Proceedings of the Edinburgh Mathematical Society (1990) **33**, 97–111 ©

SOME MATRIX GROUPS OVER FINITE-DIMENSIONAL DIVISION ALGEBRAS

by B. A. F. WEHRFRITZ

(Received 14th July 1988)

Let n be a positive integer and D a division algebra of finite dimension m over its centre. We describe in detail the structure of a soluble subgroup G of $GL(n,D)$. (More generally we consider subgroups of $GL(n,D)$ with no free subgroup of rank 2.) Of course G is isomorphic to a linear group of degree mn and hence linear theory describes G, but the object here is to reduce as far as possible the dependence of the description on m. The results are particularly sharp if $n=1$. They will be used in later papers to study matrix groups over certain types of infinite-dimensional division algebra. This present paper was very much inspired by A. I. Lichtman's work: Free subgroups in linear groups over some skew fields, *J. Algebra* **105** (1987), 1–28.

1980 *Mathematics subject classification* (1985 Revision): 20H25 (cross ref. 16A39).

Let n be a positive integer, D a division ring of finite dimension d^2 over its centre F and suppose that

(a) *G is a subgroup of $GL(n,D)$ containing no non-cyclic free subgroups.*

Then Theorem B of Lichtman's paper [**3**] describes in some detail the structure of G under the further assumptions that

(b) $d=q^m$ *for some prime* q,

(c) $n<q-1$ *and*

(d) $\operatorname{char} F\neq 0$.

We give here a quite short derivation of this, indeed of a slightly stronger structure, and without hypotheses (b), (c) and (d). We make use of our results here in [**7**] and [**8**] to study matrix groups over more general division rings. We isolate the basic results concerning finite-dimensional division algebras in this paper in case they have a wider appeal.

Below q is always a prime and m is always a positive integer. The maximal unipotent normal subgroup of G we denote by $u(G)$. Our main result is the following:

Theorem 1. *Let G satisfy* (a). *Then G has normal subgroups*

$$\langle 1\rangle \leqq U \leqq A \leqq H \leqq K \leqq G$$

such that $U=u(G)$ is unipotent, A/U is central in H, H/A is locally finite, K/H is a *subdirect product of n groups of orders at most nd and dividing n!d and G/K is isomorphic to a subgroup of the symmetric group* Sym(n) *of degree n. Moreover if* (b) *also holds then we can choose K so that K/H is a subdirect product of n groups of orders dividing d.*

Let $d=q^m$. The object of the exercise is to derive conclusions independent of q, for then certain information about skew linear groups of characteristic zero can be obtained, see [3]. With $d=q^m$ the group K/H of Theorem 1 is a finite q-group of order dividing q^{mn} and exponent dividing q^m but nilpotency class less than $\max\{2,m\}$. The latter bound is independent of q. By Schur's theorem the derived group P/U of H/U is locally finite. Thus the following is an immediate consequence of the theorem.

Corollary 1. *Assume* (a) *and* (b). *Then G has normal subgroups*

$$\langle 1\rangle \leqq U \leqq P \leqq H \leqq K \leqq G$$

such that $U=u(G)$ *is unipotent,* P/U *is locally finite,* H/P *is abelian,* K/H *is finite nilpotent of class less than* $\max\{2,m\}$ *and the index* $(G:K)$ *divides* $n!$. *If also* (d) *holds then* P *itself is locally finite.*

Lichtman [3, Theorem B] is essentially Corollary 1 assuming also (c) and (d) and with $(G:K)\leqq(n!)^2$ instead of $(G:K)|n!$.

In Theorem 1 again let P/U be the derived group of H/U and suppose G is soluble. The derived length of U is at most $-[-\log_2 n]$, of H/P is at most 1, of K/H is at most the number of prime divisors of $n!d$ (at most $\max\{1,-[-\log_2 m]\}$ if $d=q^m$) and of G/K is less than n. If char $F\neq 0$ then Zalesskiĭ's theorem (see [4, 2.3.1]) yields that P/U is isomorphic to a linear group of degree n. If char $F=0$ by another theorem of Zalesskiĭ (see [4, 2.4.4]) there is a metabelian normal subgroup of P/U of index bounded by a function of n only. Thus the following is also a consequence of Theorem 1.

Corollary 2. *Let G satisfy* (a) *with G soluble. Then G has derived length bounded by a function of n and the number of prime divisors* (*with multiplicities*) *of d only.*

Suppose $d=q^m$ in Corollary 2. Again the bound depends on m and n but not on q. Explicit bounds for the derived length of G in this case are given by

$$-[-\log_2 n]+3n+\max\{1,-[-\log_2 m]\} \quad \text{if char } F\neq 0,$$

and

$$-[-\log_2 n]+f_s(n)+2+\max\{1,-[-\log_2 m]\}+n \quad \text{if char } F=0,$$

where $f_s(n)$ is the function of [4, 2.4.4].

In Corollary 1 one cannot (as claimed in [3]) choose K/H to have nilpotency class less than m. For example suppose $F=\mathbb{R}$ and D is the real quaterion algebra. Set $G=\langle j,\mathbb{C}^*\rangle\leqq D^*=GL(1,D)$. Here $q=2$, $m=1$ and $n=1$. Necessarily $U=\langle 1\rangle$ and $K=G$.

If $H=G$ then $G'=\mathbb{R}^{>0}$ is periodic, which it is not. Consequently $H\neq G$ and K/H has nilpotency class $1=m$.

We can copy this construction in any characteristic. (Thus [3, Theorem B] needs a slight modification, namely $\gamma_{m,2}(U)$ to be replaced by $\gamma_{k,2}(U)$ for $k=\max\{2,m\}$.) For let $R=GF(p^q)[x]$ be the skew polynomial ring for any primes p and q, where x acts on the coefficient field as the Frobenius automorphism. Then R has a division ring D of quotients. If F is the centre of D then $(D:F)=q^2$. Let ζ be a primitive (p^q-1)th root of unity in $GF(p^q)$ and set $E=F(\zeta)$ and $G=\langle x,E^*\rangle$. In the notation of Theorem 1, we have $d=q$, $m=n=1$ and necessarily $U=\langle 1\rangle$ and $K=G$. Now G' is not periodic, for

$$G'=[E^*,x]=\langle a^{-1}a^x : a\in E^*\rangle$$

and so G' contains the element $(\zeta+x^q)^{-1}(\zeta^p+x^q)$ of infinite order. Thus $H\neq G$ and again K/H has nilpotency class $m=1$. It is not difficult to produce examples of characteristic zero for odd, q, cf. Point 4 below.

After the proof of Theorem 1 we construct further examples. In particular we show that the structure given in Theorem 1 for $d=q^m$ is essentially the best possible. If in Theorem 1 the degree $n=1$ then much more can be said. Certainly we must have $U=\langle 1\rangle$ and $K=G$.

