Mathematical Research Letters **6**, 271–286 (1999)

NORMALIZERS OF FINITE SUBGROUPS OF DIVISION ALGEBRAS OVER LOCAL FIELDS

Thomas Hewett

1. Introduction

The subject of finite subgroups of finite dimensional division algebras has been examined by many people. In [A], Amitsur proved a classification theorem describing the isomorphism type of finite groups which embed in division algebras. Yamada, [Y], computed the subgroup of the Brauer group that consists of division algebras spanned by a finite subgroup, the so called Schur algebras. In [H] we considered the problem of classifying the groups embedded in a specified division algebra over a local field, F, with Hasse invariant $a/b + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. The purpose of this analysis is to examine the normalizers of such groups.

Throughout this paper a local field will be assumed to have characteristic zero and finite residue field. In sections 1 to 4 the residue characteristic, p, is odd and in section 5 it is 2. In sections 1 to 5 we consider non-abelian subgroups and in section 6 we treat the cyclic groups.

Let F be a local field. It is well known that the finite dimensional division algebras with center F are given by the cyclic algebras

$$\langle K/F, \sigma, a\rangle = K \oplus K u_\sigma \oplus \cdots \oplus K u_\sigma^{n-1},$$

where $\mathrm{Gal}(K/F) \cong \mathbb{Z}_n$ is generated by σ, and the multiplication is determined by the relations $u_\sigma^n = a \in F$ and $u_\sigma^{-1} k u_\sigma = k^\sigma$ where $k \in K$. The Hasse invariant, $\mathrm{Inv}_F : B(F) \longrightarrow \mathbb{Q}/\mathbb{Z}$ is an isomorphism and we denote by $D(F, a/b)$ the division algebra in the Brauer class $\mathrm{Inv}_F^{-1}(a/b + \mathbb{Z})$. This is given explicitly as follows,

$$D(F, a/b) = \langle F_b/F, \sigma, \pi^a\rangle,$$

where $a/b \in \mathbb{Q}/\mathbb{Z}$ is reduced, i.e., $0 \leq a < b$ and $(a, b) = 1$, F_b is the unique unramified extension of F of degree b, π is a uniformizing parameter in F and σ is the Frobenius automorphism of F_b/F. Division algebras of this type arise in various places in mathematics. For example as rings of isogenies of Abelian varieties or as endomorphisms of formal group laws. It is in the latter context

Received September 9, 1999.

that they appear in homotopy theory, where the group $S(b)$ of units in the maximal order of $D(\widehat{\mathbb{Q}}_p, 1/b)$ is the 'Morava stabilizer group'. The calculation of its cohomology with trivial, or certain twisted coefficients, is an important stage in the chromatic approach to understanding the stable homotopy of spheres.

The cohomology calculations have been performed by Henn [He] and Gorbunov-Siegel-Symonds [GSS] in the case of $S(2)$ at the prime 3 with trivial coefficients and by Symonds with twisted coefficients. Such computations for the full stabilizer group appear to be difficult in general. Hopkins and Miller have shown that the finite subgroups of $S(b)$ give rise to 'higher real K-theories' which may prove to be more tractable for the purposes of calculations. It was these ideas that initially motivated our study of the finite subgroups of division algebras over local fields. The finite subgroups of $D(F, a/b)^*$ are of a very restricted nature.

Definition 1.1. *The group, $G_{m,r}$, is defined by the presentation*

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

where $r \in \mathbb{Z}_m^*$ has order e and $t = m/(r-1, m)$.

Theorem 1.2. [H,1.1] *If F is a local field with odd residue characteristic, p, then all the non-abelian, 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) *$e | [F(\zeta_\ell, \zeta_p) : F(\zeta_\ell)]$.*
(3) *$q - 1 | r - 1$.*
(4) *$\left(\frac{q-1}{\ell}, e\right) = 1$.*

where 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 e.*

Proposition 1.3. [H,6.2] *If $G_{m,r}$ embeds in a division algebra $D(F, a/b)$, then it has a presentation as a semidirect product,*

$$G_{m,r} = \langle C, B : C^{p^\alpha} = 1, BCB^{-1} = C^r, B^{\ell e} = 1 \rangle,$$

where α, ℓ, r, e are as in the statement of 1.2*. The order of $G_{m,r}$ is $p^\alpha \ell e$. In addition, $G'_{m,r} =< C >\cong \mathbb{Z}_{p^\alpha}$, $Z(G_{m,r}) =< B^e >\cong \mathbb{Z}_\ell$ and e is the order of $r \in \mathbb{Z}_{p^\alpha}^*$.*

2. Automorphisms of $G_{m,r}$

In this section we calculate the groups $\mathrm{Aut}(K)$, $\mathrm{Inn}(A)$ and $\mathrm{Out}(K)$ where $K \cong G_{m,r}$ is a subgroup of some $D(F, a/b)^*$. We assume that the scalars m, r, e, α, q and ℓ have the meanings assigned in 1.1–1.3.

Lemma 2.1. *If $x \equiv 1 \mod e$, then $p^\alpha | \frac{1-r^{xe\ell}}{1-r^x}$.*

Proof. If $x \equiv 1 \mod e$ then $r^x \equiv r \mod p^\alpha$ so $1-r^x \equiv 1-r \mod p^\alpha$. However, p does not divide $1-r$ as $(r-1, p^\alpha \ell) = \ell$ and so $1-r^x$ is a unit in $\mathbb{Z}_{p^\alpha}$. As $1-r^{xe\ell} \equiv 1-r^{el} \equiv 0 \mod p^\alpha$, the lemma follows. □

Lemma 2.2. *$e|\ell$ and thus $\phi(e\ell) = e\phi(\ell)$, where ϕ is the Euler function.*

Proof. By 1.2 part (4), $(\frac{q-1}{\ell}, e) = 1$ where q is a power of p. As $e|p-1$, by 1.2 part (2), the Lemma follows. □

In view of the presentation in 1.3, any $\phi \in \mathrm{Aut}(K)$ has the form $\phi(C) = C^v$ and $\phi(B) = C^w B^x$, where:

(1) $v \in \mathbb{Z}^*_{p^\alpha}$,
(2) $w \in \mathbb{Z}_{p^\alpha}$,
(3) $x \in \mathbb{Z}^*_{e\ell}$.

We check the defining relations of K to determine exactly when such a map, ϕ, is an element of $\mathrm{Aut}(K)$. One gets the following:

(1′) $\phi(C)^{p^\alpha} = C^{p^\alpha v} = 1$,
(2′) $\phi(B)\phi(C)\phi(B)^{-1} = C^{vr^x}$ and $\phi(C)^r = C^{vr}$,
(3′) $\phi(B)^{e\ell} = C^{w(1-r^{ex\ell})/(1-r^x)}$.

We see that (2′) implies the condition $vr^x \equiv vr \mod p^\alpha$. As v and r are both in $\mathbb{Z}^*_{p^\alpha}$ we get $r^{x-1} \equiv 1 \mod p^\alpha$ or $e|x-1$ so $x \equiv 1 \mod e$. The lemma above then insures that $\phi(B)^{e\ell} = 1$ in (3′).

Proposition 2.3. *The map, ϕ, defined by $\phi(C) = C^v$ and $\phi(B) = C^w B^x$ is an automorphism of K above for any choice of $v \in \mathbb{Z}^*_{p^\alpha}$, $w \in \mathbb{Z}_{p^\alpha}$ and $x \in$ $\mathrm{Ker}(\mathbb{Z}^*_{e\ell} \longrightarrow \mathbb{Z}^*_e) = \Delta$. The set $R = \mathbb{Z}_{p^\alpha} \times \mathbb{Z}^*_{p^\alpha} \times \Delta$ is a group with multiplication given by*

$$(w', v', x') * (w, v, x) = (wv' + w', vv', xx').$$

The map $\phi \mapsto (w, v, x)$ is an isomorphism of $\mathrm{Aut}(K)$ with this group.

