

STRUCTURE OF FINITE, MINIMAL NONABELIAN GROUPS AND TRIANGULARIZATION

MITJA MASTNAK AND HEYDAR RADJAVI

To Tom Laffey on his sixty-fifth birthday

ABSTRACT. Motivated by problems concerning simultaneous triangularization, we study the structure of finite, minimal nonabelian groups. Using the structure result of Miller and Moreno we explicitly describe all irreducible representations of such groups. We illustrate the usefulness of results of this type on several examples.

0. INTRODUCTION

Certain finite subgroups of matrices have a significant role in proving reducibility and triangularizability results for semigroups of operators. By *reducibility* of a collection \mathcal{S} of bounded linear operators on a Banach space \mathcal{X} (of finite or infinite dimension), we mean the existence of a nontrivial closed subspace of \mathcal{X} , invariant under (every operator in) \mathcal{S} . By (simultaneous) *triangularizability* of \mathcal{S} is meant the existence of a maximal chain of subspaces of \mathcal{X} each member of which is invariant under \mathcal{S} . Of particular interest to us is the case in which \mathcal{S} is a semigroup, i.e., is closed under multiplication. At least when \mathcal{S} contains some nonzero compact operator (or in particular when \mathcal{X} is finite-dimensional), its reducibility is often determined by that of finite matrix groups associated with it. These are minimal nonabelian groups of a special type, and it is useful to know as much as possible about their structure and representations.

They are all solvable groups, of course, and much of the structure results presented below, especially about the nilpotent case, can be obtained from abstract group theory [4].

The relevant parts of our results, e.g., Theorems 2.2.6, 2.3.2, and Corollary 2.3.3, (although easily deduced from basic group representation theory) seem to be new. One of our main contributions is unified notation which makes the results more accessible to operator theorists and easier to use in the context of simultaneous triangularizability.

Using the structure results we will provide new answers to questions of the following form. Let f be a homogeneous polynomial in two noncommuting variables. What conditions can be imposed on f so that whenever, for all A, B in a semigroup, $f(A, B)$ is “small” in some sense (e.g. is zero, nilpotent, quasinilpotent,

etc.), then the semigroup is triangularizable, or at least reducible. We believe that our results on the structure of these matrix groups will find further applications, including simplifications of known triangularizability theorems.

1. NOTATION

If q is a power of a prime, then \mathbb{F}_q denotes the field with q elements. If m is a positive integer, then C_m denotes the cyclic group of order m and Γ_m denotes the $m \times m$ ‘cycle matrix’, i.e.,

$$\Gamma_m = \begin{pmatrix} 0 & 1 & & & \\ & \ddots & \ddots & & \\ & & 0 & 1 & \\ 1 & & & & 0 \end{pmatrix}.$$

If G is a group, then we denote the subset of its n -th powers by $G^n = \{g^n \mid g \in G\}$. We denote group commutators by $[-, -]$ and ring commutators by $[-, -]_r$, more precisely, if $x, y \in G$, $a, b \in R$, where G is a group and R is a ring, then $[x, y] = xyx^{-1}y^{-1}$ and $[a, b]_r = ab - ba$. All representations we consider are over complex numbers.

1.1. (p, q) -polynomials and (p, q) -matrices. In our considerations certain polynomials play a very central role.

Definition 1.1.1. *Let p, q be primes (not necessarily distinct). We say that a monic polynomial $f \in \mathbb{Z}[x]$ is a (p, q) -polynomial provided that:*

- (1) *if $p \neq q$, then f modulo q is an irreducible factor of $x^p - 1 \in \mathbb{F}_q[x]$ distinct from $x - 1$,*
- (2) *if $p = q \neq 2$, then $f(x) = (x - 1)^2$,*
- (3) *if $p = q = 2$, then either $f = 0$, or $f(x) = x + 1$.*

Remark 1.1.2. *If p, q are distinct primes and $f(x) = a_0 + \dots + a_{m-1}x^{m-1} + x^m \neq x - 1$ is an irreducible factor of $x^p - 1 \in \mathbb{F}_q[x]$, then the coefficient $a_0 \in \mathbb{F}_q$ is nonzero and for at least one choice of f , the coefficient a_{m-1} is invertible as well (since $1 = \sum_f a_{m-1}(f)$).*

We use (p, q) -polynomials to define groups of diagonal matrices.

Definition 1.1.3. *If p, q are primes and $f(x) = a_0 + \dots + a_{m-1}x^{m-1} + x^m$ is a (p, q) -polynomial, then we define a group of diagonal $p \times p$ matrices $\mathcal{D} = \mathcal{D}(p, q; f)$ as follows:*

- (1) *if $(p, q, f) \neq (2, 2, x + 1)$, then*

$$\mathcal{D} = \{ \text{diag}(\theta_1, \dots, \theta_p) \mid \theta_j^{a_0} \theta_{j+1}^{a_1} \cdot \dots \cdot \theta_{j+m-1}^{a_{m-1}} \theta_{j+m} = 1, \theta_j^q = 1 \},$$

(2) if $(p, q, f) = (2, 2, x + 1)$, then

$$\mathcal{D} = \{\pm I_2, \pm \text{diag}(i, -i)\}.$$

Remark 1.1.4. If $p|q - 1$ then $f(x) = x - \lambda$ and

$$\mathcal{D}(p, q; f) = \left\{ \text{diag} \left(\theta, \theta^\lambda, \dots, \theta^{\lambda^{p-1}} \right) \mid \theta^q = 1 \right\}.$$

If the smallest integer m such that $p|q^m - 1$ is $p - 1$, then $f(x) = 1 + x + \dots + x^{p-1}$ and $\mathcal{D}(p, q; f)$ consists of all order q diagonal matrices of determinant 1.

If $p \neq 2$, then

$$\mathcal{D}(p, p, f) = \left\{ \theta^j I, \theta^j \text{diag} \left(1, \theta^k, \dots, \theta^{(p-1)k} \right) \mid j, k = 0, \dots, p - 1 \right\},$$

where θ is any primitive p -th root of 1.