Theorem 2. *Assume* (a) *and* (b) *and let* $n=1$. *Then* G *has normal subgroups*

$$\langle 1\rangle\leqq A\leqq H\leqq G$$

such that A *is abelian,* $H=C_G(A)$ *and either* (1) $(G:H)$ *divides* q^m *and* $A=H$, *or* (2) char $F=0$, $q=2$, $(G:H)$ *divides* 2^{m-1} *and* H/A *is isomorphic to* Alt(4), Sym(4), *or* Alt(5), *or* (3) char $F=0$, $q=2$, $(G:H)$ *divides* 2^{m-2} *and* H/A *is isomorphic to* Sym(5).

In proving Theorem 2 we describe the groups involved more explicitly. We also give examples to show that all the above cases do in fact arise. Note that Theorem 2 gives an excellent bound for the derived length of G for G soluble, $n=1$ and $d=q^m$.

Suppose in Theorem 1 that either char $F=0$ or G is soluble. It is an easy consequence of our proof below of Therorem 1, that A can be chosen so that $(G:A)$ is finite and bounded by a function of nd only. Theorems 1 and 2 suggest that if $d=q^m$ then $(G:A)q^{-mn}$ should be boundable by a function of n only (we abbreviate this phrase to "n-bounded"). The best we have obtained is the following.

Theorem 3. *Assume* (a) *and* (b) *and suppose that either* char $F=0$ *or* G *is soluble. Then subgroups* U, A, H *and* K *can be chosen as in Theorem 1 along with a normal subgroup* Q *of* G *with* $A\leqq Q\leqq H$ *such that* Q/A *is an elementary abelian* q*-group of rank at most* $2mn$ *such that* $(Q:A)(K:H)$ *divides* q^{2mn} *and* $(H:Q)$ *is* n*-bounded. Further there is an abelian normal subgroup* A_1/U *containing* A/U *of* Q/U *such tht* $(Q:A_1)(K:H)$ *divides* q^{mn}.

Thus in Theorem 3 both $(G:A)q^{-2mn}$ and $(G:A_1)q^{-mn}$ are n-bounded.

As a final comment before the proofs we remark that division rings D of prime power dimension over their centre do arise naturally in some contexts. For example if L is a Lie algebra of characteristic $p>0$ and finite dimension l then the division ring of quotients of the universal enveloping algebra of L has finite dimension p^{2m} over its centre for some m with $2m \leqq l^2$, see [**1**, pages 204 and 189]. This fact is used crucially in [**3**, **7**, **8**].

The proof of Theorem 1

We deal first with the case $d=1$, so G is now a subgroup of $GL(n,F)$.

1. *If $d=1$ then G has normal subgroups $\langle 1\rangle \leqq U \leqq A \leqq H \leqq G$ with $U=u(G)$ unipotent, A/U central in H, H/A locally finite and G/H isomorphic to a subgroup of* $\mathrm{Sym}(n)$.

Proof. We may assume that F is algebraically closed. Passing to $G/u(G)$, we may also assume that G is completely reducible. By Tits' theorem (see [**5**] or [**6**, 10.17]) there is a soluble normal subgroup A of G with G/A locally finite. Replacing A by its connected component of the identity we may assume that A is Zariski connected. By the Lie–Kolchin theorem (see [**6**, 5.8]) the group A is triangularizable. Since $u(A) \leqq u(G) = \langle 1\rangle$ the group A is abelian. Set $H=C_G(A)$. By a result of Blichtfeldt (see [**6**, 1.12]) the group G/H is isomorphic to a subgroup of $\mathrm{Sym}(n)$ via its permutational representation on the set of homogeneous components of A. The proof is complete.

Schur's theorem and 1 yield the following.

2. *Let G be as in 1. Then G has normal subgroups $\langle 1\rangle \leqq U \leqq P \leqq H \leqq G$ with U unipotent, P/U locally finite, H/P abelian and G/H isomorphic to a subgroup of* $\mathrm{Sym}(n)$.

Suppose G is as in Theorem 1 and let E be a maximal subfield of D. Then G can be regarded as a subgroup of $GL(nd,E)$ in an obvious way. Thus by 1 there are normal subgroups U, A and H of G with U, A/U and H/A as in Theorem 1 and with G/H isomorphic to a subgroup of $\mathrm{Sym}(nd)$. It is difficult to see how to reduce the dependence here of G/H on d. We need to make a more subtle use of 1. Set $U=u(G)$. By [**4**, 1.1.2] we may pass to G/U and assume that G is a completely reducible subgroup of $GL(n,D)$.

3. *With G as in Theorem 1 and with G a completely reducible subgroup of $GL(n,D)$, let A be any maximal abelian normal subgroup of G and set $H=C_G(A)$.*

(a) *There exists a normal subgroup $L \supseteq H$ of G such that L/H is a subdirect product of $s \leqq n$ groups of orders dividing $n_i d$, $i=1,2,\ldots,s$, where $n_1+\cdots+n_s \leqq n$, and G/L is isomorphic to a subgroup of* $\mathrm{Sym}(s)$.

(b) *Suppose $d=q^m$. Then there is a normal subgroup $K \supseteq H$ of G such that K/H is a subdirect product of n groups of orders dividing q^m and G/K is isomorphic to a subgroup of* $\mathrm{Sym}(n)$.

Suppose for the moment that we have proved 3. By 1 there is a maximal abelian normal subgroup A of G such that G/A is locally finite and in fact any such A has G/A locally finite. Then Theorem 1 is now an immediate consequence of 3.

Proof of 3. Let $V = D^n$ be row n-space over D, regarded as a $D-G$ bimodule in the standard way. Let $V_1, \dots, V_r$ be the homogeneous components of V as $D-A$ module. By Clifford's theorem $V = \bigoplus V_i$, so if $n_i = \dim_D V_i$ then $r \leqq n$ and $n_1 + \cdots + n_r = n$. Let R denote the F-subalgebra of $D^{n \times n}$ generated by A. Then R is commutative and semisimple Artinian (e.g. [4, 1.1.12a]). Thus $R = F_1 \oplus \cdots \oplus F_s$ where each F_1 is an extension field of F.

On each $D-A$ irreducible submodule of V the F-algebra R acts as a simple ring (see [4, 1.1.12b]). Hence for each i there is a unique j such that F_j acts non-trivially on V_i. Thus $s \leqq r \leqq n$ and we can number the components such that F_i acts non-trivially on V_i for $1 \leqq i \leqq s$. In particular there is an F-algebra embedding of F_i into $\mathrm{End}_D V_i \cong D^{n_i \times n_i}$. Hence by Theorem 4.11 on p. 244 of [2] $\dim_F F_i$ divides $(\dim_F \mathrm{End}_D V_i)^{1/2} = n_i d$. Let G_i denote the Galois group of F_i over F. Then the order of G_i divides $n_i d$ too. Clearly G permutes the summands F_i of R under conjugation. Set $L = \bigcap_{i=1}^s N_G(F_i)$. Then G/L is isomorphic to a subgroup of $\mathrm{Sym}(s)$ and L/H is isomorphic to a subgroup of $G_1 \times G_2 \times \cdots \times G_s$. This proves (a).