Proof. All that remains is to check that the given multiplication law on R corresponds to composition of automorphisms. This is routine. □

Proposition 2.4. *The group R above is isomorphic to a semidirect product $\mathbb{Z}_{p^\alpha} \rtimes (\mathbb{Z}^*_{p^\alpha} \times \Delta)$ where the map $\mathbb{Z}^*_{p^\alpha} \times \Delta \longrightarrow \mathrm{Aut}(\mathbb{Z}_{p^\alpha})$ is just projection to the first factor composed with the canonical identification $\mathbb{Z}^*_{p^\alpha} \cong \mathrm{Aut}(\mathbb{Z}_{p^\alpha})$.*

Proof. This is a consequence of the relation $(0,v,x)*(w,1,1)*(0,v,x)^{-1} = (wv,1,1)$. □

If we recall the identifications, $K' = \langle C\rangle$ and $Z(K) = \langle B^e\rangle$, we see that the propositions above can be restated as follows:

Proposition 2.5. *There is an exact sequence*

$$0 \longrightarrow K' \xrightarrow{\alpha} \mathrm{Aut}(K) \xrightarrow{\beta} \mathrm{Aut}(K') \times \mathrm{Aut}(K^{ab}) \xrightarrow{\gamma} \mathrm{Aut}(K^{ab}/\overline{Z(K)}) \longrightarrow 0.$$

Moreover, $\mathrm{Aut}(K)$ *splits as a semidirect product of* K' *and* $\mathrm{Im}(\beta)$ *where the structure map* $\mathrm{Im}(\beta) \longrightarrow \mathrm{Aut}(K')$ *is projection to the first factor. The maps* β *and* γ *are the canonical ones. The map* α *is given by* $\alpha(d)(C) = C$ *and* $\alpha(d)(B) = dB$.

Corollary 2.6. $\#\,\mathrm{Aut}(K) = p^\alpha\phi(p^\alpha)\phi(e\ell)\phi(e)^{-1} = p^\alpha\phi(\#K)\phi(e)^{-1}$.

Proof. The first equality follows from Proposition 2.3. The latter follows as $(e\ell, p) = 1$ and $p^\alpha e\ell = \#K$. □

Next we calculate $\mathrm{Inn}(K)$. Conjugating in K by B and C we see that $\mathrm{Inn}(K)$ is identified with the subgroup of R generated by $(1-r,1,1)$ and $(0,r,1)$. As $r-1$ is prime to p, $1-r$ generates $\mathbb{Z}_{p^\alpha} \subseteq R$ and thus $\mathrm{Inn}(K)$ is identified with $\mathbb{Z}_{p^\alpha} \rtimes (\langle r\rangle \times \langle 1\rangle) \subseteq R$. It follows that:

Proposition 2.7. *The isomorphism* $\mathrm{Aut}(K) \cong R$ *of* 2.4 *identifies* $\mathrm{Inn}(K)$ *with* $\mathbb{Z}_{p^\alpha} \rtimes (\langle r\rangle \times \langle 1\rangle)$ *which has order* $p^\alpha e$. *Thus,* $\mathrm{Out}(K) \cong \mathbb{Z}_{p^\alpha}^*/\langle r\rangle \times \Delta$ *has order* $\phi(p^\alpha\ell)\phi(e)^{-1}$.

3. Normalizers

If K is a subgroup of the units of $D = D(F, a/b)$, then we have a diagram with exact rows and columns as follows:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & Z(K) \arrow[r] \arrow[d] & K \arrow[r, "\Theta|_K"] \arrow[d] & \mathrm{Inn}(K) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & C_D(K)^* \arrow[r] \arrow[d] & N_{D^*}(K) \arrow[r, "\Theta"] \arrow[d] & \mathrm{Aut}(K) \arrow[d] & \\
0 \arrow[r] & C_D(K)^*/Z(K) \arrow[r] \arrow[d] & N_{D^*}(K)/K \arrow[r, "\overline{\Theta}"] \arrow[d] & \mathrm{Out}(K) \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Here $\Theta(d)$ is conjugation by d on K. We would like a description of $\mathrm{Im}\,\Theta$.

Definition 3.1. *Let ϕ be an embedding of a group $G_{m,r}$ in D with $\mathrm{Im}(\phi) = K$. The F subspace of D spanned by K carries a $F[G_{m,r}]$ module structure as follows. $R(\phi) = \sum_{k \in K} Fk$ and the multiplication is given by $g * k = \phi(g)k$ for $g \in G_{m,r}$ and $k \in K$.*

Now, suppose that ϕ and ψ are two embeddings of $G_{m,r}$ in D with $\mathrm{Im}(\phi) = \mathrm{Im}(\psi) = K$. The space $R(\phi) = R(\psi)$ carries two $G_{m,r}$ actions. The multiplication induced by ϕ will be denoted $*$ and the multiplication induced by ψ will be denoted $\circ$. If $d \in N_{D^*}(K)$ then we have a diagram:

$$\begin{tikzcd}
G_{m,r} \arrow[r, "\phi"] \arrow[d, "\Gamma(d)"'] & K \arrow[d, "\Theta(d)"] \\
G_{m,r} \arrow[r, "\psi"] & K
\end{tikzcd}$$

If M is a $G_{m,r}$ module then, for $\rho \in \mathrm{Aut}(G_{m,r})$, we denote by M^ρ the module with multiplication given by $g *^\rho m = \rho(g) * m$. We also write $\mathrm{Stab}(M) = \{\rho \in \mathrm{Aut}(G_{m,r}) : M^\rho \cong M\}$.

Proposition 3.2. *The map $\Theta(d)$, thought of as a map from $R(\phi)$ to $R(\psi)^{\Gamma(d)}$, is a $G_{m,r}$ module isomorphism.*

Proof.

$$\begin{aligned}
\Theta(d)(g * k) &= \Theta(d)(\phi(g)k) \\
&= d\phi(g)d^{-1}dkd^{-1} \\
&= \psi(\Gamma(d)(g))\Theta(d)(k) \\
&= \Gamma(d)(g) \circ \Theta(d)(k) \\
&= g \circ^{\Gamma(d)} \Theta(d)(k).
\end{aligned}$$

□

Now, suppose that ϕ and ψ are both the inclusion, I, of K in D. Then, for $d \in N_{D^*}(K)$, $\Theta(d) = \Gamma(d)$ is an isomorphism of $R(I)$ with $R(I)^{\Theta(d)}$ so $\mathrm{Im}(\Theta) \subseteq \mathrm{Stab}(R(I))$. We will see that this inclusion is an equality. Suppose that $\mu : R(I) \longrightarrow R(I)^\rho$ is an isomorphism for $\rho \in \mathrm{Aut}(K)$, i.e. $\rho \in \mathrm{Stab}(R(I))$. $\mu(1) \neq 0$ and so, as $R(I)$ is a division algebra, $\hat{\mu} = \mu.\mu(1)^{-1}$ is also an isomorphism $R(I) \xrightarrow{\hat{\mu}} R(I)^\rho$. We have $\hat{\mu}(kh) = \rho(k)\hat{\mu}(h)$ and, setting $h = 1$ we get $\hat{\mu}(k) = \rho(k)$. In particular, we have a diagram,

$$\begin{tikzcd}
K \arrow[r, "I"] \arrow[d, "\rho"'] & R(I) \arrow[d, "\hat{\mu}"] \\
K \arrow[r, "I"] & R(I)
\end{tikzcd}$$

where ρ is a group homomorphism. It follows that $\hat{\mu}$ is an algebra homomorphism and so, by the Noether-Skolem Theorem, that $\hat{\mu}$ is induced by conjugation in D. Thus $\rho \in \mathrm{Im}(\Theta)$ so $\mathrm{Im}(\Theta) = \mathrm{Stab}(R(I))$, giving:

Proposition 3.3. *In the notations above, there is an exact sequence*

$$0 \longrightarrow C_D(K)^* \longrightarrow N_{D^*}(K) \xrightarrow{\Theta} \mathrm{Stab}(R(I)) \longrightarrow 0.$$

In [H, 6.11] it is shown that any two isomorphic subgroups of D^* are conjugate. On the other hand, two embeddings of the same group need not be conjugate and, in fact, fixing $\mathrm{Im}(\psi)$, there are, up to conjugacy by elements of D^*, $\phi(p^\alpha \ell)/e\phi(e)$ different classes of embeddings of the form $G_{m,r} \xrightarrow{\psi} K \subseteq D^*$ [H, remark pre 6.8]. These classes correspond to cosets of $\mathrm{Im}(\Theta)$ in $\mathrm{Aut}(K)$ and so we get $[\mathrm{Aut}(K) : \mathrm{Im}(\Theta)] = \phi(p^\alpha \ell)/e\phi(e)$. Using the results of 2.6 and 2.4 we conclude:

Proposition 3.4. *The order of* $\mathrm{Im}(\Theta)$ *is* $p^\alpha e^2$.

Remark. It is particularly noteworthy that the order of $\mathrm{Im}(\Theta)$ depends only on the isomorphism class of K and not on the ambient division algebra. It follows then that every element of $\mathrm{Im}(\Theta)$ is induced by conjugation in $R(I) = F(K)$, the division algebra generated by K.

Proposition 3.5. *Under the identification of 2.3,*

$$\mathrm{Aut}(K) = \mathbb{Z}_{p^\alpha} \rtimes (\mathbb{Z}_{p^\alpha}^* \times \Delta),$$

the group $\mathrm{Im}(\Theta)$ *corresponds to,*

$$\mathrm{Im}(\Theta) = \mathrm{Stab}(R(I)) = \mathbb{Z}_{p^\alpha} \rtimes (\langle r \rangle \times \Gamma),$$

where, $\Gamma = \mathrm{Ker}(\mathbb{Z}_{e\ell}^* \longrightarrow \mathbb{Z}_\ell^*)$ *is cyclic of degree e. In other words, $\phi \in \mathrm{Im}(\Theta)$, if and only if $\phi(C) = C^v$ and $\phi(B) = C^w B^x$ where v is a power of r mod p^α and $x \equiv 1$ mod ℓ.*

Proof. Let τ denote the Galois automorphism of $F(C, B^e)$ induced by conjugation by B, i.e., $\tau(C) = C^r$ and $\tau(B^e) = B^e$. Let Z be the fixed field of τ. The subalgebra of D generated by K can be determined because there is a surjection

$$\langle F(C, B^e)/Z, \tau, B^e \rangle \longrightarrow R(I)$$

mapping τ to B. As the cyclic algebra is simple, this is an isomorphism and we regard it as an identification. By the remark preceding this proposition, $\phi \in \mathrm{Im}(\Theta)$ is induced by conjugation by some $d \in R(I)$. In particular, ϕ induces an element of $\mathrm{Gal}(F(C, B^e)/Z) = \langle \tau \rangle$ and so v is a power of r mod p^α. Also, $B^e \in Z$ so $\phi(B^e) = B^e$. In $K^{ab} = K/\langle C \rangle$, $\overline{B^e} = \overline{B^{xe}}$ but $\overline{B}$ is of order ℓe, so $x \equiv 1$ mod ℓ. Thus we have shown that $\mathrm{Im}(\Theta) \subseteq \mathbb{Z}_{p^\alpha} \rtimes (\langle r \rangle \times \Gamma)$. On the other hand, we know that $|\,\mathrm{Im}(\Theta)| = p^\alpha e^2$ so we are finished if we can show that $|\Gamma| = e$. This follows from 2.2 as does the isomorphism $\Gamma \cong \mathbb{Z}_e$. □

Remark 3.6. It follows from the above that we have an exact diagram:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & Z(K) \arrow[r] \arrow[d] & K \arrow[r, "\Theta|_K"] \arrow[d] & \mathrm{Inn}(K) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & C_D(K)^* \arrow[r] \arrow[d] & N_{D^*}(K) \arrow[r, "\Theta"] \arrow[d] & \mathrm{Stab}(R(I)) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & C_D(K)^*/Z(K) \arrow[r] \arrow[d] & N_{D^*}(K)/K \arrow[r, "\overline{\Theta}"] \arrow[d] & \Gamma \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

where the final column is split by the inclusion of Γ in $\mathrm{Aut}(K)$.

Proposition 3.7. *Let $Z = Z(F(K))$ where $K \subseteq D(F, a/b)^*$ is a subgroup presented as in* 1.3. *Let $\tau(C) = C^r$, then $F(K) = \langle Z(C)/Z, \tau, B^e\rangle$ is a cyclic algebra of degree e. $Z(B) \subset F(K)$ is a maximal unramified extension of Z of degree e in $F(K)$.*

Proof. The natural algebra homomorphism from the cyclic algebra to $F(K)$ is well defined because the defining relations of the algebra hold in $F(K)$. It is an isomorphism as the cyclic algebra is simple. The remainder of the proposition follows as $[Z(B) : Z] = e$ and B is a p' root of unity. □

Next we wish to consider the valuation, v, on $N_{D^*}(K)$. We assume that v is normalized so that $v(F) = \mathbb{Z}$ and hence, by the result below, $v(D(F, a/b)) = 1/b\mathbb{Z}$.

Proposition 3.8. *If w is a valuation on a local field F, normalized so that $w(F^*) = \mathbb{Z}$, and, if D is a finite dimensional division algebra with center F, then there is a unique extension of w to a valuation, v, on D. If $\dim_F(D) = n^2$ then $e(D/F) = f(D/F) = n$ and so $v(D^*) = 1/n\mathbb{Z}$.*

Proof. For a description of valuation theory on division algebras see [P]. □

Proposition 3.9. *If $K \cong G_{m,r}$ is a subgroup of $D(F, a/b)^*$, then*

$$v(N_{D^*}(K)) = \frac{f(F(\zeta_m)/F)}{b}\mathbb{Z}.$$

Proof. By 3.7 and the structure theorem for division algebras over local fields, we see that $F(K) \cong \langle Z(B)/Z, \tau, \pi^g\rangle \cong D(Z, g/e)$ for some g coprime to e, where τ is the Frobenius of $Z(B)/Z$ and π is a uniformizing parameter in Z. By 3.6 with $D = F(K)$ we see that there is an element, $d \in F(K)$, which normalizes K and corresponds to the Frobenius in $\mathrm{Gal}(Z(B)/Z) = \Gamma$. Thus du_τ^{-1} centralizes

$Z(B)$ which is a maximal subfield if $F(K)$. It follows that $d = \gamma u_\tau$ for some $\gamma \in Z(B)$ and so $d^e = N(\gamma)u_\tau^e = N(\gamma)\pi^g$, where N is the norm of the extension $Z(B)/Z$. If $c = g^{-1} \bmod e$ then $d^{ce} = N(\gamma)^c\pi^{1+\rho e}$ and, as $Z(B)/Z$ is unramified, $N(\gamma) = u\pi^{v(\gamma)e}$ for some unit $u \in Z$. Let $h = d^c/\pi^{\rho+v(\gamma)c}$. Then $h^e = u^c\pi$ and so $v(h)\mathbb{Z} = v(\pi)/e\mathbb{Z} = v(F(K))$. On the other hand, $h \in N_{D^*}(K)$ and thus $v(F(K)) \subseteq v(N_{D^*}(K))$. From 3.6 we see that h maps to a generator of Γ and so $v(N_{D^*}(K))$ is generated by $v(h)$ and $v(C_D(K)^*)$.

