Journal of Algebra **226**, 451–478 (2000)
doi:10.1006/jabr.1999.8201, available online at http://www.idealibrary.com on IDEAL®

Intersections of Matrix Algebras and Permutation Representations of PSL(n, q)

J. Siemons and A. Zalesskii

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, United Kingdom

Communicated by Jan Saxl

Received July 21, 1999

If G is a group, H a subgroup of G, and Ω a transitive G-set we ask under what conditions one can guarantee that H has a regular orbit ($=$ of size $|H|$) on Ω. Here we prove that if $PSL(n,q) \subseteq G \subseteq PGL(n,q)$ and H is cyclic then H has a regular orbit in every non-trivial G-set (with few exceptions). This result is obtained via a mixture of group theoretical and ring theoretical methods: Let R be the ring of all $n \times n$ matrices over the finite field F and let Z be the subring of scalar matrices. We show that if A and M are proper subrings of R containing Z, and if A is commutative and semisimple, then there exists an element $x \in SL(n,F)$ such that $xAx^{-1} \cap M = Z$ or $n = 2 = |F|$.

1. INTRODUCTION

Let G be a group, H a subgroup of G, and Ω a transitive G-set. Under what conditions can one guarantee that H has a regular orbit ($=$ of size $|H|$) on Ω? In this paper we prove that if $PSL(n,q) \subseteq G \subseteq PGL(n,q)$ and H is cyclic then H has a regular orbit in every non-trivial G-set (with few exceptions). To avoid trivialities we say that a permutation presentation of the group $G \supseteq PSL(n,q)$ is trivial, and that the corresponding G-set is trivial, if its kernel contains $PSL(n,q)$.

THEOREM 1.1. *Let $PSL(n,q) \subseteq G \subseteq PGL(n,q)$ and let H be a cyclic subgroup of G. Then H has a regular orbit in every non-trivial G-set Ω unless one of the following holds*:

(a) $(n,q) \in \{(2,2),(2,3)\}$, *or*

(b) $(n,q) = (4,2)$, $|H| = 15$, *and* $|\Omega| = 8$.

0021-8693/00 $35.00

The result is no longer valid for arbitrary abelian group H. Let p be a prime such that p divides q. Lemma 3.9 in [15] and Proposition 1.6 of [14] say that if P_i is the stabilizer of a subspace of dimension i in $G = PSL(n, q)$ and $H_i = O_p(P_i)$ then H_i is abelian and H_i has no regular orbit on the cosets of P_j in G unless $i + j = n$. (For $j = 1$, $n > 3$ this is obvious as $|H_i| \geq q^{2(n-1)} > q^n - 1 \geq |G : P_1|$.)

There is a related module theoretic problem: If K is a field, under what conditions does the permutation KG-module $K\Omega$ restricted to H contain a regular KH-submodule? For cyclic groups H these problems are equivalent to each other for arbitrary G and K. If H is not cyclic, the second problem is easier (at least via our approach). We treat the second problem under a more general setting assuming that H is abelian with cyclic Sylow p-subgroup.

THEOREM 1.2. *Let $SL(n, q) \subseteq G \subseteq GL(n, q)$ where $q = p^m$ for some m. Let H be an abelian subgroup of G with cyclic Sylow p-subgroup. Let K be a field of characteristic 0 or coprime to $|G|$ and let M be a non-trivial permutation KG-module. Set $\overline{H} = H/H_0$ where $H_0 = \{h \in H : h|M = \mathrm{Id}\}$. Then M, viewed as an $\overline{H}$-module, contains a regular $K\overline{H}$-submodule unless one of the following holds*:

(a) $(n, q) \in \{(2,2), (2,3)\}$ *or*

(b) $(n, q) = (4, 2)$, $|H| = 15$ *and* $\dim M = 8$.

We heavily use the machinery of ring theory. Formally, we could avoid this by dealing with the group of units of a ring instead of the ring itself. However, we see no reason to strive for group theoretical purity. We do hope that some of the ring theoretical results obtained here might be useful in other circumstances. The most essential result of ring theoretical nature is the following:

THEOREM 1.3. *Let $R = M(n, F)$ and let Z be the subring of scalar matrices. Let A, M be proper subrings of R containing Z with A being commutative and semisimple. Then there exists an element $x \in SL(n, F)$ such that $xAx^{-1} \cap M = Z(R)$ unless $n = 2 = |F|$.*

Let V be the standard vector space for $GL(n, q)$ and $PSL(n, q) \subseteq G \subseteq PGL(n, q)$. Let $\mathscr{L}$ be the set of one-dimensional subspaces in V and let $K\mathscr{L}$ denote the respective permutation module. Our method is based on a theorem saying that if $H \subset G$ is not transitive on $\mathscr{L}$ then the permutation module associated with the action of G on the cosets of H contains a submodule isomorphic to $K\mathscr{L}$. This reduces the problem to analyzing the case where H is transitive on $\mathscr{L}$. Such subgroups H are known (Huppert, Hering): with few exceptions H normalizes either the projective symplectic group or the image in G of the group of units of a subring of $M(n, q)$

isomorphic to $M(n/k, q^k)$ with $k|n$. We use ring theoretic machinery to deal with this second case.

This shows that in order to extend Theorem 1.2 by replacing the abelian group H by a more complicated group B one would first have to guarantee the existence of the regular KB-submodule in $K\mathscr{L}$ and then to deal with two other cases. As much as we are aware, very little is known about the action of subgroups of $PGL(n, q)$ on the cosets of $X \subset PGL(n, q)$ when X is a quotient of $SL(n/k, q^k)$ with $k > 1$. The problem of characterizing the groups $H \subset GL(n, q)$ which have a regular orbit on $\mathscr{L}$ is known to be very difficult. Some progress has been made when $(|H|, q) = 1$ and q is large enough; see Liebeck [13] and Goodwill [4]. Our notation necessarily varies a little as we progress but it is explained at the beginnings of Sections 2, 3, 5, and 7 for each of those parts of the paper.

2. SOME GENERAL OBSERVATIONS ON PERMUTATION MODULES

Here we collect the general facts about permutation actions and modules we shall use in this paper. First recall the usual notation. Let G be some group and Ω a G-set. The image of $\omega \in \Omega$ under $g \in G$ is denoted by $g\omega$ and if $H \subseteq G$ then $H\omega$ is the orbit of ω under H. The stabilizer of ω in G is G_ω and if $\Gamma \subseteq \Omega$ then $g\Gamma := \{g\gamma : \gamma \in \Gamma\}$. We assume throughout that all G-sets are finite. The number of G-orbits on Ω of given size k is denoted by $n_\Omega(G, k)$ or just $n(G, k)$. If K is a field then KG is the group ring over K and $K\Omega$ denotes the natural KG-module with Ω as a basis. We use KG also to indicate the regular module of G over K. If a normal subgroup $G^* \subseteq G$ acts trivially on a submodule M then we often regard M as a $K(G/G^*)$-module.

2.1. *Embedding Permutation Modules*

Let Δ and Ω be two G sets. We are interested in conditions which guarantee the existence of a KG-embedding $K\Omega \hookrightarrow K\Delta$. In general this is not an easy task. However, when G is doubly transitive on Ω then this problem presents itself as a simple alternative:

THEOREM 2.1. *Suppose that G acts doubly transitively on Ω and also transitively on Δ, where $|\Omega| \geq 2$. (Neither action needs to be faithful.) Let K be a field whose characteristic does not divide the order of G. Then one and only one of the following occurs*:

(i) *There exists an injective KG-homomorphism φ: $K\Omega \to K\Delta$.*

(ii) *For any $\omega \in \Omega$ and $\delta \in \Delta$ we have $G = G_\omega \cdot G_\delta$.*

We refer to (i) as the *embedding* case and to (ii) as the *factorization* case. The condition $G = G_\omega \cdot G_\delta$ means that G_δ is transitive on Ω or, equivalently, that G_ω is transitive on Δ. This theorem is from [3] and as its proof is very short we will repeat it here.

Proof. If (ii) holds then G_ω has two orbits on Ω but only one orbit on Δ. However, an injective G-homomorphism $\varphi\colon K\Omega \to K\Delta$ would imply that the multiplicity of the trivial KG_ω-module in $K\Omega$ is no larger that the multiplicity of the trivial KG_ω-module in $K\Delta$. These multiplicities are the numbers of G_ω-orbits on Ω and Δ, respectively, and so there can be no such embedding.

Fix some $\omega \in \Omega$ and suppose that G_ω has an orbit $\Phi \neq \Delta$ on Δ. Define a KG-homomorphism $\varphi\colon K\Omega \to K\Delta$ by extending $\varphi(\omega) := \sum_{\delta \in \Phi} \delta$ linearly to all of $K\Omega$. It remains to show that φ is injective. As G is doubly transitive $K\Omega = A \oplus B$ decomposes into the one-dimensional module $A = \langle \sum_{\omega \in \Omega} \omega \rangle$ and the irreducible module $B = \langle \omega - \omega^* : \omega, \omega^* \in \Omega \rangle$. So there are only few possibilities for the kernel C of φ: as $\varphi \neq 0$ it remains to show that $C \neq A$ and $C \neq B$. Clearly, $\varphi(\sum_{\omega \in \Omega} \omega)$ is of the form $x \cdot \sum_{\delta \in \Delta} \delta$ and a simple counting argument shows that $x = |\Omega|\,|\Phi|\,|\Delta|^{-1}$. So x is a divisor of $|G|$ and $\neq 0$ in F. This rules out $C \supseteq A$. As $\Phi \neq \Delta$ we have $\varphi(\omega) \notin \langle \sum_{\delta \in \Delta} \delta \rangle \subseteq \varphi(F\Omega)$ so that $\varphi(K\Omega)$ is not 1-dimensional. This rules out $C \supseteq B$ and so φ is injective. ∎

2.2. *Regular Decompositions*

Here we analyze permutation modules in terms of regular modules. Let G be a group, Ω a G-set, and K some field. We arrange the normal subgroups of G as $G =: G_r, G_{r-1}, \ldots, G_1 := 1$ in such a fashion that $s > t$ implies $|G_s| \geq |G_t|$. Then let n_1 be the multiplicity of the regular $K(G/G_1)$-module in $K\Omega$ and let $n_1 KG =: R_1$ be the corresponding submodule of $K\Omega$. Next let n_2 be the multiplicity of the regular $K(G/G_2)$ module in $K\Omega/R_1$ and let $R_2 \supseteq R_1$ be the KG-submodule of $K\Omega$ for which $R_2/R_1 = n_2 K(G/G_1)$, etc. In this fashion we obtain the *regular sequence* $R_r \supseteq R_{r-1} \supseteq \cdots \supseteq R_1$ of KG-submodules corresponding to $G_r, \ldots, G_1$ and we shall say that $K\Omega$ has a *regular decomposition* if there is an arrangement of the G_i for which the corresponding regular sequence ends in $K\Omega$.

LEMMA 2.2. *Let K be a field, G a group, and Ω a G-set. Suppose that G^* is normal in G with G/G^* cyclic of order n and that $K\Omega$ contains the regular $K(G/G^*)$ module. Then G has an orbit $\Omega^* \subseteq \Omega$ which is the union of n orbits of G^*, all of the same size.*

Proof. Let $g \in G$ be a generator of G/G^* and suppose that φ: $K(G/G^*) \hookrightarrow K\Omega$ is a KG-embedding of the regular G/G^* module. Then $\varphi(G^*)$ can be written as

$$\begin{aligned}\varphi(G^*) = {} & \lambda_0 A + \lambda_1 gA + \cdots + \lambda_{r-1} g^{r-1}A \\ & + \mu_0 B + \mu_1 gB + \cdots + \mu_{s-1} Bg^{s-1} \\ & + \cdots \\ & + \nu_0 C + \nu_1 gC + \cdots + \nu_{t-1} g^{t-1}C,\end{aligned}$$

where $A := \Sigma\{\alpha^* \in \alpha^{G^*}\}$, $B, \dots, C$ denote sums of the points in suitable G^*-orbits, where further all $g^iA, g^jB, \dots, g^kC$ are pairwise distinct with all coefficients $\lambda, \mu, \dots, \nu \in K$ non-zero. Clearly $s, t, \dots, u$ are divisors of n.