Write $i \sim j$ if $F_i \cong_F F_j$ and $n_i = n_j$. Let S be the normalizer in $\mathrm{Sym}(s)$ of the $\sim$ equivalence classes in $\{1, 2, \dots, s\}$. Then part of the automorphism group of R as F-algebra can be identified with the split extension $W = S[G_1 \times \cdots \times G_s$, with $G_1 \times \cdots \times G_s$ acting componentwise and S naturally permuting the components. Assume now that $d = q^m$. It follows from Sylow's theorem that G_i contains a subgroup Q_i of order dividing q^m and index dividing n_i. (If $q | n_i$ then Q_i may not be a Sylow subgroup of G_i.) Now right multiplication by G_i on the right cosets of Q_i determines a homomorphism of G_i into $\mathrm{Sym}(n_i)$ with kernel say $K_i \leqq Q_i$. With a coherent choice of the Q_i the group $K_1 \times \cdots \times K_s$ is normal in W. Clearly K_i has order dividing q^m. Also $W/K_1 \times \cdots \times K_s$ is isomorphic to a subgroup of the split extension

$$T = S[\mathrm{Sym}(n_1) \times \cdots \times \mathrm{Sym}(n_s).$$

Note that this uses that $n_i = n_j$ if $i \sim j$. Since $n_1 + \cdots + n_s \leqq n$ the group T is isomorphic to a subgroup of $\mathrm{Sym}(n)$.

The natural conjugation action of G on R determines an embedding of G/H into W. Let K be the inverse image of $K_1 \times \cdots \times K_s$ in G under this map. Then $K \supseteq H$ is a normal subgroup of G, K/H is a subdirect product of s groups of orders dividing q^m and G/K is isomorphic to a subgroup of $\mathrm{Sym}(n)$. Part b is proved.

If in 3(b) one replaces $G/K \hookrightarrow \mathrm{Sym}(n)$ by the weaker condition that $(G:K) | n!$ then the above proof can be considerably shortened, since early on one can reduce to the case $V = V_1$.

4. Some examples

Let Q be a prime field of characteristic $p \geqq 0$. If $p > 0$ set $E = GF(p^{q^m}) \supseteq Q$, pick ζ so that $E = Q(\zeta)$ and let ξ be the Frobenius automorphism of E of order q^m. If $p = 0$ there exists by Dirichlet's theorem on primes in arithmetic progressions a prime l with $l\equiv 1$ modulo q^m. Let $E=Q(\zeta)$ where ζ is a primitive lth root of unity in $\mathbb{C}$. Then E has an automorphism ξ of order q^m.

The skew polynomial ring $E[x]$, with x acting on E as ξ, is a Noetherian domain; let D be its division ring of quotients. Set $F=C_E(x)(x^{q^m})$; then F is a central subfield of D with $(D:F)=q^{2m}$. If Z is the centre of D then x normalizes ZE and acts on it as an automorphism of order q^m. Thus $(ZE:Z)=q^m$. But ZE is a subfield of D, so $(D:Z)\geqq q^{2m}$ and therefore $F=Z$.

Set $G_1=\langle A_1,x\rangle\leqq D^*$ where A_1 is the multiplication group of the field FE. Then A_1 is an abelian normal subgroup of G_1, $C_{G_1}(A_1)=A_1$ and $(G_1:A_1)=q^m$. Suppose A is an abelian normal subgroup of G_1 with G/A periodic. Let K be the fixed field of $x^{q^{m-1}}$ in FE. Then A_1/K is not periodic; for example $(\zeta+x^{q^m})^r$ is not in K for every positive integer r. (For if otherwise

$$(\zeta+x^{q^m})^r=(\zeta^{q^{m-1}}+x^{q^m})^r,$$

which is not the case since $E[x^{q^m}]$ is a unique factorization domain.) It follows that $H\subseteq C_{G_1}(A\cap A_1)=A_1$, so $(G_1:H)\geqq q^m$ for all possible choices of A. Thus the structure of G/H given in Theorem 1 is the best possible for $n=1$ and $d=q^m$.

We now extend this construction to arbitrary n. Let S be the set of permutation matrices in $GL(n,D)$, identity G_1 with

$$\{\operatorname{diag}(g,l,\dots,l)\in GL(n,D): g\in G_1\}$$

and set $G_n=\langle S,G_1\rangle\cong G_1\wr\operatorname{Sym}(n)$ (permutational wreath product). If $A_n=\langle A_1^g: g\in G_n\rangle$, then A_n is an abelian normal subgroup of G_n and $A_n=C_{G_n}(A_n)$. Also $G_n/A_n\cong C\wr\operatorname{Sym}(n)$, where C is cyclic of order q^m. Since G_n is irreducible its unipotent radical is trivial. Let A be an abelian normal subgroup G_n with G_n/A periodic. Then by the above $C_{G_1}(A\cap A_1)=A_1$ and so with the notation as in Theorem 1,

$$H\leqq C_{G_n}(A)\leqq C_{G_n}(A\cap A_n)=A_n.$$

Thus we must have $H=A_n$ and $K/H=O_q(G_n/H)$, as then $(K:H)=q^{mn}$ and $G_n/K\cong\operatorname{Sym}(n)$, and this is for all possible choices of A. Thus the structure given in Theorem 1 for G/H is the best possible if $d=q^m$, for all n, q, m and characteristics $p\geqq 0$.

The theory of linear groups shows that even if $d=1$ there exists G such that necessarily $U\neq\langle 1\rangle$, A/U is infinite and H/A is non-trivial and, in positive characteristic, infinite. Such examples can be combined with the above to produce examples exhibiting simultaneously and non-trivially all the facets of Theorem 1.

The proof of Theorem 2

Here we have $d=q^m$ and $n=1$. Let A be any maximal abelian normal subgroup of G and set $H=C_G(A)$. By 3 we have that $(G:H)$ divides q^m. Let S be the maximal soluble normal subgroup of H, which exists, note, since G is isomorphic to a linear group (of degree q^m over a maximal subfield of D for example). Let B/A be an abelian normal subgroup of G/A in S/A, and maximal among such. Then $B \cap C_G(B) = A$ by the maximal choice of A and so $C_S(B) = A$ by the maximal choice of B. By the theory of linear groups (e.g. the Lie–Kolchin theorem) S has an abelian subgroup of finite index that is normal in G. Hence $(S{:}A)$, and in particular $(B{:}A)$, are finite.