We have the following diagram of inclusions of algebras

$$\begin{tikzcd}
 & & F(K) \arrow[rd] & & \\
F \arrow[r] & Z \arrow[ru] \arrow[rd] & & C_D(Z) \arrow[r] & D \\
 & & C_D(K) \arrow[ru] & &
\end{tikzcd}$$

where, by the double centralizer theorem, $C_D(Z) \cong F(K) \otimes_Z C_D(K)$ and $[F(K) : Z] = e^2$ and $[C_D(K) : Z] = s^2$ are relatively prime. It follows from 3.8 that $v(C_D(K)) = v(\pi)/s\mathbb{Z}$ and so, by the above, $v(N_{D^*}(K)) = v(\pi)/s\mathbb{Z} + v(\pi)/e\mathbb{Z} = v(\pi)(e,s)/se\mathbb{Z} = v(\pi)/se\mathbb{Z}$.

To finish the proof of this proposition we must consider $v(\pi)$. From the diagram of algebras and the Double Centralizer Theorem, we have

$$\begin{aligned}
b^2 &= \dim_F(D) \\
&= \dim_F(Z)\dim_F(C_D(Z)) \\
&= [Z : F]^2 \dim_Z(C_D(Z)) \\
&= [Z : F]^2 e^2 s^2,
\end{aligned}$$

so $b = [Z : F]es = e(Z/F)f(Z/F)es$. On the other hand, $v(\pi) = 1/e(Z/F)$ and so

$$\frac{v(\pi)}{es} = \frac{1}{ese(Z/F)} = \frac{f(Z/F)}{b}.$$

$F(\zeta_m)/Z$ is totally ramified, [H, 6.2], and so $f(F(\zeta_m)/F) = f(Z/F)$ giving

$$v(N_{D^*}(K)) = \frac{f(F(\zeta_m)/F)}{b}\mathbb{Z}.$$

□

Proposition 3.10. *If $K \cong G_{m,r}$ is a subgroup of $D(F, a/b)^*$ then there is a split exact sequence*

$$0 \longrightarrow K.U(C_D(K)) \longrightarrow N_{D^*}(K) \longrightarrow \frac{f(F(\zeta_m)/F)}{b}\mathbb{Z} \longrightarrow 0,$$

where the quotient map is the valuation v and $U(C_D(K))$ is the group of units in the maximal order of $C_D(K)$.

Proof. All we need to show is that the kernel of the valuation on $N_{D^*}(K)$ is contained in $K.U(C_D(K))$. From 3.6, we see that every $x \in N_{D^*}(K)$ has the form $x = h^\alpha cg$ where h is the element in the proof of Proposition 3.9 so the image of h generates Γ,$\alpha = 0, 1, \ldots, e-1$, $c \in C_D(K)$ and $g \in K$. If $v(x) = 0$ then $\alpha v(h) + v(c) = \alpha v(\pi)/e + \beta v(\pi)/s = 0$ where s is as per the proof of 3.9. This gives $\alpha s = -\beta e$ and, as e and s are coprime, e divides α giving $\alpha = 0$. Consequently $x = cg$ and $v(c) = 0$ so $x \in K.U(C_D(K))$ as desired. □

Proposition 3.11. *If $K \cong G_{m,r}$ is a maximal finite subgroup of $D(F, a/b)^*$ then the exact sequence of* 3.10 *becomes*

$$0 \longrightarrow K \times U^{(1)}(Z) \longrightarrow N_{D^*}(K) \longrightarrow \frac{f(F(\zeta_m)/F)}{b}\mathbb{Z} \longrightarrow 0,$$

where $Z = Z(F(K))$ and $U^{(1)}(Z)$ denotes the units congruent to 1 *modulo the uniformizing parameter. The action of the cyclic quotient group on $U^{(1)}(Z)$ is trivial and on K, factors through the subgroup $\Gamma \subseteq \mathrm{Aut}(K)$.*

Proof. If K is maximal then, by [H, 5.2], $C_D(K) = Z$ and so, in the notation of the proof of 3.9, $s = 1$ and $v(h)\mathbb{Z} = v(\pi)/e\mathbb{Z} = v(N_{D^*}(K))$ and so the sequence splits by mapping the generator of the quotient group to $h \in F(K)$. The proof is then complete if we establish that $K.U(Z) = K \times U^{(1)}(Z)$. However, $U(Z) = \mu_{p'}(Z) \times U^{(1)}(Z)$ and, as $Z(K)$ has order prime to p, we have $K \cap U(Z) \subseteq \mu_{p'}(Z)$. By maximality of K, $\mu_{p'}(Z) \subseteq K \cap U(Z)$ giving $K \cap U(Z) = \mu_{p'}(Z)$ and consequently, $K.U(Z) = K \times U^{(1)}(Z)$. □

Proposition 3.12. *Let O denote the ring of integers in $D(F, a/b)$ and let $K \cong G_{m,r}$ be a subgroup of $D(F, a/b)^*$ and hence of O^*. Let π be a uniformizing parameter in $D(F, a/b)$. The O^* conjugacy classes of subgroups of O^*, isomorphic to $G_{m,r}$ are uniquely represented by the groups $\pi^{-i}K\pi^i$, where $i = 0, 1, \ldots, f(F(\zeta_m)/F) - 1$.*

Proof. By [H, 6.11], any two groups, H and K, in $D(F, a/b)^*$, isomorphic to $G_{m,r}$ are conjugate to one another and thus $\pi^i uHu^{-1}\pi^{-i} = K$ for some unit $u \in O^*$. Writing $f = f(F(\zeta_m)/F)$, we have $v(N_{D^*}(K)) = f/b\mathbb{Z}$ and $v(\pi) = 1/b$ and so by conjugating by an appropriate element of $N_{D^*}(K)$, we can assume that $0 \leq i < f$. Thus $uHu^{-1} = \pi^{-i}K\pi^i$ so the groups listed do indeed represent all conjugacy classes. If, on the other hand, $\pi^{-i}K\pi^i$ and $\pi^{-j}K\pi^j$ are conjugate in O^* then there would exist $u \in O^*$ so that $\pi^j u\pi^{-i} \in N_{D^*}(K)$. Taking the valuation, $(j-i)/b \in f/b\mathbb{Z}$ and thus f divides $j - i$. Hence the groups listed do indeed represent distinct conjugacy classes. □

4. Examples

While [H] describes the isomorphism type of the finite groups found in division algebras over local fields, explicit embeddings, in terms of the usual cyclic algebra presentation, are not generally forthcoming. Warrington, in his senior thesis, [W], describes, explicitly, the groups of order $p(p-1)^2$ at $p = 3,\ 5$ and 7.

Example 4.1. If $p = 3$ let $D = D(\widehat{\mathbb{Q}}_3, 1/2) = \langle \widehat{\mathbb{Q}}_3(\zeta_8)/\widehat{\mathbb{Q}}_3, \sigma, 3\rangle$ then the group $K \cong G_{6,5} \cong \langle C, B : C^3 = B^4 = 1, BCB^{-1} = C^2\rangle$ embeds in D^* via the identification, $B = \zeta_8^2$ and $C = \frac{-1+b\sigma}{2}$ where $b \in \widehat{\mathbb{Q}}_3(\zeta_8)$ and $N_{\widehat{\mathbb{Q}}_3(\zeta_8)/\widehat{\mathbb{Q}}_3}(b) = -1$. For example, $b = \zeta_8$. In this case, $e = \ell = 2$ and the non-trivial element of Γ is represented by the outer automorphism $\phi(C) = C$, $\phi(B) = B^3$ which is induced by conjugation by $b\sigma = 2C + B^2$.

