Pacific Journal of Mathematics

AUTOMORPHISM GROUPS OF FINITE SUBGROUPS OF DIVISION RINGS

RALPH JASPER FAUDREE, JR.

Vol. 26, No. 1 November 1968

PACIFIC JOURNAL OF MATHEMATICS
Vol. 26, No. 1, 1968

AUTOMORPHISM GROUPS OF FINITE SUBGROUPS OF DIVISION RINGS

R. J. FAUDREE

If a finite group G can be embedded in the multiplicative group of a division ring, then G can be embedded in a division ring D generated by G such that any automorphism of G can be uniquely extended to be an automorphism of D. It seems natural then to investigate the relation between the automorphism group of G and the automorphism group of D.

We will prove that the automorphism group of G determines the automorphism group of D modulo the inner-automorphism group of D (i.e. every automorphism of D can be written as a product of an inner-automorphism of D and an automorphism of G). The automorphism group of G does not completely determine the automorphism group of D for the rational quaternions contain an isomorphic copy of Q_8, the quaternion group of order 8. There are infinitely many automorphisms of the rational quaternions but the automorphism group of Q_8 is finite.

Amitsur determined which finite groups can be embedded in a division ring [2]. We will use his conditions, but first some definitions will be given and certain algebraic structures will be discussed.

Let m and r be relatively prime integers, $s = (r-1, m)$ $t = m/s$ and $n =$ minimal integer satisfying $r^n \equiv 1 \pmod m$.

$$G_{m,r} = Gp(A, B \mid A^m = 1, BAB^{-1} = A^r, B^n = A^t) .$$

$\mathfrak{T}$, $\mathfrak{O}$, and $\mathfrak{J}$ will denote the binary tetrahedral, binary octahedral and binary icosahedral groups.

If ε_m is a primitive m^{th} root of unity and σ_r is the automorphism of $Q(\varepsilon_m)$ determined by the map $\varepsilon_m \to \varepsilon_m^r$, then

$$\mathfrak{A}_{m,r} = (Q(\varepsilon_m), \sigma_r, \varepsilon_m^t)$$

will denote the cyclic algebra determined by the field $Q(\varepsilon_m)$, the automorphism σ_r and the element ε_m^t. The map $A \to \varepsilon_m$ and $B \to \sigma_r$ determines an isomorphic embedding of $G_{m,r}$ into the algebra $\mathfrak{A}_{m,r}$. Under this identification we have

$$\mathfrak{A}_{m,r} = (Q(A), B, A^t) .$$

The algebra $\mathfrak{A}_{m,r}$ is a division algebra if and only if $G_{m,r}$ can be embedded in a division ring [2]. The following diagram gives some subalgebras of $\mathfrak{A}_{m,r}$ which will be of importance in this paper. Here $Z_{m,r}$ denotes the center of $\mathfrak{A}_{m,r}$.

$$\begin{array}{c} \mathfrak{A}_{m,r} \\ | \\ Q(A) \\ | \\ Z_{m,r} \\ | \\ Q(A^t) \\ | \\ Q \end{array}$$

For a discussion of the algebra $\mathfrak{A}_{m,r}$ and a proof of the following proposition see [2].

PROPOSITION 1. A finite group G can be embedded in a division ring if and only if G is isomorphic to one of the following:

(1) Cyclic group

(2) $G_{m,r}$ where m and r satisfy condition C.

(3) A direct product of $\mathfrak{T}$ and $G_{m,r}$ where $G_{m,,r}$ is cyclic of order m or of the preceding type, $(6, |G_{m,r}|) = 1$, and 2 has odd order (mod m).

(4) $\mathfrak{O}$ and $\mathfrak{J}$.