Clearly B is nilpotent of class at most 2 with centre A. If A_1 is a maximal abelian subgroup of B then A_1 is normal in B and $A_1 = C_B(A_1)$. Thus $(B{:}A_1)$ divides q^m by 3. If P/A is the Sylow p-group of B/A for $p \neq q$ then $P \leqq A_1$, P is abelian and so $P = A$. Therefore B/A is a finite q-group, say of exponent q^e. Since B is nilpotent of class at most 2, so B' has eponent dividing q^e. Thus if $e > 1$ then $AB^{q^{e-1}}$ is abelian and hence is A. Consequently B/A is an elementary abelian q-group. Let T denote the torsion subgroup of B. Since H' is periodic we have $[B, H] \leqq B \cap H' \leqq T$.

5. *If G is soluble and T is abelian then $A = H$.*

For here T lies in A and H centralizes A and B/T. By stability theory $H/C_H(B)$ is isomorphic to a subgroup of $\mathrm{Hom}(B/A, T)$. The latter is a finite q-group since B/A is a finite q-group and T is abelian of rank at most 1. As G is soluble, $S = H$ and $C_H(B) = A$. Therefore G/A is a finite q-group.

Suppose $A \neq H$. Then there exists $h \in H/A$ such that hA is central in G/A. But then $\langle h, A \rangle$ is an abelian normal subgroup of G greater than A. This contradiction shows that $A = H$.

Assume from now on that 5 does *not* apply.

6. *Then* $\mathrm{char}\, F = 0$ *and either* (1) *G is insoluble or* (2) *G is soluble, $q = 2$ and $T = Q(A \cap T)$ where Q is* (*locally*) *quaternion of order 2^α and $3 \leqq \alpha \leqq \infty$.*

For suppose $\mathrm{char}\, F \neq 0$. By [4, 2.3.1] the group H' is abelian, so G is soluble. By the same result T is abelian. Thus $\mathrm{char}\, F = 0$. Suppose G is soluble. Then as 5 does not apply T is non-abelian. Then $T = Q \times Q_1$ where Q is a 2-group and Q_1 is a 2′-group, and necessarily Q_1 is abelian (see [4, 2.5.3]) and Q is (locally) quaternion (see [4, 2.1.2]). In particular $Q_1 \leqq A$, so $T = Q(A \cap T)$. Finally B/A is a q-group and $T/(A \cap T)$ is a non-trivial 2-group, so $q = 2$.

7. *If G is soluble and $(T{:}A \cap T) = 2$ then $A = H$.*

Here H stabilizes the series $\langle 1 \rangle \leqq A \cap T \leqq T \leqq B$. Stability theory produces embeddings of $H/C_H(B/A \cap T)$ into the finite 2-group $\mathrm{Hom}(B/AT, T/A \cap T)$ and of $C_H(B/A \cap T)/C_H(B)$ into the finite 2-group $\mathrm{Hom}(B/A, A \cap T)$. Thus $G/A = G/C_H(B)$ is a finite 2-group and we obtain $A = H$ exactly as in the second paragraph of the proof of 5.

8. *Assume G is soluble and 5 and 7 do not apply. Then $\alpha = 3$, there is an element g of G of odd order modulo A not centralizing Q, $B = QA$, $(G{:}H)$ divides 2^{m-1} and H/A is isomorphic to* Alt(4) *or* Sym(4).

Note that 7 and 8 settle completely Case (2) of 6. Suppose $\alpha > 3$. Then Q has a characteristic abelian subgroup A_1 of index 2. Then $A_1 \leqq A$. Consequently $(T{:}A \cap T) = 2$ and 7 applies. Hence $\alpha = 3$. Now suppose no such element g exists. The outer automorphism group of Q is Sym(3). Thus there is a (cyclic) subgroup of Q of order 4 and normal G. Again this implies that $(T{:}A \cap T) = 2$ so such an element g does exist.

Suppose $QA \neq B$. Now G/H is a finite 2-group and H centralizes the finite 2-group B/QA. Hence there exists $b \in B \backslash QA$ such that $[b, G] = \subseteq QA$. If b centralizes Q then the centre of $QA\langle b\rangle$ is normal in G and contains $A\langle b\rangle$. This contradicts the maximality of A and so b induces an automorphism of Q of order 2. If b induces an inner automorphism of Q there is some b_1 in QAb centralizing Q. Replacing b by b_1 produces a contradiction. Thus b induces a non-trivial outer automorphism of Q. Therefore

$$\langle b, g\rangle Q/C_{\langle b,g\rangle Q}(Q)Q \cong \mathrm{Sym}\,(3) \cong \mathrm{Out}\,(Q).$$

But the image of $B \cap \langle b, g\rangle Q$ in Sym (3) is then a non-trivial normal 2-subgroup of Sym (3). This contradiction shows that $B = QA$.

Thus $A = C_H(B) = C_H(Q)$ and H/A embeds into the automorphism group of Q, which is isomorphic to Sym (4). Moreover H/A contains the non-trivial element gA of odd order and the normal Klein 4-subgroup QA/A. Thus H/A is isomorphic to Alt (4) or Sym (4).

It remains only to prove that $(G:H)$ divides 2^{m-1} and we know already that it divides 2^m. Let y be an element of Q of order 4. Then $A\langle y\rangle$ is abelian and $(G:N_G(A\langle y\rangle))$ divides 3. By 3 again $(N_G(A\langle y\rangle):C_G(A\langle y\rangle))$ divides 2^m. Also $(Q:C_Q(y)) = (Q:\langle y\rangle) = 2$, so 2 divides $(H:C_G(A\langle y\rangle))$. Hence $2(G:H)$ divides $(G:C_G(A\langle y\rangle))$, which divides 2^m3. Since $(G:H)$ is a power of 2, it follows that $(G:H)$ divides 2^{m-1}.

Assume from now on that Case (1) of 6 holds. Let $L = H'$ and $C = C_G(L)$. Then L is locally finite and insoluble, so by Amitsur's theorem (see [**4**, 2.1.4 or 2.1.11]) we have L isomorphic to $SL(2, 5)$. In particular $C \cap L = \langle -1\rangle$.

Let E be the $\mathbb{Q}$-subalgebra of D generated by L. Then E is a quaternion algebra over $\mathbb{Q}(\sqrt{}5)$, see the proof of [**4**, 2.1.11]. In particular $(E:\mathbb{Q}) = 8$. Thus $FE = F[L] \leqq D$ is a non-communative division F-algebra of dimension over F at most 8. Since FE has dimension a square over its centre, this degree must be 4 and

$$4 \,\big|\, (FE:F) \,\big|\, (D:F).$$

Therefore:

9. *we have* $q = 2$.

The automorphism group of $SL(2, 5)$ is $PGL(2, 5) \cong \mathrm{Sym}\,(5)$. Thus either $G = CL$ and $G/C \cong \mathrm{Alt}\,(5)$, or $(G:CL) = 2$ and $G/C \cong \mathrm{Sym}\,(5)$.