Note that $(1 + g + \cdots g^{s-1}) \cdot (\lambda_0 A + \lambda_1 gA + \cdots + \lambda_{r-1} g^{r-1}A) = (\lambda_0 + \lambda_1 + \cdots + \lambda_{s-1}) \cdot \overline{A}$, where $\overline{A}$ is the sum of all points in α^G, and so this expression is G-invariant. Similarly $(1 + g + \cdots + g^{s-1})(1 + g + \cdots + g^{t-1}) \cdots (1 + g + \cdots + g^{u-1}) \cdot \varphi(G^*)$ and hence $(1 + g + \cdots + g^{s-1})(1 + g + \cdots + g^{t-1}) \cdots (1 + g + \cdots + g^{u-1}) \cdot (G^*)$ are G-invariant. However, up to a scalar multiple $(1 + g + \cdots + g^{n-1}) \cdot G^*$ is the only such element in $K(G/G^*)$. Therefore $(1 + g + \cdots + g^{s-1})(1 + g + \cdots + g^{t-1}) \cdots (1 + g + \cdots + g^{u-1}) \cdot (G^*) = \lambda(1 + g + \cdots + g^{n-1}) \cdot G^*$ for some $\lambda \in K$. From this we conclude that the polynomial $x^n - 1$ divides $(x^s - 1)(x^t - 1) \cdots (x^u - 1)$ and so a primitive nth root of unity in a suitable extension field is among the roots of order $s, t, \dots, u$. Thus $n \in \{s, t, \dots, u\}$ which completes the proof. ∎

THEOREM 2.3. *Let K be a field, G a cyclic group, and Ω a G-set. Then $K\Omega$ has a regular decomposition. In particular, if $K\Omega = R_r \supseteq R_{r-1} \supseteq \cdots \supseteq R_1$ is any regular decomposition, with multiplicities $n_1, \dots, n_r$, then $n_i = n_\Omega(G, k_i)$ is the number of orbits of length $k_i := |G : G_i|$ and $R_{i+1} = n_\Omega(G, k_{i+1}) \cdot K(G/G_i) + R_i$ for $1 \le i \le r - 1$.*

Proof. Let $G =: G_r, G_{r-1}, \dots, G_1 := 1$ be arranged in such a way that $s > t$ implies $|G_s| \ge |G_t|$. If G has just one orbit on Ω then $K\Omega = K(G/G_1)$ and the result holds. So suppose that there are several orbits and let $\Omega_1, \Omega_2, \dots, \Omega_n$ be all the orbits of maximal size $m < |\Omega|$. Let s be the least index for which $|G : G_s| = m$. We claim that $R_1 = R_2 = \cdots = R_{s-1} = 0$. For if $K(G/G_j)$ with $1 \le j < s$ was involved in $K\Omega$ then by Lemma 2.2 G would have to have an orbit whose size is a multiple of $|G : G_j|$, a contradiction.

Among the groups $G_s, \dots, G_t$ of index m we find the stabilizer G_α of $\alpha \in \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_n$. As $G/G_\alpha \cong G/G_u$ for any $s \le u \le t$ we see that $R_s = n_s K(G/G_s)$ where $n_s \ge n$, accounting for the n orbits of length m. Put $\Omega^* = \Omega \setminus \bigcup_i \Omega_i$ so that $K\Omega = K\Omega_1 + \cdots + K\Omega_n + K\Omega^*$. Using

Lemma 2.2 again we see that the regular $K(G/G_s)$-module is not involved in $K\Omega^*$ and this implies that $n_s \leq n$. Clearly, also $n_{s+1} = \cdots = n_t = 0$ and the result now follows by induction. ∎

We note two immediate corollaries. The second one is the version of this theorem which is most relevant for this paper.

COROLLARY 2.4 (Brauer's permutation lemma [2]). *Two permutations have isomorphic permutation modules if and only if they have the same cycle type.*

COROLLARY 2.5. *If G is cyclic and acts faithfully on Ω then the multiplicity of the regular KG-module in $K\Omega$ is equal to the number of regular orbits of G on Ω.*

Combining the results on regular modules with the theorem on embeddings in the preceding sections yields the following:

THEOREM 2.6. *Suppose that G acts doubly transitively on Ω. Let $B_1, \dots, B_m \subseteq G$ be representatives of all those conjugacy classes of subgroups which act transitively on Ω. For $i = 1, \dots, m$ denote the cosets of B_i in G by Δ_i and let H be a subgroup of G.*

(i) *Suppose that H is cyclic. If H has at least k regular orbits on each Δ_i with $i = 1, \dots, m$ and on Ω then H has at least k regular orbits on any G-set.*

(ii) *Let K be a field whose characteristic does not divide the order of G. Suppose that $K\Delta_i|_H$, for each $i = 1, \dots, m$, and $K\Omega|_H$ have a submodule isomorphic to a direct sum of m copies of the regular KH-submodule. Then for any G-set Λ the restriction $K\Lambda|_H$ contains a submodule isomorphic to a direct sum of m copies of the regular KH-submodule.*

Proof. For (i) select any field whose characteristic is co-prime to $|G|$. Then apply Theorem 2.1 and Corollary 2.5. Similarly, part (ii) follows from Theorems 2.1 and 2.3. ∎

3. THE NATURAL ACTION OF $PGL(n, q)$

In order to apply the ideas arrived at in the last section we need some preliminary information about the natural action of the projective general linear groups. So let V be the n-dimensional vector space underlying $GL(n, q)$ and let $\mathscr{L}$ denote the set of all one-dimensional subspaces of V. The center of $GL(n, q)$ is denoted by Z and the group $PGL(n, q) =$

$GL(n,q)/Z$ acts on $\mathscr{L}$. This action is doubly transitive on $\mathscr{L}$ and $\mathscr{L}$ is called the *natural* $PGL(n,q)$*-set*. Observe that also the action of $PSL(n,q)$ on $\mathscr{L}$ is doubly transitive.

3.1. *Regular Orbits of Abelian Subgroups in the Natural Action*

PROPOSITION 3.1. *Let $q = p^{\alpha}$. Let H be an abelian subgroup of $PGL(n,q)$ with cyclic Sylow p-subgroup. Then H has a regular orbit on $\mathscr{L}$.*

Proof. Let $H = B \times U$ where U is the Sylow p-subgroup of H. Observe first that the claim is true if H is irreducible. Indeed, in this case $H = B$ is contained in K^* where $K = \langle H \rangle$ is a field by Schur's lemma; clearly, $|Kv| = |K|$ for each $0 \neq v \in V$ so K^*/Z^* has a regular orbit on the one-dimensional subspaces of V. Next suppose that H is indecomposable. Put $K = \langle B \rangle$. Then K is a field for otherwise K has a non-trivial idempotent e so H preserves both eV and $(e - \mathrm{Id})V$. View V as a vector space V_K over K. Then U is contained in $GL(V_K)$ as U and K elementwise commute. As U is cyclic, it has a regular orbit on the one-dimensional subspaces of V_K, equivalently, on irreducible K-submodules in V. Let $W \neq 0$ be an irreducible K-submodule such that the orbit $\{uW\}_{u \in U}$ is of length $|U|$. Let $0 \neq w \in W$. Then Bw contains $|B|$ elements and all of them are in W. As for $u, u' \in U$ the spaces uW and $u'W$ have no nonzero element in common; the orbit UBw is regular. Moreover, if $B_Z = B \cap Z$ then the number of one-dimensional subspaces in Bw is $|B/B_Z|$. Therefore $H/(H \cap Z)$ has a regular orbit on the one-dimensional subspaces of V. Finally, assume that $V = V_1 \oplus V_2$ where V_1, V_2 are H-modules. Set $H_i = H \,|\, V_i$ for $i = 1,2$. By induction, there are vectors $v_i \in V_i$ such that $|H_i v_i| = |H_i|$ and the orbit $H_i\langle v_i \rangle$ is of size $|H_i/(Z_i \cap H_i)|$ where Z_i is the set of scalar matrices in $\mathrm{End}(V_i)$. Then the H-orbit of $v = v_1 + v_2$ has size $|H|$. In order to show that the H-orbit of the line Zv is of size $|H/(H \cap Z)|$ just observe that $av \in Zv$ if and only if $a \in Z$. Indeed, if $av = zv$ for $z \in Z$ then $av_i = zv_i$ for $i = 1,2$. By the above, $a \,|\, V_i$ is scalar, say, z_i. Then $av_i = z_i v_i = zv_i$; hence $z_i = z$. ∎

3.2. *Embedding the Natural $PGL(n,q)$ Permutation Module*

Now suppose that $PGL(n,q)$ acts on some set Δ and that K is a field whose characteristic does not divide $|PGL(n,q)|$. We are interested in embeddings $\varphi\colon K\mathscr{L} \to K\Delta$ and so we investigate the factorizations of the projective linear group. These have been determined by Hering [5]; see also [12].

THEOREM 3.2. *Let $SL(n,q) \subseteq G \subseteq GL(n,q)$ be a subgroup and let B be a maximal subgroup of G which is transitive on $V \setminus \{0\}$ and does not contain*

$SL(n,q)$. Then B is conjugate to one of the following groups:

(i) $N_G(L^*)$ *where L is a subfield of R containing Z with* $|L:Z| = n$,

(ii) $N_G(SL(n/l, q^l))$ *where l is a prime dividing n*,

(iii) $N_G(Sp(n,q)) = HSp(n,q)$ *for $n > 2$ even*,

(iv) $N_G(Q_8)$ *for $n = 2$ and $q = 5, 7, 23$*,

(v) $N_G(SL(2,5))$ *for $n = 2$ and $q = 9, 11, 19, 29, 59$, and*

(vi) A_7 *for* $(n,q) = (4,2)$.

Remark. The transitive group $N_G(D_8 \circ Q_8)$ for $G = SL(4,3)$ given in [12] is contained in $HSp(4,3)$. In (ii) $SL(n/l, q^l)$ is understood to be the image of the embedding induced by an embedding of F_{q^l} into $M(l,q)$.

The following is therefore immediate from Theorem 2.1:

THEOREM 3.3. *Let $G = PSL(n,q)$ act naturally on the points $\mathscr{L}$ of projective space and let Δ be some transitive primitive G-set. Suppose that K is a field whose characteristic does not divide $|G|$. Then exactly one of the following holds*:

(i) *there exists an injective G-homomorphism $K\Omega \to K\Delta$, or*

(ii) *there is some $\delta \in \Delta$ such that the pre-image of G_δ in $SL(n,q)$ is conjugate to one of the subgroups listed in Theorem 3.2. (G_δ stands for the stabilizer of $\delta \in \Delta$ in G.)*

Together with Corollary 2.5 and Proposition 3.1 this yields the main result in the embedding case:

THEOREM 3.4. *Let $g \in G = PGL(n,q)$ and let $K\mathscr{L} = R_r \supseteq R_{r-1} \supseteq \cdots \supseteq R_1$ be a regular decomposition for $\langle g \rangle$ when K is a field whose characteristic does not divide $|PGL(n,q)|$. Suppose that Δ is some G-set and that G_δ, for some $\delta \in \Delta$, is not conjugate to any of the groups H in Theorem 3.2. Then $K\Delta|_{\langle g \rangle}$ has $K\langle g \rangle$-submodules isomorphic to R_i for $i = 1, \dots, r$. In particular, g has at least $n_{\mathscr{L}}(g, |g|) \geq 1$ regular orbits on Δ.*

4. COUNTING REGULAR ORBITS AND THE BASE OF INDUCTION

Let $B, H \subset G$ be finite groups. First we derive an upper bound for the order of G in terms of B and H if H acts on the cosets of B without a regular orbit. This bound is very rough but sometimes useful.

