THE FINITE QUOTIENTS OF THE MULTIPLICATIVE GROUP OF A DIVISION ALGEBRA OF DEGREE 3 ARE SOLVABLE

BY

L. H. ROWEN

Department of Mathematics, Bar-Ilan University
Ramat Gan 52900, Israel
e-mail: rowen@macs.biu.ac.il

AND

Y. SEGEV*

Department of Mathematics, Ben-Gurion University of the Negev
Beer Sheva 84105, Israel
e-mail: yoavs@math.bgu.ac.il

ABSTRACT

Let D be a finite dimensional division algebra. It is known that in a variety of cases, questions about the normal subgroup structure of $D^\times$ (the multiplicative group of D) can be reduced to questions about finite quotients of $D^\times$. In this paper we prove that when $\deg(D) = 3$, finite quotients of $D^\times$ are solvable. The proof uses Wedderburn's Factorization Theorem.

0. Introduction

In this paper D is a finite dimensional division algebra over its center $F := Z(D)$. Recall that the degree of D is the square root of the dimension of D as a vector space over F. We denote by $D^\times$ (resp. $F^\times$) the multiplicative group of D (resp. F). The purpose of this paper is to prove the following theorem.

* Partially supported by grant no. 427–97–1 from the Israeli Science Foundation and by grant no. 6782–1–95 from the Israeli Ministry of Science and Art.
Received March 19, 1998

MAIN THEOREM: *Let D be a finite dimensional division algebra of degree 3 over its center $F := Z(D)$. Let N be a normal subgroup of $D^\times$ containing $F^\times$ such that $H := D^\times/N$ is finite. Then*

(1) *Let $x \in H$ and let $y \in N_H(\langle x \rangle)$. If $\gcd(|y|, 3) = 1$, then $y \in C_H(x)$, and if $\gcd(|x|, 3) = 1$, then $y^3 \in C_H(x)$, where $|h|$ is the order of h. In particular,*

(2) *Let $\mathrm{Inv}(H)$ be the set of involutions of H. Then $\langle \mathrm{Inv}(H) \rangle$ is elementary abelian. Hence*

(3) *$H/O_2(H)$ has odd order and hence H is solvable.*

We mention that the proof of the Main Theorem is basically self-contained, except the conclusion that H is solvable, which relies on the Feit–Thompson Odd Order Theorem. We also prove the following general lemma.

LEMMA 1: *Let D be a finite dimensional division algebra of degree n over its center $F := Z(D)$. Let N be a normal subgroup of $D^\times$ containing $F^\times$ and let $H := D^\times/N$. Then $Z(H)$ is of exponent n, in particular, $H/[H, H]$ is of exponent n.*

Note that in Lemma 1, H is not necessarily finite. Lemma 1 is an immediate consequence of Wedderburn's Factorization Theorem, which is also useful in the proof of the Main Theorem and seems quite useful in connecting the multiplicative structure with the additive structure of D.

As is well known (see [1], Cor. 20, p. 334, or [7], 14.4.1, p. 239), the multiplicative group of D (noncommutative) is never solvable. Further, by a theorem of Margulis and Prasad (see [4], Thm. 9.8, p. 516), if F is a number field, then any noncentral normal subgroup of $D^\times$ has finite index.

Not much is known about the structure of the multiplicative group of a division algebra. Thus any result in this area seems worthwhile; in particular, results on the structure of $D^\times$ are related to the Margulis–Platonov conjecture on the normal subgroup structure of algebraic groups over number fields (see [8] and [9]).

1. Notation and preliminaries

All through this paper D is a finite dimensional division algebra over its center $F := Z(D)$. Let $D^\times = D \setminus \{0\}$ and $G = D^\times$ be the multiplicative group of D. We set $F^\times = F \setminus \{0\}$. We let N be a normal subgroup of G such that $F^\times \leq N$ and G/N is finite. We use the following notational convention. We denote $G^* = G/N$ and, for $a \in G$, we let a^* denote its image in G^* under the canonical homomorphism, that is $a^* = Na$. If H^* is a subgroup of G^*, then by convention, $H \leq G$ is the full inverse image of H^* in G.

(1.1) *Remark:* Note that since $F^\times \leq N$, for all $a \in G$ and $\alpha \in F^\times$, $(\alpha a)^* = a^*$. We'll use this fact without further reference.