10. *Suppose* $G = CL$. *Then* $A = C \cap H$, $H = AL$, $H/A \cong \mathrm{Alt}\,(5)$, $(G:H)$ *divides* 2^{m-1} *and* $G/A = C/A \times H/A$.

For clearly the 2-group G/H is soluble, so C is soluble. Also G/C is simple, so every abelian normal subgroup of G lies in C. Further $[C, L] = \langle 1\rangle$ and $CL = G$, so the abelian normal subgroups of C are exactly the abelian normal subgroups of G. In particular A is a maximal abelian normal subgroup of C. Let Q be a Sylow 2-subgroup of L, so Q is quaternion of order 8, and let y be an element of Q or order 4. Then $A\langle y\rangle$ is a maximal abelian normal subgroup of CQ, for if $A_1 \geqq A\langle y\rangle$ is abelian and normal in CQ, then $A_1 \cap C = A$ and $CA_1 \neq CQ$ as y is central in CA_1. But $(CQ:C)=4$ and $(C\langle y\rangle:C)=2$. Therefore $C\langle y\rangle = CA_1$ and $A\langle y\rangle = A_1$ as claimed.

By 8 we have $A\langle y\rangle = C_{CQ}(A\langle y\rangle)$ and $(CQ:A\langle y\rangle)$ divides 2^m. Hence $A \leqq C\cap H \leqq C\cap A\langle y\rangle = A$. Also $-1 \in A\cap\langle y\rangle$, $CQ/\langle -1\rangle = C/\langle -1\rangle \times Q/\langle -1\rangle$ and $(Q:\langle y\rangle)=2$. Consequently $(C:A)$ divides 2^{m-1}. Clearly $H=(C\cap H)L = AL$ and $G=CH$. Hence $G/A = C/A \times H/A$, $H/A \cong G/C \cong \mathrm{Alt}(5)$ and $(G:H)=(C:A)$ divides 2^{m-1}.

Assume now that $G \neq CL$. Pick $g \in G\backslash CL$ with $g^2 \in C$. Since $G/C \cong \mathrm{Sym}(5)$ has no non-trivial abelian normal subgroups, again the abelian normal subgroups of G lie in C. In particular $A \leqq C$ and $AL \leqq H$.

11. *We have* $m \geqq 2$.

For suppose otherwise; that is assume $(D:F)=4$. Now $E=\mathbb{Q}[L] \leqq D$ has degree 4 over $\mathbb{Q}(\surd 5)$ and $FE = F(\surd 5)\otimes_{\mathbb{Q}(\surd 5)} E$, for example by [2, p.218, Theorem 4.7]. Hence

$$4 = (FE:F(\surd 5)) \leqq (D:F) = 4.$$

Therefore $FE=D$, $F(\surd 5)=F$ and $\mathbb{Q}(\surd 5)$ is central in D. Thus g induces a $\mathbb{Q}(\surd 5)$ automorphism of E by conjugation.

By the Skolem–Noether theorem (see [2, p. 222]) there exists $e \in E$ inducing by conjugation the same automorphism of E as g. Now E naturally sits inside the real quaternion algebra $\mathbb{R}(E)$. Then $\mathbb{R}(e) \leqq \mathbb{R}E$, as a non-trivial finite extension of $\mathbb{R}$, is a copy of $\mathbb{C}$. Since $g^2 \in C$ we have $e^2 \in \mathbb{R}$, $e \notin \mathbb{R}$. Hence $e = \alpha f$ for some non-zero real α and some $f \in \mathbb{R}(e)$ with $f^2 = -1$. Clearly f induces by conjugation the same automorphism on L as e and g. Therefore $\langle f\rangle L$ is a finite insoluble subgroup of the division algebra $\mathbb{R}E$ not isomorphic to $SL(2,5)$. This contradiction of Amitsur's theorem proves that $m \geqq 2$.

We make one further subdivision, according to whether or not $H \leqq CL$.

12. *Suppose* $H \leqq CL$. *Then* $A = C\cap H$, $H = AL$, $H/A \cong \mathrm{Alt}(5)$, $(G:H)$ *divides* 2^{m-1}, $CL/A = C/A \times H/A$ *and* $G/C \cong \mathrm{Sym}(5)$.

Notice here that H/A is not a direct factor of G/A, for if it were we would have $G = H\,.\,C_G(H/A)$ and $\mathrm{Sym}(5) = \mathrm{Alt}(5)\,.\,C_{\mathrm{Sym}(5)}(\mathrm{Alt}(5))$. This is really the distinguishing feature between Cases 10 and 12.

A is actually a maximal abelian normal subgroup of $\langle g\rangle C$ for if $A_1 \geqq A$ is abelian and normal in $\langle g\rangle C$, then $A_1 \leqq H \leqq CL$, so $A_1 \leqq \langle g\rangle C \cap CL = C$. Thus A_1 is normalized by $\langle g\rangle C$ and centralized by L and therefore A_1 is normal in $\langle g\rangle CL = G$. Consequently $A_1 = A$. Again G/H and C are soluble. There is a Sylow 2-subgroup Q of L normalized by g with a subgroup $\langle y\rangle$ of order 4 inverted by g. Suppose $A_2 \geqq A\langle y\rangle$ is an abelian normal subgroup of $\langle g\rangle CQ$. Then $A_2 \cap \langle g\rangle C = A$, $(CQ:C)=4$, $(C\langle y\rangle:C)=2$ and y is central in CA_2 but is not central in CQ. But

$$A_2 \leqq H \cap \langle g \rangle CQ \leqq CL \cap \langle g \rangle CQ = CQ.$$

Therefore $CA_2 = C\langle y \rangle$, $A_2 = A\langle y \rangle$ and $A\langle y \rangle$ is a maximal abelian normal subgroup of $\langle g \rangle CQ$.

By 8 we have that $A\langle y \rangle = C_{\langle g \rangle CQ}(A\langle y \rangle)$ and $(\langle g \rangle CQ : A\langle y \rangle)$ divides 2^m. In particular

$$A \leqq C \cap H \leqq C \cap A\langle y \rangle = A.$$

Also $L \leqq H \leqq CL$, so $H = (C \cap H)L = AL$, $CL = CH$ and $CL/A = C/A \times H/A$. Further $H/A \cong L/\langle -1 \rangle \cong \mathrm{Alt}(5)$ and $(G:H) = 2(C:A)$. But

$$(\langle g \rangle)CQ : A\langle y \rangle) = (\langle g \rangle CQ : CQ)(C:A)(Q:\langle y \rangle) = 4(C:A)$$

divides 2^m. Therefore $(C:A)$ divides 2^{m-2} and $(G:H)$ divides 2^{m-1}. Finally that $G/C \cong \mathrm{Aut}(L) \cong \mathrm{Sym}(5)$ we have already recorded.