It will turn out that $\mathcal{D}(p, q; f)$ is invariant under the conjugation by Γ_p . In view of this we define:

Definition 1.1.5. If p, q are primes, $0 \neq \beta \in \mathbb{C}$, and f a (p, q) -polynomial, then we define a group of $p \times p$ matrices $\mathcal{G} = \mathcal{G}(p, q; \beta; f)$ by

$$\mathcal{G} = \left\{ D(\beta \Gamma_p)^k \mid D \in \mathcal{D}(p, q; f), 1 \leq k \leq p^j \right\}.$$

Observe that if $\beta^p = 1$, then $\mathcal{G}(p, q; \beta; f) \simeq \mathcal{G}(p, q; 1; f)$.

Definition 1.1.6. If p, q are primes and j a positive integer, then a group of matrices \mathcal{G} is said to be a (p, q, j) -matrix group, if there exists a primitive p^j -th root of unity β and a (p, q) -polynomial f (with $f(x) = x + 1$, if $(p, q, j) = (2, 2, 2)$), such that, up to simultaneous similarity, we have $\mathcal{G} = \mathcal{G}(p, q; \beta; f)$.

One of the main results in this paper is that every irreducible, finite, minimal nonabelian matrix group is a (p, q, j) -matrix group, and that for a fixed triple (p, q, j) , all (p, q, j) -matrix groups are, up to similarity, the same.

2. STRUCTURE THEORY

Finite, minimal nonabelian groups were first investigated by Miller and Moreno [4]. They first proved that they are solvable and then used solvability to obtain a comprehensive structure result for such groups (see Theorems 2.1.2 and 2.2.2). It should be noted that O. J. Schmidt extended their solvability result to finite, minimal nonnilpotent groups [8].

Below we deduce the structure results of Miller and Moreno. For the sake of completeness and also to make the results more accessible to operator theorists we include the proofs. Our approach is slightly different from that of Miller and Moreno, focusing mostly on describing groups in terms of generators and relations rather than exploring their abstract structure (e.g. counting the the number of Sylow subgroups of certain size). This enables us to explicitly describe irreducible representations of these groups.

Throughout this section, G denotes a finite, minimal nonabelian group. Note that the commutator subgroup $[G, G]$ of G is (due to solvability) a proper subgroup of G and is thus abelian. Also observe that, due to minimality, every pair of noncommuting elements generates G . It is worth pointing out that a homomorphic image of a minimal nonabelian group is either abelian or minimal nonabelian. Hence the range of every nonscalar irreducible representation of a minimal nonabelian group is also a minimal nonabelian group.

2.1. The nilpotent case. If G is nilpotent, then note that G must be a p -group for some prime p . Indeed, one of Sylow subgroups of G must be nonabelian (since G is not abelian and is a direct product of its Sylow subgroups) and by minimality G is equal to that group.

Let G_n be the n -fold iterated commutator of G (i.e., $G_0 = G$ and $G_n = [G, G_{n-1}]$ for $n \geq 1$). Let r be minimal such that $G_r = 1$. Note that $r \geq 2$ as G is not commutative. Let $a \in G_{r-2}$ and $b \in G$ be a pair of noncommuting (hence generating) elements of G . Note that $[a, b] \in G_{r-1} \subseteq Z(G)$ (and hence $r = 2$). Without loss we may also assume that a^p, b^p lie in $Z(G)$ (continue to replace a by a^p or b by b^p until this is so).

We have shown that G is generated by a of order, say p^i , and b of order p^j and $a^p, b^p, [a, b] \in Z(G)$. We assume that $i + j$ is minimal possible. Since $[a, b]$ is a central element, every element of G can be written in the form $[a, b]^{n_1} a^{n_2} b^{n_3}$.

If a^p is a p -th power of a central element, then $a^p = 1$ (if $a^p = x^p$, where $x \in Z(G)$, then replace a by ax^{-1}). The same holds for b^p . Note also that $[a, b]^p = [a^p, b] = 1$.

The structure of G is thus determined up to the structure of its centre $Z(G) = \langle a^p, b^p, [a, b] \rangle$ (if a commutes with $[a, b]^{n_1} a^{n_2} b^{n_3}$, then a must commute with b^{n_3} and hence n_3 must be divisible by p).

Lemma 2.1.1. *If $p \neq 2$, then $\langle a^p \rangle \cap \langle b^p \rangle = 1$. Furthermore, if $p = 2$, then either $\langle a^p \rangle \cap \langle b^p \rangle = 1$, or $\langle a^p \rangle = \langle b^p \rangle$ and $i = j = 2$.*

Proof. Assume $1 \neq a^{rp^n} = b^{sp^m}$, where r, s are coprime to p and $1 \leq n < i$ and $1 \leq m < j$. With no loss of generality we assume that $r = s = 1$ and that $n \leq m$. If $n < m$, then we could replace a by $ab^{-p^{m-n}}$, contradicting the minimality of $i + j$. Hence $n = m$. Since $1 = a^{p^i} = (a^{p^n})^{p^{i-n}} = (b^{p^n})^{p^{i-n}} = b^{p^i}$, we must have $i \leq j$. A symmetric argument shows that $j \leq i$ and thus $i = j$. Note that $[ab^{-1}, b] = [a, b]$ and $(ab^{-1})^{p^n} = a^{p^n} b^{-p^n} [a, b]^{\binom{p^n}{2}} = [a, b]^{\binom{p^n}{2}}$. If either $n > 1$, or $p \neq 2$, then $\binom{p^n}{2}$ is divisible by p and hence replacing a by ab^{-1} would contradict the minimality of $i + j$. Assume now that $n = 1$ and $p = 2$. Then $a^p = b^p$. Also, if $i > 2$, then $(ab^{-1})^{p^2} = 1$ and replacing a by ab^{-1} would again contradict the minimality of $i + j$. \square

We may assume without loss of generality that either $\langle a^p \rangle \cap \langle b^p \rangle = 1$, or $a^p = b^p$ with $p = i = j = 2$. The order of G is $|Z(G)|p^2$. If $a^p = b^p$, then the size of $Z(G)$

is either p^i (if $[a, b] \notin \langle a \rangle$) or p^{i-1} . If $\langle a \rangle \cap \langle b \rangle = 1$, then the size of $Z(G)$ is either p^{i+j-1} (if $[a, b] \notin \langle a, b \rangle$), or p^{i+j-2} .

Observe that $[G, G] = \langle [a, b] \rangle$ is a cyclic group of order p and that every element of $[G, G]$ is a commutator. Indeed, $[a, b]^i = [a^i, b] = [a, b^i]$.