(1.2) NOTATION FOR GROUPS. Let H be a group. For $x, y \in H$, $x^y = y^{-1}xy$ and $[x, y] = x^{-1}y^{-1}xy$. For a subset $S \subseteq H$, $\langle S \rangle$ denotes the subgroup generated by S. For subgroups $X, Y \leq H$, $[X, Y] = \langle [x, y]: x \in X \text{ and } y \in Y \rangle$. Recall that if H is finite and p is a prime, $O_p(H)$ is the largest normal p-subgroup of H. We denote by $\mathrm{Inv}(H)$ the set of involutions of H (i.e., elements $1 \neq h \in H$ such that $h^2 = 1$). Given $h \in H$, we denote by $|h|$ the order of h. Finally, recall that if H is a finite p-group (p a prime), then $\Omega_1(H) = \langle h \in H : |h| = p \rangle$.

(1.3) NOTATION FOR ALGEBRAS. Given $x, y \in D$, we denote by $[\![x, y]\!]$ their *additive commutator*, that is $[\![x, y]\!] = xy - yx$.

Let $a \in D \setminus F$. We let $[\![a, D]\!] = \{[\![a, d]\!] : d \in D\}$, $[\![a, D]\!]^\times = [\![a, D]\!] \setminus \{0\}$, and

$$\Gamma(a) = \{a^{[\![a,x]\!]^{-1}} : [\![a, x]\!] \in [\![a, D]\!]^\times\}.$$

We denote by $m_a(\lambda) \in F[\lambda]$ the (monic) minimal polynomial of a over F. We let

$$\nu\colon D^\times \to F^\times$$

be the reduced norm.

Below we collect a number of preliminary results. These results are well known and appear in [10]. See also [3], [5] and [6]. We include proofs for the sake of completeness. In what follows λ is a commutative indeterminate over D. We consider polynomials in $D[\lambda]$ written as "left polynomials", i.e., in the form $\sum d_i\lambda^i$ for $d_i \in D$; if f, g are polynomials we say that g divides f if $f = hg$, for some h in $D[\lambda]$. Also, given $f = \sum d_i\lambda^i$ in $D[\lambda]$, we write $f(d)$ for $\sum d_i d^i$, i.e., "right substitution" for d.

(1.4): *Let $f(\lambda), g(\lambda) \in D[\lambda]$ and $d \in D$. Then*

(1) $(f + g)(d) = f(d) + g(d)$.

(2) *If $f = \sum d_i\lambda^i$, then $(fg)(d) = \sum d_i g(d) d^i$.*

(3) *If $g(d)$ commutes with d, then $(fg)(d) = f(d)g(d)$.*

Proof: (1) is obvious. For (2) note that if $f = \sum d_i\lambda^i$, then $fg = \sum d_i g(\lambda)\lambda^i$ (because λ is a commutative indeterminate). By (1), $(fg)(d) = \sum d_i(g(\lambda)\lambda^i)(d)$ $= \sum d_i g(d) d^i$. Now if $g(d)$ commutes with d, then

$$(fg)(d) = \sum d_i g(d) d^i = \sum d_i d^i g(d) = f(d)g(d). \qquad \blacksquare$$

(1.5): *Given $f \in D[\lambda]$ and $d \in D$, we have*

$$f(\lambda) = q(\lambda)(\lambda - d) + f(d).$$

In particular, d is a root of f iff $\lambda - d$ divides f.

Proof: By induction on $\deg(f)$. If $f = a\lambda + b$, then $f = a(\lambda - d) + ad + b = a(\lambda - d) + f(d)$, so take $q = a$. Suppose $\deg(f) = m > 1$ and let d_m be the leading coefficient of f. Set $g = f - d_m\lambda^{m-1}(\lambda - d)$. Then $\deg g < \deg f$, so by induction there exists $q_1 \in D[\lambda]$ such that $g = q_1(\lambda - d) + g(d)$. Hence $f - d_m\lambda^{m-1}(\lambda - d) = q_1(\lambda - d) + g(d)$. Note now that by 1.4.2, $g(d) = f(d)$ and hence we get $f = (q_1 + d_m\lambda^{m-1})(\lambda - d) + f(d)$. ∎

(1.6): *Let $f \in D[\lambda]$ and suppose $f = hg$, for some $h, g \in D[\lambda]$. Put $\bar{f} = h(\lambda)g(d)$; then $\bar{f}(d) = f(d)$.*

