BULL. AUSTRAL. MATH. SOC. 16K20
VOL. 59 (1999) [105–110]

SOME APPLICATIONS OF WEDDERBURN'S FACTORISATION THEOREM

YOAV SEGEV

The structure of finite quotients of "large" subgroups of the multiplicative group of a finite dimensional division algebra is interesting and is related to the Margulis-Platonov conjecture. We develop machinery to handle such quotients and we conjecture that finite quotients of the multiplicative group of a finite dimensional division algebra are solvable. The proofs rely on Wedderburn's Factorisation Theorem.

0. INTRODUCTION

The purpose of this paper is to continue building up machinery to handle finite quotients of various "large" subgroups of the multiplicative group of a finite dimensional division algebra. In the paper [5] we developed some such machinery, and this was applied in [6] to show that the multiplicative group of a finite dimensional division algebra has no non-abelian finite simple quotients. This, in turn, solved the Margulis–Platonov conjecture for inner forms of anistropic algebraic groups of type A_n (see [**6, 5, 3**] and [**2,** Chapter 9]). The techniques of this paper are very different from the techniques developed in [5] (and are easier in some sense). We hope that together with [5] and additional machinery, yet to be discovered, we shall have enough theory to attack the last remaining open case of the Margulis-Platonov conjecture – the outer forms of anistropic algebraic groups of type A_n (see [**2,** Chapter 9]), which is a major goal we have in mind. In addition, we get results on finite dimensional division algebras over any field, and not only over number fields.

Since we are dealing with machinery, the nature of our two main theorems is somewhat technical. However, the applications are already at hand; initial results using ideas incorporated in Theorem 1 below were used in [4] where we proved that the finite quotients of the multiplicative group of a division algebra of degree 3 are solvable. Further applications are deferred to a later paper. Hopefully a strengthening of these theorems will prove the conjecture we formulate below.

Received 26th June, 1998
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.

Throughout this paper D is a finite dimensional division algebra over its centre $F := Z(D)$. We denote $D^\times = D\backslash\{0\}$ and we let $G = D^\times$, the multiplicative group of D. We set $F^\times = F\backslash\{0\}$. We let N be a normal subgroup of G such that $F^\times \leqslant N$ 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 $a^* = Na$. In what follows λ is a commutative indeterminate over D and all polynomials are taken from $D[\lambda]$–the ring of polynomials over D.

THEOREM 1. *Let $a \in D\backslash N$ and let $|a^*|$ be the order of a^* in G^*. Let $m_a(\lambda)$ be the minimal polynomial of a over F. Suppose $|a^*|$ is an odd prime and that $1 < k_2, \ldots, k_i < |a^*|$ are distinct integers and satisfy: $(a^*)^{k_j}$ is conjugate to a^* in G^*, $2 \leqslant j \leqslant i$. Then we can write*

$$m_a(\lambda) = h(\lambda)(\lambda - d_i)(\lambda - d_{i-1})\cdots(\lambda - d_1)$$

where $d_1 = a$, and $d_j^* = (a^*)^{k_j}$, $2 \leqslant j \leqslant i$.

Theorem 1 is of course related to Wedderburn's Factorisation Theorem (see Theorem 1.1 in Section 1), it says that to a certain extent we can "control" the images in G^* of the elements d_j appearing in a factorisation. As a corollary to Theorem 1 we get the following Theorem 2, which, as the reader can observe, already invites applications. In Theorem 2, $\mathrm{Aut}_{G^*}(\langle a^*\rangle)$ is the normaliser of $\langle a^*\rangle$ modulo the centraliser of $\langle a^*\rangle$ in G^*. Also $\deg(a)$ is the degree of the minimal polynomial of a.

THEOREM 2. *Let $a \in G\backslash N$ be such that $|a^*| = p$ is an odd prime. Let $\alpha = |\mathrm{Aut}_{G^*}(\langle a^*\rangle)|$. Then either $\alpha = 1$ or $\alpha < \deg(a) - 1$, or $\alpha = \deg(a)$.*

Finally we mention that by [6], the Margulis-Platonov conjecture holds for inner forms of anisotropic algebraic groups of type A_n, in particular, if F is a number field (= finite extension of $\mathbb{Q}$), then finite quotients of $D^\times$ are solvable. Further in [6] we proved that finite quotients of $D^\times$ are never nonabelian simple. In view of this, the results in [4] and Theorem 2, we formulate the following conjecture.