Let T be a subgroup contained in $H \cap B$. Let $r(T,B)$ denote the number of G-conjugates of B that contain T, and let $n(T,B)$ be the number of the subgroups in B that are G-conjugate to T. Consider the set

$$X = \left\{ \left(gTg^{-1}, hBh^{-1} \right) : g, h \in G \text{ and } gTg^{-1} \subseteq hBh^{-1} \right\}.$$

Then there are $|G : N_G(T)|$ conjugates of T and each is contained in $r(T, B)$ conjugates of B. Therefore $|X| = |G : N_G(T)| \cdot r(T, B)$. On the other hand, there are $|G : N_G(B)|$ conjugates of B, each containing $n(T, B)$ conjugates of T. So $|X| = |G : N_G(B)| \cdot n(T, B)$ and hence

$$r(T, B) = \frac{|N_G(T)|}{|N_G(B)|} \cdot n(T, B).$$

THEOREM 4.1. *Suppose that G is a finite group with subgroups B and H such that H has no regular orbit on the cosets of B in G. Let $S_1, \dots, S_m$ be representatives of all conjugacy classes of subgroups of prime order contained in $B \cap H$. Then*

$$|G| \leq \sum_{i=1}^{m} N_G(S_i) \cdot n(S_i, B) \cdot n(S_i, H).$$

Proof. By assumption we have: $(*)$ $\forall g \in G$ the intersection $H \cap gBg^{-1}$ is non-trivial. Let $S_1, \dots, S_m$ be representatives of all conjugacy classes of subgroups of prime order contained in $B \cap H$. If H intersects a conjugate of B then this intersection contains a conjugate T of some S_i and there will be $r(T, B) = r(S_i, B)$ conjugates of B containing T. Therefore H intersects non-trivially at most $\sum_{i=1}^{m} r(S_i, B) \cdot n(S_i, H)$ conjugates of B and so $\sum_{i=1}^{m} r(S_i, B) \cdot n(S_i, H) \geq |G : N_G(B)|$ if $(*)$ holds. From the expression for $r(S_i, B)$ one obtains the required inequality. ∎

EXAMPLES. (1) If B is cyclic then $n(S_i, B) = 1$ so that $|G| \leq \sum_{i=1}^{m} N_G(S_i) \cdot n(S_i, H)$.

(2) Suppose that any two conjugates $T_1, T_2 \subseteq H$ of S_i are conjugate in H. Then $n(S_i, H) = |H : N_H(S_i)|$ and so $|G : H| \leq \sum_{i=1}^{m} |N_G(S_i)/N_H(S_i)|$.

Now we turn to the proof of Theorem 1.1 when $(n, q) = (2, q)$ for arbitrary q and $(n, q) = (4, 2)$. This will serve as a basis for induction later on.

LEMMA 4.2. *Let $PSL(2, q) \subseteq G \subseteq PGL(2, q)$ with $3 < q$ and let $B \subset G$ with $B \not\supseteq PSL(2, q)$. If H is an abelian subgroup of G then there is some $g \in G$ for which $B \cap H^g = 1$.*

Proof. Suppose that B intersects every conjugate of H non-trivially. We may assume that $H = S_1 \times S_2 \times \cdots \times S_m$ where the S_i are simple cyclic. We may also assume that each S_i has a conjugate contained in B

and that $m \geq 2$ for otherwise B is contained the normal subgroup generated by the conjugates of H. First assume that the intersections between B and the conjugates of H are always contained in $PSL(2, q)$ so that we may as well assume $B, H \subseteq PSL(2, q)$. It follows from Theorem 8.27 in [6] that H is one of the following: (i) $C_2 \times C_2$, (ii) cyclic of order dividing $(q \pm 1)/k$ where $k = (q-1, 2)$ and $N_G(H)$ is dihedral of order $2(q \pm 1)/k$, or (iii) elementary abelian of order dividing q. Each of these cases can be ruled out by elementary arguments and the use of Theorem 4.1. In the remaining case assume that B meets some conjugate H^g such that $H^g \cap B := \langle h \rangle \neq 1$ but $H^g \cap B \cap PSL(2, q) = 1$. Then H is contained in the centralizer of the involution h and this can be ruled out in the same fashion. ∎

LEMMA 4.3. *Let* $G = \mathrm{Alt}(8) \cong SL(4, 2)$ *and* $B \subset G$ *with* $8 < |G : B|$. *If* H *is an abelian subgroup of* G *then there is some* $g \in G$ *with* $B \cap H^g = 1$.

Proof. Suppose that B intersects every conjugate of H non-trivially. Then $|H|$ has at least two different prime divisors and clearly 7 cannot divide $|H|$. If 5 divides $|H|$ then $H \cong C_3 \times C_5$ as C_5 is irreducible in $SL(4, 2)$. Hence $B \cap H^g$ is of order 3, 5 or 15. Then B contains elements of order 3 and 5, and for every partition of type $(5, 3)$ of the eight points there would be a 3-cycle or a 5-cycle in B preserving the two sets of the partition. It follows that B has an orbit of length 7 or 8 and from this that $B \cong \mathrm{Alt}(7)$ or $B \cong \mathrm{Alt}(8)$. ∎

5. INTERSECTIONS OF SUBALGEBRAS

We now begin with the ring theoretical discussion. The notation is as follows. If B is a group then B' is the derived subgroup of B and $Z(B)$ is the center of B. If X is a ring with identity then X^* is the group of units (= invertible elements) of X and $Z(X)$ is the center of X. We often write X' instead of $X^{*\prime}$. The algebra of $(n \times n)$-matrices over a field F is denoted by $M(n, F)$. We set $R = M(n, F)$ and $Z = Z(M(n, F))$. Let $V = F^{(n)}$ be the natural R-module. We set $G = R^* = GL(n, F)$. Observe that X is an F-subalgebra of R containing the identity of R if and only if X contains Z. If S is a subset of R then $\langle S \rangle$ denotes the least F-algebra (= Z-algebra) containing S. If $S, T \subseteq R$ are subsets we write $\langle S, T \rangle$ instead of $\langle S \cup T \rangle$. The field of q elements is denoted by $\mathbf{F}_q$. We write $M(n, q)$ and $GL(n, q)$ instead of $M(n, \mathbf{F}_q)$ and $GL(n, \mathbf{F}_q)$, respectively.

THEOREM 5.1. (1) *Let S be a simple subring of R containing Z. Then the following hold*:

(i) *If a is an automorphism of S trivial on Z then there exists $g \in G$ such that $a(s) = gsg^{-1}$ for all $s \in S$* [16, *Sect*. 12.6].

(ii) *Let $C = C_R(S)$. Then C is simple, $S = C_R(C)$, and* $(S:Z)(C:Z) = n^2$ [16, *Sect*. 12.7].

(iii) *If S is a field and $k = S:Z$ then $C \cong M(n/k, S)$. Furthermore, C is irreducible and if $S:Z$ is a prime then C is a maximal subring of R.*

(iv) *Isomorphic simple subrings of R containing Z are conjugate in R* [16].

(2) *Let T be a semisimple subring of R such that $Z \subset T$, and $L = C_R(T)$. Then L is semisimple, $C_R(L) = T$, $Z(T) = Z(L)$. Further, L is simple if and only if T is simple.*

(3) *If K is a maximal simple subring R such that $Z \subseteq K$ then $Z(K): Z$ is a prime.*

Proof. (1) (iii): Obviously V is a vector space over S of dimension n/k and C is exactly $\mathrm{Hom}_S(V, V) \cong M(n/k, S)$. Each finitely generated module over $M(n/k, S)$ is a direct sum of simple ones. If V is not irreducible as an C-module then $S = \mathrm{Hom}_C(V, V)$ contains a non-trivial idempotent which is not the case.

(2) Let $T = S_1 \oplus \cdots \oplus S_k$ where $S_1, \ldots, S_k$ are simple. Let $e_i \in S_i$ be central idempotents of S_i. Let $V_i = e_i V$ and $n_i = \dim V_i$. Then the centralizer of the set $\{e_1, \ldots, e_k\}$ in R is $M(n_1, F) \oplus \cdots \oplus M(n_k, F)$ and $S_i \in M(n_i, F)$ is a simple subring. Therefore $L = L_1 \oplus \cdots \oplus L_k$ where L_i is the centralizer of S_i in $M(n_i, F)$. So the result follows from (1) (ii).

(3) Clearly, K is irreducible so $C = C_R(K)$ is a field. Hence $C = Z(K)$. If $C:Z$ is not a prime then C contains a proper subfield C_1 containing Z and $C_R(C_1) \neq k$ by (1) (ii). ∎

THEOREM 5.2 (see 2a). *Let H be a non-central subgroup of $GL(n, F)$ invariant under G'. Suppose that $(n, |F|) \neq (2,2), (2,3)$. Then H contains $SL(n, F)$.*

COROLLARY 5.3. *Let $T = \oplus T_i$ where $T_i \cong M(n_i, F_i)$ and F_i are fields of the same characteristic. Let $\phi_i \colon T \to T_i$ be the natural projection. Let H be a subgroup of T^* invariant under T'. Suppose that H contains an element h of order p. Then H contains a subgroup H such that $\phi_i(X) = SL(n_i, F_i)$ for those i for which $h \notin \ker(\phi_i)$ and $\phi_i(X) = \mathrm{Id}$ for all other i.*

The following lemma is a very particular case of a result in [1].

LEMMA 5.4. *Let S be a proper subring of R. Suppose that $g^{-1}Sg = S$ for all $g \in G'$. Then either $S \subset Z$, or $(n, |F|) = (2,2)$ and S is the field of four elements.*

Proof (*sketch*). If $(n, |F|) \in \{(2,2),(2,3)\}$ then the lemma can be verified directly. Suppose that $(n, |F|) \neq (2,2),(2,3)$. Observe that $S \cap G \not\subseteq Z(G)$ unless $|F| = 2$ and S is a direct sum of the fields of two elements. In the first case S^* contains G' by Theorem 5.2. It is well known that for $(n, |F|) \neq (2,2)$ the group G' is absolutely irreducible. Therefore $\langle G' \rangle = M(n, F)$ and so $S = M(n, F)$. This is a contradiction. Let S be a direct sum of k copies of the field of two elements. Then $n \geq k > 1$ and hence G' permutes these k summands. It follows that G' has a normal subgroup L such that G'/L is isomorphic to a subgroup of Sym_k, the symmetric group of degree k. It follows from Theorem 5.2 that $L \subseteq Z(G)$. This is impossible as $|PSL(n, F)| > k!$ for $n \geq k$. ∎

COROLLARY 5.5. *Let $L \neq Z$ be a minimal subring of R containing Z. Then $g^{-1}Lg \cap M \subseteq Z$ for some $g \in G'$, unless $(n, |F|) = (2,2)$ and $M = L \cong \mathbf{F}_4$.*

Proof. Let $g \in G'$. If $g^{-1}Lg \cap M \not\subset Z$ then $g^{-1}Lg \subseteq M$ by minimality of L. If this is true for all $g \in G'$ then $L \subset Y = \bigcap_{g \in G'} gMg^{-1} \neq Z$. By Lemma 5.4 $(n, |F|) = (2,2)$ and $L \cong \mathbf{F}_4$ as $Y = gYg^{-1}$ for all $g \in G'$. In the exceptional case the claim is obvious. ∎

LEMMA 5.6. *Let $A \subset R$ be a semisimple commutative F-algebra and let D be any maximal proper F-subalgebra of A. If $Z \cong \mathbf{F}_2$ and A contains a proper subfield L such that $Z \subset L \cong \mathbf{F}_4$ suppose additionally that D contains L. Let $A = A_1 \oplus \cdots \oplus A_l$ and $D = D_1 \oplus \cdots \oplus D_k$, where $A_1, \dots, A_l$ and $D_1, \dots, D_k$ are fields. Then $k \leq l \leq k+1$ and the summands A_i, D_j can be reordered such that $D_i = A_i$ for $i = 1, \dots, k-1$.*

Proof. Obviously, $k \leq l$ and after reordering the A_i's one can assume that $D_1 \subset A_1 \oplus \cdots \oplus A_{i_1}$, $D_2 \subset A_{i_1+1} \oplus \cdots \oplus A_{i_2}, \dots, D_k \subset A_{i_{k-1}+1} \oplus \cdots \oplus A_{i_k}$. As D is maximal, after reordering the D_i's and A_i's we have $D_1 = A_1, \dots, D_{k-1} = A_{k-1}, D_k \subset A_k \oplus \cdots \oplus A_l$. Moreover, it follows from the maximality of D that the last sum should contain at most two summands, i.e., $k = l$ or $l = k+1$. If $k = l$ then $D_k \subset A_k$ is a field extension. If $l = k+1$ then $A_k \cong A_{k+1} \cong D_k$ (as $Z \subset D$ the identity of $A_k + A_{k+1}$ is contained in D_k). ∎

Proof of Theorem 1.3. Suppose the contrary. Take for R a minimal counterexample; i.e., we assume that the theorem holds for $m < n$. Further, as every F-subalgebra of A is semisimple, we assume that A is a minimal counterexample, in the sense that for any proper F-subalgebra B of A the theorem holds; i.e., there exists an element $x \in SL(n, F)$ such that $xBx^{-1} \cap M \subseteq Z$.