13. *Suppose $H \nleqq CL$. Then $A = C \cap H$, $H/A \cong \mathrm{Sym}(5)$, $(G:H)$ divides 2^{m-2} and $G/A = C/A \times H/A$.*

Here $G = CH$. Again C is soluble. Let $A_1 \geqq A$ be a maximal abelian normal subgroup of C. By 8 we have $A_1 = C_C(A_1)$ and $(C:A_1)$ divides 2^m. Clearly CL normalizes A_1 and $A_1 \cap A_1^g$ is normal in G. The maximality of A yields that $A = A_1 \cap A_1^g$ and C/A is a finite 2-group. Hence $\langle g \rangle C/A$ is also a finite 2-group.

Suppose $A \neq C \cap H$. Then there exists $b \in C \cap H \setminus A$ such that $\langle b \rangle A$ is normal in $\langle g \rangle C$. Then $\langle b \rangle A$ is abelian and normal in $\langle g \rangle CL = G$. This contradiction of the maximality of A proves that $A = C \cap H$. In particular $G/A = C/A \times H/A$ and $H/A \cong G/C \cong \mathrm{Sym}(5)$. We can choose $g \in H$ and then $H = \langle g \rangle AL$ and $g^2 \in C \cap H = A$ in this case.

Sym(5) contains a 5-cycle acted on faithfully by a 4-cycle, e.g. (12345) and (2354). Thus L contains e of order 5 and an element k such that gk normalizes $\langle e \rangle$ and acts on it as a 4-cycle, and $(gk)^2 = g^2 l$ where l has order 4. We claim that $A\langle e \rangle$ is a maximal abelian normal subgroup of $C\langle e, gk \rangle$. It certainly is abelian and normal. Suppose $A_2 \geqq A\langle e \rangle$ is abelian and normal in $C\langle e, gk \rangle$. Now $C\langle e, gk \rangle / C$ is the holomorph of a cyclic group of order 5. Thus $A_2 \leqq C\langle e \rangle$. But $C \cap A_2 \leqq C \cap H = A$ and so $A_2 = A\langle e \rangle$ as claimed. From 8 it follows that $(C\langle e, gk \rangle : A\langle e \rangle)$ divides 2^m. Now $(C\langle e, gk \rangle : C\langle e, g^2 l \rangle) = 2, C\langle e, g^2 l \rangle = C\langle e, l \rangle$, $CL/\langle -1 \rangle = C/\langle -1 \rangle \times L/\langle -1 \rangle$ and $l^2 = -1$. Thus

$$(C\langle e, g^2 l \rangle : A\langle e \rangle) = (C:A)(\langle e, l \rangle : \langle e, -1 \rangle) = 2(C:A).$$

Consequently $(G:H) = (C:A)$ divides 2^{m-2}.

14. Some further examples

We have seen in 4 that Case (1) of Theorem 2 does arise for all q, m and char F. We concentrate here on Cases (2) and (3) and consider first the types where Sym(5) is not involved.

https://doi.org/10.1017/S0013091500028923 Published online by Cambridge University Press

Let L be the binary tetrahedral group $SL(2,3)$, the binary octahedral group or the binary icosahedral group $SL(2,5)$. We can regard L as a subgroup of the real quaternion algebra R. Let $y_1,\ldots,y_{m-1}$ be commuting indeterminates over R. For each i let ξ_i be the R-automorphism of the function field $E=R(y_1,\ldots,y_{m-1})$ defined by

$$\xi_i: y_j \mapsto (1-2\delta_{ij})y_j$$

(Kronecker δ). The skew polynomial ring $E[x_1,\ldots,x_{m-1}]$, where each x_i acts on E as ξ_i, is a Noetherian domain, and therefore has a division ring D of quotients. Let $F=\mathbb{R}\,(x_i^2, y_i^2\colon 1\leqq i<m)$. Then F is a central subfield of D with $(D{:}F)=2^{2m}$. If Q is a Sylow 2-subgroup of L then Q is quaternion of order 8. Let $y\in Q$ have order 4. Then $\langle x_i^2, y_i, y\colon 1\leqq i<m\rangle$ is a maximal abelian subgroup of index 2^m of the nilpotent group $\langle Q, x_i, y_i\colon 1\leqq i<m\rangle$ of class 2. Hence by 3 the degree of D over its centre is at least 2^{2m} and therefore F is the centre of D.

Let $C=\langle x_i,y_i{:}1\leqq i<m\rangle$, $G=CL$ and $A=\langle -1,x_1^2,\ldots,x_{m-1}^2,y_1,\ldots,y_{m-1}\rangle$. Then G is the central product of C and L, $C\cap L=\langle -1\rangle$, $A=C_C(A)$ is a maximal abelian normal subgroup of G, $H=C_G(A)=AL$ and $(G{:}H)=(C{:}A)=2^{m-1}$. Further $H/A\cong L/\langle -1\rangle\cong$ Alt (4), Sym (4) or Alt (5).

The question arises as to whether there is any better choice of A. Let A_1 be any maximal abelian normal subgroup of G. If $L\cong SL(2,5)$ then G/C is simple and $A_1\leqq C$. Thus A_1 is also a maximal abelian subgroup of C. Hence with $H_1=C_G(A_1)$ we have $H_1=A_1L$, $H_1/A_1\cong$ Alt (5) and $(G{:}H_1)=(C{:}A_1)=2^{m-1}$.

Suppose now that L is soluble. Then $Q/\langle -1\rangle$ is the unique non-trivial abelian normal subgroup of $L/\langle -1\rangle$, so $A_1\leqq CQ$. Suppose $A_1\nleqq C$. Since CA_1 is normal in G we have $CA_1=CQ$. Let $a=cx$ where $a\in A_1$, $c\in C$ and $x\in Q$, with x of order 4. There exists $l\in L$ of order 3 with $Q=\langle x,x^l\rangle$. Then A_1 contains $a=cx$ and $[a,l]=x^{-1}x^l$. The latter is either x^{l^2} of x^{-l^2}. Thus A_1 contains x,x^l and hence Q. This contradiction shows that $A_1\leqq C$. Then with $H_1=C_G(A_1)$ we obtain $A_1=C_C(A_1)$, $H_1=A_1L$, $H_1/A_1\cong$ Alt (4) or Sym (4) and $(G{:}H_1)=2^{m-1}$. We have thus constructed examples as in 8 and 10.

It is possible to produce a number of variations of the above construction. Suppose L is soluble. Then either $L=\langle l\rangle Q$ where $|l|=3$ or $L=\langle l\rangle\langle k\rangle Q$ where $|k|=3$ and $l^2=-1$. With the division ring D constructed above now set

$$G=CQ\langle 2l\rangle \quad \text{and} \quad A=\langle -1,x_1^2,\ldots,x_{m-1}^2 \quad y_1,\ldots,y_{m-1}, 8=\langle 2l\rangle^3\rangle$$

in the first case and

$$G=CQ\langle k,2l\rangle \quad \text{and} \quad A=\langle -1,x_1^2,\ldots,x_{m-1}^2, \quad y_1,\ldots,y_{m-1}, -4=(2l)^2\rangle$$

in the second. Then these are examples that in the first case does not contain a binary tetrahedral subgroup and in the second does not contain a binary octahedral subgroup. Of course if G is not soluble G must contain a binary icosahedral subgroup.