Proof: This is obvious; write $h = \sum d_i\lambda^i$, then $\bar{f} = \sum d_i g(d)\lambda^i$, so $\bar{f}(d) = \sum d_i g(d)d^i = f(d)$, by 1.4.2. ∎

(1.7) (Wedderburn): *Let $f \in D[\lambda]$ and suppose $f = hg$, for some $h, g \in D[\lambda]$. Let $d \in D$ and suppose d is a root of f but not of g. Then $g(d)dg(d)^{-1}$ is a root of h.*

Proof: Let $\bar{f} = h(\lambda)g(d)$. Then, by 1.6, d is a root of $\bar{f}$, so, by 1.5, $\lambda - d$ divides $\bar{f}$. It follows that $\lambda - g(d)dg(d)^{-1}$ divides $g(d)\bar{f}g(d)^{-1} = g(d)h(\lambda)$, and hence it divides h. ∎

(1.8) COROLLARY: *Let $f(\lambda) \in F[\lambda]$ and let $a \in D$ be a root of f. Let $b \in \Gamma(a)$; then $f = h(\lambda)(\lambda - b)(\lambda - a)$.*

Proof: Write $b = a^{[\![a,x]\!]^{-1}}$, for some $[\![a,x]\!] \in [\![a,D]\!]^{\times}$. Set $f = g(\lambda)(\lambda - a)$. Let $d = a^{x^{-1}}$; then d is a root f distinct from a. By 1.7, $(d - a)d(d - a)^{-1}$ is a root of $g(\lambda)$. But $d - a = a^{x^{-1}} - a = xax^{-1} - a = [\![x,a]\!]x^{-1}$. Thus $(d - a)d(d - a)^{-1} = [\![x,a]\!]x^{-1}xax^{-1}x[\![x,a]\!]^{-1} = a^{[\![x,a]\!]^{-1}} = a^{[\![a,x]\!]^{-1}}$. ∎

(1.9) *Remark:* We mention that by Prop. 1.1 in [3], given $a \in D \setminus F$, $\Gamma(a)$ is the set of all elements $b \in D$ such that $m_a(\lambda) = h(\lambda)(\lambda - b)(\lambda - a)$.

(1.10): *Let $a, b \in D$, with $v := [\![a,b]\!] \neq 0$. Then $vav^{-1} = b$, iff $a + b$ commutes with ba.*

Proof: $vav^{-1} = b$ iff $va = bv$ iff $(ab - ba)a = b(ab - ba)$ iff $aba - ba^2 = bab - b^2a$ iff $aba + b^2a = bab + ba^2$ iff $(a + b)ba = ba(a + b)$ as asserted. ∎

(1.11): *Suppose* $\deg(D) = 3$ *and let* $f = (\lambda - d_3)(\lambda - d_2)(\lambda - d_1) \in F[\lambda]$. *Suppose* $v := \llbracket d_1, d_2 \rrbracket \neq 0$. *Then*

(1) $\llbracket d_i, d_j \rrbracket \in \{v, -v\}$ *for all* $i, j \in \{1, 2, 3\}$, *with* $i \neq j$.

(2) $vd_1v^{-1} = d_2$, $vd_2v^{-1} = d_3$ *and* $vd_3v^{-1} = d_1$.

(3) $v^3 \in F$.

Proof: For (1), note that $d_1 + d_2 + d_3 = \alpha \in F$. Suppose $i = 1$. Then we may assume $j = 3$ and then $\llbracket d_1, d_3 \rrbracket = \llbracket d_1, \alpha - d_1 - d_2 \rrbracket = \llbracket d_1, -d_2 \rrbracket = -v$. A similar argument works if $(i, j) = (2, 3)$.

Next, since $f \in F[\lambda]$, $d_3d_2d_1 = d_1d_3d_2 = d_2d_1d_3 \in F$ and $d_1 + d_2 + d_3 \in F$. Thus d_jd_i commutes with $d_i + d_j$, for $(i, j) \in \{(1, 2), (2, 3), (3, 1)\}$. Thus by (1.10) and (1), (2) holds. (3) follows from the fact that v^3 commutes with d_1, d_2 and d_3, so $v^3 \in F(d_1) \cap F(d_2) = F$. ∎

(1.12): *Let* $a \in D \setminus F$ *be a separable element. Let* $x \in F(a)$, *with* $F(x) = F(a)$. *Then*

(1) $D = C_D(a) \oplus \llbracket a, D \rrbracket$.