The above discussion is summarized in the proposition below.

Theorem 2.1.2 (cf. [4]). *If G is a finite, nilpotent, minimal nonabelian group, then*

- (1) *For some prime p , G is a p -group and is generated by $a, b \in G$ such that a^p, b^p and $[a, b]$ are central elements.*
- (2) *If $p \neq 2$, then we can additionally assume that $\langle a^p \rangle \cap \langle b^p \rangle = 1$. If $p = 2$, then either $\langle a^2 \rangle \cap \langle b^2 \rangle = 1$, or $a^2 = b^2$ and $a^4 = 1 = b^4$.*
- (3) *$[G, G] = \langle [a, b] \rangle \simeq C_p$, and every element of $[G, G]$ is a commutator.*

□

Corollary 2.1.3. *If G is a finite, nilpotent, minimal nonabelian group with a cyclic centre, then G is generated by $a, b \in G$ such that $a^p = 1$, and $b^p, [a, b] \in Z(G)$.*

Theorem 2.1.4. *Any irreducible nonscalar representation of G has size p and is given by $a \mapsto A = A_{\alpha, \theta}$, $b \mapsto B = B_{\beta}$, where*

$$A = \alpha \operatorname{diag} (1, \theta, \dots, \theta^{p-1}), \quad B = \beta \Gamma_p,$$

where θ is a primitive p -th root of unity and $\alpha^{p^i} = 1 = \beta^{p^j}$. If $a^p = b^p$, then we have $\alpha^p = \beta^p$. If $[a, b] \in \langle a^p, b^p \rangle$, say $[a, b] = a^{i_0 p} b^{j_0 p}$, then we have $\theta = \alpha^{i_0 p} \beta^{j_0 p}$.

Representations associated to (α, β, θ) and $(\alpha', \beta', \theta')$ are isomorphic if and only if $(\alpha^p, \beta^p, \theta) = (\alpha'^p, \beta'^p, \theta')$.

Proof. Observe that $[A, B] = \theta^{-1}I$, $A^p = \alpha^p I$, $B^p = \beta^p I$ and hence $a \mapsto A$ and $b \mapsto B$ is indeed a representation of G . It is clearly irreducible. Suppose that representations associated to (α, β, θ) and $(\alpha', \beta', \theta')$ are isomorphic. Then there is an invertible matrix C such that $CA_{\alpha, \theta}C^{-1} = A_{\alpha', \theta'}$ and $CB_{\beta}C^{-1} = B_{\beta'}$. Hence $\theta'^{-1}I = [A_{\alpha', \theta'}, B_{\beta'}] = C[A_{\alpha, \theta}, B_{\beta}]C^{-1} = C(\theta^{-1}I)C^{-1} = \theta^{-1}I$ and therefore $\theta = \theta'$. Also $\alpha'^p I = A_{\alpha'}^p = CA_{\alpha}^p C^{-1} = \alpha^p I$ and $\beta'^p I = B_{\beta'}^p = CB_{\beta}^p C^{-1} = \beta^p I$. Hence $(\alpha^p, \beta^p, \theta) = (\alpha'^p, \beta'^p, \theta')$.

It is now sufficient to prove that representations associated to (α, β, θ) for pairwise distinct $(\alpha^p, \beta^p, \theta)$ together with the scalar representations (which are given by characters on $G/[G, G] = G/\langle [a, b] \rangle$) exhaust all possibilities. This is done by using a counting argument. One must, according to the structure of $Z(G)$, consider four cases. Here is one of the cases (the others work almost the same way). Assume that $a^p \neq b^p$ and that $[a, b] \notin \langle a^p, b^p \rangle$. In this case $|G| = p^2 |Z(G)| = p^{i+j+1}$.

Summation of sizes of representations described above gives

$$\begin{aligned} \sum_{\rho} \dim(\rho)^2 &= \sum |\{(\alpha^p, \beta^p, \gamma)\}| p^2 + \sum |G/[G, G]|^2 \\ &= p^{i-1} p^{j-1} (p-1) p^2 + p^{i+j+1-1} = p^{i+j+1} = |G| \end{aligned}$$

□

2.2. The nonnilpotent case. Assume that G is not nilpotent. Let $a \in [G, G]$ and $b \in G$ generate G . Note that without any loss of generality we can assume that $a^{q^i} = 1 = b^{p^j}$, where p and q are primes, and i, j are positive integers. We assume that j is smallest possible, and hence b^p commutes with a .

We first show that if $p = q$, then G is a q -group and therefore nilpotent. Let $H = \langle b^r a^s b^{-r} \mid r, s \rangle$ be the normal subgroup of G generated by a . The group H is abelian as $H \leq [G, G]$, and therefore it is a q -group since it is generated by elements of exponent a power of q . Note that every $g \in G$ can be written in the form $g = b^n h$, where $h \in H$. Observe that $(b^n h)^m = b^{nm} h'$ for some $h' \in H$ and hence $G^{p^j} = \{g^{p^j} \mid g \in G\} \subseteq H$. Thus if $p = q$, then the exponent of G must divide q^{i+j} .

From now on assume that $p \neq q$ and observe that $\langle b \rangle \cap H = 1$. Hence $G = H \rtimes \langle b \rangle$ ($H \rtimes \langle b \rangle$ is a noncommutative subgroup of G and is therefore equal to G).

We will show that $i = 1$, i.e., $a^q = 1$. Due to minimality of G we may assume that $H = [G, G] = [H, G]$ and that $H^q = \{x^q \mid x \in H\}$ is a central subgroup of G . Note that every nontrivial commutator $[x, y] = xyx^{-1}y^{-1}$, where $x \in H$, has exponent q . Indeed, since x commutes with $[x, y]$ we have $[x, y]^q = [x^q, y] = 1$. Thus a and hence also H have exponent q . Observe also that $b^p \in Z(G)$. Hence $G \simeq (\mathbb{F}_q^r, +) \rtimes C_{p^j}$, where the action of $C_{p^j} = \langle b \rangle$ on \mathbb{F}_q^r is given by $b(\mathbf{u}) = B\mathbf{u}$, where $B \in GL_r(\mathbb{F}_q)$, $B^p = I$. If $\mathbf{u} \in \mathbb{F}_q^r$, and $b^n \in C_{p^j}$, then we identify $\mathbf{u} = \mathbf{u} \rtimes 1 \in G$ and $b^n = \mathbf{0} \rtimes b^n \in G$.

