. Given m and r prime to m we define $D^F_{m,r}$ to be the cyclic algebra,

$$D^F_{m,r} = \langle F(\zeta_m), \sigma, \zeta_m^t \rangle,$$

where $\sigma_r(\zeta_m) = \zeta_m^r$ and $t = m/(r-1, m)$.

$$Z^F_{m,r} = Z\big(D^F_{m,r}\big).$$

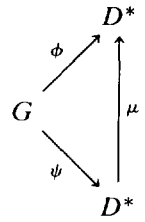
Note. $D^F_{m,r}$ is only defined if σ_r gives a well defined automorphism of $F(\zeta_m)$. If $G_{m,r} \xrightarrow{\phi D^*}$, where D is a division algebra over F, then $F\phi G_{m,r} \cong D^F_{m,r}$ and so:

PROPOSITION 2.8. $G_{m,r}$ *embeds in a division algebra over F if and only if* $D^F_{m,r}$ *is defined and is a division algebra.*

$D^F_{m,r}$ will be a division algebra if and only if its degree equals its exponent. The degree of $D^F_{m,r}$ is $o(r|m)$. The calculation of the exponent is a rather more subtle matter which is solved in Yamada's book [10].

3. Conjugacy

We consider embeddings $\phi: G \hookrightarrow D^*$ of a finite group, G into the units of a central division algebra over F. Two such embeddings, ϕ and ψ, are "conjugate" if there is an F-algebra automorphism, μ, of D such that the following diagram commutes.



By the Noether-Skolem Theorem this amounts to the existence of $d \in D^*$ such that $\phi(g) = d\psi(g)d^{-1}$ for all $g \in G$.

Definition 3.1. If $\phi: G \hookrightarrow D^*$ then we define a representation of G, over F, as follows. $R(\phi) = F\phi G$ and for $g \in G$ let $z_g \in F$,

$$\bar{g} * \sum_{g \in G} z_g \phi(g) = \sum_{g \in G} z_g \phi(\bar{g}g).$$

Proposition 3.2. *If ϕ and ψ are conjugate, via $\mu \in \mathrm{Aut}_F D$, then $\mu: R(\psi) \longrightarrow R(\phi)$ is an $F[G]$-module isomorphism.*

Proof. $\mu(g * \psi g') = \mu(\psi(gg')) = \phi(gg') = g * \phi g' = g * \mu(\psi g')$. ∎

Lemma 3.3. *If $\mu : F\psi G \longrightarrow F\phi G$ is F-linear and $\mu\psi = \phi$ then μ is an F-algebra homomorphism if and only if it is an $F[G]$-module homomorphism.*

Proof.

$$\begin{aligned} \mu \text{ is an } F[G]\text{-module map} &\Leftrightarrow \mu(g\psi g') = g * \mu(\psi g'), \\ &\Leftrightarrow \mu(\psi g \psi g') = \phi(g)\phi(g'), \\ &\Leftrightarrow \mu(\psi g \cdot \psi g') = \mu(\psi g) \cdot \mu(\psi g'), \\ &\Leftrightarrow \mu \text{ is a ring map.} \end{aligned}$$

Certainly $\mu(1) = 1$ and so the result follows. ∎

Lemma 3.4. *If $\mu : F\psi G \longrightarrow F\phi G$ is an $F[G]$-module isomorphism then, composing with right multiplication by $\mu(1)^{-1}$ we get an algebra isomorphism, $\hat{\mu}(x) = \mu(x)\mu(1)^{-1}$, such that $\hat{\mu}\psi = \phi$.*

Proof. Let $\hat{\mu}(x) = \mu(x)\mu(1)^{-1}$. We want to show that $\hat{\mu}\psi = \phi$ then the result would follow from Lemma 3.3, as $\hat{\mu}$ is certainly a G-module map.

$$\hat{\mu}(\psi g) = \hat{\mu}(g * 1) = g * \hat{\mu}(1) = g * 1 = \phi(g).$$

∎

PROPOSITION 3.5. *Two embeddings $\phi, \psi: G \to D^*$ are conjugate if and only if the $F[G]$ modules $R(\phi)$ and $R(\psi)$ are isomorphic.*

Proof. By Proposition 3.2, Lemma 3.4 and the Noether–Skolem Theorem. ∎

4. METACYCLIC GROUPS

A group is metacyclic if it is an extension of a cyclic group by a cyclic group. That is, there is an exact sequence

$$0 \to \mathbb{Z}/m \to G \to \mathbb{Z}/n \to 0.$$

Such groups are determined by the following theorem of Hôlder [11].

THEOREM 4.1. *The metacyclic groups are exactly the groups*

$$\langle A, B : A^m = 1, BAB^{-1} = A^r, B^n = A^t \rangle,$$

where $0 < n, m$, $m | r^n - 1$ and $m | t(r-1)$. ∎

DEFINITION 4.2.. $G(m, r, n, t) = \langle A, B : A^m = 1, BAB^{-1} = A^r, B^n = A^t \rangle$, where n, m, r and t satisfy the conditions of Theorem 4.1.

PROPOSITION 4.3. *If $\ell | n$ then $G(m, r^\ell, n/\ell, t)$ embeds in $G(m, r, n, t)$.*

Proof. Consider the subgroup $\langle A, B^\ell \rangle \subseteq \langle A, B \rangle = G(m, r, n, t)$. There is a sequence

$$0 \to \mathbb{Z}/m \to \langle A, B^\ell \rangle \to \mathbb{Z}/(n/\ell) \to 0$$

as B^ℓ has order n/ℓ modulo $\langle A \rangle$. $B^\ell A B^{-\ell} = A^{r^\ell}$ and $(B^\ell)^{n/\ell} = B^n = A^t$ so $\langle A, B^\ell \rangle \cong G(m, r^\ell, n/\ell, t)$. ∎

The following is a result of Beyl [2] and [3].

PROPOSITION 4.4. *If $\ell = |H^2(G(m, r, n, t), \mathbb{C}^*)|$, then*

$$G(m, r, n, t) \cong G(m, r, n, \ell m/(r-1, m)).$$

Proof. Omitted. ∎

PROPOSITION 4.5. *If* $(\nu, n) = 1$ *then* $G(m, r, n, t) \cong G(m, r^\nu, n, \nu t)$.

Proof. $(\nu, n) = 1$ so $\langle A, B^\nu \rangle = \langle A, B \rangle$. $B^\nu A B^{-\nu} = A^{r^\nu}$ and $(B^\nu)^n = B^{\nu n} = A^{t\nu}$ so $\langle A, B^\nu \rangle \cong G(m, r^\nu, n, \nu t)$. ∎

PROPOSITION 4.6. $G(m, r, n, t)' = \langle A^{(m, r-1)} \rangle$ *is cyclic of order* $m/(m, r-1)$. *If* $n = o(r|m)$, *then* $Z(G(m, r, n, t)) = \langle A^{m/(r-1, m)} \rangle$ *has order* $(r-1, m)$.

Proof. Let $G = G(m, r, n, t)$. $[B, A] = A^{r-1}$ so $A^{r-1} \in G'$. Now, $\langle A^{r-1} \rangle = \langle A^{(m, r-1)} \rangle$. This is a normal subgroup with abelian quotient and the first statement follows. The condition $n = o(r|m)$ ensures that $Z(G) \subseteq \langle A \rangle$. Now, $A^i \in Z(G)$ if and only if $A^{ir} = A^i$, or $m | i(r-1)$, or $(m/(r-1, m)) | i$. The second claim follows. ∎

DEFINITION 4.7. The groups $G_{m,r}$ can be described as follows:

$$G_{m,r} = G\big(m, r, o(r|m), m/(r-1, m)\big).$$

Remark. If $G \cong G_{m,r}$, then $m = |G'||Z(G)|$, so m is an invariant of the isomorphism class of $G_{m,r}$.

PROPOSITION 4.8. $|H^2(G_{m,r}, \mathbb{C}^*)| = 1$.

Proof. By Curtis and Reiner [4, Example p. 301],

$$H^2(G_{m,r}, \mathbb{C}^*) \cong \mathbb{Z}/f \text{ where } f = \left(\frac{m}{(r-1, m)}, \frac{r^n - 1}{r-1} \right) \frac{(m, r-1)}{m}.$$

Now, $m | r^n - 1$ so

$$\frac{m}{(r-1, m)} \Bigg| \frac{r-1}{(r-1, m)} \cdot (r^{n-1} + \cdots + r + 1).$$

But, $m/(r-1, m)$ and $(r-1)/(r-1, m)$ are relatively prime, thus,

$$\frac{m}{(r-1, m)} \Bigg| \frac{r^n - 1}{r-1}$$

and so $f = 1$. ∎

PROPOSITION 4.9. *If* $n = o(r|m)$ *and* $(\nu, n) = 1$ *then* $G_{m,r} \cong G_{m,r^\nu}$. *In other words, if* $\langle r \rangle = \langle s \rangle \subseteq (\mathbb{Z}/m)^*$ *then* $G_{m,r} \cong G_{m,s}$.

Proof.

$$\begin{aligned} G_{m,r} &\cong G\big(m, r, o(r|m), m/(r-1,m)\big) \\ &\cong G\big(m, r^{\nu}, o\big(r^{\nu}|m\big), \nu m/(r-1,m)\big) && \text{(Proposition 4.5)} \\ &\cong G\big(m, r^{\nu}, o\big(r^{\nu}|m\big), m/(r^{\nu}-1,m)\big) && \text{(Proposition 4.4)} \\ &\cong G_{m,r^{\nu}}. \end{aligned}$$

∎

PROPOSITION 4.10. *If a metacyclic group, $G = G(m, r, n, t)$, embeds in the unit group of a division algebra, D, then, if $\nu = o(r|m)$ we have $G \cong G_{mn/\nu, r'}$ where r' is the residue* mod *mn/ν such that*

$$\begin{aligned} r' &\equiv r \bmod m \\ &\equiv 1 \bmod n(r-1,m)/\nu. \end{aligned}$$

If $\nu = n$, then $G \cong G_{m,r}$. G is cyclic if and only if $r \equiv 1$ mod m.