Example 4.2. If $p = 5$ we can take $D = D(\widehat{\mathbb{Q}}_5, 1/4) = \langle \widehat{\mathbb{Q}}_5(\zeta_{16})/\widehat{\mathbb{Q}}_5, \sigma, 5\rangle$ which contains a group of order 80 given by $K \cong G_{20,13} \cong \langle C, B : C^5 = B^{16} = 1, BCB^{-1} = C^3\rangle$. The identification can be made by $B = \zeta_{16}$, $C = -1/4 + qb\sigma/4 + i(b\sigma)^2/4 + (b\sigma)^3/4q$ where $q \in \widehat{\mathbb{Q}}_5$ satisfies $q^2 = 2 - i$ and $b \in \widehat{\mathbb{Q}}_5(\zeta_{16})$ has $N_{\widehat{\mathbb{Q}}_5(\zeta_{16})/\widehat{\mathbb{Q}}_5}(b) = -1$. For example, $b = \zeta_{16}^2$. In this case $e = \ell = 4$ and the outer automorphism $\phi(C) = C$, $\phi(B) = B^{13}$ generates $\Gamma \cong \mathbb{Z}_4$ and corresponds to conjugation by $b\sigma$.

Example 4.3. If $p = 7$ we take $D = D(\widehat{\mathbb{Q}}_7, 1/6) = \langle \widehat{\mathbb{Q}}_7(\zeta_{36})/\widehat{\mathbb{Q}}_7, \sigma, 7\rangle$. This contains of group of order 252 given by $K \cong G_{42,17} \cong \langle C, B : C^7 = B^{36} = 1, BCB^{-1} = C^3\rangle$. The identification is made via $B = \zeta_{36}$, $C = -1/6 + \zeta_6 q^2 b\sigma/6 + q(b\sigma)^2/6 + (b\sigma)^3/6 - (b\sigma)^4/6q - \zeta_6^2(b\sigma)^5/6q^2$. Where $q \in \widehat{\mathbb{Q}}_7$ satisfies $q^3 = 1 - 3\zeta_6$ and $N_{\widehat{\mathbb{Q}}(\zeta_{36})/\widehat{\mathbb{Q}}_7}(b) = -1$. Here, $e = \ell = 6$ and the outer automorphism $\phi(C) = C$, $\phi(B) = B^{-5}$ generates $\Gamma \cong \mathbb{Z}_6$ and corresponds to conjugation by $b\sigma$.

Lemma 4.4. *Let $b = p^n(p-1)k$ and $t = (p^{p^n k} - 1)(p-1)$, then $\widehat{\mathbb{Q}}_p(\zeta_t)$ is the unramified extension of $\widehat{\mathbb{Q}}_p$ of degree b.*

Proof. Reducing the second factor of $p^b - 1 = (p^{p^n k} - 1)(p^{p^n k(p-2)} + \cdots + p^{p^n k} + 1)$ modulo $p-1$ we see that $t | p^b - 1$ so $\zeta_t \in \widehat{\mathbb{Q}}_p(\zeta_{p^b-1})$.On the other hand, $p^{p^n k} - 1 | t$ so $[\widehat{\mathbb{Q}}_p(\zeta_t) : \widehat{\mathbb{Q}}_p] = p^n k\beta$ for some $\beta | p-1$. Then $t | p^{p^n k\beta} - 1$ so, as $p^{p^n k\beta} - 1 = (p^{p^n k} - 1)(p^{p^n k(\beta-1)} + \cdots + p^{p^n k} + 1)$, we have $p - 1 | p^{p^n k(\beta-1)} + \cdots + p^{p^n k} + 1$. Reducing modulo $p-1$ we get $\beta \cong 0$ so $p - 1 | \beta$. Thus $\beta = p - 1$ and so $\widehat{\mathbb{Q}}_p(\zeta_t) = \widehat{\mathbb{Q}}_p(\zeta_{p^b-1})$ as stated. □

Let $D = D(\widehat{\mathbb{Q}}_p, a/b) = \langle \widehat{\mathbb{Q}}_p(\zeta_{p^b-1})/\widehat{\mathbb{Q}}_p, \sigma, p^a\rangle$ where $b = p^n(p-1)k$ then, by [H,6.18], the maximal finite non-commutative subgroups of D^* are given as $G_\alpha = G_{m_\alpha, r_\alpha}$ where $m_\alpha = p^\alpha(p^{kp^{n+1-\alpha}} - 1)$, $e = p - 1$, $\ell = p^{kp^{n+1-\alpha}} - 1$ and r_α generates $\mathbb{Z}_p^*$. G_α is generated by x, of order p^α and y, of order ℓe. α takes values in $1, 2, \ldots, n+1$. By the lemma above, $\ell e | p^b - 1$ and so, after a possible conjugation, $y \in \widehat{\mathbb{Q}}_p(\zeta_{p^b-1})$. In fact, we identify $y = \zeta_{p^b-1}^{\frac{p^b-1}{\ell e}}$.

Lemma 4.5. *In the notation above, the subalgebra, $\widehat{\mathbb{Q}}_p(G_\alpha) \subseteq D$, generated by G_α is isomorphic to $\langle \widehat{\mathbb{Q}}_p(x, y^{p-1})/Z_p^\alpha(y^{p-1}), \tau, y^{p-1}\rangle$ where τ is the Galois automorphism induced by conjugation by y and Z_p^α is the unique field of degree $p^{\alpha-1}$ over $\widehat{\mathbb{Q}}_p$ contained in $\widehat{\mathbb{Q}}_p(\zeta_{p^\alpha})$. In other words, $Z(\widehat{\mathbb{Q}}_p(G_\alpha)) \cong Z_p^\alpha(y^{p-1})$.*

Proof. Certainly there is an algebra surjection from a cyclic algebra to $\widehat{\mathbb{Q}}_p(G_\alpha)$ of the form

$$\langle \widehat{\mathbb{Q}}_p(x, y^{p-1})/Z, \tau, y^{p-1}\rangle \longrightarrow \widehat{\mathbb{Q}}_p(G_\alpha),$$

where Z is the fixed field in $\widehat{\mathbb{Q}}_p(x, y^{p-1})$ of conjugation by y. The map takes u_τ to y. As cyclic algebras are simple, this is an isomorphism. The field Z satisfies $\widehat{\mathbb{Q}}_p(y^{p-1}) \subseteq Z \subseteq \widehat{\mathbb{Q}}_p(y^{p-1}, x)$ and $[\widehat{\mathbb{Q}}_p(y^{p-1}, x) : Z] = p-1$. These conditions determine Z, as $\mathrm{Gal}(\widehat{\mathbb{Q}}_p(y^{p-1}, x)/\widehat{\mathbb{Q}}_p(y^{p-1})) \cong \mathbb{Z}_{p^{\alpha-1}(p-1)}$, so $Z \cong Z_p^\alpha(y^{p-1})$. □

Now we describe explicitly a copy of G_1 in $D(\widehat{\mathbb{Q}}_p, a/b)^*$. By 4.4 we have an isomorphism $D(\widehat{\mathbb{Q}}_p, a/b) = \langle \widehat{\mathbb{Q}}_p(y)/\widehat{\mathbb{Q}}_p, \sigma, p^a\rangle$ where $y = \zeta_{(p^{p^n k}-1)(p-1)}$ and σ acts on $\widehat{\mathbb{Q}}_p(y)/\widehat{\mathbb{Q}}_p$ as the Frobenius. Let $\tau = \sigma^{p^n k}$ so $u_\tau = u_\sigma^{p^n k}$ and $u_\tau^{(p-1)} = p^a$. If $F \subseteq \widehat{\mathbb{Q}}_p(y)$ is the fixed field of τ then $\widehat{\mathbb{Q}}_p(y)/F$ is an unramified extension with Frobenius, τ. Let N denote the norm map for this extension. Set $\delta = 2(p^b-1)/(p^{p^n k}-1)$. Then δ is even and divides $p^b - 1$ so $\zeta_\delta \in \widehat{\mathbb{Q}}_p(y)$. As $\tau(\zeta_\delta) = \zeta_\delta^{p^{p^n k}}$,

$$N(\zeta_\delta) = \zeta_\delta^{1+p^{p^n k}+\cdots+p^{(p-2)p^n k}} = \zeta_\delta^{\delta/2} = -1.$$