We next show that $r = m$, where m is the minimal positive integer such that $q^m - 1$ is divisible by p . Note that the field \mathbb{F}_{q^m} is the smallest field extension of \mathbb{F}_q containing a primitive p -th root of unity. Recall that the Galois group of this extension is cyclic and is generated by $\varphi: \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}$, $\varphi(x) = x^q$. The order of φ is m (and hence m divides $p-1$). We denote the induced (entrywise) action on \mathbb{F}_q^r by φ as well. Observe that the irreducible factors of $x^p - 1$ over \mathbb{F}_q are $x - 1$ and $f_\omega = (x - \omega)(x - \omega^q) \dots (x - \omega^{q^{m-1}})$. Also note that $f_{\omega_1} = f_{\omega_2}$ if and only if ω_1 and ω_2 are in the same orbit under the action of $\langle \varphi \rangle$ (i.e., if $\omega_2 = \omega_1^{q^i}$).

Let $\bar{B}: \mathbb{F}_{q^m}^r \rightarrow \mathbb{F}_{q^m}^r$ be the linear transformation induced by B and let $\mathbf{u} \in \mathbb{F}_{q^m}^r$ be a nonzero eigenvector corresponding to an eigenvalue $\omega \neq 1$ (such an eigenvalue

exists as $\overline{B} \neq I$, $\overline{B}^p = I$, and $\text{char}\mathbb{F}_{q^m} = q$ does not divide p). Define

$$\Omega = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \omega & \omega^q & \dots & \omega^{q^{m-1}} \\ \vdots & \vdots & & \vdots \\ \omega^{m-1} & \omega^{(m-1)q} & \dots & \omega^{(m-1)q^{m-1}} \end{pmatrix}$$

and note that the matrix

$$X = (\mathbf{u} \quad \varphi(\mathbf{u}) \quad \dots \quad \varphi^{m-1}(\mathbf{u})) \Omega$$

has entries in \mathbb{F}_q (they are fixed under φ) and that $\text{rank } X = m$ (Ω is an invertible Vandermonde matrix and $\mathbf{u}, \varphi(\mathbf{u}), \dots, \varphi^{m-1}(\mathbf{u})$ are eigenvectors belonging to distinct eigenvalues of B). Observe that $\text{Col} X$, the column space of X , is an invariant subspace for B and that $(\text{Col} X) \rtimes \langle b \rangle$ is a nonabelian subgroup of G . Hence $\text{Col} X = \mathbb{F}_q^r$ and $r = m$. Observe also that B is irreducible: if $\mathcal{U} \subseteq \text{Col} X = \mathbb{F}_q^r$ is an invariant subspace for B , then $B_{\mathcal{U}} \neq I$, as $\overline{B}_{\text{Col} X}$ has no nontrivial fixed points, and hence $\mathcal{U} \rtimes \langle B \rangle$ is a nonabelian subgroup of G .

Let $f(x) = a_0 + a_1x + \dots + a_{m-1}x^{m-1} + x^m$ be the characteristic polynomial of B (which is also the minimal polynomial and $f = f_{\omega}$ for some ω). Note that for any nonzero vector $\mathbf{v}_0 \in \mathbb{F}_q^m$, the vectors

$$\mathbf{v}_0, B\mathbf{v}_0, \dots, B^{m-1}\mathbf{v}_0$$

form a basis for \mathbb{F}_q^m and that

$$B = B_f = \begin{pmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & -a_{m-1} \end{pmatrix}$$

with respect to this basis.

Definition 2.2.1. We write $G_f = G_{f,j} = \mathbb{F}_q^m \rtimes \langle b | b^{p^j} = 1 \rangle$, where the action of b on \mathbb{F}_q^m is given by B_f .

Observe that if $g(x) \neq x-1$ is another irreducible divisor of x^p-1 , then $G_f \simeq G_g$. If f and g are associated to ω_1 and ω_2 , where $\omega_2 = \omega_1^i$, then the isomorphism is induced by $B_g \mapsto B_g^i$ and $\mathbf{u}_0 \mapsto \mathbf{v}_0$.

Assume now that $G = G_f$. Observe that $[G, G] = \mathbb{F}_q^m$. We will show that every element of $[G, G]$ is a commutator. Define $K = \{b\mathbf{u}b^{-1}\mathbf{u}^{-1} | \mathbf{u} \in \mathbb{F}_q^m\}$ and note that K is a normal subgroup of $[G, G]$. Since $b\mathbf{u}b^{-1}\mathbf{u}^{-1} = (B-I)\mathbf{u}$ and $B-I$ is invertible, it follows that $K = \mathbb{F}_q^m$. We have thus proven the following theorem.

Theorem 2.2.2 (cf. [4]). *If G is a finite, nonnilpotent, minimal nonabelian group, then $G \simeq G_f$ for some irreducible divisor f of $\frac{x^p-1}{x-1} \in \mathbb{F}_q[x]$. The size of G is $q^m p^j$.*

The commutator subgroup $[G, G]$ is isomorphic to C_q^m . Every element of $[G, G]$ is a commutator. □

2.2.3. Representations. Here we describe the irreducible complex representations of $G = G_{f,j} = (\mathbb{F}_q^m, +) \rtimes C_{p^j}$. All such representations are obtained as follows (cf. [5, Proposition 25]). Choose χ , a character on $H = (\mathbb{F}_q^m, +)$ and ρ , a character on $C_{p^j} = \langle b^p \rangle \simeq C_{p^i}$. The corresponding irreducible representation of G is then induced by $\chi \otimes \rho$, a representation of $H \rtimes C_{p^i} \leq G$. More precisely, if $1 \neq \chi \in \widehat{H}$ and $\beta \in \mathbb{C}$, $\beta^{p^i} = 1$, then G acts on $V = V(\chi, \beta)$, a vector space with basis v_0, \dots, v_{p-1} , by $hv_i = \chi(b^i hb^{-1})v_i$ and $bv_i = \beta v_{i+1}$. Note that representations $V(\chi, \beta)$ and $V(\chi', \beta')$ are isomorphic if and only if $\chi' = b^i(\chi)$ for some integer $0 \leq i < p$ and $\beta^p = \beta'^p$. Observe, that if $\beta^p = 1$, then without any loss of generality we may assume that $\beta = 1$. If $\chi = 1$, then we get the 1-dimensional representations given by $h \mapsto 1$, $h \in H$, $b \mapsto \beta$, $\beta^{p^j} = 1$. We summarize the discussion above in the theorem below.