Proof. Let $G = G(m, r, n, t)$ then, as T, O and I are not metacyclic (Theorem 7.2), it follows that $G \cong G_{\tilde{m},\tilde{r}}$ for some $\tilde{m}$ and $\tilde{r}$ and thus, by Proposition 4.8, $|H^2(G; \mathbb{C}^*)| = 1$. By Proposition 4.4, $G \cong G(m, r, n, m/(r-1,m)) = \langle A, B\rangle$ where $A^m = 1$, $B^n = A^{m/(r-1,m)}$ and $BAB^{-1} = A^r$. Now, by Proposition 4.3, we have $H = \langle A, B^{\nu}\rangle \cong G(m, r^{\nu}, n/\nu, m/(r-1,m)) \subseteq G$. H is abelian, hence cyclic, so $H \cong \mathbb{Z}/(mn/\nu)$. H is normal in G and hence we have an isomorphism, $G \cong G(mn/\nu, r', \nu, t')$, for some r' and t'. The class of r' mod mn/ν is determined by the automorphism of H induced by conjugating by B. This is given by $BAB^{-1} = A^r$ and $BB^{\nu}B^{-1} = B^{\nu}$ and hence r' is determined by the congruences,

$$\begin{aligned} r' &\equiv r \bmod m \\ &\equiv 1 \bmod o(B^{\nu}) = n(r-1,m)/\nu. \end{aligned}$$

$o(r'|mn/\nu) = \nu$ and so, by Proposition 4.4, $G \cong G_{mn/\nu, r'}$. The last two statements of the proposition are evident. ∎

PROPOSITION 4.11. *If $G_{m,r}$ is a subgroup of the units of a division algebra, D, and $\ell | o(r|m)$ then $G_{m,r^{\ell}}$ embeds in $G_{m,r}$.*

Proof.

$$\begin{aligned} G_{m,r} &= G\big(m, r, o(r|m), m/(m, r-1)\big) \\ &\supseteq G\big(m, r^{\ell}, o\big(r^{\ell}|m\big), m/(m, r-1)\big) && \text{(Proposition 4.3)} \\ &\cong G_{m,r^{\ell}}. && \text{(Proposition 4.10)} \end{aligned}$$

∎

THEOREM 4.12. *If $G_{m,r}$ embeds in the unit group of a division algebra, D, then the subgroups of $G_{m,r}$ are the groups of the form, $G_{\ell n/s\nu, r(s,\ell)}$ where:*

(1) $\ell | m$.

(2) $n = o(r|m)$, $s|n$ and $\nu = o(r^s|\ell)$.

(3) $\left(\frac{m}{\ell}, \frac{r^n - 1}{r^s - 1}\right) \Big| \frac{m}{(r-1, m)}$.

Given ℓ and s satisfying the above, $r(s, \ell)$ is determined by:

(4) $r(s, \ell) \equiv r^s \bmod \ell$.

(5) $r(s, \ell) \equiv 1 \bmod \frac{n(r^s - 1, \ell)}{s\nu}$.

This group is cyclic if and only if $r^s \equiv 1 \bmod \ell$.

Proof. If, $H \subseteq G_{m,r}$ then $H = \langle A^{m/\ell}, A^i B^s \rangle$ for some ℓ, i and s such that $\ell | m$, $s|n$ and $H \cap \langle A \rangle = \langle A^{m/\ell} \rangle$. Now, $(A^i B^s)^{n/s} = A^{i(r^n - 1)/(r^s - 1) + m/(r-1, m)}$ is in $H \cap \langle A \rangle$ and so,

$$\frac{m}{\ell} \Big| i\left(\frac{r^n - 1}{r^s - 1}\right) + \frac{m}{(r-1, m)},$$

giving (3). We have $H \cong G(\ell, r^s, n/s, t)$ for some t and, by 4.10, we conclude that $H \cong G_{\ell n/s\nu, r(s,\ell)}$, where $r(s, \ell)$ satisfies (4) and (5). If, on the other hand, ℓ and s satisfy (1), (2) and (3). By (3),

$$\frac{m}{\ell} \Big| i\left(\frac{r^n - 1}{r^s - 1}\right) + \frac{m}{(r-1, m)}$$

for some i. Then let $H = \langle A^{m/\ell}, A^i B^s \rangle$. $H \cap \langle A \rangle = \langle A^{m/\ell} \rangle$ and so $H \cong G(\ell, r^s, n/s, t)$ for some t and, by 4.10, $H \cong G_{\ell n/s\nu, r(s,\ell)}$. ∎

Remark. 4.10–4.12 hold for division algebras with any center, not exclusively local fields.

5. PRELIMINARIES

THEOREM 5.1. *If $D = \langle L/K, \sigma, \zeta \rangle$ is a cyclic division algebra over a local field, K, and ζ is a root of unity in K then L/K is totally ramified.*

Proof. Let $K \subseteq E \subseteq L$ where E is the maximal unramified extension of K in L. Gal $(L/K) = \langle \sigma \rangle \cong \mathbb{Z}/n$ and Gal $(E/K) = \langle \bar{\sigma} \rangle \cong \mathbb{Z}/m$ where $ml = n$;

$$\sigma^m(\alpha\sigma^i) = (\alpha^{\sigma^m} \cdot \sigma^i) \cdot \sigma^m$$

for all $\alpha \in L$ and so

$$\begin{aligned} C_D(K(\sigma^m)) &= E \cdot 1 + E \cdot \sigma + \cdots + E \cdot \sigma^{n-1} \\ &= E(\sigma^m) \cdot 1 + E(\sigma^m) \cdot \sigma + \cdots + E(\sigma^m) \cdot \sigma^{m-1} \\ &\cong \langle E(\sigma^m)/K(\sigma^m), \sigma, \sigma^m \rangle \end{aligned}$$

$(\sigma^m)^l = \sigma^n = \zeta$ so σ^m is a root of unity. We want to show $E(\sigma^m)/K(\sigma^m)$ is unramified as then $C_D(K(\sigma^m))$ splits as a matrix algebra which is impossible unless $m = 1$ so L/K is totally ramified. Let f be the relative degree, $f(K(\sigma^m)/K)$. Now, m and f are relatively prime, otherwise $E \cap K(\sigma^m)$ would contain a non-trivial cyclotomic extension of K which is impossible as $K(\sigma^m) \cap E = K$. Let Q be the maximal unramified extension of K in $K(\sigma^m)$. We have the following diagram:

$$\begin{array}{ccccc} E & \longrightarrow & EQ & \longrightarrow & E(\sigma^m) \\ \uparrow m & & \uparrow & & \uparrow m \\ K & \xrightarrow{f} & Q & \xrightarrow{e} & K(\sigma^m) \end{array}$$

where the integers m, f and e denote the degrees of the extensions. For the corresponding residue fields

$$\begin{array}{ccccc} \mathbb{F}_{q^m} & \longrightarrow & \mathbb{F}_{q^{fm}} & \longrightarrow & \mathbb{F}_{q^{fm}} \\ \uparrow & & \uparrow & & \uparrow \\ \mathbb{F}_q & \longrightarrow & \mathbb{F}_{q^f} & \longrightarrow & \mathbb{F}_{q^f} \end{array}$$

As $(f, m) = 1$, $\mathbb{F}_{q^{fm}} = \mathbb{F}_{q^f} \cdot \mathbb{F}_{q^m} = \bar{Q} \cdot \bar{E} \subseteq \overline{EQ}$ but, as $[EQ : K] = fm$, EQ/K is unramified. It follows that EQ/Q is unramified of degree m and $K(\sigma^m)/Q$ is totally ramified so $E(\sigma^m)/K(\sigma^m)$ is unramified. This finishes the proof. ∎

PROPOSITION 5.2. *If G is a finite subgroup of the unit group, D^*, where D is a division algebra with center F then*

(1) $C_D(Z(FG)) \cong FG \underset{Z(FG)}{\otimes} C_D(G)$.

If G is a maximal, finite subgroup, then:

(2) $C_D(Z(FG)) = FG$.

(3) $C_D(FG) = Z(FG)$.

Proof. Let $Z = Z(FG)$ and $D' = C_D(Z)$. Certainly, $FG \subseteq C_D(Z)$ and these two algebras have the same center, Z. By the Double Centralizer Theorem,

$$D' \cong FG \underset{Z}{\otimes} C_{D'}(FG),$$

but $C_{D'}(FG) = C_D(G)$. If G is maximal then $C_D(G) = Z$, otherwise we could find a finite subgroup, H, of $C_D(G)^*$, that is not contained in Z. G would then be properly contained in the finite group $G \otimes H$. This finishes the proof. ∎

COROLLARY 5.3. *If $G \subseteq D(F, a/b)^*$ is a maximal subgroup, then*

(1) $\mathrm{Inv}_{Z(FG)}(FG) = [Z(FG): F]a/b + \mathbb{Z}$.

(2) $\mathrm{Deg}_{Z(FG)}(FG) = b/[Z(FG): F]$.

Proof. By Proposition 5.2, part (2). ∎

COROLLARY 5.4. *If $G \subseteq D(F,a/b)^*$ is a maximal, finite subgroup and $G \cong G_{m,r}$ is nonabelian, then*:

(1) $p|m$,

(2) $[F(\zeta_m): F] = b$,

(3) $\mu(F(\zeta_m)) = \langle \zeta_m \rangle$.