Additional notation must be given before condition C can be stated. Let p be a fixed prime dividing m. $\alpha = \alpha_p$ is the highest power of p dividing m η_p is the minimal integer satisfying $r^{\eta_p} \equiv 1 \bmod (mp^{-\alpha})$. μ_p is the minimal integer satisfying $r^{\mu_p} \equiv p^{\mu'} \bmod (mp^{-\alpha})$ some integer μ'. $\delta'_p = \mu_p \delta_p / \eta_p$.

Condition C. Integers m and r satisfy condition C if either

(I) $(n, t) = (s, t) = 1$

or (II) $n = 2n'$, $m = 2^\alpha m'$, $s = 2s'$ where $\alpha \geqq 2$, m', s', and n' are odd integers; $(n, t) = (s, t) = 2$ and $r \equiv -1 \bmod 2^\alpha$.

and either (III) $n = s = 2$ and $r \equiv -1 \bmod m$

or (IV) For every $q \mid n$ there exists a prime $p \mid m$ such that $q \nmid \eta_p$ and that either

(1) $p \neq 2$ and $(q, (p^{\delta'_p} - 1)/s) = 1$ or

(2) $p = q = 2$, II holds and $n/4 \equiv \delta'_2 \equiv 1 \pmod 2$.

A group G has property E if G can be embedded in the multiplicative group of a division ring, property EE if G can be embedded in some division ring D generated by G such that any automorphism of G can be extended uniquely to D, and property EEE if the automorphism group of G determines the automorphism group of D modulo the inner-automorphism group of D.

A relation between the above properties is given by

PROPOSITION 2. A finite group with property E has property EE. For a proof see [3].

We will prove

THEOREM. *A finite group with property E has property EEE.*

In the remaining discussion G will denote a finite group with property E, $A(G)$ will denote the group of automorphisms of G, and $I(G)$ will denote the group of inner-automorphisms of G. If G has property EE with respect to a division ring D, then $I_D^*(G)$ will denote the subgroup of elements of $A(G)$ which can be extended to an inner-automorphism of D. $A(D)$ and $I(D)$ will denote the automorphism group and inner-automorphism group of D respectively. $Z(G)$ and $Z(D)$ will denote the center of G and D respectively.

A slightly stronger statement than Proposition 2 is true. A finite group with property E has property E with respect to a division ring D of characteristic 0 which is uniquely determined up to isomorphism and G has property EE with respect to D, [2] and [3]. Thus $A(G)$ can be considered as a subgroup of $A(D)$. Since D is uniquely determined up to isomorphism, $I_D^*(G)$ does not depend upon D and $I_D^*(G)$ can be replaced by $I^*(G)$. It is easily seen that $A(G)$ determines $A(D)$ modulo $I(D)$ if and only if $[A(G): I_D(G)] = [A(D): I(D)]$.

We will break the proof of the Theorem into 9 lemmas.

LEMMA 1. *All finite cyclic groups G have property EEE.*

Proof. Assume G has order m. Let ε_m be a primitive m^{th} root of unity. Each automorphism of the field $Q(\varepsilon_m)$ is determined by the map $\varepsilon_m \rightarrow \varepsilon_m^r$ where $(r, m) = 1$. Each of these maps also determines an automorphism of the cyclic group (ε_m).

LEMMA 2. *The groups $\mathfrak{O}$ and $\mathfrak{J}$ have property EEE.*

Proof. $\mathfrak{O}$ can be embedded in $\mathfrak{A}_{8,-1}$ [2, Th. 6b]. $|A(\mathfrak{O})| = 48$, and $|I(\mathfrak{O})| = 24$ and there is an automorphism of $\mathfrak{O}$ which can be extended to $\mathfrak{A}_{8,-1}$ and which does not leave $Z(\mathfrak{A}_{8,-1})$ elements-wise fixed [3, Lemma 3]. Therefore $[A(\mathfrak{O}): I^*(\mathfrak{O})] = 2$. But $[A(\mathfrak{A}_{8,-1}): I(\mathfrak{A}_{8,-1})] = [Z(\mathfrak{A}_{8,-1}): \Delta]$ where Δ is the fixed field of $A(\mathfrak{A}_{8,-1})$ [5, p. 163]. $[Z(\mathfrak{A}_{8,-1}): Q] = 2$, thus

$$[A(\mathfrak{A}_{8,-1}): I(\mathfrak{A}_{8,-1})] = 2 = [A(\mathfrak{O}): I^*(\mathfrak{O})] \text{ ,}$$