Theorem 2.2.4. *Let G be a nonnilpotent, finite, minimal nonabelian group. Then $G = G_{f,j} = (\mathbb{F}_q^m, +) \rtimes \langle b | b^{p^j} = 1 \rangle$. If $\mathbf{0} \neq \mathbf{u} \in \mathbb{F}_q^m$, then every nonscalar representation of G is determined by $\mathbf{u} \mapsto A$ and $b \mapsto B$, where A is an arbitrary nonidentity element of $\mathcal{D}(p, q; f)$ and $B = \beta \Gamma_p$, with $\beta^{p^j} = 1$. Representations associated to $(A, \beta \Gamma_p)$ and $(A', \beta' \Gamma_p)$ are isomorphic if and only if $A = A'$ and $\beta^p = \beta'^p$.*

Proof. Abbreviate $\mathbf{e}_i = (0, \dots, 1, \dots, 0) \in \mathbb{F}_q^m$. Without any loss of generality assume that $\mathbf{u} = \mathbf{e}_1$. Now observe that nontrivial characters χ discussed above are in bijective correspondence with $\mathcal{D}(p, q; f)$. This correspondence is given by $\chi_A(\mathbf{e}_j) = \theta_j$, where $A = \text{diag}(\theta_1, \dots, \theta_p) \in \mathcal{D}(p, q; f)$. □

Corollary 2.2.5. *If $p \neq q$, then the size of $\mathcal{D} = \mathcal{D}(p, q; f)$ is q^m . If $(\psi_0, \dots, \psi_{m-1})$ is an m -tuple of complex numbers of order q , then for every integer i , there exists a unique element $D = \text{diag}(\theta_1, \dots, \theta_p)$ of \mathcal{D} such that $\theta_{i+k} = \psi_k$, for $0 \leq k \leq m-1$. □*

The following is result about the frequency with which entries in $\mathcal{D}(p, q; f)$ occur is of some interest.

Theorem 2.2.6. *If $f(x) \neq x-1$ is an irreducible divisor of $x^p - 1 \in \mathbb{F}_q$ and $\theta^q = 1$ (θ can be 1), then the expected number of θ 's in a random $D \in \mathcal{D} = \mathcal{D}(p, q, f)$ is $\frac{p}{q}$. In particular, if $q > p$, then there are members of \mathcal{D} containing no θ .*

Proof. The number of all θ 's in any fixed diagonal position in \mathcal{D} is q^{m-1} (fix that entry, the $m-1$ entries following it are arbitrary, the other entries are uniquely determined). Hence the total number of diagonal entries in elements of \mathcal{D} that are equal to θ is pq^{m-1} . The expected number of θ 's in a random member of \mathcal{D} is therefore $\frac{pq^{m-1}}{|\mathcal{D}|} = \frac{p}{q}$. □

2.3. Summary. Here we summarize some of the results proven in sections 2.1 and 2.2 about properties that hold for nilpotent as well as nonnilpotent finite, minimal nonabelian groups.

Theorem 2.3.1. *Let G be a finite, minimal nonabelian group. Then there exist $a, b \in G$, positive integers i, j , and primes p, q (not necessarily distinct), such that $\text{ord}(a) = q^i$, $\text{ord}(b) = p^j$, $G = \langle a, b \rangle$, p, q are the only primes dividing $|G|$, and $i = 1$ whenever $p \neq q$. Furthermore*

- (1) *Every element in the commutator group of G is a commutator.*
- (2) *The group G is nilpotent if and only if $p = q$.*
- (3) *If f is any (p, q) -polynomial (other than $x + 1$, if $p = q = 2$), then all nonscalar irreducible representations of G are of size p and are given by $a \mapsto \alpha A$, $b \mapsto \beta \Gamma_p$, where $\alpha^{q^i} = 1 = \beta^{p^j}$, and A is a nonscalar element of $\mathcal{D}(p, q; f)$.*

□

Theorem 2.3.2. *If $\mathcal{G} \subseteq \mathcal{M}_p(\mathbb{C})$ is an irreducible, finite, minimal nonabelian, matrix group then \mathcal{G} is a (p, q, j) -matrix group.*

□

Corollary 2.3.3. *Let p, q be primes, $A = \text{diag}(\theta_1, \dots, \theta_p)$ with $\theta_r^q = 1$, $\alpha, \beta \in \mathbb{C}$ such that $\alpha^{q^i} = 1 = \beta^{p^j}$, and $\mathcal{G} = \langle \alpha A, \beta \Gamma_p \rangle$. If either $(p, q) \neq (2, 2)$, or $(\alpha, \beta) = (1, 1)$, then*

- (1) *Minimal nonabelian subgroups of \mathcal{G} are all similar.*
- (2) *If $p = q$ then there is a unique minimal nonabelian subgroup of \mathcal{G} .*

□

3. APPLICATIONS

We start by recording the following useful fact which easily follows from the structure theory of minimal nonabelian groups we have developed.

Proposition 3.0.1. *(cf. [3]) If \mathcal{G} is a finite, nonabelian matrix group, then the spectral radius of some ring commutator $AB - BA$, $A, B \in \mathcal{G}$ is at least $\sqrt{3}$. We can further assume that this ring commutator commutes with every element of the derived subgroup $[\mathcal{G}, \mathcal{G}]$.*

Proof. Without loss of generality we assume that \mathcal{G} is a minimal nonabelian group. Note that $AB - BA = AB(I - A^{-1}B^{-1}AB)$. Hence for every $D \in [\mathcal{G}, \mathcal{G}]$ some ring commutator has the spectral radius equal to the spectral radius of $I - D$. □

Recall that if G is a group, then $g \in G$ is called a 2-element if $g^{2^r} = 1$ for some integer r .