Proof. If m is prime to p then $FG \cong \langle F(\zeta_m), \sigma_r, \zeta_m^t \rangle$ splits completely, as $F(\zeta_m)/F$ is unramified and so ζ_m^t is a norm. This cannot occur, unless G is cyclic, but it is not. This proves (1). Let $Z = Z(FG)$. $[F(\zeta_m): F] = [F(\zeta_m): Z][Z: F] = \mathrm{Deg}(FG)[Z: F] = b$, by Corollary 5.3. This proves (2). The final claim follows from the containment $G \subseteq \langle \mu(F(A)), B \rangle$, where A and B are the generators of $G = G_{m,r}$ as per Definition 2.1, part (1). ∎

6. Odd Residue Characteristic

PROPOSITION 6.1. *If $G_{m,r}$ and $G_{m',r'}$ are metacyclic groups that embed in division algebras over F, a local field with odd residue characteristic, p, then then following are equivalent*:

(1) $G_{m,r} \cong G_{m',r'}$,

(2) $m = m'$ *and* $\langle r \rangle = \langle r' \rangle \subseteq (\mathbb{Z}/m)^*$,

(3) $m = m'$ *and* $|G_{m,r}| = |G_{m',r'}|$.

Proof. Proposition 4.9 proves that (2) implies (1). By the remark after Definition 4.7, we see that (1) implies (3). It remains to show that (3)

implies (2). Let $m = m' = p^\alpha \ell$, where ℓ is prime to p. Applying Theorem 5.1 to thecyclic algebras $FG_{m,r}$ and $FG_{m',r'}$, we see that $r \equiv r' \equiv 1 \bmod \ell$. If we write $(\mathbb{Z}/m)^* = (\mathbb{Z}/p^\alpha)^* \times (\mathbb{Z}/\ell)^*$, then $\langle r \rangle$ and $\langle r' \rangle$ are contained in the first factor. This is cyclic, for p odd, and so (3) implies $|\langle r \rangle| = |\langle r' \rangle|$ which, in turn, implies (2). ∎

PROPOSITION 6.2. *Let F be a local field with odd residue characteristic, p. Let $G \subseteq D(F, a/b)^*$ be a nonabelian subgroup with $G = \langle A, B : A^m = 1, BAB^{-1} = A^r, B^n = A^t \rangle \cong G_{m,r}$, where $n = o(r|m)$, $t = m/(r-1, m)$ and $m = p^\alpha \ell$ with ℓ prime to p.*

(1) *$n \| [F(\zeta_\ell, \zeta_p) : F(\zeta_\ell)]$.*

(2) *$\alpha \geq 1$ and $(r-1, m) = \ell$.*

(3) *$Z(G) \cong \mathbb{Z}/\ell$.*

(4) *$G' \cong \mathbb{Z}/p^\alpha$ is a p-Sylow subgroup of G.*

(5) *$\langle A \rangle = Z(G).G'$ is a characteristic subgroup of G.*

(6) *$G \to G^{ab}$ is an isomorphism on $\langle B \rangle$.*

(7) *$G \cong G(p^\alpha, r, \ell n, 0)$ is a semidirect product.*

(8) *$FG = \langle F(A)/Z, B, A^t \rangle$ is a cyclic division algebra of degree n, where $Z = Z(FG)$ is the fixed field of $A \mapsto A^r$. $F(A) \cong Z(\zeta_p) \cong Z(\zeta_{p^\alpha})$ and $F(A)/Z$ is totally ramified.*

Proof. By Theorem 5.1, we have $r \equiv 1 \bmod \ell$ and so, $n | [F(\zeta_m) : F(\zeta_\ell)]$. G is nonabelian, so $n \neq 1$, and thus $\alpha \geq 1$. By Yamada [10, Th. 4.7], $n | p - 1$ but

$$[F(\zeta_m) : F(\zeta_\ell)] = [F(\zeta_m) : F(\zeta_\ell, \zeta_p)][F(\zeta_\ell, \zeta_p) : F(\zeta_\ell)],$$

where the former factor is a power of p. It follows that $n | [F(\zeta_\ell, \zeta_p) : F(\zeta_\ell)]$, proving (1). Thus, $\zeta_p \notin F$. Apply this to the algebra FG to get $\zeta_p \notin Z(FG)$ and so, $|Z(G)|$ is prime to p. Proposition 4.6 then gives (2), (3), (4) and (5). By (2), $t = p^\alpha$ and thus $\langle B \rangle$ has order ℓn which is prime to p. This gives (6). We have a short exact sequence, $G' \to G \to G^{ab}$. The corresponding presentation of G is (7). To show (8) all we need to check is that $F(A) \cong Z(\zeta_p)$, but $p | m$ and so $Z \subseteq Z(\zeta_p) \subseteq F(A)$. $[F(A) : Z(\zeta_p)]$ is a power of p and, as $n | p - 1$, by (1), we have $Z(\zeta_p) = F(A)$. ∎

PROPOSITION 6.3. *Let F be a local field with odd residue characteristic, p, and let K/F be a totally ramified, cyclic extension of degree e dividing $p - 1$. Let $\mu'(F)$ be the group of p' roots of unity in F. Let $N = N_{K/F}$. The canonical map*

$$\mu'(F)/\mu'(F)^e \to F^*/N(K^*)$$

is an isomorphism.

Proof. For a local field, L, let $U_L^{(1)}$ denote the group of units in L, congruent to 1 modulo the prime. Let λ be a uniformizing parameter in K. Then $K^* = \langle \lambda \rangle \times \mu'(F) \times U_F^{(1)}$ and $F^* = \langle N(\lambda) \rangle \times \mu'(F) \times U_F^{(1)}$, where N is the norm from K to F. N maps $\langle \lambda \rangle$ to $\langle N(\lambda) \rangle$, $\mu'(F)$ to itself and $U_K^{(1)}$ to $U_F^{(1)}$, thus $\mu'(F)/N(\mu'(F))$ injects into $F^*/N(K^*)$. As $\mu'(F) \subseteq F$, the restriction of N to $\mu'(F)$ maps x to x^e. Now, $e|p-1$ and $|\mu'(F)| = |\bar{F}| - 1$, so $e||\mu'(F)|$ and thus $\mu'(F)/\mu'(F)^e$ is isomorphic to $\mathbb{Z}/e$. By Class Field Theory [7], so is $F^*/N(K^*)$, and thus the result follows. ∎

THEOREM 6.4. *Let F be a local field with odd residue characteristic, p, such that the residue field of F is $\mathbb{F}_q$. Assume that $F(\zeta_p) = F(\zeta_{p^\alpha})$ and $F(\zeta_p)/F$ is totally ramified of degree e with Galois generator, σ_r, that satisfies $\sigma_r(\zeta_{p^\alpha}) = \zeta_{p^\alpha}^r$. Denote the group of p^α'th roots of unity in $F(\zeta_p)$ by μ_{p^α} and, for $\ell | q-1$, the group of ℓ'th roots of unity in F by μ_ℓ. Let $G = \langle x, y : x^{p^\alpha} = 1, y^{\ell e} = 1, yxy^{-1} = x^r \rangle$. For every $\bar{x} \in \mu_{p^\alpha} - \{1\}$ and $\bar{y} \in \mu_\ell$ there is a surjection of F algebras,*

$$F[G] \xrightarrow{\phi(\bar{x},\bar{y})} \langle F(\zeta_p)/F, \sigma_r, \bar{y} \rangle,$$

taking $x \mapsto \bar{x}$ and $y \mapsto \sigma_r$. The F algebra isomorphism type of the cyclic algebra is determined by the residue of $\bar{y}$ in μ_{q-1}/μ_{q-1}^e. The representations of $F[G]$ induced by $\phi(\bar{x}, \bar{y})$ and $\phi(\bar{x}_1, \bar{y}_1)$ are isomorphic if and only if $\bar{y} = \bar{y}_1$ and $\bar{x}$ and $\bar{x}_1$ are conjugate over F. There are $N = (p^\alpha - 1)/e$ distinct conjugacy classes of $\bar{x} \in \mu_{p^\alpha} - \{1\}$ over F. Let $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_N$ be representatives of these classes. There is an isomorphism of F-algebras,

$$F[G] \cong \left(\prod_1^N \prod_{\bar{y} \in \mu_\ell} \langle F(\zeta_p)/F, \sigma_r, \bar{y} \rangle \right) \times F[\mathbb{Z}/\ell e].$$

The projection maps to the cyclic algebra factors are the maps $\phi(\bar{x}_i, \bar{y})$ for $i = 1, 2, \ldots, N$ and $\bar{y} \in \mu_\ell$. The map to the final factor, a product of fields, is induced by the quotient map $G \to \mathbb{Z}/\ell e$.

Proof. The existence of the maps, $\phi(\bar{x}, \bar{y})$, is immediate. The statement concerning the isomorphism type of the cyclic algebras follows from Theorem 6.3. The representations induced by $\phi(\bar{x}, \bar{y})$ and $\phi(\bar{x}_1, \bar{y}_1)$ are isomorphic if and only if there is a map of F algebras, θ, such that $\theta\phi(\bar{x}, \bar{y}) = \phi(\bar{x}_1, \bar{y}_1)$. This corresponds to the condition that $\bar{x}$ be conjugate to $\bar{x}_1$ and $y = \bar{y}_1$. As $F(\zeta_{p^\alpha}) = F(\zeta_p)$ has degree e over F, it follows that every element of $\mu_{p^\alpha} - \{1\}$ has e conjugates which gives the equation $N = (p^\alpha - 1)/e$. We know that the maps $\phi(\bar{x}_i, \bar{y})$, for $i = 1, 2, \ldots, N$ and $\bar{y} \in \mu_\ell$, correspond to distinct simple factors of the group ring, $F[G]$. To

prove the isomorphism, we only need to show that the dimension of the right hand side is large enough. This follows from the equation, $N\ell e^2 + \ell e = p^\alpha \ell e = |G|$. ∎

In fact, we will not be concerned with all the factors of the semisimple decomposition in the theorem above, but only with those such that $\phi(\bar{x}_i, \bar{y})$ maps G injectively into a division algebra.