$\mathfrak{J}$ can be embedded in $\mathfrak{A}_{10,-1}$ [2, Th. 6c]. Since $|A(\mathfrak{J})| = 120$, $|(I(\mathfrak{J})| = 60$ and there is an automorphism of $\mathfrak{J}$ which is not an inner-automorphism of $\mathfrak{A}_{10,-1}$, [3, Lemma 4], $[A(\mathfrak{J}): I^*(\mathfrak{J})] = 2$. Since $[Z(\mathfrak{A}_{10,-1}): Q] = 2$, $[A(\mathfrak{G}_{10,-1}): I(\mathfrak{A}_{10,-1})] = 2 = [A(\mathfrak{J}): I^*(\mathfrak{J})]$.

LEMMA 3. *Let H be the subgroup of the automorphism group of $Q(A)$ determined by the integers $\{l \mid (l, m) = 1, l \equiv 1 \,(\mathrm{mod}\, n)\}$. Let Δ_H be the subfield of $Q(A)$ left fixed by the group H. If $G_{m,r}$ has property E, then Δ_H contains the fixed field of the subgroup of $Gp(A(G), I(\mathfrak{A}_{m,r}))$ of $A(\mathfrak{A}_{m,r})$. In particular, $Q(A^t)$ contains the fixed field of $Gp(A(G), I(\mathfrak{A}_{m,r}))$.*

Proof. If $(l, m) = 1$ and $l \equiv 1 \,\mathrm{mod}\, n$, then the map $A \to A^l$ and $B \to A^{t(l-1)/n}B$ determines an automorphism of G. Thus by Proposition 2, the map of $Q(A)$ determined by $A \to A^l$ be extended to be an automorphism in $Gp(A(G), I(\mathfrak{A}_{m,r}))$. Hence Δ_H contains the fixed field of $Gp(A(G), I(\mathfrak{A}_{m,r}))$.

For $(l, m) = 1$, the map of $Q(A)$ determined by $A \to A^l$ leaves A^t fixed if and only if $A^{tl} = A^t$ or $l \equiv 1 \,(\mathrm{mod}\, s)$. But if $l \equiv 1 \,(\mathrm{mod}\, s)$, then $l = 1 \,(\mathrm{mod}\, n)$ and $Q(A^t) \supseteqq \Delta_H$.

LEMMA 4. *A group $G_{m,r}$ with m and r satisfying* (I) *of Condition C has property EEE.*

Proof. Let σ be an automorphism of $\mathfrak{A}_{m,r}$ and $A' = \sigma(A)$ and $B' = \sigma(B)$. Then $\sigma^{-1}(A^t) = A^{tw}$ with $(w, m) = 1$.

The map $A' \to A^l$ determines an automorphism τ of $Q(A')$ onto $Q(A)$ if $(l, m) = 1$. There is an integer l such that $l \equiv 1 \,(\mathrm{mod}\, t)$, $wl \equiv 1 \,(\mathrm{mod}\, s)$ and $(l, m) = 1$. Therefore by Lemma 3 and [5, p. 162, Th. 1], τ can be extended to an automorphism of $\mathfrak{A}_{m,r}$ in $Gp(A(G), I(\mathfrak{A}_{m,r}))$. We will denote this extension also by τ.