Lemma 3.0.2. *Let \mathcal{G} be a finite, minimal nonabelian matrix group. If the spectrum of every group commutator $[X, Y] = XYX^{-1}Y^{-1}$ contains at most two elements, then either \mathcal{G} contains a noncentral 2-element, or \mathcal{G} is nilpotent.*

Proof. It is sufficient to prove the statement when $\mathcal{G} = \mathcal{G}(p, q; \beta; f)$ is a (p, q, j) -matrix group with $p \neq q$. We use the fact that every element of the commutator subgroup is a commutator. Suppose if possible, that $p \neq 2 \neq q$. Let $f(x) = x^m + a_{m-1}x^{m-1} + \dots + a_1x + a_0$. If $m \geq 3$, then first three diagonal entries of every element of $\mathcal{D}(p, q; f) = [\mathcal{G}, \mathcal{G}]$ are arbitrary q -th roots of unity; contradicting the assumption. If $m = 1$, then $\mathcal{D}(p, q; f) = \left\{ \text{diag} \left(\theta, \theta^\lambda, \dots, \theta^{\lambda^{p-1}} \right) \right\}$ and we again have a commutator with at least 3 distinct eigenvalues. Assume now that $m = 2$ and $f(x) = x^2 + a_1x + a_0$. Without loss of generality we may assume that neither a_0 , nor a_1 is divisible by q (Remark 1.1.2). If θ is a primitive p -th root of unity, then $\text{diag}(1, \theta, \theta^{-a_1}, \dots), \text{diag}(\theta, 1, \theta^{-a_0}, \dots) \in \mathcal{D}$. If either a_0 or a_1 is different from $-1 \in \mathbb{F}_q$, then we get a contradiction. If $a_0 = a_1 = -1$, then $\text{diag}(\theta, \theta^{-1}, 1, \dots) \in \mathcal{D}(p, q; f)$. Again a contradiction. \square

Lemma 3.0.3. *If \mathcal{G} is an irreducible, finite, minimal nonabelian, matrix group and the spectrum of every ring commutator $AB - BA$, $A, B \in \mathcal{G}$ is an \mathbb{R} -collinear subset of \mathbb{C} , then the spectrum of every group commutator has at most two elements.*

Proof. If $A = \text{diag}(\theta_1, \dots, \theta_p) \in \mathcal{G} = \mathcal{G}(p, q; \beta; f)$, then $A(\beta\Gamma_p) - (\beta\Gamma_p)A$ has eigenvalues $\beta(\theta_i - \theta_{i+1})$. If all these values are \mathbb{R} -collinear this means that at most two of θ_i 's can be distinct. \square

Corollary 3.0.4. *Let \mathcal{G} be a compact group of matrices. Assume that the spectrum of every ring commutator $AB - BA$, $A, B \in \mathcal{G}$ is an \mathbb{R} -collinear subset of \mathbb{C} . If \mathcal{G} contains no noncentral 2-elements, then \mathcal{G} is abelian.*

Proof. Assume that \mathcal{G} contains no noncentral 2-elements and suppose that \mathcal{G} is not abelian. Since a compact group is abelian if and only if every finite subgroup is such [3], we may, without any loss of generality, assume that \mathcal{G} is a minimal nonabelian group. If \mathcal{G} is not nilpotent, then we are done by Lemma 3.0.3 and Corollary 3.0.4. Assume now that \mathcal{G} is nilpotent. Then \mathcal{G} is a p -group for some prime $p \neq 2$. Block diagonalize \mathcal{G} , note that one of the nonscalar irreducible blocks is similar to a (p, p, j) -matrix group $\mathcal{G}(p, p; \beta; f) = \langle A, B \rangle$, where $A = \text{diag}(1, \theta, \dots, \theta^{p-1})$, $B = \beta\Gamma_p$, and observe that the spectrum of $AB - BA$ is not \mathbb{R} -collinear. \square

If \mathcal{S} is a semigroup, then $\overline{\mathbb{R}^+\mathcal{S}} = \overline{\{rS \mid r > 0, S \in \mathcal{S}\}}$ denotes its positively homogeneous closure.

Theorem 3.0.5. *Let $\mathcal{S} = \overline{\mathbb{R}^+\mathcal{S}}$ be an irreducible semigroup of matrices and let L be the convex hull of the spectra of all ring commutators in \mathcal{S} , i.e., $L = \text{co}\{\lambda \in \sigma(ST - TS) \mid S, T \in \mathcal{S}\}$. If $L \neq \mathbb{C}$, then $L = \mathbb{R}$, or $L = i\mathbb{R}$. Furthermore, if $\mathcal{S} \setminus \{0\}$ is a group and $L = \mathbb{R}$, then \mathcal{S} contains a noncentral involution.*

Proof. Observe that if $L \neq \mathbb{C}$, then $L = \alpha\mathbb{R}$, for some nonzero $\alpha \in \mathbb{C}$. Let k be the minimal positive rank in \mathcal{S} and let E be an idempotent of rank k . If $k > 1$ then consider $E\mathcal{S}E|_{\text{Range}(E) \setminus \{0\}} = \mathbb{R}^+\mathcal{G}$, where \mathcal{G} is a compact group. Without loss of generality we assume that \mathcal{G} is a subgroup of unitary matrices. By Corollary 3.0.4 \mathcal{G} contains a noncentral 2-element $U = \begin{pmatrix} \xi I_1 & 0 \\ 0 & -\xi I_2 \end{pmatrix}$. Let $V \in \mathcal{G}$ be an element which does not commute with U and note that $H = \bar{\xi}[UV^*, V]_r = \bar{\xi}(U - VUV^*)$ is a nonzero hermitian matrix (indeed, since $U^* = \bar{\xi}^2 U$, we have $H^* = \xi(U^* + VU^*V^*) = \xi\bar{\xi}^2(U + VUV^*) = H$). Hence $L = \xi\mathbb{R}$ and since $\xi^2 I \in \mathcal{S}$ we also have $\xi^2 L = L$; which in turn implies that $\xi^2 \in \mathbb{R}$.