Let $d = \zeta_\delta u_\sigma^{p^n kc}$ where $c \cong a^{-1} \bmod p-1$, then

$$d^{p-1} = N(\zeta_\delta) u_\sigma^{p^n kc(p-1)} = -u_\sigma^{bc} = -p^{ac} = -p^{1+\beta(p-1)},$$

and so, if $h = d/p^\beta$ then $h^{(p-1)} = -p$. On the other hand, $h^{-1}yh = y^{p^{p^n kc}}$ so $yhy^{-1} = hy^{p^{p^n kc}-1} = h(y^{p^{p^n k}-1})^\gamma$. However, $y^{p^{p^n k}-1}$ is a $p-1$ root of unity and so is in $\widehat{\mathbb{Q}}_p$. Thus, y normalizes $\widehat{\mathbb{Q}}_p(h)$. By [I, 4.10] $\widehat{\mathbb{Q}}_p(h) = \widehat{\mathbb{Q}}_p(\zeta_p)$ and so $\langle y\rangle \mu_p(\widehat{\mathbb{Q}}_p(h))$ is a finite subgroup isomorphic to G_1. The element h normalizes this group and conjugation by h induces a generator for the outer automorphism group, Γ.

The other maximal subgroups, G_α, appear in a similar way. Let $f_0(x) = x$, $f_1(x) = x^p + px$ and $f_{i+1}(x) = f_i(f_1(x))$. Let $F_i(x) = f_i(x)/f_{i-1}(x)$. An easy induction shows that F_i is an Eisenstein polynomial for all i and is hence irreducible. Let d_i be a root of F_i. [I, 4.10] tells us that $\widehat{\mathbb{Q}}_p(d_i) \cong \widehat{\mathbb{Q}}_p(\zeta_{p^i})$. We may assume without loss of generality that $d_i^p + pd_i = d_{i-1}$. As $v(d_1) = 1/(p-1)$ and $v(p) = 1$ it follows by induction that $v(d_i) = 1/p^{i-1}(p-1)$ for $i = 1, 2, \ldots, n+1$. Now, if ζ_{p-1} is any $p-1$ root of unity in $\widehat{\mathbb{Q}}_p$, then $\zeta_{p-1}d_i$ is also a root of F_i and hence defines an element of $\mathrm{Gal}(\widehat{\mathbb{Q}}_p(d_i)/\widehat{\mathbb{Q}}_p)$. On the other hand, this group is isomorphic to $\mathbb{Z}_{p^{i-1}} \times \mathbb{Z}_{p-1}$ and so all Galois automorphisms of order $p-1$ have this form. Suppose now that $G_\alpha \subseteq D(\widehat{\mathbb{Q}}_p, 1/p^n(p-1)k)^*$, then $\widehat{\mathbb{Q}}_p(S_p(G_\alpha)) \cong \widehat{\mathbb{Q}}_p(\zeta_{p^\alpha}) \cong \widehat{\mathbb{Q}}_p(d_\alpha)$ and, writing $G_\alpha = \langle \zeta_{p^\alpha} \rangle \rtimes \langle y_\alpha \rangle$ where y_α has order $(p^{p^{n+1-\alpha}k} - 1)(p-1)$, we have $y_\alpha^{-1}\zeta_{p^\alpha} y_\alpha = \zeta_{p^\alpha}^r$ is of order $p-1$. It follows from the above that $y_\alpha^{-1} d_\alpha y_\alpha = \zeta_{p-1} d_\alpha$ for some $\zeta_{p-1} \in \widehat{\mathbb{Q}}_p$ and hence that $d_\alpha y_\alpha d_\alpha^{-1} = y_\alpha \zeta_{p-1}$. As $\zeta_{p-1} \in \langle y_\alpha \rangle$ we see that $d_\alpha \in N_{D^*}(G_\alpha)$. It follows that d_α is an element of $N_{D^*}(G_\alpha)$ which induces a generator of Γ when conjugating on G_α and maps to the generator of $v(N_{D^*}(G_\alpha))$ under v. Theorems 3.11 and 4.5 tell us that

$$N_{D^*}(G_\alpha) = [G_\alpha \times U^{(1)}(Z_p^\alpha(y_\alpha^{p-1}))] \rtimes \langle d_\alpha \rangle,$$

and by 3.12 there are $f = p^{n+1-\alpha}k$ non-conjugate subgroups of the integral units of D, all isomorphic to G_α.

5. Residue characteristic 2

Finally, we consider the case of residue characteristic equal to 2 which is distinguished by the presence of a non-abelian 2 group, namely the quaternion group Q_8. Let F be a local field with residue characteristic 2. In [H] we showed that $D(F, a/b)$ contains non-abelian subgroups if and only if $[F : \widehat{\mathbb{Q}}_2]$ is odd and $b = 2k$ where k is odd. Henceforth we assume these conditions. Let $D = D(F, a/b)$ and let G be a non-abelian subgroup of D^*. By [H, 7.3 and 7.4], $G \cong Q_8 \times \mathbb{Z}_\ell$ or $G \cong T \times \mathbb{Z}_\ell$ where T is the binary tetrahedral group. For convenience we will write $G \cong K \times \mathbb{Z}_\ell$ where $K = Q_8$ or T. Applying the Double Centralizer Theorem one gets a decomposition of D of the form $D = F(K) \otimes_F C_D(K)$. In both cases the former factor is the quaternion algebra, $D(F, 1/2)$ and the group $\mathbb{Z}_\ell$ embeds in the latter factor which is isomorphic to $D(F, c/k)$ where $2c \equiv a \mod k$.

We observe that $(|K|, \ell) = 1$ and so K and $\mathbb{Z}_\ell$ are characteristic subgroups. It follows that there is a canonical homomorphism, given by conjugation, of the form

$$\Theta : N_{D^*}(G) \longrightarrow \mathrm{Aut}(K) \times \mathrm{Aut}(\mathbb{Z}_\ell).$$

Identifying a generator of $\mathbb{Z}_\ell$ with a root of unity in $C_D(K)$ we may consider Θ as mapping

$$\Theta : N_{D^*}(G) \longrightarrow \mathrm{Aut}(K) \times \mathrm{Gal}(F(\zeta_\ell)/F).$$

By the Noether-Skolem Theorem, every element of $\mathrm{Gal}(F(\zeta_\ell)/F)$ can be realized by conjugation by an element of $C_D(K)$. It follows that Θ maps onto a group as follows:

$$\Theta : N_{D^*}(G) \longrightarrow \Delta \times \mathrm{Gal}(F(\zeta_\ell)/F),$$

where $\Delta \subseteq \mathrm{Aut}(K)$. $\mathrm{Ker}(\Theta) = C_{D^*}(K) = C_{C_D(K)}(\zeta_\ell)^*$ Thus $\mathrm{Ker}(\Theta)$ consists of the units of the division algebra $D(F(\zeta_\ell), c[F(\zeta_\ell) : F]/k)$. Next we determine Δ in the two cases.

Case 1: If $K = T$ then $\mathrm{Out}(K)$ is trivial so $\Theta(K) = \mathrm{Aut}(K)$ and so $\Delta = \mathrm{Aut}(K) \cong T/Z(T)$ is the tetrahedral group.