The cases $n = 1$ and $n = |F| = 2$ are obvious. Thus we assume in what follows that $n > 1$, and that $|F| > 2$ when $n = 2$.

Let $A = A_1 \oplus \cdots \oplus A_l$ where $A_1, \dots, A_l$ are fields. Let D be a maximal proper subring of A containing Z. If $D = Z$ then the theorem follows from Corollary 5.5. So we shall assume that $D \neq Z$. If $Z \cong \mathbf{F}_2$ and A contains a proper subfield L with $Z \subset L \cong \mathbf{F}_4$ then by Corollary 5.5 $A \neq L$ and we can assume that D is chosen to contain L. Let $D = D_1 \oplus \cdots \oplus D_k$ where $D_1, \dots, D_k$ are fields. By Lemma 5.6 $k \leq l \leq k + 1$ and we can assume that $D_1 = A_1, \dots, D_{k-1} = A_{k-1}$, and $D_k \subset A_k \oplus \cdots \oplus A_l$. If $k = l$ then $D_k \subseteq A_k$ is a field extension. If $l = k + 1$ then $A_k \cong A_{k+1} \cong D_k$. If A is minimal we can assume that $D \cap M \subseteq Z$. Let $C = C_R(D)$. Then $D = Z(C)$ by 5.1(ii) so C is a direct sum of exactly k simple components $C = C_1, \dots, C_k$. By reordering the C_i's we can assume that $D_i = Z(C_i)$ for $i = 1, \dots, k$. Let e_i denote the identity of D_i (and C_i). By the above, C_k contains A_k. If $l = k + 1$ then C_k contains $A_k + A_{k+1}$. Set $C_0 = D_1 \oplus \cdots \oplus D_{k-1} \oplus C_k$. Then $A \subset C_0$, and C_0 is not commutative as $Z(C) = D \neq A$. For $x_k \in C_k$ let $x = e_1 + e_2 + \cdots + e_{k-1} + x_k$. Then x_k is invertible if and only if x is. Observe that $C_k \cong M(m, D_k)$ for some $1 < m < n$ by Theorem 5.1. Let σ denote the projection $C_0 \to C_k$, so $\sigma(x) = x_k$.

Set $M_0 = M \cap C_0$, $M_\sigma = \sigma(M_0)$. Observe first that $M_\sigma \cong M_0$ as $\operatorname{Ker}(\sigma) = D_1 \oplus \cdots \oplus D_{k-1}$ and $D \cap M \subseteq Z$. Observe next that $M_\sigma \neq \sigma(C_k)$. Indeed, if $M_\sigma = \sigma(C_k) \cong C_k$ then $M_0 \cong C_k \cong M(m, D_k)$; hence $M_0 = C_k$ (as the projections of M_0 to C_i should be zeros). Then M contains D_k. This is a contradiction as $D \cap M \subseteq Z$.

Thus $M_\sigma \neq \sigma(C_k)$. As $m < n$, the theorem is true for $\sigma(C_k)$ so either there exists $x_k \in C_k' = SL(m, D_k)$ such that $x_k^{-1}\sigma(A)x_k \cap M_\sigma \subseteq \sigma(D_k) = D_k$ or $m = 2 = |D_k|$ and $\sigma(A) \cong \mathbf{F}_4$. In the former case set $x = e_1 + e_2 + \cdots + e_{k-1} + x_k$. Then $x^{-1}Ax \cap M \subseteq M \cap D \subseteq Z$, as desired. Let $m = 2 = |D_k|$. Then $F = \mathbf{F}_2$ and $M_\sigma \cong \sigma(A) \cong \mathbf{F}_4$, $l = k$, so D contains no subfield L such that $\mathrm{Id} \in L \cong \mathbf{F}_4$. As $M_0 \cong M_\sigma$, we have $M_0 \cong \mathbf{F}_4$. Let σ_i with $i < k$ be the natural homomorphism of C_0 onto D_i, $i < k$. Then $\sigma_i(M_0) \neq \{0\}$ as M_0 contains Id. Clearly, $\ker(\sigma_i) \cap M_0 = \{0\}$ as M_0 is a field. Hence $\sigma_i(M_0) \cong \mathbf{F}_4$. Therefore, D_i contains a subfield isomorphic to $\mathbf{F}_4$ for every $i < k$. It follows that A contains a subfield isomorphic to $\mathbf{F}_4$. This contradicts the assumption about D above. ∎

LEMMA 5.7. *Let $p = \operatorname{char}(F)$ and let $A \subset G$ be a finite abelian group. Let X be a subring of R such that $Z \subset X$. Suppose that the Sylow p-subgroup A_p of A is cyclic. Then there is $g \in G'$ such that $g^{-1}Ag \cap X \subset Z$.*

Proof. Let $A = A_1 \times A_p$. Set $K = \langle A_1 \rangle$. Then K is a semisimple ring by Maschke's theorem. It suffices to prove the lemma when $A_1 = K^*$ as this group contains no p-element. Thus assume that $A_1 = K^*$. If $A_p = 1$ the result follows from Theorem 1.3. Let $A_p \neq 1$ and let A_0 denote the subgroup of A_p of order p. Set $C = C_R(K)$. Write $C = C_1 \oplus \cdots \oplus C_m$ where each C_i for $i = 1, \dots, m$ is a simple ring. Let σ_i: $C \to C_i$ be the natural projection. By reordering the C_i's we can assume that $\sigma_i(A_p) \neq 1$ for $i = 1, \dots, l$ and $\sigma_i(A_p) = 1$ for $i > l$. Obviously, C_i is not commutative for $i \leq l$.

By Theorem 1.3 we can assume that (*) $K \cap X = Z$. Set $X_0 = X \cap C$ and $X_C^0 = \bigcap_{c \in C'} cX_0c^{-1}$. If $A \cap X_C^0 \subseteq Z$ then we are one. Suppose that $A \cap X_C^0 \not\subseteq Z$, and let $a \in A \cap X_C^0$ and $a \notin Z$. By $(*)$ a is not semisimple so some power of a is a non-trivial element of A_0. Hence $A_0 \subset X_C^0$. We show that this is impossible.

Let $e_i \in C_i$ be the central idempotent of C_i. As $C_i \in C$, the element $c = e_1 + \cdots + e_{i-1} + c_i + e_{i+1} + \cdots + e_m \in C'$ for each $c_i \in C_i'$ and $\sigma_i(c) = c_i$. For $x \in X_C^0$ let $x = x_1 + \cdots + x_m$ with $x_i \in C_i$. Then $cxc^{-1} - \mathrm{Id} = c_i x_i c_i - e_i^{-1}$ so $c_i x_i c_i - e_i \in C_i \cap X_C^0$. Observe that $C_i \cap X_C^0$ is not in $Z(C_i)$ for $i \leq l$. Indeed, let $1 \neq a \in A_0$. Then for $x = a$ the element $\sigma_i(x) = x_i$ is of order p so $c_i x_i c_i - e_i \notin Z(C_i)$ for some $c_i \in C_i'$. So $C_i \cap X_C^0$ is non-central C_i'-invariant subring of C_i. By Lemma 5.4 $C_i \cap X_C^0 = C_i$, except, possibly, in the case $C_i = M(2, \mathbf{F}_2)$ when $C_i \cap X_C^0$ is isomorphic to $\mathbf{F}_2$. In both the cases $Z(C_i) \subseteq X_C^0 \subseteq X$ which contradicts (*), unless $m = 1$, $Z(C_i) = Z$. Then $C = R$, $X_0 = X$, and X_C^0 is a G'-invariant subring of R. By Lemma 5.4 either $X_C^0 = R$ or $R = M(2, \mathbf{F}_2)$. The first case is impossible as $X_C^0 = X \neq R$. The second case $R = M(2, \mathbf{F}_2)$ is straightfoward. ∎

6. SUBRING NORMALIZERS

Notation. In this section $F = \mathbf{F}_q$. We first prove the following theorem.

THEOREM 6.1. *Let $|F| = q$. Let A be a commutative semisimple subring of $R = M(n, F)$ and let M be a proper subring of R, both containing Z. Set $N = N_{R^*}(M^*)$. Then there exists an element $x \in G'$ with $xAx^{-1} \cap N \subseteq Z = Z(R)$ unless $n = 2 = |F|$.*

We set $F_l := \mathbf{F}_{q^l}$. For $l \mid n$ there is an embedding of F_l into $M(l, F)$ via the regular representation of F_l over F (i.e., we consider F_l as a vector space over F of dimension l and the action of F_l on F_l by left multiplication defines the regular representation of ρ_l: $F_l \to M(l, F)$). Furthermore, for $l \mid n$ we define a subalgebra R_l of R obtained from $M(n/l, F_l)$ by means of replacing the matrix entries t_{jk} of $t \in M(n/l, F_l)$ by the elements $\rho_l(t_{jk})$.

Thus if $l \mid n$ then R_l is a simple F-subalgebra of R containing the identity of R. Hence R_l contains Z. Let Z_l be the center of R_l, so $Z_l \cong F_l$, and $Z_l : Z = l$. Observe that Z_l is a subfield of R containing Z. By Theorem 5.1(2) we have $R_l = \mathbf{C}_R(Z_l)$. We set $G_l = R_l^*$ so that G_l is isomorphic to $GL(n/l, F_l)$ and $G = R^* = GL(n, F)$. Clearly, $G_l = \mathbf{C}_G(Z_l)$. If $(n, q) \neq (2, 2)$ then $G_l' \cong SL(n/l, F_l)$.

Let N_l denote the normalizer of G_l in G. Observe that $N_l = \{g \in G : gxg^{-1} \in R_l$ for all $x \in R_l\}$ as $\langle G_i \rangle = R_i$. Obviously, $gZ_lg^{-1} = Z_l$ for $g \in N_l$. It follows that N_l/G_l is isomorphic to the Galois group of Z_l/Z. In particular, $|N_l/G_l|$ is cyclic of order l.

LEMMA 6.2. *Let l be a prime divisor of n and let $x \in N_l \setminus R_l$. Let $y = \sum_{i=0}^{l-1} \lambda_i x^i$ where $\lambda_i \in R_l$. If $y \in R_l$ then $y \in Z_l$.*

Proof. Set $J(y) = \{i \in \{0, \dots, l-1\} : \lambda_i \neq 0\}$. Suppose the contrary and choose y with minimal $|J(y)|$. If $J(y) = \{0\}$ we are done. Suppose that $J(y) \neq \{0\}$. If $\zeta \in Z_l$ then $y\zeta - x^k\zeta x^{-k}y = \sum_{k \neq i \in J(y)} \lambda_i (x^i\zeta x^{-i} - x^k\zeta x^{-k})x^i \in R_l$. By minimality of $J(y)$ we have $x^i\zeta x^{-i} = x^k\zeta x^{-k}$ for $i \in J(y)$, $i \neq k$. This is equivalent to $\zeta = x^{i-k}\zeta x^{k-i}$ for all $\zeta \in Z_l$. This is impossible as x realizes a Galois automorphism of Z_l/Z. ∎

LEMMA 6.3. *Let l, ν be prime divisors of n and let K, L be subfields of R containing Z such that $K : Z = \nu$ and $L : Z = l$. Let $N = \mathbf{N}_G(L) = \mathbf{N}_G(M)$ where $M = C_G(L)$. Then $gKg^{-1} \cap N = Z$ for some $g \in G'$.*

Proof. Observe that $N : M^* = l$ by a Galois argument. By Corollary 5.5 there is $g \in G'$ such that $gKg^{-1} \cap M \subseteq Z$. Set $L = gZ_lg^{-1}$. Suppose that $L \cap N \neq Z$. Then $N \cap L$ contains an element $x \notin M$ such that $x^l \in M$. Then $\langle x \rangle = L$ as $L : Z$ is prime. Obviously there exists $h \in G'$ such that $hxh^{-1} \notin N$. Set $K_1 = \langle hxh^{-1} \rangle$. Then K_1 is a field and $K_1 : Z = l$. It follows that $K_1 \cap M \subseteq Z$ (otherwise, $K_1 \subseteq M$ and $x \in M \subset N$). We show that $K_1 \cap N \subseteq Z$. Otherwise, let $y \in K_1 \cap M$ and $y \notin Z$. Then $y' \in K_1 \cap M \subseteq Z$. As K_1 is finite, the group K_1^*/Z^* is cyclic and hence contains a unique subgroup of order l. Therefore $y = (hxh^{-1})^i z$ where $z \in Z$, $i \in \mathbf{N}$, and $(i, p) = 1$. As $y \in N$, we have $x \in N$ which is a contradiction. ∎

LEMMA 6.4. *Let $F \subset P$ be finite fields, $S = M(k, P)$ with $k > 1$ and $D = Z(S)$. Let T be a proper F-subalgebra of S such that $\langle T, Z(S) \rangle = S$. Let N be the normalizer of T in G.*

(i) *For $x \in P$ set $d_x = \operatorname{diag}(1, \dots, 1, x)$. There exists a subfield Q of P and elements $a \in S$ and $x \in P$ such that $aTa^{-1} = d_x M(k, Q) d_x^{-1}$.*

(ii) $N = T^* Z(S)^*$.