Now assume that $k = 1$. Then it is sufficient to check the claim for $\langle A, B \rangle$ [6], where $A = \begin{pmatrix} a & 0 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 0 & b \end{pmatrix}$, with $ab \neq 1$. Note that $[A, B]_r = AB - BA = \begin{pmatrix} 1 & -a \\ b & -1 \end{pmatrix}$. The ring commutator $[A, B]_r$ is not nilpotent since $ab \neq 1$. Thus we have $a, b \in \mathbb{R}$, since $a[A, B]_r = [A^2, B]_r$ and $b[A, B]_r = [A, B^2]_r$. Hence $L = \mathbb{R}$ (if $ab < 1$) or $L = i\mathbb{R}$ (if $ab > 1$). \square

Remark 3.0.6. *The proof above also shows that both cases $L = \mathbb{R}$ and $L = i\mathbb{R}$ are possible.*

The following numerical invariant $\chi(f)$ of a polynomial f will be useful in studying (pre)triangularizing conditions on semigroups of operators.

Definition 3.0.7. *For a function $f: \mathbb{C} \rightarrow \mathbb{C}$ we define*

$$\chi(f) = \inf \left\{ \max_{\theta^p=1} |f(\theta)| \mid p \text{ prime} \right\}.$$

Proposition 3.0.8. *If $f: \mathbb{C} \rightarrow \mathbb{C}$ is a continuous function, then the following are equivalent.*

- (1) *For every prime p there is a $\theta \in \mathbb{C}$ such that $\theta^p = 1$ and $f(\theta) \neq 0$.*
- (2) $\chi(f) > 0$.

Proof. Let $M = \max_{|\theta|=1} |f(\theta)|$ and let $\theta_0 \in S^1$ be such that $f(\theta_0) = M$. Let $\delta > 0$ be such that for $|\theta - \theta_0| > \delta$ we have $|f(\theta)| > M/2$ and let p_0 be a prime such that for all primes $p \geq p_0$ there is a p -th root of 1 in the δ -neighborhood of θ_0 . Then

$$\chi(f) \geq \min \left\{ \frac{M}{2}, \max_{\theta^p=1} |f(\theta)| \mid p \text{ prime}, p < p_0 \right\} > 0$$

\square

Remark 3.0.9. *If $f: \mathbb{C} \rightarrow \mathbb{C}$ is an analytic function, then the condition (1) from the proposition above says that f is not divisible by $x^p - 1$ for any prime p .*

When f is a polynomial then the following result provides a sufficient condition, independent of the degree of f , for $\sqrt{3} \leq \chi(f)$.

Proposition 3.0.10. *Let f be a monic polynomial such that $f(1) = 0$. If no roots of f lie in the region*

$$D = \left\{ z \in \mathbb{C} \mid \operatorname{Re}(z) < \frac{\sqrt{3}}{3} - \frac{1}{2}, 0 < |z| < 2 \right\}$$

then $\chi(f) \geq \sqrt{3}$.

Proof. Let $f(x) = (x-1)(x-\xi_1)\dots(x-\xi_n)$ and let p be a prime. Let θ be the p -th root of unity closest to -1 with nonnegative imaginary part, i.e., $\theta = e^{(p-1)\pi i}$ and note that $|(\theta-1)(\bar{\theta}-1)| \geq 3$ and that for any $\xi \notin D$ we have $|(\theta-\xi)(\bar{\theta}-\xi)| \geq 1$. The latter is clear if either $\xi = 0$ or $|\xi| \geq 2$. Now assume ξ is such that $\frac{\sqrt{3}}{3} - \frac{1}{2} \leq \operatorname{Re}(\xi)$. Note that it is sufficient to prove the statement for $\operatorname{Re}(\xi) = \frac{\sqrt{3}}{3} - \frac{1}{2}$. Examine the triangle with vertices $\theta, \bar{\theta}$ and ξ . Let $h = \frac{\sqrt{3}}{3} - \frac{1}{2} - \operatorname{Re}(\theta)$ and $s = \operatorname{Im}(\theta) = -\operatorname{Im}(\bar{\theta}) \geq 0$. The area A of the triangle in question is hs . Let $a = |\theta - \xi|$ and $b = |\bar{\theta} - \xi|$. If $A \geq \frac{1}{2}$, then we are done as $ab \geq 2A$. Note that if $p = 3$, then $2A = 1$ and that if $p = 5$, then $2A \approx 1.04 > 1$. Note also that if $p \geq 7$, then $h > s$. In this case let γ be the angle at ξ and let γ' be the angle at $\xi' := \operatorname{Re}(\xi)$ of the triangle $(\theta, \bar{\theta}, \xi')$ and note that $\gamma < \gamma' < \frac{\pi}{2}$. Define $d = \sqrt{h^2 + s^2}$ and observe that in this case $ab = d^2 \frac{\sin(\gamma)}{\sin(\gamma')} \geq d^2$. Finally if $p \geq 7$, then $d^2 \geq 1$. Indeed, if $p = 7$, then $d^2 \approx 1.14 > 1$. If $p \geq 11$, then already $h > 1$ (if $p = 11$, then $h \approx 1.03 > 1$). \square

Remark 3.0.11. *With some care the region D in the theorem above could be shrunk to*

$$D' = \{ z \in \mathbb{C} \mid \forall \text{ prime } p, |(z - e^{(p-1)\pi i})(z - e^{(p+1)\pi i})| \geq 1 \}.$$

The quantity $\frac{\sqrt{3}}{3} - \frac{1}{2} \approx 0.077$ is fairly close to 0.

Definition 3.0.12. *If $g \in \mathbb{C}\langle x, y \rangle$ is a polynomial in two noncommuting variables, then define $g_1, g_2: \mathbb{C} \rightarrow \mathbb{C}$ by $g_1(t) = g(t, 1)$, $g_2(t) = g(1, t)$, $\chi_1(g) = \chi(g_1)$, $\chi_2(g) = \chi(g_2)$ and $\chi(g) = \max\{\chi_1(g), \chi_2(g)\}$.*

Theorem 3.0.13. *Let g be a homogeneous polynomial in two noncommuting variables of joint degree r . If $0 \leq k < \chi(g)$, then every finite group \mathcal{G} of matrices satisfying*

$$\rho(g(xy, yx)) \leq k\rho(x)^r \rho(y)^r,$$

for all $x, y \in \mathcal{G}$ is abelian.