Thus $\tau\sigma(A) = A^l$ and $\tau\sigma(B) = B''$. If $l \equiv 1 \,(\mathrm{mod}\, n)$ then by Lemma 3 and [5, p. 162, Th. 1] $\tau\sigma$ is in $Gp(A(G), I(\mathfrak{A}_{m,r}))$. And hence σ is in $Gp(A(G), I(\mathfrak{A}_{m,r}))$. Assume $l \not\equiv 1 \,(\mathrm{mod}\, n)$. $B'' = \alpha_0 + \alpha_1 B + \cdots + \alpha_{n-1}B^{n-1}$ for α_i in $Q(A)$. Since $B''A = A^r B''$,

$$\sum_{i=1}^{n-1} \alpha_i A^{ri} B^i = \sum_{i=1}^{n-1} \alpha_i A^r B^i \,.$$

Thus $\alpha_i = 0$ for $i \neq 1$, and $B'' = \alpha B$ for α in $Q(A)$. $(\alpha B)^n = (A^l)^t$ and therefore $\alpha\theta(\alpha) \cdots \theta^{n-1}(\alpha) = A^{t(l-1)}$ where θ is the automorphism of $Q(A)$ induced by B. Since $l \not\equiv 1 \,(\mathrm{mod}\, n)$, this contradicts the fact that $\mathfrak{A}_{m,r}$ is a division algebra [1, p. 75, Th. 12 and 14, p. 149, Th. 32].

LEMMA 5. *Let G be a finite group with property EE with respect* *to the division ring D. Let H be a characteristic subgroup of G such that D', the subdivision ring of D generated by H, contains $Z(D)$. Let μ be the map $A(G) \to A(H)$. Let R be the subgroup of $\mu(A(G))$ which $\tau \to \tau/H$ leaves $Z(D)$ element-wise fixed. Then*

$$[\mu(A(G)): R] = [A(G): I^*(G)] .$$

Proof. If τ is in $A(G)$, then τ is in $I(D)$ and hence in $I^*(G)$ if and only if τ leaves $Z(D)$ element-wise fixed, [5, p. 162]. Since $Z(D) \subset D'$, τ is in $I^*(G)$ if and only if $\mu(\tau)$ leaves $Z(D)$ element-wise fixed. Therefore $\mu(I^*(G)) = R$ and the lemma follows from an elementary theorem of group theory.

LEMMA 6. *Let $G_{m,r}$ be a group with property E in which* (A) *is a characteristic subgroup. Let Δ_A be the fixed field of $A(\mathfrak{A}_{m,r})$ and Δ_G the fixed field of $Gp(A(G_{m,r}), I(\mathfrak{A}_{m,r}))$, then*

$$[\Delta_G: \Delta_A][A(G_{m,r}): I^*(G_{m,r})] = [A(\mathfrak{A}_{m,r}): I(\mathfrak{A}_{m,r})] .$$

Proof. In the notation of the previous lemma let $G = G_{m,r}$, $H = (A)$ and $D = \mathfrak{A}_{m,r}$. Then $D' = Q(A)$ and $Z(D) = Z_{m,r}$. If σ is the automorphism of $\mathfrak{A}_{m,r}$ induced by B, $R = \mu((\sigma))$. Therefore by Lemma 5, $[A(G_{m,r}): I^*(G_{m,r})] = [\mu(A(G_{m,r})): \mu((\sigma))]$. Δ_G is the subfield of $Q(A)$ left fixed by $\mu(A(G_{m,r}))$, thus by Galois theory $[\mu(A(G_{m,r})): \mu((\sigma))] = [Z_{m,r}: \Delta_G]$.