(2) $\llbracket a, D \rrbracket = \llbracket x, D \rrbracket$.

Proof: (1): For every $w \in D$, with $\llbracket a, w \rrbracket \neq 0$, we know that $a^{\llbracket a, w \rrbracket^{-1}} \in \Gamma(a)$ (see 1.3 and 1.9). Since the minimal polynomial of a is separable, Theorem 4.3 in [3] implies that $\llbracket a, w \rrbracket \notin C_D(a)$. Hence $C_D(a) \cap \llbracket a, D \rrbracket = 0$, which implies (1), since $\dim(C_D(a)) + \dim(\llbracket a, D \rrbracket) = \dim(D)$.

(2): Notice that $C_D(a) = C_D(F(a)) = C_D(F(x)) = C_D(x)$. We show that for all $w \in D$, $\llbracket a, w \rrbracket \in \llbracket x, D \rrbracket$, the lemma follows from symmetry. Now by (1), $w = c + \llbracket x, d \rrbracket$, for some $c \in C_D(a)$ and $d \in D$. Thus, $\llbracket a, w \rrbracket = \llbracket a, c + \llbracket x, d \rrbracket \rrbracket = \llbracket a, \llbracket x, d \rrbracket \rrbracket$. But, by the Jacobi identity, $\llbracket a, x, d \rrbracket + \llbracket x, d, a \rrbracket + \llbracket d, a, x \rrbracket = 0$. Since $\llbracket a, x \rrbracket = 0$, we get that $\llbracket a, w \rrbracket = \llbracket a, \llbracket x, d \rrbracket \rrbracket = \llbracket d, a, x \rrbracket \in \llbracket x, D \rrbracket$ as asserted. ∎

2. The proof of the Main Theorem and Lemma 1

We continue the notation and hypotheses of Section 1. In addition, unless otherwise specified, we assume here that $\deg(D) = 3$. We start with

(2.1): *Let* $a \in G \setminus N$ *and let* $H^* = C_{G^*}(a^*)$. *If* $\llbracket a, D \rrbracket \cap H \neq \emptyset$, *then* $|a^*| = 3$.

Proof: Let $\llbracket a, d \rrbracket \in \llbracket a, D \rrbracket \cap H$. Let $b = a^{\llbracket a, d \rrbracket^{-1}}$. Then

$$m_a(\lambda) = (\lambda - c)(\lambda - b)(\lambda - a), \quad \text{for some } c \in G$$

and, by 2.2.1 (ahead), there exists $v \in G$ such that $c^v = b$, $b^v = a$ and $a^v = c$. Note that $a^* = b^*$ and hence $c^* = (a^*)^{v^*} = (b^*)^{v^*} = a^*$. Thus, $a^* = b^* = c^*$. But $cba \in F$, so $(a^*)^3 = c^*b^*a^* = 1^*$, and the lemma holds. ∎

(2.2): *Let* $a \in G \setminus N$, $\llbracket a,x \rrbracket \in \llbracket a, D \rrbracket^\times$ *and set* $b := a^{\llbracket a,x \rrbracket^{-1}}$, $c := \nu(a)a^{-1}b^{-1}$. *Then*

1. (1) *There exists* $1 \neq v \in G$ *such that* $v^3 \in F(a)$, $c^v = b$, $b^v = a$, $a^v = c$ *and* $v^{-1}\llbracket a,x \rrbracket \in F(a)$.
2. (2) *If* $(a^*)^{\llbracket a,x \rrbracket^*} \in \langle a^* \rangle$, *then* $\llbracket a,x \rrbracket^*$ *induces an automorphism of order 1 or 3 on* $\langle a^* \rangle$*; and if* $\llbracket a,x \rrbracket^* \in C_{G^*}(a^*)$, *then* $(a^*)^3 = 1^*$.