Case 2: $\widehat{\mathbb{Q}}_2[Q_8] \cong \widehat{\mathbb{Q}}_2^4 \times D(\widehat{\mathbb{Q}}_2, 1/2)$ and every $\phi \in \mathrm{Aut}(Q_8)$ induces $\bar{\phi} \in \mathrm{Aut}(\widehat{\mathbb{Q}}_2[Q_8])$ and hence $\hat{\phi} \in \mathrm{Aut}(D(\widehat{\mathbb{Q}}_2, 1/2))$ so that the diagram below commutes

$$\begin{tikzcd}
Q_8 \arrow[r] \arrow[d, "\phi"'] & \widehat{\mathbb{Q}}_2[Q_8] \arrow[r] \arrow[d, "\bar{\phi}"'] & D(\widehat{\mathbb{Q}}_2, 1/2) \arrow[d, "\hat{\phi}"'] \\
Q_8 \arrow[r] & \widehat{\mathbb{Q}}_2[Q_8] \arrow[r] & D(\widehat{\mathbb{Q}}_2, 1/2)
\end{tikzcd}$$

where the horizontal maps are respectively inclusion and projection. By the Noether-Skolem theorem, $\hat{\phi}$ is inner and hence $\phi \in \Delta$, proving $\Delta = \mathrm{Aut}(Q_8)$ which is isomorphic to S_4. More explicitly, $\mathrm{Aut}(Q_8)$ is generated by the inner automorphisms and two outer automorphisms given by conjugating by $i + j$ and $1 + i + j + k$.

Putting this together we have shown:

Theorem 5.1. *With the notation above, there is an exact sequence*

$$0 \longrightarrow C_{D^*}(G) \longrightarrow N_{D^*}(G) \longrightarrow \mathrm{Aut}(K) \times \mathrm{Gal}(F(\zeta_\ell)/F) \longrightarrow 0,$$

where $\mathrm{Aut}(K)$ *is isomorphic to the tetrahedral group or to* S_4 *depending on whether* K *is isomorphic to* T *or* Q_8 *respectively.*

$$\mathrm{Inv}_{F(\zeta_\ell)}(C_D(G)) = (a-k)[F(\zeta_\ell) : F]/2k \mod \mathbb{Z}.$$

Next we consider the image of $N_{D^*}(G)$ under the valuation v. We assume, as for p odd, that $v(F) = \mathbb{Z}$. $D = F(K) \otimes C_D(K)$ so

$$C_D(K) \cong \langle F(\zeta_{q^k-1})/F, \sigma, \pi^c \rangle,$$

where $q = |\overline{F}|$ and σ is the Frobenius automorphism. As $(\ell, 2) = 1$, we may assume $F \subseteq F(\zeta_\ell) \subseteq F(\zeta_{q^k-1})$ and so, putting $h = u_\sigma^d$, where $1 = dc + \beta k$ for some β, $h^k = u_\sigma^{dk} = \pi^{cd} = \pi^{1-\beta k}$. Let $H = h\pi^\beta \in C_{D^*}(K) \cap N_{D^*}(G)$. $H^k = \pi$ so H has valuation $1/k$. It follows that $v(C_{D^*}(K) \cap N_{D^*}(G)) = v(C_D(K)) = 1/k\mathbb{Z}$.

Let X be a set of elements of $N_{D^*}(G)$ which map under θ to $\mathrm{Aut}(K)$. For example, if $K = T$ then $X = T$. If $K = Q_8$ then $F(Q_8)$ contains a group isomorphic to T. Letting $R = (1 + i + j + k)/2$, we get $\langle Q_8, R \rangle = T$. $\Theta(T) \subseteq \mathrm{Aut}(Q_8)$ has index 2. Conjugating by $S = i + j$ realizes an automorphism not in $\Theta(T)$ and so we may take $X = T \cup ST$.

From Theorem 5.1 and the observation that $\Theta(C_{D^*}(K) \cap N_{D^*}(G)) = \mathrm{Gal}(F(\zeta_\ell)/F)$, we get

$$v(N_{D^*}(G)) = v(X)\mathbb{Z} + v(C_{D^*}(K) \cap N_{D^*}(G)) + v(C_D(G)),$$

but $C_{D^*}(G) \subseteq C_{D^*}(K) \cap N_{D^*}(G)$ and $v(C_{D^*}(K) \cap N_{D^*}(G)) = 1/k\mathbb{Z}$ so

$$v(N_{D^*}(G)) = v(X)\mathbb{Z} + 1/k\mathbb{Z}.$$

As $v(T) = 0$ and $v(S) = 1/2$ we see that $v(N_{D^*}(G)) = 1/k\mathbb{Z}$ or $1/2k\mathbb{Z}$ depending on whether $K = Q_8$ or T respectively.

It remains to compute the kernel of the valuation on $N_{D^*}(G)$. We assume that $C_D(G) \subseteq C_D(K)$ is identified with $C_{C_D(K)}(\zeta_\ell)$ and as H, defined above, conjugates $F(\zeta_\ell)$ to realize a generator of the Galois group over F, $H^{[F(\zeta_\ell):F]}$ is an element of $C_D(G)$. In fact it is a uniformizing parameter in $C_D(G)$ as $F(\zeta_\ell)/F$ is unramified and the degree of $C_D(G)$ is $k/[F(\zeta_\ell) : F]$. It follows from Theorem 5.1 that every element $y \in N_{D^*}(G)$ can be written in the form $y = xH^\beta H^{\gamma[F(\zeta_\ell):F]}u = xH^\delta u$ where $x \in X$ as defined above and u is a unit in $C_D(G)$. Furthermore we may decompose $x = s^\epsilon t$ where $t \in T$ and $\epsilon = 0$ if $K = T$ and $\epsilon = 0$ or 1 if $K = Q_8$. Taking the valuation we get $v(y) = \epsilon/2 + \delta/k = (\epsilon k + 2\delta)/k$. This is zero if and only if $\epsilon k = -2\delta$. As k is odd this implies $\epsilon = \delta = 0$. In other words, $y \in \mathrm{Ker}(v)$ if and only if $y = tu$. We now state the above considerations as a theorem.

Theorem 5.2. *If $G \subseteq D(F; a/b)^*$ is a non-abelian subgroup, then $b = 2k$ for k odd and $G \cong T \times \mathbb{Z}_\ell$ or $Q_8 \times \mathbb{Z}_\ell$. If v is the valuation on $D(F, a/b)$, normalized so $v(F) = \mathbb{Z}$, then we have a split exact sequence*

$$0 \longrightarrow T.U(C_D(G)) \longrightarrow N_{D^*}(G) \xrightarrow{v} 1/d\mathbb{Z} \longrightarrow 0,$$

where $d = k$ if $G \cong T \times \mathbb{Z}_\ell$ and $d = 2k$ if $G \cong Q_8 \times \mathbb{Z}_\ell$. $U(C_D(G))$ denotes the units in the maximal order of the division algebra $C_D(G)$ which has center isomorphic to $F(\zeta_\ell)$ and Hasse invariant $(a - k)[F(\zeta_\ell) : F]/2k \mod \mathbb{Z}$.

Theorem 5.3. *Let $D = D(F, a/b)$ and let $G \subseteq D^*$ be a subgroup isomorphic to $K \times \mathbb{Z}_\ell$ where $K = Q_8$ or T. Let O^* denote the units in the maximal order of D and let π in D be a uniformizing parameter. Let $\overline{G} \subseteq D^*$ be isomorphic to G. If $K = Q_8$ then $\overline{G}$ is conjugate to G in O^*. If $K = T$ then $\overline{G}$ is conjugate in O^* to exactly one of G or $\pi G \pi^{-1}$.*

Proof. It follows from the Noether-Skolem theorem that $\pi^{-i}u^{-1}\overline{G}u\pi^i = G$ for some $u \in O^*$ and $i \in \mathbb{Z}$. In view of Theorem 5.2, we may, in fact, assume that $i = 0$ if $K = Q_8$ and $i = 0$ or 1 if $K = T$. Thus $u^{-1}\overline{G}u = \pi G \pi^{-1}$ or G as required. It remains to show that for $K = T$, G and $\pi G \pi^{-1}$ are not conjugate in O^*. This follows from Theorem 5.2 and the fact that $v(\pi) = 1/2k$. □

Example 5.4. In the units of the maximal order in the Quaternion algebra, $D(\widehat{\mathbb{Q}}_2, 1/2)$ the two non-conjugate copies of T may be given as $\langle i, j, (1+i+j+k)/2\rangle$ and $\langle i, j, (1+i+j-k)/2\rangle$.