Hence

$$\begin{aligned}[A(\mathfrak{A}_{m,r}): I(\mathfrak{A}_{m,r})] &= [Z_{m,r}: \Delta_A] \text{ by [5, p. 163]} \\ &= [Z_{m,r}: \Delta_G][\Delta_G: \Delta_A] \\ &= [A(G_{m,r}): I^*(G_{m,r})]\cdot[\Delta_G: \Delta_A] .\end{aligned}$$

LEMMA 7. *A group $G_{m,r}$ where m and r satisfy* (II) *and* (III) *of Condition C has property EEE.*

Proof. Let u and v be integers with $0 \leqq u, v < m$ and $(u, m) = 1$. The map of $G_{m,r}$ determined by $A \to A^u$ and $B \to A^v B$ is an automorphism of $G_{m.r}$. Therefore any automorphism of (A) can be extended to an automorphism of $G_{m,r}$. Hence Q is the fixed field of $Gp(A(G_{m,r}), I(A_{m,r}))$ and of $A(A_{m,r})$.

$A^l B$ has order 4 for any integer l. Thus if $m > 4$, (A) is a characteristic subgroup of $G_{m,r}$. Therefore by Lemma 6,

$$[A(G_{m,r}): I^*(G_{m,r})] = [A(\mathfrak{A}_{m,r}): I(\mathfrak{A}_{m,r})] .$$

If $m = 4$, then $G_{m,r}$ is isomorphic to Q_8, the quaternions. Since the center of $\mathfrak{A}_{4,-1}$ is Q, all automorphisms of $\mathfrak{A}_{4,-1}$ are inner-automorphisms [5, p. 162]. Thus Q_8 trivially has property *EEE*.

LEMMA 8. *If m and r satisfy* (II) *and* (IV) *of Condition C, then $G_{m,r}$ is isomorphic to $Q_8 \times G_{m',r'}$ where $G_{m',r'}$ is cyclic of order m' or satisfies Condition C, $(6, |G_{m',r'}|) = 1$ and 2 has odd order* $(\bmod m')$.

Proof. By (IV), r has even order $(\bmod (m/p^{\alpha_p}))$ for any prime $p \mid m$ and $p \neq 2$. Therefore r has odd order $(\bmod m/2^\alpha)$, $m/4 \equiv 1 \pmod 2$, and $\alpha = 2$.

By the above remarks r and hence r^4 has order $n/2 \pmod{m/4}$. Therefore $Gp(A^4, B^4)$ is isomorphic to $G_{m',r'}$ where $m' = m/4$ and $r' = r^4$. Also $Gp(A^{m/4}, B^{ns/4})$ is isomorphic to Q_8.

Direct calculation verifies that appropriate elements commute and hence $G_{m,r} = Gp(A^4, B^4) \times Gp(A^{m/4}, B^{ns/4}) \cong G_{m',r'} \times Q_8$. $(6, |G_{m',r'}|) = 1$ and 2 having odd order $(\bmod m')$ follows from [4, Corollary, Th. 2].

LEMMA 9. *A group G satisfying* (3) *of Proposition* 1 *or* (II) *and* (IV) *of Condition C has property EEE.*

Proof. By Lemma 8, G is isomorphic to $H \times G_{m,r}$ where H is Q_8 or $\mathfrak{T}$. $\mathfrak{T}$ contains an isomorphic copy of Q_8. In either case G can be embedded in $\mathfrak{A}_{4m,r_1}$ where $r_1 \equiv r \pmod m$ and $r_1 \equiv -1 \bmod 4$. [2, Th. 6a]. $\mathfrak{A}_{4m,r_1}$ is isomorphic to $\mathfrak{A}_{4,-1} \otimes_Q \mathfrak{A}_{m,r}$. Therefore by proper identification, there is no loss of generality in assuming that $H \subset \mathfrak{A}_{4,-1}$, $G_{m,r} \subset \mathfrak{A}_{m,r}$. Since $Z(\mathfrak{A}_{4,-1}) = Q$, and $Z(\mathfrak{A}_{4m,r_1}) = Z(\mathfrak{A}_{m,r}) = Z_{m,r}$,

$$\mathfrak{A}_{4m,r_1} = (\mathfrak{A}_{4,-1}, Z_{m,r}) \otimes_{Z_{m,r}} \mathfrak{A}_{m,r} ;$$

where $(\mathfrak{A}_{4,-1}, Z_{m,r})$ is a normal division algebra of order 4 over $Z_{m,r}$ and $\mathfrak{A}_{m,r}$ is a normal division algebra of order n^2 over $Z_{m,r}$.