In Theorem 2, if $H/A\cong$ Sym (4) then necessarily $G=HC_G(Q)$. If $H/A\cong$ Alt (4) then one can have $(G{:}HC_G(Q))=2$, at least if $m\geqq 2$. Briefly one can construct a division ring $D=R(x_i,y_i,e,f\colon 1\leqq i<m-1)$ of degree 2^{2m} over its centre, where R and the x_i and y_i are

as above, e and f centralize $R(x_i, y_i: 1 \leqq i < m-1)$ and $efe = f$. Suppose $L = \langle l \rangle \langle k \rangle Q$ is binary octahedral, where we have chosen l and k so that $kl = lk^2$. Now set

$$G = \langle ek, fl, x_i, y_i, Q: 1 \leqq i < m-1 \rangle$$

and

$$A = \langle e^3, f^2, -1, x_i^2, y_i: 1 \leqq i < m-1 \rangle.$$

Then with $H = C_G(A)$ we have $H/A \cong \langle k \rangle Q / \langle -1 \rangle \cong \mathrm{Alt}(4)$ and $(G: HC_G(Q)) = 2$.

We now consider types that do involve Sym(5). In the quaternion algebra $D_1 = F_1 \oplus F_1 i \oplus F_1 j \oplus F_1 ij$ over $F_1 = \mathbb{Q}(\sqrt{5})$ let $x = -\frac{1}{2} - \frac{1}{4}(1+\sqrt{5})j - \frac{1}{4}(1-\sqrt{5})ij$ and $y = x^2 j$. Then (multiplicatively) x has order 3, y has order 5 and $(xy)^2 = -1$ is central of order 2. Thus $\langle x, y \rangle$ is an image of $SL(2,5)$, cf. the proof of [**4**, 2.1.11], with non-trivial centre. Consequently $\langle x, y \rangle$ is a copy of $SL(2,5)$.

Define the automorphism γ of D_1 of order 2 by

$$\gamma: \sqrt{5} \mapsto -\sqrt{5}, \quad i \mapsto -i, \quad j \mapsto ij.$$

Then $x^\gamma = x$ and $y^\gamma = x^2 ij = -yi$. But

$$i = y^2 xjy(xj)^2 j \in \langle x, y \rangle,$$

so $y^\gamma \in \langle x, y \rangle$ and γ normalizes $\langle x, y \rangle$. It also normalizes the Sylow 2-subgroup $\langle i, j \rangle$ of $\langle x, y \rangle$, but does not normalize $\langle j \rangle$. It follows that γ induces an outer automorphism of $\langle x, y \rangle$. The automorphism group of $\langle x, y \rangle$ is Sym(5) with Alt(5) corresponding to the inner automorphism group.

The skew polynomial ring $R_2 = D_1[g]$, with g acting on D_1 as γ, is a Noetherian domain. Let D_2 be its division ring of quotients and denote the centre of D_2 by F_2. Then $F_2 = \mathbb{Q}(g^2)$ and $(D_2 : F_2) = 2^4$. Let $G_2 = \langle g, x, y \rangle$, $A_2 = \langle g^2, -1 \rangle$ and $H_2 = C_{G_2}(A_2)$. Then A_2 is the unique maximal abelian normal subgroup of G_2, $H_2 = G_2$, $H_2/A_2 \cong$ Sym(5) and $(G_2 : H_2) = 2^0$.

Let $m > 2$. Exactly as in the previous class of examples we can construct an extension division ring D of D_2 with dimension 2^{2m} over its centre F and a subgroup $G = CG_2$ of D^* where $[C, G_2] = \langle 1 \rangle$, $C \cap G_2 = \langle -1 \rangle$ and C has the presentation

$$C = \langle x_i, y_i, z, i = 1, 2, \ldots, m-2: [x_i, y_j] = [x_i, x_j] = [y_i, y_j] = [x_i, z] = [y_i, z] = 1,$$

$$[x_i, y_i] = z, z^2 = 1 \quad \text{for all } i, j, \quad i \neq j \rangle.$$

If A is any maximal abelian normal subgroup of G then $A = A_C A_2$, for A_C some maximal abelian normal subgroup of C. Then $H = C_G(A) = A_C G_2$, $H/A \cong$ Sym(5) and $(G : H) = 2^{m-2}$. Also $L = H' = \langle x, y \rangle$ and $C_G(L) = CA_2$, so $G = C_G(L)L$. This is an example of a group as in 13.

Suppose $m > 2$. Set

$$G_0=\langle x_2,\dots,x_{m-2},y_1,\dots,y_{m-2},x_1g,x,y\rangle \leqq G,$$

$$A_0=\langle x_2^2,\dots,x_{m-2}^2,y_1,\dots,y_{m-2},x_1^2g^2,-1\rangle$$

and $H_0=C_{G_0}(A_0)$. Then A_0 is a maximal abelian normal subgroup of G_0, $H_0=A_0\langle x,y\rangle$, $H_0/A_0\cong \mathrm{Alt}(5)$ and $(G_0{:}H_0)=2^{m-1}$. If we set $L_0=H_0'$ and $C_0=C_{G_0}(L_0)$ then $L_0=\langle x,y\rangle$, $C_0=\langle x_2,\dots,x_{m-1}\rangle A_0$ and $C_0L_0\neq G_0$. Thus this is an example as in 12.

For this final example we needed $m>2$. If $m=2$ we can construct an example as follows. Let $E_1=D_1(h)$ be the (ordinary) ring of rational functions in the one variable h. Define the automorphism δ of E_1 of order 2 by $\delta|_{D_1}=\gamma$ and $h^\delta=h^{-1}$. Form the skew polynomial ring $S_2=E_1[g]$ with g acting on E_1 as δ. Then S_2 has a division ring E_2 of quotients that has degree 4 over its centre. Set $G=\langle g,h,x,y\rangle$. Then $A=\langle g^2,h,-1\rangle$ is the unique maximal abelian normal subgroup of G, $H=C_G(A)=A\langle x,y\rangle$, $H/A\cong \mathrm{Alt}(5)$ and $(G{:}H)=2$. Again $L=H'=\langle x,y\rangle$, $C_G(L)=A$ *and* $C_G(L)L=\langle g^2,h,x,y\rangle\neq G$. Thus this gives an example as in 12 with $m=2$.