COROLLARY 6.5. *With the assumptions of Theorem* 6.4, *a factor,* $\langle F(\zeta_p), \sigma_r, \bar{y}\rangle$, *in the decomposition of* $F[G]$ *is a division algebra if and only if the residue of* $\bar{y}$ *has order* e *in* μ_{q-1}/μ_{q-1}^e. *Such factors exist if and only if* $\mu_\ell \to \mu_{q-1}/\mu_{q-1}^e$ *is surjective, i.e.,* $((q-1)/\ell, e) = 1$. *If they exist, there are* $N\ell\phi(e)/e$ *of them, where* ϕ *is the Euler function. As F-algebras they are the* $\phi(e)$ *central division algebras over F with degree equal to e. Each one appears* $N\ell/e$ *times.*

Proof. Immediate from Proposition 6.3 and Theorem 6.4. ∎

COROLLARY 6.6. *With the assumptions of Theorem* 6.4, $\phi(\bar{x}, \bar{y})$ *is injective on G if and only if* $\bar{x}$ *and* $\bar{y}$ *are generators of* μ_{p^α} *and* μ_ℓ, *respectively.*

Proof. $|\phi(\bar{x}, \bar{y})(G)| = |\langle \bar{x}, \sigma_r\rangle| = |\langle \bar{x}\rangle|\,|\langle \bar{y}\rangle|e$. ∎

COROLLARY 6.7. *Let the assumptions of Theorem* 6.4 *hold and let* $((q-1)/\ell, e) = 1$. *If C is a central division algebra, over F, of degree e then there are F-algebra maps,* $\phi_i : F[G] \to C$ *for* $i = 1, \ldots, M = N\ell/e$, *and a subgroup, H, of* C^*, *such that*

(1) $\phi_i(G) \subseteq H$, *for* $i = 1, 2, \ldots, M$,

(2) $H \cong G$,

(3) *The representations of G induced by the* ϕ_i *are exactly the irreducible representations of* $F[G]$ *with endomorphism algebras isomorphic to C.*

Proof. By Corollary 6.5, we see that C corresponds to a choice of generator of μ_{q-1}/μ_{q-1}^e. We may pick a generator, $\bar{y}$, of μ_ℓ so that $C \cong \langle F(\zeta_p)/F, \sigma_r, \bar{y}\rangle$. Let $H = \langle \mu_{p^\alpha}, \sigma_r\rangle$, then certainly (2) holds. The projections corresponding to the representations described in (3) are the maps $\phi(\bar{x}_i, \bar{y}(\bar{y}')^e)$, where $i = 1, 2, \ldots, N$, $\bar{y}' \in \mu_{q-1}$ and $(\bar{y}')^e \in \mu_\ell$. In fact, this implies that $\bar{y}' \in \mu_\ell$. Suppose z is a generator of μ_{q-1}, then $\bar{y}' = z^a$, for some a, and $(\bar{y}')^e \in \mu_\ell$ implies that $z^{ae\ell} = 1$ so $q - 1 | ae\ell$ and, as $((q-1)/\ell, e) = 1$, $((q-1)\ell)|a$. Thus, $\bar{y}' = z^a$ has exponent ℓ. There is an algebra isomorphism, $\theta(\bar{y}')$, that takes

$$\langle F(\zeta_p)/F, \sigma_r, \bar{y}(\bar{y}')^e\rangle \to \langle F(\zeta_p)/F, \sigma_r, \bar{y}\rangle.$$

which fixes ζ_p and takes σ_r to $\sigma_r \bar{y}'$. The maps $\phi_1, \phi_2, \ldots, \phi_M$ are the maps of the form $\theta(\bar{y}')\phi(\bar{x}_i, \bar{y}(\bar{y}')^e)$. Note, the image of G under this map is $\langle \bar{x}_i, \sigma_r \bar{y}' \rangle$, which is contained in H, as $\bar{x}_i \in \mu_{p^\alpha}$ and $\bar{y}' \in \mu_\ell$ is a power of $\bar{y}$ and hence of σ_r. ∎

Remark. $\phi_i : G \to H$ will be an isomorphism if and only if $\phi(\bar{x}_i, \bar{y}(\bar{y}')^e)$ is injective on G. Using Corollary 6.6, we see that this happens $\phi(m)/e\phi(e)$ times, where ϕ is the Euler function.

THEOREM 6.8. *Let F be a local field with odd residue characteristic, p. Let $G \cong G_{m,r}$ be a nonabelian group. G embeds in a division algebra over F if and only if the following conditions are satisfied:*

(1) $m = p^\alpha \ell$ *where* $\alpha \geq 1$, ℓ *is prime to* p *and* $(r - 1, m) = \ell$,

(2) $o(r|m) | [F(\zeta_\ell, \zeta_p) : F(\zeta_\ell)]$,

(3) $q - 1 | r - 1$,

(4) $((q - 1)/\ell, o(r|m)) = 1$.

where q is the order of the residue field of $F(\zeta_m)$.

Proof. Proposition 6.2 gives (1) and (2). (3) is the statement that $F(A)/Z$ is totally ramified, in the notation of Proposition 6 part (8). Consequently (1), (2), and (3) are necessary conditions. Now, suppose (1), (2) and (3) hold. There is a map $\theta : \mathrm{Gal}(F(\zeta_m)/F(\zeta_\ell)) \to (\mathbb{Z}/m)^* \cong (\mathbb{Z}/\ell)^* \times (\mathbb{Z}/p^\alpha)^*$ given by $\theta(\sigma_s) = s \bmod m$ if $\sigma_s(\zeta_m) = \zeta_m^s$. $\mathrm{Im}(\theta) \subseteq (\mathbb{Z}/p^\alpha)^*$ which is cyclic and so has a unique subgroup of order $[F(\zeta_m) : F(\zeta_\ell)]$, consisting of those $s \bmod p^\alpha$ with $o(s|p^\alpha) | [F(\zeta_m) : F(\zeta_\ell)]$ and thus, by (1) and (2), $\sigma_r \in \mathrm{Gal}(F(\zeta_m)/F(\zeta_\ell))$. Now, let Z be the fixed field of σ_r in $F(\zeta_m)$. By (3), $F(\zeta_m)/Z$ is totally ramified. Also, $Z \subseteq Z(\zeta_p) \subseteq F(\zeta_m)$ and $[F(\zeta_m) : Z] = o(r|m)$ divides $p - 1$, by (2), while $[F(\zeta_m) : Z(\zeta_p)]$ is a power of p, thus, $Z(\zeta_p) = F(\zeta_m)$. It follows that Z satisfies the conditions on the coefficient field of Theorem 6.4. Part (1) and the proof of Proposition 6.2, part (7) show that $G \cong G(p^\alpha, r, \ell o(r|m), 0)$ is the group of Theorem 6.4. Now, G embeds in a division algebra over F if and only if it embeds in a division algebra over Z. By Corollary 6.5 and Corollary 6.6, this occurs if and only if (4) holds. ∎

COROLLARY 6.9. *If F is a local field with odd residue characteristic, p, and $G \cong G_{m,r}$ is nonabelian, then G embeds in $D(F, a/b)^*$ if and only if* (1) *through* (4) *of Theorem* 6.8 *hold and, in addition,*

(5) $b = [F(\zeta_m) : F]s$ *for some integer, s, prime to $e = o(r|m)$.*

If ϕ is an embedding of G in $D(F, a/b)^*$, then

$$F\phi G \cong D\left(Z, as^{-1}/e\right) \quad \text{and} \quad C_{D(F,a/b)}(\phi G) \cong D\left(Z, ae^{-1}/s\right),$$

where s^{-1} *denotes the inverse of* s mod e *and* e^{-1} *denotes the inverse of* e mod s.

Proof. Let Z be the fixed field of σ_r in $F(\zeta_m)$. Given (1)–(4), $Z[G]$ has $\phi(e)$ distinct division algebras as simple factors, namely $D(Z, c/e)$ where c is prime to e. G embeds in $D(F, a/b)^*$ if and only if one of these is a subalgebra of $D(F, a/b)$. We know that G embeds in the $D(Z, c/e)$ by Corollaries 6.5 and 6.6. The condition $Z \subseteq D(F, a/b)$ is equivalent to $b = [Z : F]s'$ for some integer, s'. Then, $\mathrm{Inv}_Z(C_{\{D(F,a/b)\}}(Z)) = a/s' \bmod \mathbb{Z}$ and so, by Proposition 2.5, $D(Z, c/e) \subseteq D(F, a/b)$ if and only if $s' = es$ where s is prime to e and $c \equiv as^{-1} \bmod e$, i.e., $b = e[Z : F]s = [F(\zeta_m) : F]s$. All that remains is to calculate $\mathrm{Inv}_Z(C_{D(F,a/b)}(\phi G))$ but this follows from Proposition 5.2 which gives us the identity,

$$\frac{a}{es} = \frac{as^{-1}}{e} + \mathrm{Inv}_Z\big(C_{D(F,a/b)}(\phi G)\big) \bmod \mathbb{Z}.$$

∎

The above two results give criteria, involving F, m, and r, to determine when a given metacyclic group, $G_{m,r}$, embeds in a division algebra over F. If $F/\hat{\mathbb{Q}}_p$ is unramified these conditions simplify further, in particular, for $F = \hat{\mathbb{Q}}_p$.

COROLLARY 6.10. *Let* $F/\hat{\mathbb{Q}}_p$ *be an unramified extension. Let* $G \cong G_{m,r}$ *be nonabelian.* G *embeds in* $D(F, a/b)^*$ *if and only if the following conditions are satisfied*:

(1) $m = p^\alpha \ell$ *where* $\alpha \geq 1$, ℓ *is prime to* p *and* $(r - 1, m) = \ell$,

(2) $o(r|m) | p - 1$,

(3) $q - 1 | r - 1$,

(4) $((q - 1)/\ell, o(r|m)) = 1$,

(5) $b = o(p^{[F:\hat{\mathbb{Q}}_p]}|\ell)\phi(p^\alpha)s$, *where* $(s, o(r|m)) = 1$.