Proof. Assume with no loss of generality that $\chi(g) = \chi_1(g)$. Suppose that \mathcal{G} is a minimal nonabelian group satisfying $\rho(g(xy, yx)) \leq k\rho(x)^r \rho(y)^r = k$. Hence $\rho([x, y], I) \leq k$, for all $x, y \in G$. By the structure theorem, every element of the

commutator subgroup is a commutator and for some prime p , every p -th root of unity is in the spectrum of some commutator. Hence we have

$$\chi_1(g) \leq \max_{\theta^p=1} |g(1, \theta)| \leq k < \chi(g).$$

This is clearly a contradiction. \square

We can extend Theorem 3.0.13 to the general semigroup setting. Recall that a property \mathcal{P} that a semigroup \mathcal{S} of complex matrices may possess is called pretriangularizing [1] if the following holds:

- (1) \mathcal{P} is similarity invariant.
- (2) \mathcal{P} passes to subsemigroups, homogenized closures and semisimplifications.
- (3) If $\mathcal{S} \oplus 0$ has property \mathcal{P} , then so does \mathcal{S} .
- (4) Totally reducible semigroups with \mathcal{P} have no non-zero nilpotents.
- (5) Finite groups with \mathcal{P} are abelian.

It should be noted that reasonable matrix semigroup properties satisfy the conditions (1)-(3) and that it is usually sufficient to check (4) for irreducible semigroups. In [1] it was proven that groups satisfying a pretriangularizing property are always reducible and have triangularizable commutator subgroups. It was also shown that if r is the minimal nonzero rank in a semigroup $\mathcal{S} = \overline{\mathbb{R}^+ \mathcal{S}}$ satisfying a pretriangularizing property, then \mathcal{S} has a chain of invariant subspaces of length at least r . It is implicit in the proof of [1, Theorem 5.1] that the last statement can be extended to semigroups of compact operators on a Banach space. More precisely, if \mathcal{X} is a Banach space and $\mathcal{S} = \overline{\mathbb{R}^+ \mathcal{S}}$ is a semigroup of compact operators on \mathcal{X} satisfying a property \mathcal{P} , which is pretriangularizing for matrix semigroups, then \mathcal{S} has a chain of closed invariant subspaces of length at least r ; where r is the minimal nonzero rank (possibly infinite) in \mathcal{S} .

Theorem 3.0.14. *Let g be a homogeneous polynomial in two noncommuting variables of joint degree r such that either $g(t, 0) \neq 0$ or $g(0, t) \neq 0$. If $0 \leq k < \chi(g)$, then the property*

$$\rho(g(xy, yx)) \leq k\rho(x)^r \rho(y)^r, \text{ for all } x, y \in \mathcal{S}$$

for matrix semigroups \mathcal{S} is a pretriangularizing property.

Proof. Conditions (1),(2), and (3) are clearly satisfied. Condition (5) is the content of Theorem 3.0.13. Note that it is sufficient to check condition (4) for irreducible semigroups \mathcal{S} . Assume, if possible that \mathcal{S} is an irreducible semigroup satisfying $\rho(g(xy, yx)) \leq k\rho(x)^r \rho(y)^r$, for all $x, y \in \mathcal{S}$ and that \mathcal{S} contains a nonzero nilpotent N . Without loss of generality assume that $\mathcal{S} = \mathbb{R}^+ \mathcal{S}$, $g(t, 0) \neq 0$, and that $N^2 = 0$. Note that for every $X \in \mathcal{S}$, the matrix $g(X, N)$ is nilpotent. Write

$$N = \begin{pmatrix} 0 & M \\ 0 & 0 \end{pmatrix}, X = \begin{pmatrix} X_{1,1} & X_{1,2} \\ X_{2,1} & X_{2,2} \end{pmatrix}$$

and note that the matrices $g(MX_{2,1}, 0)$ and $g(0, X_{2,1}M)$ are nilpotent. Hence $g^n(MX_{2,1}, 0) = 0 = g^n(0, X_{2,1}M)$. Thus the union of spectra of all $MX_{2,1}$ is a finite set; and hence these spectra are $\{0\}$ due to homogeneity of \mathcal{S} . Therefore $f: \mathcal{M}_n \rightarrow \mathbb{C}$, $f(X) = \text{tr}MX_{2,1}$ defines a nonzero functional which is 0 on \mathcal{S} . This contradicts the irreducibility of \mathcal{S} . \square

Remark 3.0.15. *The case $g(t, s) = t - s$ was already investigated in [3].*

From the theorem above we obtain the following corollary.

Theorem 3.0.16. *Let g be a homogeneous polynomial in two noncommuting variables of joint degree r , such that either $g(t, 0) \neq 0$ or $g(0, t) \neq 0$. Let \mathcal{S} be any semigroup of compact operators on a Banach space such that*

$$(1) \quad \rho(g(AB, BA)) \leq k\rho(A)^r \rho(B)^r,$$

for all $A, B \in \mathcal{S}$ and some fixed k , with $0 \leq k < \chi(g)$. Then either \mathcal{S} is reducible or it contains operators of rank 1.

Proof. This follows from the fact that (1) is a pretriangularizing property for matrix semigroups combined with the discussion following Theorem 3.0.13. \square

If g is rigid in the sense of [6], then taking $\beta = 0$ we obtain the triangularizing condition of Theorem 4.2 of [6].

ACKNOWLEDGEMENT

We would like to thank the referee for directing us to the original paper [4].

REFERENCES

- [1] J. Bernik, R. Drnovšek, T. Košir, L. Livshits, M. Mastnak, M. Omladič, and H. Radjavi, *Approximate permutability of traces on semigroups of matrixes*, Operators and Matrices, Vol. 1, No. 4 (2007), 455–467.
- [2] J. Bernik, R. Guralnick, M. Mastnak, *Reduction theorems for groups of matrices*, Linear Algebra Appl. 383 (2004), 119–126.
- [3] J. Bernik, H. Radjavi, *How small can nonzero commutators be?*, Indiana Univ. Math. J. 54 (2005), 309–320.
- [4] G. A. Miller, H. C. Moreno, *Non-Abelian groups in which every subgroup is abelian*, Trans. AMS, Vol. 4, No. 4 (1903), pp. 398–404
- [5] J. P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977.
- [6] H. Radjavi, *Polynomial conditions on operator semigroups*, J. Operator Theory 53:1 (2005), 197–220.
- [7] H. Radjavi, P. Rosenthal, *Simultaneous triangularization*, Springer, New York, 2000.
- [8] O. J. Schmidt. *Ueber Gruppen deren sämtliche Teiler spezielle Gruppen sind*, Math. Sbornik 31 (1924) 366–372.