(iii) *Let $e \in S$ be an idempotent such that $0 \neq e \neq 1$, and $K = \langle Z(S), e \rangle$. Then there exists $g \in S'$ such that $gKg^{-1} \cap N \subset Z(S)$.*

(iv) *Let L be a subfield of S containing D. Then $L \cap T \subseteq Z$ implies that $L \cap N \subseteq Z$.*

Proof. (i) Obviously, T should be simple, so by Wedderburn's theorem $T \cong M(l, Q)$ where Q/F is a field extension. Then $S = \langle T, Z(S) \rangle \cong M(l, Q) \otimes P \cong M(l, Q \otimes P)$. This implies $k = l$ and $Q \subset P$. Obviously, there exists $c \in GL(k, P)$ such that $cTc^{-1} = M(k, Q)$. Let $x = \det(c^{-1})$. Then $a = d_x c \in S'$ and we are done.

(ii) follows from 5.1(i) and (i) above. Indeed, it suffices to prove (ii) for $T = M(k, Q)$. Let $x \in N$. Then the automorphism $t \mapsto xtx^{-1}$ $(t \in T)$ of T is inner (5.1) and so $x = yc$ where $y \in T$ and $c \in C_G(T)$. However, $C_G(T) = Z(S)$ so $c \in Z(S)$, as desired.

(iii) Set $M^x(k, Q) = d_x M(k, Q) d_x^{-1}$. By (i) we can assume that $T = M^x(k, Q)$ for some $x \in P$. Then the entires of matrices of T are in Q, except in positions (i, j) with $i = n$, $j \neq n$ and $i \neq n$, $j = n$ where the entries belong to the set xQ and $x^{-1}Q$, respectively. Let $k = \operatorname{rank}(e)$. Then there exist $h \in S$ such that $heh^{-1} = e_0 = \operatorname{diag}(1, \dots, 1, 0, \dots, 0)$. Let $u = \det(h^{-1})$. Then $g = d_u h \in S'$. As $k < n$, we have $geg^{-1} = e_0$. Hence we can assume that $e = e_0$. Pick $y \in P$, $y \notin xQ$ and set $a = \mathrm{Id} + ye_{1k}$ (here e_{1k} denotes the matrix with 1 positioned at $(1, k)$ and zeros elsewhere). Then $\det(a) = 1$ so $a \in S'$. Set $e_1 = aea^{-1} = e_0 + ye_{1k}$. Hence we can assume that $e = e_0 + ye_{1k}$. Next let $b \in K \cap N$, $b \notin Z(S)$. Then $b = p_1 + p_2 e$ for some $p_1, p_2 \in P$, $(p_1 \neq 0 \neq p_2)$ so that $b = \operatorname{diag}(p_1 + p_2, \dots, p_1 + p_2, p_1, \dots, p_1) + yp_2 e_{1k}$. As $bT^*b^{-1} = T^*$, we have $bTb^{-1} = T$. Then b induces an automorphism b_1 of T trivial on $Z(T)$ as $Z(T)$ consists of scalar matrices. Therefore, b_1 is inner; i.e., $btb^{-1} = ctc^{-1}$ for some $c \in T^*$. Then $c^{-1}bt = tc^{-1}b$ for all $t \in T$, so $c^{-1}b \in C_{GL(k, P)}(T)$. The right hand side group consists of scalar matrices over P by Schur's lemma. Hence $b \in N$ implies the existence of $r \in P$ such that $rp_1 \in Q$, $r(p_1 + p_2) \in Q$, $ryp_2 \in xQ$. This implies $rp_2 \in Q$, and then $y \in xQ$. This is impossible unless $p_2 = 0$. However, $p_2 = 0$ means that $b \in Z(T)$, which is a contradiction.

(iv) Suppose the contrary and let $a \in L \cap N$. By (ii) we can express $a = td$ for some $t \in T$ and $d \in D$. As $d \in L$, we have $t \in L$ so $t \in L \cap T \in Z$. ▮

Proof of Theorem 6.1. Consider a minimal counterexample; i.e., we assume that the theorem holds for $m < n$. The cases $n = 1$ and $n = q = 2$ are obvious. Thus we assume in what follows that $n > 1$ and $nq > 4$.

Furthermore, $\langle N \rangle = R$ by Theorem 1.3 applied to $\langle N \rangle$. This implies that M is semisimple. Indeed, if $U = \mathrm{Rad}(M) \neq 0$ then $xUx^{-1} = U$ for each $x \in N$. Therefore $\{\Sigma u_i x_i\}_{u_i \in U, x_i \in N}$ forms a two sided ideal of $R = \langle N \rangle$, which is a contradiction. (This is in fact the Clifford theorem.) We denote by r the number of simple components of M and set $s = n/r$. Let $e_1, \dots, e_r$ be the minimal central idempotents of M. By the Clifford theorem all they have the same rank s. As A is semisimple, we can also assume that A is minimal in the sense that for any proper F-subalgebra B of A there exists an element $x \in G'$ such that $xBx^{-1} \cap N \subseteq Z$.

Step 1. Here we prove the theorem for the case where A is a field. Let D be a maximal subfield of A containing Z. Set $A : D = \nu$. Clearly, ν is a prime. By minimality of A we can assume that $D \cap N \subseteq Z$.

Consider first the case $D = Z$. Then $A : Z = \nu$ is a prime.

Suppose first that $r > 1$. We can assume that $A = \mathrm{diag}(a, \dots, a)$, where a runs over a subfield of $M(\nu, F)$. Let us view $R = M(n, F)$ as $M(r, M(s, F))$; i.e., we view the matrices of $M(n, F)$ as block matrices with entries in $M(s, F)$. Let Y_m denote the $m \times m$-matrix with 1 in position $(1, m)$ and zeros elsewhere. By conjugating N by a suitable element $u \in G'$ we can assume that

$$e_i = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & E_s & 0 & \cdots & 0 & Y_s \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \qquad \text{for } i < r,$$

where E_s is the identity matrix of size s and non-zero entries occur in the ith row. The matrix u can be taken to have 1's on the diagonal and in positions $(1, n)$, $((ks) + 1, n)$ with $k = 1, \dots, r - 1$, and zeros elsewhere. Hence for $i = r$ we have

$$e_r = \begin{pmatrix} 0 & 0 & \cdots & 0 & Y_s \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & Y_s \\ 0 & 0 & \cdots & 0 & E_s \end{pmatrix}.$$

Suppose that $A \cap N \not\subseteq Z$, and let $X \in A \cap N$, $X \notin Z$. Then $X = \mathrm{diag}(x, \dots, x)$, where $x \in GL(\nu, F)$ is irreducible as ν is prime. The conjugacy action of X permutes e_i's. Observe that $Xe_1X^{-1} \neq e_1$ (otherwise, $xY_\nu x^{-1} = Y_\nu$ or $xY_\nu = Y_\nu x$; as x is irreducible, and $r > 1$, this contradicts the Schur lemma). Hence $Xe_1X^{-1} = e_j$ where $j > 1$. Suppose that $\nu \leq s$. Then, obviously, $j = r$ and $xY_\nu x^{-1} = Y_\nu$. This contradicts Schur's lemma.

Suppose that $\nu > s$. As $\nu > 1$, $r > 1$, the top ν rows of the matrix Xe_1X^{-1} have shape

$$\left(xE_\nu x^{-1} \mid 0 \mid \cdots \mid 0 \mid xY_\nu x^{-1}\right).$$

Let $v_1, \dots, v_n$ be the standard basis in V, the natural module for $M(n, F)$. Set $W = \langle v_1, \dots, v_\nu \rangle$. Then $X \mid W = x$ so $XW = W$. Let t be the maximal natural number such that $e_t V \subseteq W$. Set $e_0 = e_1 + \cdots + e_t$. Then $e_0 V \subseteq W$ so $Xe_0X^{-1}V \subseteq W$. It follows that $Xe_0X^{-1} = e_0$ as X permutes e_i's and $(\Sigma e_j)V = \Sigma e_j V$ with summation over any subset of $\{1, \dots, r\}$. Hence $e_0 W = W$ so ν is a multiple of s, say, $\nu = st$. Suppose first that $\nu < n$. Then $xYx^{-1} = Y$, where

$$Y = \begin{pmatrix} 0 & \cdots & Y_s \\ \cdots & \cdots & \cdots \\ 0 & \cdots & Y_s \end{pmatrix}$$

is a $(\nu \times \nu)$-matrix with t blocks Y_s at the right hand side columns and 0's elsewhere. By Schur's lemma Y is non-degenerate. This is a contradiction. Suppose next that $\nu = n$. As $\nu = n$ is prime, we have $r = 1$. Obviously, we then have $gAg^{-1} \cap M \subset Z$ for each $g \in G'$. Choose g such that $gxg^{-1} \notin N$. Show that $A \cap N \subset Z$. Indeed, if $y \in A \cap N$ is not scalar then y permutes e_i's so $y^\nu \in Z$. As A is cyclic, we have $x = y^j z$ for some integer $1 \leq j < \nu$ and $z \in Z$. But then $x \in N$ which is a contradiction.

It follows that $r = 1$. This means that M is simple. Then $L = Z(M)$ is a field. Let l be some prime dividing $L : Z$, and let L_1 be a subfield of L such that $L_1 : Z = l$. As L_1 is unique, N normalizes L_1 so $N \subseteq N_G(L_1)$. This means that it suffices to prove that $gAg^{-1} \cap N_G(L_1) \subseteq Z$ for some $g \in G'$. However, this follows from Lemma 6.3.

Next, suppose that $D \neq Z$. Set $S = C_R(D)$. By the above $D \cap N \subseteq Z$. Set $M_0 = M \cap S$. Clearly, $M_0 \neq S$ (otherwise, $D \subseteq S = M$ which is not the case). Hence M_0 is a proper Z-subalgebra of S. Besides, $A \subseteq S$ and $A \neq S$ as $A \neq D$ (see 5.1(2)). As $S = M(k, D)$ for some $k < n$, we can use the induction assumption if M_0 is a D-subalgebra of S. If $\langle M_0, D \rangle \neq S$, we are done by induction as $N_0 = N \cap S$ normalizes $\langle M_0, D \rangle$. Suppose that $\langle M_0, D \rangle = S$. By Lemma 6.4(iv) $A \cap N \subseteq D$. As $D \cap N \subseteq Z$, we are done.