$q = p^{[F:\hat{\mathbb{Q}}_p]o(p^{[F:\hat{\mathbb{Q}}_p]}|\ell)}$ *and* ϕ *is the Euler function.*

Proof. For any a we have:

$$\begin{array}{ccccc} \hat{\mathbb{Q}}_p(\zeta_{p^\alpha}) & \longrightarrow & F(\zeta_{p^\alpha}) & \longrightarrow & F(\zeta_\ell, \zeta_{p^\alpha}) \\ \uparrow & & \uparrow & & \uparrow \\ \hat{\mathbb{Q}}_p & \longrightarrow & F & \longrightarrow & F(\zeta_\ell) \end{array}$$

Now, $F/\hat{\mathbb{Q}}_p$ and $F(\zeta_\ell)/F$ are unramified and $\hat{\mathbb{Q}}_p(\zeta_{p^\alpha})/\hat{\mathbb{Q}}_p$ is totally ramified. It follows that the horizontal extensions are unramified and the

vertical ones are totally ramified, also $\hat{\mathbb{Q}}_p = F \cap \hat{\mathbb{Q}}_p(\zeta_{p^\alpha})$ and $F = F(\zeta_{p^\alpha}) \cap F(\zeta_\ell)$. $[F(\zeta_\ell) : F] = t$ where $t = \text{Min}\{t' : \ell | p^{[F:\hat{\mathbb{Q}}_p]t'} - 1\}$, i.e., $[F(\zeta_\ell) : F] = o(p^{[F:\hat{\mathbb{Q}}_p]} | \ell)$. From the diagram we also have $[F(\zeta_{p^\alpha}) : F] = [F(\zeta_\ell, \zeta_{p^\alpha}) : F(\zeta_\ell)] = \phi(p^\alpha)$. Thus, $[F(\zeta_\ell, \zeta_p) : F(\zeta_\ell)] = p - 1$, hence (2), and $[F(\zeta_m) : F(\zeta_\ell)] = \phi(p^\alpha)$, giving $[F(\zeta_m) : F] = o(p^{[F:\hat{\mathbb{Q}}_p]} | \ell)\phi(p^\alpha)$, hence (5). Finally, $q = p^{[F(\zeta_\ell):\hat{\mathbb{Q}}_p] = p[F:\hat{\mathbb{Q}}_p]o(p^{[F:\hat{\mathbb{Q}}_p]} | \ell)}$. ∎

PROPOSITION 6.11. *If F is a local field with odd residue characteristic, p, and $G \cong G_{m,r}$ is nonabelian then any two subgroups of $D(F, a/b)^*$ that are isomorphic to G are conjugate*

Proof. Let ϕ and ψ be embeddings of G in $D(F, a/b)^*$. From the proof of Corollary 6.9 we see that $F\phi G \cong F\psi G \cong D(Z, as^{-1}/e)$, where $b = [F(\zeta_m) : F]s$, $e = o(r|m)$ and $(s, e) = 1$. By the Noether–Skolem Theorem, we may assume that $F\phi G = F\psi G = C$. By Corollary 6.7, there are maps $\phi_1, \phi_2, \ldots, \phi_M$ of $G \to C^*$ with $\phi_i(G) \subseteq H$ for some subgroup H of C^*, isomorphic to G and the representations $R(\phi)$ and $R(\psi)$ (Definition 3.1) are among the representations $R(\phi_1), R(\phi_2), \ldots, R(\phi_M)$. By Proposition 3.5, ϕG and ψG are conjugate to H. ∎

Remark. From the remark after Corollary 6.7 we see that, although isomorphic subgroups are conjugate, there are $\phi(m)/e\phi(e)$ nonconjugate embeddings of such a G.

The preceding results enable us to determine when a particular group embeds in a particular division algebra. Next we look at determining which division algebras contain nonabelian groups. In view of Corollary 5.4 we show:

THEOREM 6.12. *For a p-adic field, F, and a positive integer, b, the integers, m, that satisfy*:

(1′) $[F(\zeta_m) : F] = b$,

(2′) $p|m$,

(3′) $\mu(F(\zeta_m)) = \langle \zeta_m \rangle$.

are those of the form,

$$m = m(F, b, \alpha) = p^\alpha\left(p^{k\gamma p^{n+\beta(F)-\alpha}} - 1\right),$$

where $\beta(F)$, n, k, γ and α are defined by the following:

(1) $\beta(F) = \text{Max}\{\beta : \zeta_{p^\beta} \in F(\zeta_p)\}$,

(2) $b = p^n[F(\zeta_p) : F]k$ where $(k, p) = 1$,

(3) $\beta(F) \leq \alpha \leq \beta(F) + n$,

(4) $\gamma = \gamma(F, \alpha)$ *is the relative degree,* $f(F(\zeta_{p^\alpha})/\hat{\mathbb{Q}}_p)$,

(5) $F(\zeta_{p^{\alpha+1}})/F(\zeta_{p^\alpha})$ *is totally ramified or* $\alpha = \beta(F) + n$.

Proof. Suppose m satisfies (1'), (2') and (3'). Let $m = p^\alpha \ell$ where $(\ell, p) = 1$. We have the following diagram:

$$\begin{array}{ccccc} F & \longrightarrow & F(\zeta_p) & \longrightarrow & F(\zeta_{p^\alpha}) \\ & & \uparrow & & \uparrow \\ \hat{\mathbb{Q}}_p(\zeta_p) & \longrightarrow & F(\zeta_p) \cap \hat{\mathbb{Q}}_p(\zeta_{p^\alpha}) & \longrightarrow & \hat{\mathbb{Q}}(\zeta_{p^\alpha}) \end{array}$$

Now, $\mathrm{Gal}(\hat{\mathbb{Q}}_p(\zeta_{p^\alpha})/\hat{\mathbb{Q}}_p(\zeta_p)) \cong \mathbb{Z}/p^{\alpha-1}$ and the intermediate field extensions are

$$\hat{\mathbb{Q}}_p(\zeta_p) \subseteq \hat{\mathbb{Q}}_p(\zeta_{p^2}) \subseteq \cdots \subseteq \hat{\mathbb{Q}}_p(\zeta_{p^{\alpha-1}}) \subseteq \hat{\mathbb{Q}}_p(\zeta_{p^\alpha}).$$

(2'), (3') and (1) imply that $\alpha \geq \beta(F)$ so, $F(\zeta_p) \cap \hat{\mathbb{Q}}(\zeta_{p^\alpha}) = \hat{\mathbb{Q}}_p(\zeta_{p^{\beta(F)}})$ and so $[F(\zeta_{p^\alpha}) : F] = p^{\alpha-\beta(F)}[F(\zeta_p) : F]$. The residue field $\overline{F(\zeta_{p^\alpha})}$ is $\mathbb{F}_{p^\gamma}$. Also, $F(\zeta_m)/F(\zeta_{p^\alpha})$ is unramified and so $[\overline{F(\zeta_m)} : \mathbb{F}p^\gamma] = [F(\zeta_m) : F(\zeta_{p^\alpha})]$ giving $\overline{F(\zeta_m)} = \mathbb{F}_{p^{\gamma b/[F(\zeta_{p^\alpha}):F]}}$ By (3'), $\ell = |\overline{F(\zeta_m)}| - 1$ so, as

$$\begin{aligned} \frac{\gamma b}{[F(\zeta_{p^\alpha}) : F]} &= \frac{\gamma p^n [F(\zeta_p) : F] k}{p^{\alpha-\beta(F)}[F(\zeta_p) : F]} \\ &= \gamma k p^{n+\beta(F)-\alpha}, \end{aligned}$$

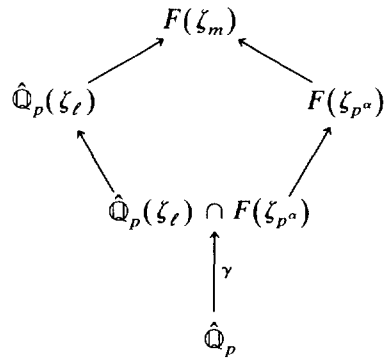
we get $m = m(F, b, \alpha)$. Also $\gamma[\overline{F(\zeta_m)} : \mathbb{F}_p] = \gamma k p^{n+\beta(F)-\alpha}$ and $(k, p) = 1$ so $\alpha \leq n + \beta(F)$. Suppose that $\alpha < n + \beta(F)$. The formula $[F(\zeta_{p^\alpha}) : F] = p^{\alpha-\beta(F)}[F(\zeta_p) : F]$ implies that $[F(\zeta_{p^{\alpha+1}}) : F(\zeta_{p^\alpha})] = p$ so this extension is either unramified or totally ramified. Suppose it were unramified, then we have $F(\zeta_{p^{\alpha+1}})p = F(\zeta_{p^\alpha}, \zeta_t)$ where $(t, p) = 1$ and $\mathbb{F}_{p^{\gamma p}} = \mathbb{F}_{p^\gamma}(\zeta_t)$. As $\alpha < \beta(F) + n$, p divides $[F(\zeta_m) : F(\zeta_{p^\alpha})] = kp^{n+\beta(F)-\alpha}$ so $\mathbb{F}_{p^{\gamma p}} \subseteq \overline{F(\zeta_m)}$ and so $\zeta_t \in F(\zeta_m)$ thus $F(\zeta_{p^{\alpha+1}})p \subseteq F(\zeta_m)$ which contradicts (3'). Thus we conclude that, if $\alpha < \beta(F) + n$, then $F(\zeta_{p^{\alpha+1}})/F(\zeta_{p^\alpha})$ is totally ramified. This completes the proof that m has the form described.

Conversely, let $m = m(F, b, \alpha)$ where α, n, $\beta(F)$, k and γ are as in the statement of the theorem. By definition $\beta(F) \geq 1$ so $\alpha \geq 1$ and so $p|m$ proving (2').