Let θ be an automorphism of $\mathfrak{A}_{4m,r_1}$. Since $(4, n^2) = 1$ there is an automorphism τ of $\mathfrak{A}_{4m,r_1}$ over $Z_{m,r}$ (i.e. the elements of $Z_{m,r}$ are left point-wise fixed) such that $\tau\theta(\mathfrak{A}_{m,r}) = \mathfrak{A}_{m,r}$ and $\tau\theta((\mathfrak{A}_{4,-1}, Z_{m,r})) = (\mathfrak{A}_{4,-1}, Z_{m,r})$ [1, p. 77]. τ is in $I(\mathfrak{A}_{4m,r_1})$ [5, p. 162]; and $\tau\theta$ restricted to $\mathfrak{A}_{m,r}$ is in $A(\mathfrak{A}_{m,r})$. Thus the fixed field of $A(\mathfrak{A}_{m,r})$ is equal to the fixed field of $A(\mathfrak{A}_{4m,r_1})$. Therefore

$$[A(\mathfrak{A}_{4m,r_1}) \colon I(\mathfrak{A}_{4m,r_1})] = [Z_{m,r} \colon \Delta] = [A(\mathfrak{A}_{m,r}) \colon I(\mathfrak{A}_{m,r})] ,$$

where Δ is the fixed field of $A(\mathfrak{A}_{m,r})$, [5, p. 113].

$$A(G) = A(H) \times A(G_{m,r}) , \quad \text{and since} \quad Z(\mathfrak{A}_{4,-1}) = Q ,$$

all automorphisms of $\mathfrak{A}_{4,-1}$ are inner-automorphisms and $I^*(H) = A(H)$. If θ is in $A(G)$ but not in $I^*(H) \times I^*(G_{m,r})$, then θ moves an element of $Z_{m,r}$. Consequently $I^*(G) = I^*(H) \times I^*(G_{m,r})$ and $[A(G): I^*(G)] = [A(G_{m,r}): I^*(G_{m,r})]$. Since $(|G_{m,r}|, 6) = 1$, m and r satisfy (I) of condition C. Thus by Lemma 4, $[A(G_{m,r}): I^*(G_{m,r})] = [A(\mathfrak{A}_{m,r}); I(\mathfrak{A}_{m,r})]$ and $[A(\mathfrak{A}_{4m,r_1}): I(\mathfrak{A}_{4m,r_1})][A(G): I^*(G)]$.

The theorem is a consequences of Lemmas 1, 2, 4, 7 and 9.

BIBLIOGRAPHY

1. A. A. Albert, *Structure of Algebras*, Amer. Math. Soc. Colloq. Publ. Vol. 24, Amer. Math. Soc., Providence, R. I., 1939.
2. S. A. Amitsur, *Finite subgroups of division rings*, Trans. Amer. Math. Soc. **80** (1955), 361-386.
3. R. J. Faudree, *Subgroups of the multiplicative group of a division ring*, Trans. Amer. Math. Soc. **124** (1966), 41-48.
4. ———, *Embedding theorems for ascending nilpotent groups*, Proc. Amer. Math. Soc. **18** (1967), 148-154.
5. N. Jacobson, *Structure of Rings*, Amer. Math. Soc. Colloq. Publ. Vol. 37, Amer. Math. Soc., Providence, R. I., 1956.

Received July 6, 1967. In partial support by the NSF Foundation Grant GP-3990.

UNIVERSITY OF CALIFORNIA
BERKELEY, CALIFORNIA
UNIVERSITY OF ILLINOIS
URBANA, ILLINOIS

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics

Vol. 26, No. 1 November, 1968