6. Cyclic groups

Let F be a local field with arbitrary residue characteristic. As always, we assume that the valuation is normalized so that $v(F) = \mathbb{Z}$. It remains to consider the cyclic groups in $D = D(F, a/b)$. Is is well known that $D(F, a/b)$ contains an element of order m if and only if $[F(\zeta_m) : F]\big| b$. We assume that m has this property. Let $m = p^\alpha \ell$. By the Noether-Skolem theorem, all subgroups of D^*, isomorphic to $\mathbb{Z}_m$ are conjugate, so we pick $\zeta_m \in D^*$ and consider its normalizer. We have a diagram of inclusions of fields as follows:

$$\begin{tikzcd}
 & F(\zeta_{p^\alpha}) \arrow[r, "f_2"] & F(\zeta_m) \arrow[r, "f_3"] & F(\zeta_{m\bar{\ell}}) & \\
F = F_0 \arrow[r, "f_1"] & F_1 \arrow[u, "f_4"'] \arrow[r, "f_2"] & F_2 \arrow[u, "f_4"'] \arrow[r, "f_3"] & F_3 \arrow[u, "f_4"'] \arrow[r, "f_4"] & F_4,
\end{tikzcd}$$

where $F(\zeta_{m\bar{\ell}})$ is a maximal subfield of D which is unramified over $F(\zeta_m)$. F_1, F_2, and F_3 are the unramified closures of F in $F(\zeta_{p^\alpha})$, $F(\zeta_m)$, and $F(\zeta_{m\bar{\ell}})$ respectively. F_4 is a maximal unramified subfield of D. If we define $f_i = [F_i : F_{i-1}]$ for $i = 1, 2, 3, 4$, then the various inclusions have the degrees indicated on the diagram. The horizontal inclusions are unramified and the vertical ones are totally ramified. By the Noether-Skolem theorem, every element of $\mathrm{Gal}(F(\zeta_{p^\alpha})/F_1)$ is realized by conjugation in $C_D(F_3)$. As this group is cyclic, we may choose an element $\tau \in C_D(F_3)$ which realizes a generator. Now, $v(\tau) \in v(C_D(F_3) = 1/f_4\mathbb{Z}$. On the other hand, $v(F(\zeta_{m\bar{\ell}})) = 1/f_4\mathbb{Z}$ and so we may multiply τ by an element of $F(\zeta_{m\bar{\ell}})$ to force $v(\tau) = 0$ without changing the other properties required of it.

Let $\sigma \in N_D(F(\zeta_{m\bar{\ell}}))$ be an element which, by conjugation, realizes the Frobenius automorphism of F_3/F, and hence also of F_2/F. It follows that the elements $X = \{\sigma^i \tau^j\}$, where $0 \le i < f_1 f_2$ and $0 \le j < f_4$, are elements of $N_D(F(\zeta_m))$ which surject, via conjugation, onto $\mathrm{Gal}(F(\zeta_m)/F)$. Thus we may write every $x \in N_D(\zeta_m)$ in the form $x = \sigma^i \tau^j \pi^k u$ where i and j are as above, $k \in \mathbb{Z}$, π is a uniformizing parameter in $C_D(\zeta_m)$ and u is a unit in $C_D(\zeta_m)$. If $v(\sigma) = \gamma/b$, then $v(x) = (i\gamma + kf_1 f_2)/b$ and it follows that $v(N_D(\zeta_m)) = (\gamma, f_1 f_2)/b\mathbb{Z}$. Now, $\mathrm{Gal}(F_4/F) \cong \mathbb{Z}_b$ and the Frobenius is realized by some $\phi \in D$. As $\mathrm{Inv}_F(D) = a/b \bmod \mathbb{Z}$, we get $v(\phi) = a/b$. Restricting to conjugation on F_3 we get $\phi\sigma^{-1} \in C_D(F_3)$. As $v(C_D(F_3)) = 1/f_4\mathbb{Z}$, this gives $(a-\gamma)/b \in 1/f_4\mathbb{Z}$, or $a \equiv \gamma \bmod f_1 f_2 f_3$. In particular, $(\gamma, f_1 f_2) = (a, f_1 f_2)$ and as $f_1 f_2 | b$ which is prime to a, $(\gamma, f_1 f_2) = 1$ and so $v(N_D(\zeta_m)) = 1/b\mathbb{Z}$. These considerations give us the following.

Theorem 6.1. *Let m satisfy $[F(\zeta_m) : F]|b$. Then $\zeta_m \in D(F, a/b)$ and there is an exact diagram*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & U(C_D(\zeta_m)) \arrow[r] \arrow[d] & C_{D^*}(\zeta_m) \arrow[r, "v"] \arrow[d] & \frac{[F_2:F]}{b}\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & N_{O^*}(\zeta_m) \arrow[r] \arrow[d] & N_{D^*}(\zeta_m) \arrow[r, "v"] \arrow[d] & \frac{1}{b}\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Gal}(F(\zeta_m)/F_2) \arrow[r] \arrow[d] & \mathrm{Gal}(F(\zeta_m)/F) \arrow[r] \arrow[d] & \mathbb{Z}_{[F_2:F]} \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

where F_2 is the unramified closure of F in $F(\zeta_m)$ and O is the maximal order in $D(F, a/b)$.

Proof. The only part of the diagram that needs any further comment is the bottom left hand corner. That it is correct as stated follows from the observation that the elements τ^j are in $N_{O^*}(\zeta_m)$ and realize $\mathrm{Gal}(F(\zeta_m)/F_2)$ by conjugation. □

Corollary 6.2. *Any two cyclic subgroups of O^* of the same order are conjugate.*

Proof. As per Theorems 3.12 and 5.3 , this follows from the fact that $v(N_D(\zeta_m) = 1/b\mathbb{Z}$. □

Note that, in general, this does not imply that any two elements of the same order are conjugate. This only happens when $\mathrm{Gal}(F(\zeta_m)/F_2)$ acts transitively on the m-th roots of unity.

References

[A] S.A. Amitsur, *Finite subgroups of division rings*, Trans. Amer. Math. Soc. **80** (1995), 361–386.

[GSS] V. Gorbounov, S. Siegel, and P. Symonds, *The cohomology of the Morava stabilizer group $\mathbb{S}_2$ at the prime 3*, preprint.

[He] H-W. Henn, *Centralizers of elementary abelian p-subgroups and mod-p cohomology of profinite groups*, preprint.

[H] T.J. Hewett, *Subgroups of division algebras over local fields*, J. Algebra **173** (1995), 518–548.

[I] K. Iwasawa, *Local class field theory*, Oxford Science Publications. Oxford Mathematical Monographs., The Clarendon Press, Oxford University Press, New York, 1986.

[P] R.S. Pierce, *Associative algebras*, Graduate Texts in Mathematics, 88. Studies in the History of Modern Science, 9, Springer-Verlag, New York-Berlin, 1982.

[W] G. Warrington, *Explicit embeddings of finite subgroups of division algebras over the p-adics*, Senior thesis, Princeton, 1995.

[Y] T. Yamada, *The Schur subgroup of the Brauer group*, Lecture Notes in Mathematics, Vol. 397, Springer-Verlag, Berlin-New York, 1974.

Mathematics Department, Fine Hall, Princeton University, Princeton, NJ 08540
E-mail address: hewett@princeton.edu, tjhewett@alumni.stanford.org