Now, $\beta(F)$ and γ are defined in such a way that

$$\begin{aligned} [F(\zeta_{p^\alpha}) : F] &= p^{\alpha-\beta(F)}[F(\zeta_p) : F] \\ \overline{F(\zeta_{p^\alpha})} &= \mathbb{F}_{p^\gamma}. \end{aligned}$$

We have the following diagram:



$$\begin{aligned}\left[F(\zeta_m):F(\zeta_{p^\alpha})\right] &= \left[\hat{\mathbb{Q}}_p(\zeta_\ell):\hat{\mathbb{Q}}_p(\zeta_\ell)\cap F(\zeta_{p^\alpha})\right]\\ &= \left[\hat{\mathbb{Q}}_p(\zeta_\ell):\hat{\mathbb{Q}}_p\right]/\gamma\\ &= kp^{n+\beta(F)-\alpha},\end{aligned}$$

and so

$$\begin{aligned}\left[F(\zeta_m):F\right] &= \left[F(\zeta_m):F(\zeta_{p^\alpha})\right]\left[F(\zeta_{p^\alpha}):F\right]\\ &= kp^{n+\beta(F)-\alpha}.p^{\alpha-\beta(F)}\left[F(\zeta_p):F\right]\\ &= p^n\left[F(\zeta_p):F\right]k\\ &= b.\end{aligned}$$

This proves (1'). In the diagram above, the extension $\hat{\mathbb{Q}}_p(\zeta_\ell)/\hat{\mathbb{Q}}_p$ is unramified and $F(\zeta_{p^\alpha})/\hat{\mathbb{Q}}_p(\zeta_\ell)\cap F(\zeta_{p^\alpha})$ is totally ramified, as $|\overline{F(\zeta_{p^\alpha})}|-1$ divides ℓ. It follows that $F(\zeta_m)/\hat{\mathbb{Q}}_p(\zeta_\ell)$ is totally ramified and thus

$$\overline{F(\zeta_m)} = \overline{\hat{\mathbb{Q}}_p(\zeta_\ell)} = \mathbb{F}_{p^{\gamma kp^{n+\beta(F)-\alpha}}}.$$

We conclude that the p' parts of $\langle\zeta_m\rangle$ and $\mu(F(\zeta_m))$ coincide. To prove (3') all we need to show is that $\zeta_{p^{\alpha+1}}$ is not in $F(\zeta_m)$. If it were, we would have $F(\zeta_{p^\alpha})\subseteq F(\zeta_{p^{\alpha+1}})\subseteq F(\zeta_m)$ which would imply that $F(\zeta_{p^{\alpha+1}})/F(\zeta_{p^\alpha})$ were unramified, contrary to the assumption of the theorem, unless $\alpha = \beta(F)+n$. In this case we would, however, have $[F(\zeta_{p^{\alpha+1}}):F(\zeta_{p^\alpha})]\,|\,[F(\zeta_m):F(\zeta_{p^\alpha})]$ so $p\,|\,kp^{n+\beta(F)-\alpha}$ and so $p\,|\,k$. This is also a contradiction. ∎

Remark. The condition that $F(\zeta_{p^{\alpha+1}})/F(\zeta_{p^\alpha})$ is totally ramified can be characterized in terms of the function $\gamma = \gamma(F,\alpha) = f(F(\zeta_{p^\alpha})/\hat{\mathbb{Q}}_p)$. It satisfies

$$\gamma(F,\alpha+1) = \gamma(F,\alpha)p^{\epsilon(F,\alpha)},$$

where $\epsilon(F,\alpha) = 0$ or 1. $\epsilon(F,\alpha) = 0$ if and only if $F(\zeta_{p^{\alpha+1}})/F(\zeta_{p^\alpha})$ is totally ramified. $\gamma(F,\alpha) = f(F(\zeta_{p^\alpha})/\hat{\mathbb{Q}}_p(\zeta_{p^\alpha}))$ which divides $[F:\hat{\mathbb{Q}}_p]$ and so $\gamma(F,\alpha)$ is constant for large α. Now

$$\frac{\gamma(F,\alpha)}{\gamma(F,\beta(F))}\,\Bigg|\,\frac{[F:\hat{\mathbb{Q}}_p]}{f(F/\hat{\mathbb{Q}}_p)} = e(F/\hat{\mathbb{Q}}_p),$$

thus, if $e(F/\hat{\mathbb{Q}}_p)$ is prime to p, every α such that $\beta(F) \le \alpha \le \beta(F)+n$ gives $m(F,b,\alpha)$ satisfying the conditions of Theorem 6.12. In particular, this holds for $F = \hat{\mathbb{Q}}_p$.

PROPOSITION 6.13. *If $m = m(F,b,\alpha)$, as above, then there is a unique subfield K such that $F \cap K \cap F(\zeta_m)$ and K is minimal subject to the conditions*:

(1) *$F(\zeta_m)/K$ is totally ramified,*

(2) *$[F(\zeta_m):K] \mid p-1$.*

The extension $F(\zeta_m)/K$ is cyclic of degree e_F, where e_F is the ramification index, $e(F(\zeta_p)/F)$.

Proof. Now, $m = p^\alpha(p^c-1)$. Write $\ell = p^c - 1$. If $F(\zeta_m)/K$ is totally ramified then $\zeta_\ell \in K$. $F(\zeta_m) = F(\zeta_\ell,\zeta_{p^\alpha})$ so $\mathrm{Gal}(F(\zeta_m)/F(\zeta_\ell))$ maps injectively by restriction to $\mathrm{Gal}(\hat{\mathbb{Q}}_p(\zeta_{p^\alpha})/\hat{\mathbb{Q}}_p)$ which is isomorphic to $\mathbb{Z}/p^{\alpha-1}(p-1)$. This has a unique subgroup of exponent $p-1$ which is cyclic of order $p-1$. It follows that $\mathrm{Gal}(F(\zeta_m)/F(\zeta_\ell))$ has a unique maximal subgroup of order dividing $p-1$. The fixed field of this group is K. $[F(\zeta_m):K]$ is the p' part of $[F(\zeta_m):F(\zeta_\ell)]$.

It remains to prove that $[F(\zeta_m):K] = e_F$. We let $\bar{F} = \mathbb{F}_{p^\tau}$, $\overline{F(\zeta_p)} = \mathbb{F}_{p^{\tau\rho}}$, $\overline{F(\zeta_{p^\alpha})} = \mathbb{F}_{p^{\tau\rho\pi}}$ so $\gamma = \tau\rho\pi$ and $\overline{F(\zeta_\ell)} = \mathbb{F}_{p^{\tau\rho\pi kp^{\beta(F)+n-\alpha}}}$. It follows that

$$[F(\zeta_p,\zeta_\ell):F(\zeta_p)] = \pi k p^{\beta(F)+n-\alpha}$$

and, as $[F(\zeta_p):F] = \rho e_F$, we get

$$[F(\zeta_p,\zeta_\ell):F] = \rho e_F \pi k p^{\beta(F)+n-\alpha}.$$

Now, $[F(\zeta_\ell):F] = \rho\pi k p^{\beta(F)+n-\alpha}$ and thus $[F(\zeta_p,\zeta_\ell):F(\zeta_\ell)] = e_F$. From

the diagram

$$\begin{array}{ccccccc} & & F(\zeta_\ell) & \longrightarrow & F(\zeta_p,\zeta_\ell) & \longrightarrow & F(\zeta_m) \\ & & \uparrow & & \uparrow & & \uparrow \\ \hat{\mathbb{Q}}_p & \longrightarrow & F(\zeta_\ell)\cap\hat{\mathbb{Q}}_p(\zeta_{p^\alpha}) & \longrightarrow & F(\zeta_p,\zeta_\ell)\cap\hat{\mathbb{Q}}_p(\zeta_{p^\alpha}) & \longrightarrow & \hat{\mathbb{Q}}_p(\zeta_{p^\alpha}) \end{array}$$

we see that $[F(\zeta_m):\zeta_\ell]$ is a power of p and so, indeed, e_F is the p' part of $[F(\zeta_m):F(\zeta_\ell)]$. ∎

DEFINITION 6.14. Let $m = m(F, b, \alpha)$ satisfy the conditions of 6.12, let $r_m \in (\mathbb{Z}/m)^*$ be such that $\sigma_{r_m}(\zeta_m) = \zeta_m^{r_m}$ is a generator of $\mathrm{Gal}(F(\zeta_m)/K)$ where K is the field described in Proposition 6.13. Define $G_\alpha = G_{m,r_m}$.

Note. By Proposition 4.9, G_α is independent of the choice of generator, r_m.

Note. If a_p is an integer such that the residue of a_p mod p generates $(\mathbb{Z}/p)^*$, then $a_p^{p^{\alpha-1}}$ represents an element of order $p-1$ in $(\mathbb{Z}/p^\alpha)^*$ and so $a_p^{p^{\alpha-1}(p-1)/e_F}$ represents an element of order e_F. We may take r_m to be the solution of the congruences

$$r_m \equiv 1 \bmod \left(p^{k\gamma p^{n+\beta(F)-\alpha}} - 1\right)$$

$$r_m \equiv a_p^{p^{\alpha-1}(p-1)/e_F} \bmod p^\alpha.$$

COROLLARY 6.15. *G_α is abelian if and only if $F(\zeta_p)/F$ is unramified.*

Proof. Let $m = m(F, b, \alpha)$ as in 6.1.

$$G_\alpha \text{ is cyclic} \iff e_F = 1 \iff F(\zeta_p)/F \text{ is unramified.}$$

∎

PROPOSITION 6.16. *If α satisfies the conditions of Theorem 6.12 then G_α embeds in $D(F, a/b)^*$.*

Proof. Let $m = m(F, b, \alpha) = p^\alpha(p^c - 1)$. Let Z be the fixed field of σ_{r_m} in $F(\zeta_m)$. Then $F(\zeta_m)/Z$ is totally ramified of degree e_F. By Proposition 6.3, we have an isomorphism,

$$\mu_{p^c-1}/(\mu_{p^c-1})^{e_F} \to Z^*/N(F(\zeta_m)^*).$$

Now, $[F(\zeta_m):F] = b$ so $F(\zeta_m)$ is a subfield of $D(F, a/b)$ and we consider $D' = C_{D(F,a/b)}(Z)$.

$$\mathrm{Inv}_Z D' = a[Z:F]/b \bmod \mathbb{Z},$$

but then $\mathrm{Deg}(D') = [F(\zeta_m):Z]$. It follows that $F(\zeta_m)$ is a strictly maximal subfield of D', so D' can be written as a cyclic algebra $\langle F(\zeta_m), \sigma_{r_m}, \eta\rangle$. By the isomorphism above we know that we can chose η to be a root of unity. With this choice we consider the group $\langle \zeta_m, \sigma_{r_m}\rangle$. This is metacyclic of the form $G(m, r_m, o(r_m|m), t)$. By Theorem 4.10, this is isomorphic to $G_{m,r_m} = G_\alpha$. ∎

Remark. Alternatively we could simply observe that conditions (1)–(5) of Theorem 6.8 and Corollary 6.9 hold.