CONJECTURE F.SO.Q. (Finite Solvable Quotients) Finite quotients of the multiplicative group of a finite dimensional division algebra are solvable.

1. THE PROOF OF THEOREM 1 AND THEOREM 2

We continue with the notation of the introduction. In particular, D, F, G, N and G^* are as in the introduction.

REMARK 1.1. Note that since $F^\times \leqslant N$, for all $a \in G$ and $\alpha \in F^\times$, $(\alpha a)^* = a^*$. We shall use this fact without further reference.

https://doi.org/10.1017/S0004972700032640 Published online by Cambridge University Press

Recall from the introduction that λ is a commutative indeterminate over D and all polynomials are taken from $D[\lambda]$–the ring of polynomials over D. Given $a \in G\backslash F$, we denote by $m_a(\lambda) \in F[\lambda]$, the (monic) minimal polynomial of a over F and by $\deg(a)$, the degree of $m_a(\lambda)$. Given a group H and elements $x, y \in H$, $x^y := y^{-1}xy$.

The following theorem is due to Wedderburn [7], except that part (3) is an improvement due to Haile and Rowen [1], where they show that not only does there exist a factorisation as in (3) of the theorem (Wedderburn factorisation) but all factorisations are like this.

THEOREM 1.2. (Wedderburn and Haile-Rowen.) *Let $a \in D\backslash F$ with $\deg(a) = m$. Then*

(1) *There exists $a = d_1, d_2, \ldots, d_m \in D$ such that*

$$m_a(\lambda) = (\lambda - d_m)(\lambda - d_{m-1}) \cdots (\lambda - d_1).$$

Given a factorisation as in (1) set

$$f_i(\lambda) = (\lambda - d_i)(\lambda - d_{i-1}) \cdots (\lambda - d_1), \ 1 \leqslant i \leqslant m.$$

(2) *Given a factorisation as in (1), let $1 \leqslant i < m$ and write $m_a(\lambda) = h(\lambda) f_i(\lambda)$. Let $x \in G$ be such that $f_i\left(a^{x^{-1}}\right) \neq 0$ and let $y = f_i\left(a^{x^{-1}}\right)x$. Then $a^{y^{-1}}$ is a root of $h(\lambda)$. In particular, $m_a(\lambda) = q(\lambda)\left(\lambda - a^{y^{-1}}\right) f_i(\lambda)$, for some polynomial $q(\lambda)$.*

(3) *Given a factorisation as in (1), there are elements $x_1, x_2, \ldots, x_{m-1} \in G$ such that if we set*

$$y_i = f_i\left(a^{x_i^{-1}}\right)x_i, \quad 1 \leqslant i \leqslant m-1$$

then $y_i \neq 0$ and $\quad d_{i+1} = a^{y_i^{-1}}, \quad 1 \leqslant i \leqslant m-1.$

1.3. Let $a \in D\backslash F$. Let

$$m_a(\lambda) = (\lambda - d_m)(\lambda - d_{m-1}) \cdots (\lambda - d_1)$$

be a factorisation of $m_a(\lambda)$ and let the notation be as in Theorem (1.2) (1). Let $1 \leqslant i < m$ and let $x \in G$. For $1 \leqslant j \leqslant i$, set $v_j = f_j\left(a^{x^{-1}}\right)x$ and let $v_0 = x$. Then

$$(*) \qquad v_j = v_{j-1}a - d_j v_{j-1}, \quad 1 \leqslant j \leqslant i.$$

https://doi.org/10.1017/S0004972700032640 Published online by Cambridge University Press

PROOF: For $j = 1$, it is easy to check that $(*)$ holds. Let $1 < j \leqslant i$ and let $b \in D$. Then $f_j(b) = f_{j-1}(b)b - d_j f_{j-1}(b)$. Replacing b by $a^{x^{-1}}$ we get

$$\text{(i)} \qquad f_j\left(a^{x^{-1}}\right) = f_{j-1}\left(a^{x^{-1}}\right)a^{x^{-1}} - d_j f_{j-1}\left(a^{x^{-1}}\right).$$