The proof of Theorem 3

As in the proof of Theorem 1 we may assume that G is completely reducible. Let A be a maximal abelian normal subgroup of G, set $H=C_G(A)$ and assume H/A is periodic. Let S denote the maximal soluble subgroup of H. By the Hartley–Shahabi theorem (see [4, 2.5.14]) there is a soluble characteristic subgroup M of H' with $(H'{:}M)$ n-bounded (take $M=H'$ if $\operatorname{char} F\neq 0$). Then $C_H(H'/M)$ is a soluble normal subgroup of H with n-bounded index. Therefore $(H{:}S)$ is n-bounded.

Let N denote the Fitting subgroup of S'. By either 2.3.1 or 2.5.2 of [4] there is an abelian characteristic subgroup of N with n-bounded index. Thus $(N{:}A\cap N)$ is n-bounded. Consequently so is $(S{:}C_S(N/A\cap N))$. By stability theory $C_S(N/A\cap N)/C_S(N)$ is isomorphic of a subgroup of

$$\mathrm{Hom}(N/A\cap N, A\cap N).$$

Now $(N{:}A\cap N)$ is n-bounded and $A\cap N$ has rank at most n by [4, 2.3.1 or 2.5.1]. Therefore the order of

$$\mathrm{Hom}(N/A\cap N, A\cap N)$$

is n-bounded and consequently so is the index of $C=C_S(N)$ in H. Further $C'\leqq S'\cap C_S(N)\leqq N\cap C_S(N)$, since N is the Fitting subgroup of the soluble (linear) group S'. Thus $C'\leqq A$ and C is nilpotent of class 2.

By the theory of linear groups (especially the Lie–Kolchin theorem) S has an abelian subgroup of finite index that is normal in G. Therefore $(S{:}A)$ is finite. Standard arguments and the maximality of A (cf. the proof of Theorem 2) show that each Sylow subgroup of C/A is elementary abelian. Suppose we can prove that $(C{:}A)$ divides aq^b, where a is n-bounded. Let Q_1/A be the Sylow q-subgroup of C/A. Then $(H:Q_1)$ is n-bounded and hence so is $(G:C_K(H/Q_1)$, where K is as in 3, that is K/H is a finite q-group (its order dividing q^{mn}) and $(G:K)$ is n-bounded. Now $C_K(H/Q_1)/Q_1$ is nilpotent. Let $T/Q_1 = 0_q(G/Q_1)$. Then the above shows that $(G:T)$ is n-bounded. Also T/A is a finite q-group so there exists Q_2 normal in T with $A \leqq Q_2 \leqq Q_1$, $(Q_2:A)$ dividing q^b and $(Q_1:Q_2)$ dividing a. Set $Q = \bigcap_{g \in G} Q_2^g$. Then Q is a normal subgroup of G with $A \leqq Q \leqq H$, Q/A is an elementary abelian q-group of rank at most b and $(H:Q)$ is n-bounded since (Q_1, Q) divides $a^{(G:T)}$.

Thus we have to produce a bound for $(C:A)$. Consider the notation of the proof 3. For $i > s$ let F_i denote the unique F_j, $j \leqq s$ acting faithfully on V_i; this agrees with the definition for $i \leqq s$. Let $C_i = C/C_C(V_i)$ and let A_i denote the centre of C_i. Now $C_i' \leqq F_i$, so C_i' has rank at most 1. If P/A_i is a Sylow subgroup of C_i/A_i then P/A_i is a non-degenerate alternating space where the form is the commutator operation and maximal totally isotropic subspaces of P/A_i correspond to maximum abelian subgroups of P. The different P commute elementwise. Thus C_i has a maximal abelian subgroup $A_{i1} \supseteq A_i$ such that

$$(C_i:A_i) = (C_i:A_{i1})^2.$$

Now C_i lies in the centralizer S_i of F_i in $\mathrm{End}_D V_i \cong D^{n_i \times n_i}$. Also $\dim_F F_i = d_i q^{m_i}$ for some $d_i | n_i$ and $m_i \leqq m$. Then S_i has dimension $n_i^2 q^{2m}/d_i q^{m_i}$ over F and hence dimension s_i^2, for $s_i = n_i q^{m-m_i}/d_i$, over F_i by [2, Theorem 4.11, p. 224]. By the same result S_i is a matrix ring of degree, say t_i, over a division ring D_i. Since S_i is a subring of $\mathrm{End}_D V_i$ we have that t_i divides n_i. Also if e_i^2 is the dimension of D_i over its centre (F_i in fact) then $e_i t_i$ divides (actually equals) s_i. Now the unipotent radical of C_i in $\mathrm{End}_D V_i$, and hence in S_i is trivial. Thus by 3 applied to C_i as a subgroup of S_i we obtain that $(C_i:A_{i1})$ divides $(t_i! e_i)^{t_i}(t_i!)$. Thus $(C:A)$ divides $(\prod_{i=1}^r (n_i!)^{n_i+1}(n_i q^{m-m_i}/d_i)^{n_i})^2$. Consequently $(C:A)$ divides aq^b where $a = (n!)^{6n}$ say is n-bounded and $b = 2mr - 2\sum m_i$. Certainly, therefore, Q/A has rank at most $2mn$. Further C has an abelian subgroup $A_1 \geqq A$ such that $(C:A_1)$ divides $(aq^b)^{1/2}$, so $Q \cap A_1$ is an abelian subgroup of Q with $(Q:Q \cap A_1)$ dividing $q^{mr - \sum m_i}$. In the proof of 3, the order of G_i, in the above notation, divides $d_i q^{m_i}$. Thus K/H is a subdirect product of s groups, the ith of which has order dividing q^{m_i}. Hence

$$\log_q (K:H) \leqq \sum_{i=1}^{s} m_i \leqq \sum_{i=1}^{r} m_i$$

$$\log_q (Q:Q \cap A_1)(K:H) \leqq mr \leqq mn$$

and

$$\log_q (Q:A)(K:H) \leqq 2mr - \sum_{i=1}^{r} m_i \leqq 2mn.$$

The proof is complete.

REFERENCES

1. N. Jacobson, *Lie Algebras* (John Wiley & Sons, New York, 1962).

2. N. Jacobson, *Basic Algebra II* (W. H. Freeman, San Francisco, 1980).

3. A. I. Lichtman, Free subgroups in linear groups over some skew fields, *J. Algebra* **105** (1987), 1–28.

4. M. Shirvani and B. A. F. Wehrfritz, *Skew Linear Groups* (Cambridge University Press, Cambridge, 1986).

5. J. Tits, Free subgroups in linear groups, *J. Algebra* **20** (1972), 250–270.

6. B. A. F. Wehrfritz, *Infinite Linear Groups* (Springer-Verlag, Berlin, 1973).

7. B. A. F. Wehrfritz, Some skew linear groups associated with Lie algebras of characteristic zero, *J. Algebra* **121** (1989), 155–168.

8. B. A. F. Wehrfritz, Some nilpotent and locally nilpotent matrix groups, *J. Pure Appl. Algebra*, to appear.

Queen Mary College
London E1 4NS