THEOREM 6.17. *$D(F, a/b)^*$ contains nonabelian finite subgroups if and only if $F(\zeta_p)/F$ is ramified and $[F(\zeta_p):F]|b$. If e_F is the ramification index of $F(\zeta_p)/F$ then the isomorphism classes of the maximal such subgroups are exactly represented by the groups, G_α, of Definition 6.3. These have order*

$$|G_\alpha| = p^\alpha\left(p^{\gamma k p^{\beta(F)+n-\alpha}} - 1\right)e_F,$$

where $k, n, \beta(F), \gamma$ and α are as per Theorem 6.12. The number of such groups is

$$1 + \mathrm{Log}_p e\left(F(\zeta_{p^{\beta(F)+n}})/F(\zeta_p)\right).$$

Proof. Let $D = D(F, a/b)$. If $F(\zeta_p)/F$ is ramified then $e_F > 1$ so the groups G_α are nonabelian, by Corollary 6.15, and, by Proposition 6.16, there is a subgroup, G_α, in D^*, if $[F(\zeta_p):F]|b$. Conversely, suppose $G \cong G_{m',r'}$ is a finite, nonabelian, metacyclic subgroup of D^*, then, by Proposition 6.2, $p|m'$ and so $[F(\zeta_p):F]|b$. G is contained in a maximal, finite, metacyclic subgroup, $H \cong G_{m,r}$. By Corollary 5.4 and Theorem 6.12, we have $m = m_\alpha$ for some α. By Yamada, [10, Th. 4.7], $o(r|m)|p-1$. By Theorem 5.1, Proposition 6.13, and Definition 6.14, we get $\langle r\rangle \subseteq \langle r_m\rangle \subseteq (\mathbb{Z}/m)^*$. It follows that $o(r|m)|e_F$ and so $e_F > 1$ and thus $F(\zeta_p)/F$ is ramified. This proves the first claim of the theorem.

Suppose we show that every nonabelian, finite subgroup of D^* is contained in a larger subgroup that is isomorphic to G_α for some α, then we are done, as no G_α embeds in $G_{\alpha'}$ unless $\alpha = \alpha'$. If it did we would have $m(b, F, \alpha)|m(b, F, \alpha')$ and then, by (1′) and (3′) of Theorem 6.12, $\alpha = \alpha'$. We have seen above that any finite subgroup, G, is contained in a maximal, metacyclic subgroup, H, and that $H \cong G_{m,r^s}$, where $m = m_\alpha$, $r = r_m$ and $s|e_F$. By Proposition 6.16, we have $G_\alpha \subseteq D^*$ and this has a

subgroup, K, isomorphic to H, by Proposition 4.11. However, H and K are isomorphic and so, by Proposition 6.11, are conjugate in D^*. It then follows by maximality of H that $H \cong G_\alpha$ and we are done. ∎

COROLLARY 6.18. *If p is odd then $D(\hat{\mathbb{Q}}_p, a/b)^*$ has noncyclic subgroups if and only if $b = p^n(p-1)k$ for $(k,p) = 1$. The isomorphism classes of maximal, noncyclic subgroups are represented by the groups G_α, where*

$$m(F,b,\alpha) = p^\alpha\left(p^{kp^{n+1-\alpha}} - 1\right),$$

$$|G_\alpha| = p^\alpha\left(p^{kp^{n+1-\alpha}} - 1\right)(p-1)$$

for $\alpha = 1, 2, \cdots n+1$.

Proof. This is an immediate consequence of Theorem 6.17 and the remark preceding 6.13 given that, for $F = \hat{\mathbb{Q}}_p$, $\beta(F) = 1$, $[F(\zeta_p): F] = p-1$ and $e_F = p-1$. ∎

Now we look for subgroups of odd order in G_α. In fact, using Proposition 6.2, it is not difficult to see that any $G_{m,r} \subseteq D(F, a/b)^*$ has a unique largest odd order subgroup. This is nonabelian if and only if $o(r|m)$ is not a power of 2. In the notation of 6.2, we let $\ell = 2^a\ell'$ and $n = 2^b n'$, where ℓ' and n' are odd. Then B has order $2^{a+b}\ell' n'$ and, if $C = B^{2^{a+b}}$, then $H = \langle A^\ell, C\rangle$ is a normal subgroup with odd order, $|H| = p^\alpha \ell' n'$, such that the quotient has order 2^{a+b}. It follows that H contains all subgroups off $G_{m,r}$ of odd order. H is abelian if and only if $1 = [C, A^\ell] = A^{\ell(r^{2^{a+b}}-1)}$. That is, if $p^\alpha | r^{2^{a+b}} - 1$, or, if $o(r|p^\alpha)|2^{a+b}$. Now, $r \equiv 1 \bmod \ell$ so $o(r|p^\alpha) = o(r|m) = n$. It follows that H is abelian if and only of $o(r|m)$ is a power of 2.

We will say that Herstein's conjecture holds for a field F if every central division algebra, D, over F has the property that all its subgroups of odd order are cyclic.

THEOREM 6.19. *If F is a local field with odd residue characteristic, p, then Herstein's conjecture holds for F if and only if the ramification index, $e(F(\zeta_p)/F)$, is a power of 2.*

Proof. This follows from the remarks above and 6.17. ∎

In their paper, Fein and Schacher [5] prove the following which follows from the above.

COROLLARY 6.20. *If p is a Fermat prime then the Herstein conjecture holds for any p-adic field F.*

Proof. $e_F | p-1$ which is a power of 2. ∎

In fact, we get:

COROLLARY 6.21. *Herstein's conjecture holds for* $\hat{\mathbb{Q}}_p$, *p odd, if and only if p is a Fermat prime.*

Proof. $e_{\hat{\mathbb{Q}}_p} = p - 1$. ∎

PROPOSITION 6.22. *If F is a local field with odd residue characteristic, p, and p is a Fermat prime, i.e.,* $p = 2^{2^n} + 1$ *for some n, then* 2^{2^n+1} *divides the order of any nonabelian subgroup of* $D(F, a/b)^*$.

Proof. Let $G \cong G_{m,r}$ be such a subgroup. Then, by Theorem 6.8, $o(r|m)|p - 1$, so $o(r|m)$ is even. $((q-1)/\ell, o(r|m)) = 1$ so $(q-1)/\ell$ is odd and, as $q - 1 = (2^{2^n} + 1)^\gamma - 1$ for some γ, we have $2^{2^n}|q - 1$ and thus $2^{2^n}|\ell$ giving $2^{2^n+1}|\ |G|$. ∎

This result is sharp in the sense that:

PROPOSITION 6.23. *If* $p = 2^{2^n} + 1$ *is a Fermat prime, then there is a nonabelian subgroup, G, of order* $p2^{2^n+1}$ *that embeds in a central division algebra over* $\hat{\mathbb{Q}}_p$.

Proof. Let $m = p.2^{2^n}$ and let r be the solution, mod m, to the congruences $r \equiv 1 \bmod 2^{2^n}$ and $r \equiv -1 \bmod p$. Let $b = 2^{2^n}s$, where s is odd. It is easy to check that $G_{m,r}$ satisfies the conditions of Corollary 6.10 and so embeds in $D(\hat{\mathbb{Q}}_p, a/b)^*$, for any a prime to b. ∎

Theorem 6.17 and Theorem 4.12 enable us to write down all the finite subgroups of a specified division algebra and Theorem 6.1 enables us to determine when two such groups are isomorphic.

EXAMPLE. Using Corollary 6.18 and Theorem 4.12 we may show, for example, that, if a is prime to 6, then the isomorphism classes of nonabelian subgroups of $D(\hat{\mathbb{Q}}_3, a/36)^*$ are:

(1) $G_{\ell,2.3^{18}-1}$ where $24|\ell$ and $\ell|3(3^{18} - 1)$.

(2) $G_{\ell,2.3^6-1}$ where $24|\ell$ and $\ell|3^2(3^6 - 1)$.

(3) $G_{\ell,11.3^2-10}$ where $24|\ell$ and $\ell|3^3(3^2 - 1)$.

Two such groups are isomorphic exactly when they have the same order.

EXAMPLE. Amitsur [1] proves that the smallest noncyclic group of odd order to embed in a division algebra has order 63 and is unique up to isomorphism. This group occurs in the simplest possible case. The smallest odd prime that is not a Fermat prime is 7. The index of any division algebra over $\hat{\mathbb{Q}}_7$ that contains a noncyclic subgroup is at least 6, (Corollary 6.18). $D(\hat{\mathbb{Q}}_7, 1/6)$ contains a maximal subgroup isomorphic to $G_{42,19}$.

Taking $\ell = 21$ and $s = 2$ in Theorem 4.12, we see that $G_{21,4} \subseteq G_{42,19}$. $G_{21,4}$ is the desired group of order 63.