Multiplying both sides of the equality (i) by x on the right gives the lemma. □

PROPOSITION 1.4. *Let $a \in D\backslash F$ be such that $|a^*| = p$ is an odd prime. Suppose $m_a(\lambda) = h(\lambda)f_i(\lambda)$, with $1 \leqslant i < \deg(a)$, $f_i(\lambda) = (\lambda - d_i)(\lambda - d_{i-1})\cdots(\lambda - d_1)$, $d_1 = a$, $d_j^* = (a^*)^{k_j}$, and $2 \leqslant k_j < |a^*|$, $2 \leqslant j \leqslant i$. Suppose further that $k_2, \ldots, k_i$ are distinct. Let $x \in G$ be such that $\left(a^{x^{-1}}\right)^* = (a^*)^k$, with k distinct from $1, k_2, \ldots, k_i$ modulo p. Then*

(1) $f_i\left(a^{x^{-1}}\right) \neq 0$.

(2) *Let $d_{i+1} = a^{\left(f_i\left(a^{x^{-1}}\right)x\right)^{-1}}$. Then $m_a(\lambda) = g(\lambda)(\lambda - d_{i+1})f_i(\lambda)$ and $d_{i+1}^* = (a^*)^k$.*

PROOF: For $1 \leqslant j \leqslant i$, let

$$f_j(\lambda) = (\lambda - d_j)(\lambda - d_{j-1})\cdots(\lambda - d_1),$$
$$v_j := f_j\left(a^{x^{-1}}\right)x, \quad 1 \leqslant j \leqslant i,$$
$$v_0 = x.$$

By 1.3,

$$\text{(i)} \qquad v_j = v_{j-1}a - d_j v_{j-1}, \quad 1 \leqslant j \leqslant i.$$

Suppose $f_i\left(a^{x^{-1}}\right) = 0$. Let i_0 be minimal subject to $f_{i_0}\left(a^{x^{-1}}\right) = 0$. Since $k \not\equiv 1 (\mathrm{mod}\ p)$, it follows that $i_0 > 1$. By (i), $0 = v_{i_0} = v_{i_0-1}a - d_{i_0}v_{i_0-1}$. Thus $d_{i_0} = a^{v_{i_0-1}^{-1}}$. By induction on i, $d_{i_0}^* = \left(a^{v_{i_0-1}^{-1}}\right)^* = (a^*)^k$. But $d_{i_0}^* = (a^*)^{k_0}$, contradicting the choice of k. This shows (1).

Now by (i)

$$\text{(ii)} \qquad v_i = v_{i-1}a - d_i v_{i-1} = \left(a^{v_{i-1}^{-1}d_i^{-1}} - 1\right)d_i v_{i-1}.$$

Also by induction on i (or in the case $i = 1$, by definition),

$$\text{(iii)} \qquad \left(a^{v_{i-1}^{-1}}\right)^* = (a^*)^k.$$

https://doi.org/10.1017/S0004972700032640 Published online by Cambridge University Press

Thus $\left(a^{v_{i-1}^{-1}d_i^{-1}}\right)^* = (a^*)^{k-k_i}$. Note now that $\left(a^{v_{i-1}^{-1}d_i^{-1}} - 1\right)$ commutes with $\left(a^{v_{i-1}^{-1}d_i^{-1}}\right)$ in G, so

(iv) $$(a^*)^{k-k_i} \text{ commutes with } \left(a^{v_{i-1}^{-1}d_i^{-1}} - 1\right)^*.$$

Using (ii), (iii) and (iv) we get

$$\left((a^{k-k_i})^{v_i^{-1}}\right)^* = \left((a^{k-k_i})^{v_{i-1}^{-1}}\right)^{*\left(\left\{\left(a^{v_{i-1}^{-1}d_i^{-1}-1}\right)d_i\right\}^{-1}\right)^*}$$

$$= \left(a^{k(k-k_i)}\right)^{*\left(\left\{\left(a^{v_{i-1}^{-1}d_i^{-1}-1}\right)d_i\right\}^{-1}\right)^*} = (a^*)^{k(k-k_i)},$$

where the last equality follows from (iv) and the fact that $d_i^* = (a^*)^{k_i}$ (for $i > 1$ and $d_1^* = a^*$). Thus we see that $(v_i^*)^{-1}$ acts like $(x^*)^{-1}$ on $\langle (a^*)^{k-k_i}\rangle$ and hence also on $\langle a^*\rangle$ (since $|a^*|$ is a prime). Finally, by Theorem 1.2(2), since $f_i\left(a^{x^{-1}}\right) \neq 0$, $m_a(\lambda) = g(\lambda)(\lambda - d_{i+1})f_i(\lambda)$. □