Proof: Since $b \in \Gamma(a)$ (see 1.3 and 1.9), there exists $c \in D$ such that $m_a(\lambda) = (\lambda - c)(\lambda - b)(\lambda - a)$. Thus $c = \nu(a)a^{-1}b^{-1}$. If $\llbracket a,b \rrbracket \neq 0$, then take $v := \llbracket a,b \rrbracket$, and (1) holds by 1.11. So suppose $\llbracket a,b \rrbracket = 0$. Let $v := \llbracket a,x \rrbracket$. Now b is another root of $m_a(\lambda)$ in $F(a)$, so $b^{v^{-1}}$ is also such a root and necessarily $b^{v^{-1}} = c$ and $c^{v^{-1}} = a$. Then, since $a^{v^3} = a$, $v^3 \in F(a)$. This shows (1).

Assume the hypothesis of (2). Notice that by (1), $\llbracket a,x \rrbracket^*$ induces an automorphism of order 1 or 3 on $\langle a^* \rangle$ and, if $\llbracket a,x \rrbracket^*$ induces an automorphism of order 1 on $\langle a^* \rangle$, then, by 2.1, $(a^*)^3 = 1^*$. ∎

(2.3) THEOREM: *Let* $a^*, y^* \in G^*$ *with* $y^* \in N_{G^*}(\langle a^* \rangle)$. *Suppose* $y^*a^*(y^*)^{-1} = (a^*)^k$, *with* $1 \leq k < |a^*|$. *Then*

1. (1) *If* $k \neq 1$, *then* $((a^*)^{k-1})^{\llbracket a,y \rrbracket^*} = ((a^*)^{k-1})^{y^*} \in \langle (a^*)^{k-1} \rangle$.
2. (2) *If there exists a prime* $p \neq 3$ *such that* $|a^*| = p^\ell$ *and* $|y^*| = p^m$, *then* $y^* \in C_{G^*}(a^*)$.
3. (3) *If* $|a^*| = p$ *is a prime, then* $(y^*)^3 \in C_{G^*}(a^*)$.
4. (4) *If* $\gcd(|y^*|, 3) = 1$, *then* $y^* \in C_{G^*}(a^*)$.
5. (5) *If* $\gcd(|a^*|, 3) = 1$, *then* $(y^*)^3 \in C_{G^*}(a^*)$.

Proof: Of course we may assume that

$$\text{(i)} \qquad y^* \notin C_{G^*}(a^*)$$

and hence $\llbracket a,y \rrbracket \neq 0$ and

$$\text{(ii)} \qquad (a^*)^{k-1} \neq 1^*.$$

Next, $\llbracket y,a \rrbracket = (yay^{-1}a^{-1} - 1)ay$. Note now that $(yay^{-1}a^{-1})^* = (a^*)^{k-1}$, so since $(yay^{-1}a^{-1} - 1)$ centralizes $yay^{-1}a^{-1}$, in G, $(yay^{-1}a^{-1} - 1)^*$ centralizes $(yay^{-1}a^{-1})^* = (a^*)^{k-1}$ and it follows that $((a^*)^{k-1})^{\llbracket a,y \rrbracket^*} = ((a^*)^{k-1})^{y^*}$. This shows (1).

Assume the hypothesis of (2). If a is inseparable over F, then $|a^*| = 3$, a contradiction. Thus a is separable over F. Since $a^{k-1} \notin F$, $\llbracket a, D \rrbracket = \llbracket a^{k-1}, D \rrbracket$, by 1.12. So $\llbracket a,y \rrbracket = \llbracket a^{k-1}, z \rrbracket$, for some $z \in D$ and then, by 2.2.2, either $\llbracket a,y \rrbracket^* =$

$[\![a^{k-1}, z]\!]^*$ induces an automorphism of order 3 on $\langle (a^*)^{k-1}\rangle$, or $(a^*)^{(k-1)3} = 1^*$. In the first case, since $[\![a, y]\!]^*$ acts like y^* on $\langle (a^*)^{k-1}\rangle$, this implies that 3 divides $|y^*|$, contradicting $p \neq 3$. In the second case, since $p \neq 3$, we get that $(a^*)^{k-1} = 1^*$, but $1 < k < |a^*|$, a contradiction.

Assume now that $|a^*| = p$ is a prime. Notice that (1) implies that

$$a^{*[\![a,y]\!]^*} = (a^*)^{y^*}. \tag{iii}$$

By 2.2.2 and (i), y^* induces an automorphism of order 3 on $\langle a^*\rangle$ as asserted.