Step 2. Here we assume that A is not a field. Let $A = A_1 \oplus \cdots \oplus A_l$ where $A_1, \dots, A_l$ are fields. Let D be any maximal proper subring of A. If $|F| = 2$ and A contains a proper subfield L such that $\mathrm{Id} \in L \cong \mathbf{F}_4$, then we can assume that D is chosen to contain L. (Indeed, in this case L^* is of order 3. Hence $g^{-1}Ng \cap L^* \neq 1$ implies that $L^* \subset g^{-1}Ng$ for all $g \in G'$

so $L^* \subset \bigcap_{g \in G'} g^{-1}Ng$. It follows that G' has a non-central normal subgroup which is impossible.) Let $D = D_1 \oplus \cdots \oplus D_k$ where $D_1, \dots, D_k$ are fields. By Lemma 5.6 we have $k \le l \le k+1$ and after reordering the D_i's and A_i's we shall have $D_1 = A_1, \dots, D_{k-1} = A_{k-1}$, $D_k \subset A_k \oplus \cdots \oplus A_l$. If $k = l$ then $D_k \subset A_k$ is a field extension, and if $l = k+1$ then $A_k \cong A_{k+1} \cong D_k$. As A is minimal, we can assume that $D \cap N \subseteq Z$. Let $C = C_R(D)$. Observe that $D = Z(C)$ by Theorem 5.1, so C is a direct sum of exactly k simple components $C_1, \dots, C_k$. By reordering C_i's we can assume that $D_i = Z(C_i)$ for $i = 1, \dots, k$. By the above A_k (resp., $A_k + A_{k+1}$) belongs to C_k if $k = l$ (resp., $l = k+1$). Set $C_0 = D_1 \oplus \cdots \oplus D_{k-1} \oplus C_k$. Then $A \subset C_0$, and C_0 is not commutative as $Z(C) = D \neq A$. Let $\sigma\colon C_0 \to C_k$ be the natural homomorphism; i.e., σ is identical on C_k and $\ker(\sigma) = D_1 \oplus \cdots \oplus D_{k-1}$. It follows that $\sigma(C_0') = C_k'$. Let $1 = f_1 + \cdots + f_k$ where $f_i \in C_i$ for $i = 1, \dots, k$. Then $f_i \in Z(C_i) = D_i \subset D = Z(C)$, and f_i is the identity of C_i. Clearly, $\sigma(c) = f_k c$ for $c \in C_0$. For $x_k \in C_k$ let $x = f_1 + \cdots + f_{k-1} + x_k$. Then x_k is invertible if and only if so is x. Observe that $C_k \cong M(m, D_k)$ for some $m > 1$.

Suppose first that $D = Z$. Then $k = 1$ and $l = 2$ (otherwise, A is a field). Therefore, $A = \langle D, e \rangle$ for some idempotent $e \in A \subseteq S$ where $S = C_R(D)$. By Lemma 6.4(iii) there exists $g \in S'$ such that $gAg^{-1} \cap N \subseteq D$. As $D \cap N \subseteq Z$, we are done.

Let now $D \neq Z$. Set $M_0 = M \cap C_0, M_\sigma = \sigma(M_0)$. Observe first that $M_\sigma \cong M_0$ as $\mathrm{Ker}(\sigma) = D_1 \oplus \cdots \oplus D_{k-1}$ and $D \cap M \subseteq Z$. Observe next that $M_\sigma \neq \sigma(C_k)$. Indeed, if $M_\sigma = \sigma(C_k) \cong C_k$ then $M_0 \cong C_k \cong M(m, D_k)$; hence $M_0 = C_k$ by Wedderburn's theorem. Then M contains D_k. This is a contradiction.

Thus $M_\sigma \neq \sigma(C_k)$. Set $N_0 = N \cap C_0$. Then N_0 normalizes M_0 and $\sigma(N_0)$ normalizes M_σ. As $M(n, q)$ is a minimal counterexample to the theorem, either (a) $m = 2 = |D_k|$ or (b) there exists $x_k \in C_k' = GL(m, D_k)$ such that $x_k^{-1}\sigma(A)x_k \cap \sigma(N) \subseteq \sigma(D_k) \cong D_k$. Let $x = e_1 + e_2 + \cdots + e_{k-1} + x_k$. Then in case (b) $x^{-1}Ax \cap N \subseteq N \cap D \subseteq Z$, as desired. Let (a) hold. It follows that $M_\sigma \cong \sigma(A) \cong \mathbf{F}_4$, $l = k$, and D contains no subfield L such that $\mathrm{Id} \in L \cong \mathbf{F}_4$. As $M_0 \cong M_\sigma$, we have $M_0 \cong \mathbf{F}_4$. Let σ_i, $i < k$, be the natural homomorphism of C_0 onto D_i, $i < k$. Then $\sigma_i(M_0) \neq \{0\}$ as M_0 contains Id. As above, $\ker(\sigma_i) = \{0\}$ as $M_0 \cap D \subseteq Z$. Hence $\sigma_i(M_0) \cong \mathbf{F}_4$. Therefore, D_i contains a subfield isomorphic to $\mathbf{F}_4$ for every $i < k$. It follows that A contains a subfield isomorphic to $\mathbf{F}_4$. This contradicts the assumption about D above. This completes the proof.

LEMMA 6.5. *Let F be a field of order 2^{2m} with $m > 1$. Then F^* contains an element of prime order l with $l > 2m$.*

Proof. If $m = 3$ then $l = 7$. Suppose that $m \neq 3$. By Zsigmondy's theorem (see [10, 5.2.14]) there is a prime l such that l divides $2^{2m} - 1$ and does not divide $2^i - 1$ for $i < 2m$. Let h be an element of order l in F^*. It follows that h does not belong to a proper subfield of F. Therefore, the set $\{h^j\}_{j=1,\dots,l}$ contains a basis of F/F_2 so $l \geq 2m$. In fact, $l \neq 2m$ as $(1 + h)(1 + h + \cdots l^{l-1}) = 0$; hence $1 + h + \cdots + h^{l-1} = 0$. Therefore $l \geq 2m + 1$. ∎

THEOREM 6.6. *Let G, M, N be as in Theorem 6.1 and let $q = r^\alpha$ where r is a prime. Let $A \subset G$ be an abelian subgroup with cyclic Sylow r-subgroup A_q. Then $g^{-1}Ag \cap N \subset Z$ for some $g \in G'$.*

Proof. As in the proof of Theorem 6.1 we can assume that $\langle N, Z \rangle = R$ so M is semisimple. Besides, if M is not simple, it suffices to prove the result for the case where $M = \operatorname{diag}(M(n/s, F), \dots, M(n/s, F))$ where s is the number of simple components of M. Then $C_R(M) = Z(M)$. Let $e_1, \dots, e_s$ be minimal central idempotents of M, so N permutes $e_1, \dots, e_s$ and $e_1V, \dots, e_sV$ transitively.

Let A_r denote the subgroup of A_q of order r. Let $A = A_1 \times A_q$ so A_1 is an r'-group. Set $K = \langle A_1 \rangle$. By Maschke's theorem K is a semisimple ring. By Theorem 6.1 there is $g \in G'$ such that $gKg^{-1} \cap N \subset Z$. By replacing K by gKg^{-1} we can assume that $K \cap N \subset Z$. Set $C = C_R(K)$. Clearly, $C = C_R(A_1)$. Write $C = C_1 \oplus \cdots \oplus C_m$, where C_i for each $i = 1, \dots, m$ is a simple ring. Let σ_i: $C \to C_i$ be the natural projection. By reordering the C_i's we can assume that $\sigma_i(A_r) \neq 1$ for $i = 1, \dots, l$, and $\sigma_i(A_r) = 1$ for $i > l$. Observe that C_i is not commutative for $i \leq l$. Clearly $l \geq 1$. Let $C_i = SL(n_i, q_i)$.

If $c^{-1}A_q c \cap N \subset Z$ for some $c \in C'$ then we are done (as $A_r \cap Z = 1$). Suppose that $c^{-1}A_q c \cap N \not\subset Z$ for all $c \in C'$. Then $A_r \subset cNc^{-1}$ for all $c \in C'$. Therefore, $A_r \subset N_C = \bigcap_{c \in C'} cNc^{-1}$ so $N_C \cap C$ is a C'-invariant subgroup of C^*. Set $X = N_C \cap C$. By Corollary 5.3 X contains subgroups $X_i \cong SL(n_i, q_i)$ such that $\sigma_i(X_i) = SL(n_i, q_i)$ for $i = 1, \dots, l$ and $X = X_1 \cdots X_l$. As $X \subset N$, we have a homomorphism η: $X \to N/M^*$. Let $H = \ker \eta$. We show that $H \subset Z$. Observe first that $H \subset M$. (Indeed, if M is simple then H centralizes $Z(M)$; as $M = C_R(Z(M))$ then $H \subset M$. If M is not simple then H centralizes all $e_1, \dots, e_s$ so again $H \subset M$.) As H is normal in X, we have either $H \subset Z(X) \subset K$, or $X_i \subseteq H$ for some i, or $X_i \cong SL(2,2)$ or $SL(2,3)$ for some i and $H \cap X_i$ is a normal non-central subgroup of X_i. As $K \cap M \subseteq Z$, the first possibility does not hold. In the remaining cases $\langle H, Z \rangle$ contains $Z(C_i)$; hence $Z(C_i) \subseteq M$. This contradicts the fact that $K \cap M \subseteq Z$ as $Z(C_i) \subseteq K$ and $Z(C_i) \notin Z$. Thus $H \subseteq Z$.

If M is simple then $N/M^* \cong \operatorname{Gal}(Z(M)/Z)$ is cyclic whereas $\eta(X)$ is not cyclic. This is a contradiction. Suppose that M is not simple. By the previous paragraph, if $x \in X$ and $x \notin Z$ then x acts non-trivially on $\{e_1, \dots, e_s\}$. Let $l(x)$ be the order of x modulo Z^*. By a lemma of Higman (see [7, Theorem 1.10, p. 411]) the degree d of the minimal polynomial of x is not less than the maximal length ν of an orbit of x on e_i's (or V_i-s). If $l(x)$ is a prime power then $l(x) = \nu$. If $r > 2$ or $r = 2$ and $C_i \neq M(2,2)$ for some $i \in \{1, \dots, l\}$, we shall deduce a contradiction by showing that this is impossible for some $x \in X$. In the exceptional case we show that N has to be the group of all monomial matrices over $\mathbf{F}_2$. We shall handle this case by an alternative argument.

Each $SL(n_i, q_i)$ contains a subgroup $\mathrm{diag}(SL(2, q_i), \mathrm{Id}_{n_i - 2})$. Let $y = \mathrm{diag}(h, \mathrm{Id}_{n_i - 2}) \in SL(n_i, q_i)$ where h is chosen to be of order $k = r$ if r is odd and of order $k > 3$ in Lemma 6.5 if $q_i > 2$ is even. Let $x \in X_i$ be the pre-image of y so $l(x) = k$. Clearly, the minimum polynomial of x is of degree $d = 2$ if r is odd which contradicts the above inequality $r = l(x) \leq d$.

Suppose that $r = 2$, $q_i > 2$. Choose h as in Lemma 6.5. Then the minimum polynomial of x is of degree $d \leq 2q_i$ whereas $|x| > 2q_i$. This contradicts the Higman lemma. Thus, we are left with the case where $r = 2$ and $q_i = 2$ for $i = 1, \dots, l$. Then $|F| = 2$. We show that each $n_i = 2$ for $i = 1, \dots, l$. Indeed, if some $n_i > 2$ then C_i^* contains the matrix $y = \mathrm{diag}(h, \mathrm{Id}_{n_i - 3})$ where $h^7 = 1$ and $h \in SL(3,2)$. Let x be a pre-image of y in X_i. As above, the degree of the minimum polynomial of x is equal to 4 which contradicts Higman's lemma. Thus $n_i = 2$.

Set $C_0 = C_1 \oplus \cdots \oplus C_l$ and $e_0 = e_1 + \cdots + e_l$ and let $n_0 = \mathrm{rank}(e_0)$. Then $Z(C_0) \cong \mathbf{F}_2 \oplus \cdots \oplus \mathbf{F}_2$ (l summands). Therefore, $Z(C_0)^* = 1$. Then, under a basis B compatible with the decomposition $V = V_1 \oplus \cdots \oplus V_s$ each element of A_1 is of shape $\mathrm{diag}(e_0, t)$ for some $t \in GL(n - n_0, F)$. As $C = C_R(A_1)$, it follows that $l = 1$ so $X = X_1$. Let $1 \neq a \in A_r$. As $l = 1$ and $q_1 = 2$, we have $\dim(\mathrm{Id} - a)V = 1$. As a permutes V_i, it follows that $\dim V_j = 1$ for $j = 1, \dots, s$. Then N is conjugate to the group of monomial matrices over $\mathbf{F}_2$, which coincides with the group of permutational matrices for $F = \mathbf{F}_2$. Hence V^N, the subspace of the vectors fixed by N, is one-dimensional.