Notice that Theorem 1 of the introduction is an immediate corollary of Proposition 1.4. We now prove Theorem 2 of the introduction.

THEOREM 2. *Let $a \in G\backslash N$ be such that $|a^*| = p$ is an odd prime. Let $\alpha = \left|\mathrm{Aut}_{G^*}(\langle a^*\rangle)\right|$. Then either $\alpha = 1$ or $\alpha < \deg(a) - 1$, or $\alpha = \deg(a)$.*

PROOF: Suppose $\alpha > 1$. Set $\deg(a) = m$ and suppose that $\alpha \geqslant m - 1$ and $\alpha \neq m$. Let φ be a generator of $\mathrm{Aut}_{G^*}(\langle a^*\rangle)$. Without loss of generality we may assume that $\varphi(a^*) = (a^*)^d$, for some $d \mid p - 1$. Define $k_2, \ldots, k_{m-1}$ by $k_j = d^{j-1}$. If $\alpha > m$, define $k_m = d^{m-1}$. Now $1 + \sum_{i=2}^{m-1} k_i = \left(d^{m-1} - 1\right)/(d-1)$. So

(i) $$\text{if } \alpha = m - 1, \text{ then } p \text{ divides } 1 + \sum_{i=2}^{m-1} k_i,$$

while

(ii) $$\text{if } \alpha > m, \text{ then } 1 + \sum_{i=2}^{m} k_i = \frac{d^m - 1}{d-1} \text{ and } p \text{ does not divide } 1 + \sum_{i=2}^{m} k_i.$$

By Theorem 1 we can choose $a = d_1, d_2, \ldots, d_m$ such that

$$m_a(\lambda) = (\lambda - d_m)(\lambda - d_{m-1}) \cdots (\lambda - d_1)$$

https://doi.org/10.1017/S0004972700032640 Published online by Cambridge University Press

and

(iii) $$d_i^* = (a^*)^{k_i}, \text{ for } 2 \leqslant i \leqslant m-1.$$

Further if $\alpha > m$, then we can take d_m such that $d_m^* = (a^*)^{k_m}$. Note now that $(d_m d_{m-1}, \ldots, d_1)^* = 1^*$. But by (i) and (iii), if $\alpha = m-1$, then $(d_{m-1}, \ldots, d_1)^* = 1^*$, so $d_m^* = 1^*$, which is false since d_m^* in conjugate to a^*; while if $\alpha > m$, then by (ii) and (iii) $(d_m d_{m-1}, \ldots, d_1)^* \neq 1^*$, a contradiction. This proves the theorem. □

References

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

[2] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory* (Nauka Publishers, Moscow, 1991). (English translation: Pure and Applied Mathematics **139** (Academic Press, Boston MA, 1993)).

[3] A. Potapchik and A. Rapinchuk, 'Normal subgroups of $SL_{1,D}$ and the classification of finite simple groups', *Proc. Indian Acad. Sci. Math. Sci* **106** (1996), 329–368.

[4] L. Rowen and Y. Segev, 'The finite quotients of the multiplicative group of a division algebra of degree 3 are solvable', *Israel J. Math.* (to appear).

[5] Y. Segev, 'On finite homomorphic images of the multiplicative group of a division algebra', *Ann. Math* (to appear).

[6] Y. Segev and G.M. Seitz, 'Anistropic groups of type A_n and the commuting graph of finite simple groups', (submitted).

[7] J.H.M. Wedderburn, 'On division algebras', *Trans. Amer. Math. Soc.* **22** (1921), 129–135.

Department of Mathematics
Ben-Gurion University
Beer-Sheva 84105
Israel