For the proof of (4) and (5) we may assume without loss that $|a^*| = p^\ell$ and $|y^*| = r^m$, for some primes p and r. If $r = p$, then both in (4) and (5), $r = p \neq 3$, so by (2), $y^* \in C_{G^*}(a^*)$ contradicting (i). Hence we may assume that $r \neq p$. Thus in both cases by (3), $(y^*)^3 \in C_{G^*}(\Omega_1(\langle a^*\rangle))$. By [2], 24.3, p. 113, $(y^*)^3 \in C_{G^*}(a^*)$ and (5) is proved. If, in addition, $r \neq 3$, then $y^* \in C_{G^*}(a^*)$ and (4) is proved. ∎

(2.4) COROLLARY: (1) *Let* $s^*, t^* \in \mathrm{Inv}(G^*)$ *with* $t^* \neq s^*$. *Then* $s^*t^* \in \mathrm{Inv}(G^*)$.
(2) $\mathrm{Inv}(G^*) \subseteq O_2(G^*)$.

Proof: Suppose $|s^*t^*| > 2$ and set $a := st$. Since $|a^*| > 2$,

$$t^* \in N_{G^*}(\langle a^*\rangle) \setminus C_{G^*}(a^*)$$

and $|t^*| = 2$, contradicting 2.3.4. This shows part (1) of the corollary. Part (2) is immediate from part (1). ∎

We now prove the Main Theorem. Part (1) of the Main Theorem is 2.3.4 and 2.3.5. Part (2) of the Main Theorem is 2.4.1. Note now that for any $N \leq M \triangleleft G$, G/M satisfies all our hypotheses for G^* and hence, by 2.4.2, $\mathrm{Inv}(G/M) \subseteq O_2(G/M)$. This implies that for any normal subgroup $M^* \triangleleft G^*$, $\mathrm{Inv}(G^*/M^*) \subseteq O_2(G^*/M^*)$. In particular, this holds for $M^* = O_2(G^*)$, so $G^*/O_2(G^*)$ has odd order and this completes the proof of the Main Theorem. ∎

We now prove Lemma 1. So here we drop the assumption that $\deg(D) = 3$ and the assumption that G^* is finite. Let $a \in G$, with $a^* \in Z(G^*)$. Then by Wedderburn's Factorization Theorem (see [10] or Theorem 0.4, p. 181 in [5]), $m_a(\lambda) = (\lambda - d_m)(\lambda - d_{m-1})\cdots(\lambda - d_1)$, where $m = \deg(a)$, $d_1 = a$ and d_i are conjugates of a in G, $1 \leq i \leq m$. Thus d_i^* are conjugates of a^* in G^*, so since $a^* \in Z(G^*)$, $d_i^* = a^*$ for all i. Since $\prod_{i=m}^{1} d_i \in F^\times$, $(a^*)^m = 1^*$ and, as $m \mid \deg(D)$, Lemma 1 holds. ∎

The 'in particular' part of Lemma 1 is immediate since, if $N \leq M \triangleleft G$ is such that $M/N = [H,H]$, then M satisfies the hypotheses of Lemma 1 and $G/M \simeq H/[H,H]$ is abelain. ∎

References

[1] S. Amitsur, *Rational identities and application to algebra and geometry*, Journal of Algebra **3** (1966), 304–359.

[2] M. Aschbacher, *Finite Group Theory*, Cambridge University Press, 1986.

[3] D. E. Haile and L. H. Rowen, *Factorization of polynomials over division algebras*, Algebra Colloquium **2** (1995), 145–156.

[4] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, "Nauka" Publishers, Moscow, 1991 (English translation: "Pure and Applied Mathematics" series, N139, Academic Press, New York, 1993).

[5] L. H. Rowen, *Wedderburn's method and algebraic elements of simple artinian rings*, Contemporary Mathematics **124** (1992), 179–202.

[6] L. H. Rowen, *Elements of degree 3 and 4 in division algebras*, Contemporary Mathematics **184** (1995), 405–410.

[7] W. R. Scott, *Group Theory*, Prentice-Hall, Engelwood Hills, New Jersey, 1964.

[8] Y. Segev, *On finite homomorphic images of the multiplicative group of a division algebra*, Annals of Mathematics, to appear.

[9] Y. Segev and G. M. Seitz, *Anisotropic groups of type A_n and the commuting graph of finite simple groups*, submitted.

[10] J. H. M. Wedderburn, *On division algebras*, Transactions of the American Mathematical Society **22** (1921), 129–135.