For this case we show that there is $g \in G'$ such that $gAg^{-1} \cap N \subset Z$. Let $0 \neq v \in V^N$. It suffices to show that $C_A(gv) = 1$ for some $g \in G'$. If $n = 2$ or 3 then $A = A_r$ and the claim is trivial. Suppose that $n > 2$. Clearly, there is $g \in G'$ such that $e_1 gv \neq 0$ and $(\mathrm{Id} - e_1)gv \neq 0$. We can assume that this holds for v itself. Next, we shall look for g such that $ge_1 = e_1 g$. Under an appropriate basis we can assume that $g = \mathrm{diag}(g_1, g_2)$ where $g_1 \in SL(2,2)$ and $g_2 \in SL(n-2, 2)$. Obviously, there is g_1 such that A_r does not preserve the line $g_1 e_1 \langle v \rangle$. Observe that A_1 acts trivially in $e_1 V$. As the stabilizer of $(\mathrm{Id} - e_1)\langle v \rangle$ in $M(n-2, 2)$ is an $\mathbf{F}_2$-subalgebra, we can use Theorem 1.3 to conclude that there is g_2 such that A_1 does not preserve the line $g_2(\mathrm{Id} - e_1)\langle v\rangle$. It follows that A does not preserve the line $g\langle v\rangle$. This implies the lemma. ∎

PROPOSITION 6.7. (1) *Let $A \subset G$ be a cyclic group and p a prime dividing n. Then there exists an element $g \in G'$ such that $gAg^{-1} \cap N_p \subset Z$.*

(2) *Let $(n, q) \neq (2, 2)$. Let $B \subset H = PSL(n, q)$ be a cyclic subgroup, and $Y = (N_p \cap G')/Z(G')$. Then there exists an element $h \in H$ such that $hAh^{-1} \cap Y = 1$.*

Proof. (1) is a particular case of Theorem 6.6. (2) Let A, $\bar{Y}$ be a pullback of B and Y in $G' = SL(n, q)$. Then $A/(A \cap Z)$ is cyclic, and $\bar{N} \subset N_p$. By (1) there exists $g \in G'$ such that $gAg^{-1} \cap N_p \subset Z$. Let H be the projection of g in H. Then $hAh^{-1} \cap Y = 1$, as desired.

7. THE SYMPLECTIC GROUP CASE

Notation. We keep the notation $G = GL(n, q)$ and Z for the group of scalar matrices in G. In this section $n > 2$ is even and E_k is the identity $(k \times k)$-matrix. If $k = n/2$ we omit the subscript. Set $\Gamma = \left(\begin{smallmatrix} 0 & E \\ -E & 0 \end{smallmatrix}\right)$. If X is a matrix, X^t stands for transpose of X. We set $H = Sp(n, F)$, the group of all $(n \times n)$-matrices $X \in R$ such that $X\Gamma X^t = \Gamma$. The mapping $\tau\colon X \to \Gamma X^t \Gamma^{-1}$ is an involution (an involuntary anti-automorphism) of R and $H = \{X \in R : \tau(X) = X^{-1}\}$. It is known that $\mathbf{N}_G(H)$ coincides with the general symplectic group $\tilde{H} = \{X \in G : \tau(X)X \in Z\}$. Let $\sigma\colon G \to G$ be a mapping defined by $\sigma(X) = \tau(X^{-1})$ for $X \in G$. Then σ is an involuntary automorphism of G and $H = G^\sigma$ is the subgroup of elements fixed by σ. Let $S = G \cdot \{\sigma\}$ be the semidirect product of G and the cyclic group of order 2 generated by σ. Then $H = \mathbf{C}_G(\sigma)$ and $\tilde{H} = \{X \in G : [X, \sigma] \in Z\}$. For $g \in G$ set $\Gamma_g = g\Gamma g^t$, and define τ_g and σ_g by $\tau_g(X) = \Gamma_g X^t \Gamma_g^{-1}$, $\sigma_g(X) = \Gamma_g (X^{-1})^t \Gamma_g^{-1}$.

As before, V is the natural FG-module and f is an alternating bilinear form defining H. Two vectors $v, w \in V$ are called orthogonal if $f(v, w) = 0$. Clearly, if $v, w \in V$ are orthogonal and $h \in \tilde{H}$ then hv, hw are orthogonal. Let W be a subspace of V. We set $W^\perp = \{v \in V : f(w, v) = 0$ for all $w \in W\}$. The space W is called non-degenerate if $W \cap W^\perp = 0$ and degenerate otherwise. We say that W is isotropic of $f | W = 0$. A basis of V under which the matrix of f coincides with Γ is called a Witt basis of V. If F is finite, choose $0 \neq \gamma \in F$ to be non-square. Fix a Witt basis and set $\tilde{h} = \mathrm{diag}(\gamma \cdot \mathrm{Id}_k, \mathrm{Id}_k)$. Then $\tilde{h} \in \tilde{H}$ and $\tilde{H} = Z^* H\langle h\rangle$. We set $H_1 = H\langle h\rangle$.

LEMMA 7.1. *Let* $\dim V = 4$ *and let* $V = V_1 \oplus V_2$ *be a decomposition of* V *as a direct sum of two-dimensional subspaces. Let* $A \subset GL(4,q)$ *be a non-central abelian subgroup stabilizing both* V_1, V_2. *Then there exists* $g \in SL(4,q)$ *such that* $g^{-1}Ag \cap \tilde{H} \subseteq Z$ *except, possibly, when* $q = 3$ *and* A *is an elementary* 2-*group*.

Proof. Suppose the contrary. By replacing A by gAg^{-1} with $g \in SL(4,F)$ one can assume that both V_1, V_2 are non-degenerate and orthogonal to each other. Assume that this is the case. Let B_1, B_2 be bases in V_1, V_2, respectively, and $B = B_1 \cup B_2$. Under the basis B of V let $a = \operatorname{diag}(\alpha, \beta) \in A$ be a non-scalar matrix. Let

$$S = \begin{pmatrix} \mathrm{Id}_2 & \mu \\ 0 & \mathrm{Id}_2 \end{pmatrix} \in SL(4,F),$$

where $\mu \in M(2,q)$. Then $a_1 = SaS^{-1} = \left(\begin{smallmatrix} \alpha & \mu\beta - \alpha\mu \\ 0 & \beta \end{smallmatrix}\right)$. If $a_1 \in \tilde{H}$ then $a_1 V_2 = V_2$ as $a_1 V_1 = V_1$ and V_1, V_2 are orthogonal. This only holds if $\mu\beta = \alpha\mu$. Set $A_1 = A \mid V_i$ for $i = 1,2$. If $A = Z \cdot \operatorname{diag}(\pm \mathrm{Id}, \pm \mathrm{Id})$ then $A/(A \cap Z)$ is of order 2 so the claim is trivial. Otherwise, by replacing V_1 and V_2 we can assume that A_1 is not scalar.

Choose μ to be a nilpotent matrix such that μV_1 is not A_1-invariant. If A_2 is not scalar, choose μ with the additional requirement that $\mu^t V_2$ is not A_2^t-invariant (here t stands for the transpose). This is always possible unless $q = 3$ and A is an elementary 2-group. Indeed, the number of one-dimensional subspaces in V_1 is $q+1$ so there are at least $q-1$ subspaces in V_1 that are not A_1-invariant. If W is one of them then $\mu V_1 = W$ and $\mu' V_1 = W$ for $\mu' \in M(2,F)$ if and only if μ and μ' are proportional. Therefore, if μ and μ' are not proportional then $W = \mu V_1 \neq W' = \mu' V_1$. Then also μ^t and μ'^t are not proportional. Therefore, there are at least $q-3$ choices for μ such that $\mu^2 = 0$ and μV_1 is not A_1-invariant and $\mu^t V_2$ is not A_2^t-invariant. Hence the choice of μ is always possible if $q > 3$. If $q = 3$, the choice is possible if A_1 or A_2 is not diagonalizable. (Otherwise, A is an elementary 2-group.) If $q = 2$ then A is either a cyclic 2-group, or either A_1 or A_2 (or both) are irreducible. Then the number of A_1-invariant one-dimensional subspaces is at most 1, and the same for A_2^t provided A_2 is not trivial. As $q + 1 = 3$ in this case, we can still satisfy the requirement above.

Next, $\alpha\mu V_1 = \mu\beta V_1 \subseteq \mu V_1 = W$; i.e., W is invariant under α. As $\dim V_1 = 2$, there are at most two proper non-zero A_1-submodules in V_1. If α is not scalar, $A_1 W = W$ which contradicts the choice of μ. Therefore, α is scalar. Then β is not scalar, as $\alpha\mu = \mu\beta$ and a_1 is not scalar. So β, hence $A_2 t$ is not scalar. Now, as $\mu\beta = \alpha\mu$ and α is scalar, we have $\beta^t \mu^t V_2 = \alpha^t \mu^t V_2 = \mu^t V_2$; i.e., $\mu^t V_2$ is β^t-invariant; then it is A_2-invariant. This contradicts the choice of μ above. ∎

LEMMA 7.2. *Let $h \in \tilde{H}$ be a semisimple element with exactly two distinct eigenvalues α, β. Let V_α, V_β denote the eigenspaces of α, β, respectively. Then either V_α, V_β are isotropic and of equal dimensions, or V_α, V_β are non-degenerate and $\alpha = -\beta$.*

Proof. (a) Suppose that V_α, V_β are isotropic. As $V_\alpha + V_\beta = V$, their dimensions are $\dim V/2$.

(b) Suppose that (a) does not hold. Then we can assume that V_α is not isotropic. There exists $\lambda \in F$ such that $f(hu, hv) = \lambda f(u, v)$ for some $\lambda \in F$ and all $u, v \in V$. There are $u, v \in V_\alpha$ such that $f(u, v) \neq 0$. Then $f(hu, hv) = \lambda f(u, v) = \alpha^2 f(u, v)$ whence $\alpha^2 = \lambda$. If V_β is not isotropic, we similarly have $\beta^2 = \lambda$ whence $\alpha = \pm\beta$, as desired. If V_β is isotropic, let $0 \neq u \in V_\beta$. Then $V_\alpha \not\subset u^\perp$ so there is $v \in V_\alpha$ such that $f(u, v) \neq 0$. Then $f(hu, hv) = \lambda f(u, v) = \alpha\beta f(u, v)$ whence $\alpha\beta = \lambda$. As $\alpha^2 = \lambda$, we have $\alpha = \beta$ which is not the case. ∎

LEMMA 7.3. *Let $W \subset V$ be a subspace of dimension $d > 2$ and let U be a complement of W in V.*

(i) *There exists $x \in SL(V)$ such that xW is degenerate and is not isotropic.*

(ii) *Suppose that $d < \dim V - 2$. Then there exists $x \in SL(V)$ such that $x \mid W = \mathrm{Id}$ and xU is degenerate and is not isotropic.*

Proof. (i) is obvious. To prove (ii) we can assume that W is degenerate and is not isotropic. As W is degenerate, there are vectors $w \in W$, $u \in U$ with $f(w, u) = 1$.

Let $w_1 = w, \ldots, w_k \in W$ be a basis in W. To prove (2), suppose that U is either non-degenerate or isotropic. First let U be non-degenerate so $\dim U \geq 4$. Complete $u = u_1$ to a hyperbolic basis of U, say, $u_2, \ldots, u_k$ (where $k = \dim V - d$) so $f(u_1, u_2) = f(u_3, u_4) \cdots = f(u_{k-1}, u_k) = 1$ and the other inner products $f(u_i, u_j)$ are zeros. Set $U_1 = \langle u_1, u_2 - w, u_3, \ldots, u_k \rangle$. Let x transform the basis $w_1, \ldots, w_d, u_1, \ldots, u_k$ to $w_1, \ldots, w_d, u_1, u_2 - w, u_3, \ldots, u_k$. Clearly, $x \in SL(V)$ is as desired. Now suppose that U is isotropic. As above, set $U_1 = \langle u_1, u_2 - w, u_3, \ldots, u_k \rangle$ and pick x as above. Then x is as desired. This implies (ii). ∎

PROPOSITION 7.4. *Let $n > 4$. Suppose that there exists an idempotent $0, \mathrm{Id} \neq e \in R$ such that $ae = ea$ for all $a \in A$. Then there exists $g \in G'$ such that $g^{-1}Ag \cap \tilde{H} \subset Z$.*

Proof. Set $C = \mathbf{C}_R(e)$, $V_1 = (\mathrm{Id} - e)V$ and $V_2 = eV$. Let $l = \mathrm{rank}(e)$ and $k = n - l$. Then $C = C_1 \oplus C_2$ where $C_1 \cong M(k, F)$ and $C_2 \cong M(l, F)$. Clearly, $A \subset C$. By replacing e by $\mathrm{Id} - e$ we can assume $k \leq l$. As $n > 4$ we have $l > 2$. By Lemma 7.3 there exists $x \in G'$ such that $xV_2 = xex^{-1}V$

is neither non-degenerate nor isotropic. Besides, if $k > 2$, by Lemma 7.3 we can assume that xV_1 is non-degenerate and is not isotropic. By replacing e by xex^{-1} and A by xAx^{-1} we can assume that V_1, V_2 themselves have the above property. Set $T = C \cap \tilde{H}$, and let A_i, T_i denote the projections of A, T, respectively, into C_i for $i = 1, 2$. Then T_i preserves the radical of V_i, so T_i is reducible, and hence does not contain $SL(V_i)$, except for the case $k \leq 2$. Besides, if $(l, q) = (4, 2)$ then T_2 does not contain a group isomorphic to A_7 (as it is irreducible in $SL(4, 2)$). We are in a position to use an induction assumption (namely, that Theorem 1.2 is true for $l < n$), in order to conclude that

$$(*) \quad \text{there exists } x \in SL(l, F) \text{ such that } x^{-1}A_2x \cap T_2 \subseteq Z(GL(l, F))$$

and

$$(**) \quad \begin{aligned} &\text{if } k > 2 \text{ then there exists } x_1 \in SL(k, F) \\ &\text{such that } x_1^{-1}A_1x_1 \cap T_1 \subseteq Z(GL(k, F)). \end{aligned}$$

Suppose that $k > 2$. By replacing A by $g^{-1}Ag$ with $g = \operatorname{diag}(x_1, x)$ we can assume that $A \cap \tilde{H} \subseteq \operatorname{diag}(Z(M(k, F)), Z(M(l, F)))$. This automatically holds for $k = 1$. Then each $h \in A \cap \tilde{H}$ is semisimple and has at most two distinct eigenvalues. By Lemma 7.2, this implies that h is scalar, as desired.