7. Maximal Subgroups in the Case $p = 2$

Finally, we consider the case $p = 2$. Let F be a local field with residue characteristic equal to 2. In addition to the metacyclic groups, we need to consider the products of binary tetrahedral and metacyclic groups as described in Proposition 2.6. First, we consider which groups $G \cong T \times G_{m,r}$ can embed in a division algebra, D, over F. Certainly $|G_{m,r}|$ must be prime 2 and 3, otherwise, as $|T| = 2^3.3$, we get $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$ embedded in a division algebra. This is impossible. Since $|G_{m,r}| = m.o(r|m)$, m must be odd. Suppose ϕ: $T \times G_{m,r} \hookrightarrow D^*$. We have $\hat{\mathbb{Q}}_2 \phi G_{m,r} = \langle \hat{\mathbb{Q}}_2(\zeta_m), \sigma_r, \zeta_m^t \rangle$ which splits, if m is odd. This cannot be, unless $r \equiv 1 \bmod m$, so $G_{m,r} \cong \mathbb{Z}/m$. We must also have $D = D(F, a/2k)$, where k and $[F : \hat{\mathbb{Q}}_2]$ are odd (by Case 1 after Proposition 2.5);

$$D = D(F, a/2k) \cong D(F, 1/2) \underset{F}{\otimes} C_D(T)$$

and $\mathbb{Z}/m$ embeds in the second factor which has index k. It follows that $[F(\zeta_m) : F] | k$ and so $[F(\zeta_m) : \hat{\mathbb{Q}}_2]$ is odd. If, on the other hand, m and $[F(\zeta_m) : \hat{\mathbb{Q}}_2]$ are odd, then

$$\begin{pmatrix} -1, -1 \\ F(\zeta_m) \end{pmatrix}$$

is a division algebra and the group $\langle i, j, -(1 + i + j + k)/2, \zeta_m \rangle$ is isomorphic to $T \times \mathbb{Z}/m$. This lets us state:

Theorem 7.1. *If $p = 2$ then $T \times G_{m,r}$ embeds in a division algebra over F if and only if*:

(1) $G_{m,r} \cong \mathbb{Z}/m$,

(2) *m is odd*,

(3) $[F(\zeta_m) : \hat{\mathbb{Q}}_2]$ *is odd*.

Proof. This follows from the remarks above. ∎

Proposition 7.2. *T is not metacyclic and hence $T \times \mathbb{Z}/m$ does not embed in a metacyclic group.*

Proof. If T were metacyclic it would have a cyclic commutator subgroup, by Proposition 4.6. With P, Q and R as per Definition 2.1 part (2),

we have, $[R, Q] = P, [R, P] = QP^3$, so $\langle Q, P\rangle \subseteq T'$ and so T' is not even abelian. ∎

THEOREM 7.3. *If $[F:\hat{\mathbb{Q}}_2]$ is odd and $b = 2k$ where k is odd, then the maximal subgroups of $D(F, a/b)^*$ that contain a binary tetrahedral group are isomorphic to $T \times \mathbb{Z}/q^k - 1$ where the residue field of F is $\mathbb{F}_q$.*

Proof. A maximal group of this type can be written as $G = T \otimes \langle \zeta_m\rangle$ where $\langle \zeta_m\rangle \cong \mathbb{Z}/m$ is a maximal cyclic subgroup of $C_{D(F,a/b)}(T)$. $D(F, a/b) \cong FT \otimes C_{D(F,a/b)}(T)$ and so the latter factor has exponent, k. $[\hat{\mathbb{Q}}_2(\zeta_4):\hat{\mathbb{Q}}_2] = 2$ and $[F:\hat{\mathbb{Q}}_2]$ is odd so $\zeta_4 \notin F$ and $[F(\zeta_4), F] = 2$ which is prime to k and thus $\zeta_4 \notin C_{D(F,a/b)}(T)$. Now, $2|m$ as $-1 \in \hat{\mathbb{Q}}_2$ and $\langle \zeta_m\rangle$ is maximal. It follows that m has the form $m = 2n$ where n is odd. As $C_{D(F,a/b)}(T)$ has exponent, k, the maximal value of n is $q^k - 1$. Thus $G = T \otimes \mathbb{Z}/2(q^k - 1)$. But, if H and K are subgroups of F algebras A and B, then $H \otimes_F K \subseteq A \otimes_F B$ is a subgroup and we have an exact sequence

$$0 \to N \to H \times K \to H \underset{F}{\otimes} K \to 0,$$

where $N = \{(f, f^{-1}): f \in H \cap F \text{ and } f^{-1} \in K \cap F\}$. Now, $T \cap F = \{\pm 1\}$ and so we have

$$0 \to \{(1,1), (-1,-1)\} \to T \times \mathbb{Z}/2 \cdot (q^k - 1) \to$$

$$T \otimes \mathbb{Z}/2 \cdot (q^k - 1) \to 0.$$

By counting, $G \cong T \times \mathbb{Z}/q^k - 1$. ∎

PROPOSITION 7.4. *Let $G \subseteq D(F, a/b)^*$* be nonabelian and $G \cong G_{m,r}$ then

(1) *$m = 2^\alpha \ell$ where $\alpha \geq 2$ and ℓ is odd,*

(2) *$G \cong Q_\alpha \times \mathbb{Z}/\ell$, where Q_α is the generalized quaternion group of order $2^{\alpha+1}$.*

Proof. If m is odd or 2 mod 4, then $F(\zeta_m)/F$ is unramified and so FG splits. This would imply that G is abelian. Consequently, $\alpha \geq 2$. By Theorem 5.1, $\ell | r - 1$ and thus, by Proposition 4.6, G has a central, cyclic subgroup, H, of order ℓ. By Yamada [10, Thm. 5.15], Deg $(FG) = 2$, and so $|G| = 2^{\alpha+1}\ell$. G is then a product of H and its 2-Sylow subgroup. By [1, Th. 2 part (2B)], we get (2). ∎

COROLLARY 7.5. *$D(F, a/b)^*$ contains nonabelian finite subgroups if and only if $[F:\hat{\mathbb{Q}}_2]$ is odd and $b = 2k$, where k is odd.*

Proof. By Proposition 7.4 and the observation that $Q_2 \subseteq T$, we see that $D(F, a/b)^*$ contains nonabelian finite subgroups if and only if it contains Q_2, or equivalently, $\langle F(\zeta_4)/F, \sigma_{-1}, -1\rangle$. This is a division algebra if and only if $[F, \hat{\mathbb{Q}}_2]$ is odd, and embeds in $D(F, a/b)^*$ if and only if $b = 2k$, for k odd. ∎

COROLLARY 7.6. *If Q_α is a subgroup of $D(F, a/b)^*$ then $\alpha = 2$.*

Proof. Let $Z = Z(FQ_\alpha)$. Now, $Q_\alpha \cong G_{2^\alpha, -1}$ and so $FQ_\alpha \cong \langle F(\zeta_{2^\alpha})/Z, \sigma_{-1}, -1\rangle$, but then, by Corollary 7.5, $[Z : \hat{\mathbb{Q}}_2]$ is odd and so $e(F(\zeta_{2^\alpha})/\hat{\mathbb{Q}}_2) \equiv 2 \mod 4$. However, $e(\hat{\mathbb{Q}}_2(\zeta_{2^\alpha})/\hat{\mathbb{Q}}_2) = 2^{\alpha-1}$ giving $\alpha = 2$. ∎

We know, however, that $Q_2 \subseteq \langle F(\zeta_4), \sigma_{-1}, -1\rangle$ is contained in a binary tetrahedral group and so we get:

THEOREM 7.7. *$D(F, a/b)^*$ contains nonabelian finite subgroups if and only if $[F : \hat{\mathbb{Q}}_2]$ is odd and $b = 2k$, where k is odd. The maximal such groups are isomorphic to $T \times \mathbb{Z}/q^k - 1$ where q is the cardinality of the residue field of F. Any two such groups are conjugate.*

Proof. All that remains is to show the final statement. This follows by the Noether–Skolem Theorem and the fact that for any $T \subseteq D(F, a/b)^*$ there is an isomorphism $\left(\begin{smallmatrix} -1 & -1 \\ F & \end{smallmatrix}\right) \to FT$ identifying $\langle i, j, -(1 + i + j + k)/2\rangle$ with T, Theorem 2.4 part (3). The cyclic factor comes from a choice of a maximal odd root of unity in the centralizer of T. All such cyclic groups are conjugate. ∎

COROLLARY 7.8. *$D(\hat{\mathbb{Q}}_2, a/b)^*$ has nonabelian, finite subgroups if and only if $b/2 = k$ is odd. The maximal such groups are isomorphic to $T \times \mathbb{Z}/2^k - 1$.*

Proof. Immediate. ∎

Finally we observe:

PROPOSITION 7.9. *Herstein's conjecture holds for all 2-adic fields, F.*

Proof. This follows from Corollary 7.6 and the observation that the groups $T \times \mathbb{Z}/q^k - 1$ have no noncyclic subgroups of odd order. ∎

REFERENCES

1. S. A. AMITSUR, Finite subgroups of division rings, *Trans. Amer. Math. Soc.* **80** (1955), 361–386.
2. F. R. BEYL, The Schur multiplicator of metacyclic groups, *Proc. Amer. Math. Soc.* **40** (1973), 413–418.

3. F. R. Beyl, The Schur multiplicators of metacyclic groups, (addendum) *Proc. Amer. Math. Soc.* **43** (1974), 251–252.
4. C. W. Curtis and I. Reiner, "Methods of Representation Theory with Applications to Finite Groups and Orders," Vol. I, Wiley, New York, (1981).
5. B. Fein and M. M. Schacher, Embedding finite groups in rational division algebras, II, *J. Algebra* **19** (1971), 131–139.
6. D. L. Johnson, "Presentations of Groups," Cambridge Univ. Press, Cambridge, 1976.
7. J. Neukirch, "Class Field Theory," Grundlehren 280, Springer-Verlag, New York/ Berlin, 1986.
8. R. S. Pierce, "Associative Algebras," Springer-Verlang Graduate Texts in Mathematics, Vol. 88, Springer-Verlag, New York/ Berlin, (1982).
9. G. Vincent, Les Groupes Linéaires finis sans points fixes, *Comment. Math. Helv.* **20** (1947).
10. T. Yamada, "The Schur Subgroup of the Brauer Group," Lecture Notes in Mathematics, Vol. 397, Springer-Verlag, New York/ Berlin, 1974.
11. H. J. Zassenhaus, "The Theory of Groups," Chelsea, New York, 1974.