Suppose that $k = 2$. Then replacing A by $g^{-1}Ag$ with $g = \operatorname{diag}(\mathrm{Id}, x)$ we can assume that $A \cap \tilde{H} \subseteq \operatorname{diag}(M(2, F), Z(M(l, F)))$. Let W denote the radical of V_2. Then $W \neq 0$. Besides, V_2/W is non-degenerate so $\dim V_2/W$ is even. As $\dim V_2 = n - 2$ is even, we conclude that $\dim W$ is even; hence $\dim W \geq 2$. As $V_2 \subseteq W^{\perp}$ and $\dim W + \dim W^{\perp} = \dim V$, we conclude that $V_2 = W^{\perp}$ and $\dim W = 2$. As $h \mid W$ is scalar, $h \mid V/W^{\perp} = h \mid V/V_2$ is scalar. But V/V_2 and V_1 are isomorphic h-modules. Hence $A_1 \subseteq Z(M(2, F))$. So Lemma 7.2 again gives a contradiction, unless h is scalar. ∎

LEMMA 7.5. *Let Y be a G'-invariant subgroup of $\tilde{H} \cdot \{\sigma\}$. Then $Y \subseteq Z$ or Y contains G'.*

Proof. Clearly, $Y \cap \tilde{H}$ is G'-invariant. As $n \geq 2$, the lemma follows from 5.2 unless $Y \cap \tilde{H} \subseteq Z$. Observe that $Y : (Y \cap \tilde{H}) \leq 2$. Hence $Y \cap \tilde{H} \subseteq Z$ implies $Y : (Y \cap Z) \leq 2$. Then $[G', Y]$, the group generated by $gyg^{-1}y^{-1}$ with $g \in G'$, $y \in Y$, belongs to Z. Then $g \to gyg^{-1}y^{-1}$ defines a homomorphism $G' \to Z$ which has to be trivial. Hence Y centralizes G'. As $C_G(G') = Z$, we are done. ∎

LEMMA 7.6. *Let L be a cyclic Galois extension of Z such that $L : Z$ is even. Let $L_0 \subseteq L$ be the unique subfield such that $L_0 : Z = 2$. Let $K \subset L$ be a* *subfield of L such that $K : Z$ is even. Then $L_0 \subseteq K$ and if α is an automorphism of K trivial on Z then $\alpha(L_0) = L_0$.*

Proof. Let $\Gamma = \mathrm{Gal}(L/Z)$ and $\Gamma_1 = C_\Gamma(K)$. Then $\Gamma : \Gamma_1$ is even. As Γ is cyclic there is a unique subgroup Γ_2 of Γ of index 2 so $\Gamma_1 \subseteq \Gamma_2$. According to Galois theory, $L_0 = C_L(\Gamma_2) \subseteq C_L(\Gamma_1) = K$. As α is trivial on Z, it can be realized as an element of Γ. Obviously, L_0 is invariant under Γ so $\alpha(L_0) = L_0$. ∎

LEMMA 7.7. *Let $L \subset R = M(n, F)$ be a subfield containing Z. If $L \cap \tilde{H} \not\subseteq Z$ then $L : Z$ is even and L contains a unique subfield D such that $D : Z = 2$.*

Proof. Let $x \in L \cap \tilde{H}$ and $x \notin Z$. Then we have $\tau(x) = x^{-1}\lambda$ for some $\lambda \in F$. It follows that τ preserves the field $X = \langle x \rangle$. If $\tau | X = \mathrm{Id}$ then $x^2 = \lambda$ so $X : F = 2$. If $\tau | X \neq \mathrm{Id}$ then τ is an involutory automorphism of X. By Galois theory $X : Z$ is even so $L : Z$ is even. If $\Delta = \mathrm{Gal}(L/Z)$ and Δ_1 is the unique subgroup of Δ of index 2 then $C_L(\Delta_1)$ is the unique quadratic extension of Z in L. ∎

LEMMA 7.8. *Let $R = M(n, F)$ with n even and let $L \subset R$ be a subfield that is a cyclic Galois extension of Z. Suppose that $(n, q) \neq (2,2), (2,3)$. Then there exists $g \in G'$ such that $L \cap g\tilde{H}g^{-1} \subset Z$.*

Proof. Suppose the contrary. Then $L \cap g\tilde{H}g^{-1} \not\subset Z$ for each $g \in G'$. By Lemma 7.7 $L : Z$ is even and contains a unique subfield D such that $D : Z = 2$.

Step 1. Suppose first that $D = L$ so $L : Z = 2$. As $n > 2$, L is reducible (and completely reducible) in $M(n, F)$; hence there is a non-trivial idempotent $e \in M(n, F)$ that centralizes L. If $n > 4$, we are done by Lemma 7.4. The case $n = 4$ follows from Lemma 7.1 if $q \neq 3$. If $q = 3$ then the group L^* is not an elementary abelian 2-group. Hence we are again done by Lemma 7.1.

Step 2. Suppose that $D \neq L$. By minimality of L we have $D \cap gHg^{-1} \subset Z$ for some $g \in G'$. If $x \in L \cap g\tilde{H}g^{-1}$ and $x \notin Z$ then by Lemma 7.7 $X : Z$ is even where $X = \langle x \rangle$. By Lemma 7.6 $D \subseteq X$. As $\tau_g(x) = x^{-1}\lambda$ for some $\lambda \in F$, we have $\tau_g(X) = X$ so $\tau | X$ is an automorphism of X. Hence $\tau_g(D) = D$ and $\sigma_g D^*) = L^*$. Set $N = \mathbf{N}_S(D^*)$. Then $\sigma_g \in N$ for any $g \in G'$. Let Y be the subgroup of N generated by σ_g for $g \in G'$. Clearly, Y does not contain G'. As $\sigma_g = g\sigma g^{-1}$ in S, the group Y is G'-invariant. Then Y contains G'. This is a contradiction.

THEOREM 7.9. *Let $A \subset G$ be an abelian group with a cyclic unipotent subgroup $U(A)$. Then there exists $g \in G'$ such that $g^{-1}Ag \cap \tilde{H} \subseteq Z$.*

Proof. Let $A = B \times U(A)$ and set $L = \langle B \rangle$. Then L is a semisimple algebra. If L is not simple then L contains an idempotent satisfying the requirement of 7.4 so the result follows by 7.8. Thus, we can assume that $U(A) \neq 1$. Let $u \in U(A)$ be an element of order p. Set $V_0 = V$ and $V_i = (u - \mathrm{Id})V_{i-1}$ for $i > 0$. Let $V_k \neq 0$, $V_{k+1} = 0$. Then $\dim V - k \neq 1$ as $LV_k = V_k$ and $\dim V_k$ is a multiple of $L : Z$. By replacing A by a conjugate we can assume that V_k has a non-degenerate subspace of co-dimension ≤ 1. Then $A \cap \tilde{H} \subseteq B$. Indeed, if not then $u \in A \cap \tilde{H}$. Let W be the radical of V_k. Then $W \neq 0$, as if $W = 0$; then $V = V_k \oplus V_k^{\perp}$. As $u \mid V_k = \mathrm{Id}$, we have $V_i \subseteq V_k^{\perp}$ for all i. But $V_k \not\subseteq V_k^{\perp}$.

Therefore $\dim W = 1$. Let $b \in B \cap \tilde{H}$. Then $bW = W$ as $AV_k = V_k$ and $b \in A \cap \tilde{H}$. But if $b \notin Z$ then $K = \langle b \rangle$ is a subfield of dimension > 1 over Z and $KW = W$, which is impossible. It follows that $B \cap \tilde{H} \subseteq Z$. As $A \cap \tilde{H} \subseteq B$, we are done. ∎

Proof of Theorem 1.2. The theorem follows from the discussion above. Indeed, by Proposition 3.1 and Theorem 3.4 it suffices to prove it for the cases where $M = K(G/B)$ and B is either a line stabilizer of the natural module for $GL(n, q)$ or one of the groups listed in Theorem 3.2. The case where B is a line stabilizer is examined in Proposition 3.1. The case 3.2(vi) is considered by Lemma 4.3, while the cases 3.2(iv) and 3.2(v) are treated in Lemma 4.2. The case 3.2(iii) is exposed in Theorem 7.9. The cases 3.2(i) and 3.2(ii) are done by Theorem 6.6.

Proof of Theorem 1.1. The theorem follows from Theorem 1.2.

REFERENCES

1. S. Amitsur, Invariant submodules of simple rings, *Proc. Amer. Math. Soc.* **7** (1956), 987–989.
2. R. Brauer, On the connection between the ordinary and modular characters of groups of finite orders, *Ann. Math.* **42** (1941), 926–935.
2a. L. E. Dickson, Linear groups with an exposition of the Galois Field theory, Teubner, Leipzig, 1901, Reprinted by Dover Publ. Inc., New York, 1958.
3. D. Evans and J. Siemons, On the number of orbits of a group in two permutation actions, *Arch. Math.* **60** (1993), 420–424.
4. D. Goodwin, "Regular Orbits of Linear Groups," Ph.D. thesis, Imperial College, University of London, 1998.
5. C. Hering, Transitive linear groups and linear groups which contain irreducible subgroups of prime order, *Geom. Dedic.* **2** (1974), 425–460.
6. B. Huppert, "Endliche Gruppen," Springer-Verlag, Berlin, 1965.
7. B. Huppert and N. Blackbern, "Finite Groups II," Springer-Verlag, Berlin, 1982.
8. N. Jacobson, "The Theory of Rings," Am. Math. Soc., Providence, 1943.
9. G. D. James, "Representations of General Linear Groups," London Math. Soc. Lecture Note, Vol. 94, Cambridge Univ. Press, Cambridge, UK, 1984.

10. P. Kleidman and M. Liebeck, "Subgroup Structure of Classical Groups," London Math. Soc. Lecture Notes, Vol. 129, Cambridge Univ. Press, Cambridge, UK, 1990.
11. S. Lang, "Algebra," Addison-Wesley, Reading, MA, 1965.
12. M. Liebeck, Affine permutation groups of rank 3, *Proc. London Math. Soc.* (*3*) **54** (1987), 477–516.
13. M. Liebeck, Regular orbits of linear groups, *J. Algebra* **184** (1996), 1136–1142.
14. M. Liebeck and J. Saxl, Minimal degrees of primitive permutation groups, with application to monodromy groups of covers of Riemann surfaces, *Proc. London Math. Soc.* (*3*) **54** (1987).
15. M. Liebeck, J. Saxl, and G. Seitz, On the overgroups of irreducible subgroups of the finite classical groups, *Proc. London Math. Soc.* (*3*) **63** (1991), 266–314.
16. R. Pierce, "Associative Algebras," Springer-Verlag, Berlin, 1982.