FACULTY OF MATHEMATICS AND PHYSICS
UNIVERSITY OF LJUBLJANA

Gregor Cigler

GROUPS OF MATRICES WITH PRESCRIBED SPECTRUM

Doctoral dissertation

Ljubljana, 2005

FAKULTETA ZA MATEMATIKO IN FIZIKO
UNIVERZA V LJUBLJANI

Gregor Cigler

GRUPE MATRIK S PREDPISANIM SPEKTROM

Doktorska disertacija

Ljubljana, 2005

Contents

Zahvala

Zahvaljujem se profesorjema Matjažu Omladiču in Romanu Drnovšku za njuno pomoč in sugestije pri nastajanju tega dela. Rad bi se zahvalil tudi profesorju Heydarju Radjaviju za skrben pregled in jezikovne nasvete ter profesorju Thomasu J. Laffeyu za zelo koristne predloge.

Gregor Cigler

Abstract

The general form of the problem that we discuss in this work is the following. Let $\mathcal{G}$ be a (semi)group of $n \times n$ matrices over the field $\mathbb{F}$ such that each matrix from $\mathcal{G}$ is (individually) similar to a matrix with a given property $\mathcal{P}$. Is then the (semi)group $\mathcal{G}$ simultaneously similar to a (semi)group of matrices all having the property $\mathcal{P}$, i.e., can we find an invertible matrix $S \in \mathbb{F}^{n\times n}$ such that for all $X \in \mathcal{G}$ the matrix SXS^{-1} has the property $\mathcal{P}$? When the answer is negative in general, we search for additional assumptions under which the (semi)group $\mathcal{G}$ is simultaneously similar to a desired (semi)group.

In Chapters 2 and 3 we consider triangularizability of matrix (semi)groups. In this case a matrix has the property $\mathcal{P}$, if it is upper triangular and its spectrum satisfy some additional conditions.

If $\mathcal{G}$ is a matrix semigroup which is triangularized, diagonal entries on a fixed position form a subsemigroup of the multiplicative group $\mathbb{F} \setminus \{0\}$. In Chapter 2 we study the triangularizability under the assumption that the union of the spectra of all matrices from $\mathcal{G}$ forms a group Γ. When $\Gamma = \{1\}$ is the trivial group, the well-known Kolchin's theorem gives the affirmative answer to our problem: Every semigroup of unipotent matrices is triangularizable.
We investigate the case where Γ is a finite group and we show that Kolchin's theorem extends only to the case where $\Gamma = \{1, -1\}$. We give counterexamples for groups Γ not contained in the group $\{1, -1\}$.

In the search for further extensions of Kolchin's theorem in Chapter 3 we introduce p-property, which is some kind of independency condition of the eigenvalues. We investigate more closely groups of monomial matrices with this property. The main theorem of this chapter is a generalization of Kolchin's theorem to the groups with 2-property.

Chapter 4 is dedicated to the permutation-like groups, i.e., the finite groups $\mathcal{G} \subset \mathbb{C}^{n\times n}$ such that any matrix $X \in \mathcal{G}$ is similar to a permutation matrix. In this case a matrix has the property $\mathcal{P}$, if it is a permutation matrix. Since a matrix similar to a permutation matrix is determined by its spectrum, we could describe this

property in terms of the spectrum, but the previous description is more transparent. We deal with the question when a permutation-like group is simultaneously similar to a group of permutation matrices. Various examples in this chapter show that in general a permutation-like group does not have to be simultaneously similar to a group of permutation matrices. In fact, there are counterexamples for every $n \geq 6$. The low-dimensional cases $n = 2, 3, 4, 5$ are investigated in detail.

Math. Subj. Class.: 15A18, 20G05, 20C30

Keywords: Matrix group, spectrum, similarity, triangularization, permutation matrix

Povzetek

Splošni problem, ki ga obravnava to delo, lahko opišemo takole: Naj bo $\mathbb{F}$ polje in $\mathcal{M} \subset \mathbb{F}^{n\times n}$ množica kvadratnih matrik, med katerimi je vsaka podobna matriki z izbrano lastnostjo $\mathcal{P}$. Vprašanje je tedaj sledeče: Ali je $\mathcal{M}$ simultano podobna kaki množici matrik, ki imajo lastnost $\mathcal{P}$, tj. ali obstaja taka obrnljiva matrika $S \in \mathbb{F}^{n\times n}$, da ima za vsako matriko $X \in \mathcal{M}$ matrika SXS^{-1} lastnost $\mathcal{P}$?

Ponavadi privzamemo, da množica $\mathcal{M}$ ima kako algebrsko strukturo za matrično množenje (in seštevanje), npr. strukturo (pol)grupe ali algebre. V primerih, ko je odgovor na opisano vprašanje v splošnem negativen, iščemo dodatne zadostne pogoje, pri katerih je množica $\mathcal{M}$ simultano podobna kaki množici matrik s predpisano lastnostjo $\mathcal{P}$.

V okviru tega splošnega problema je posebej zanimiv primer, ko predpišemo zgornjetrikotno obliko matrik. Če je $\mathbb{F}$ algebraično zaprto polje, je vsaka matrika podobna neki zgornjetrikotni matriki, zato splošni problem *trikotljivosti* (oz. *triangularizabilnosti*) množice matrik ustreza iskanju dodatnih pogojev, ki jim mora množica zadoščati, da je simultano podobna kaki množici zgornjetrikotnih matrik.

Lastnost trikotljivosti lahko izrazimo z obstojem verige invariantnih podprostorov, ki je maksimalna kot veriga linearnih prostorov nad poljem $\mathbb{F}$.

Definicija 0.1 Množica matrik $\mathcal{M} \subset \mathbb{F}^{n\times n}$ je *trikotljiva*, če obstaja taka veriga za $\mathcal{M}$ invariantnih podprostorov

$$\{0\} = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_n = \mathbb{F}^n, \qquad \text{(chn)}$$

da je $\dim V_i = i$, tj. veriga (chn) je maksimalna veriga linearnih podprostorov.

Množici matrik $\mathcal{M} \subset \mathbb{F}^{n\times n}$, ki nima nobenega invariantnega prostora, pravimo *nerazcepna* (oz. *ireducibilna*) množica. $\diamond$

Če ima množica $\mathcal{M}$ kako algebrsko strukturo za matrično množenje (in seštevanje), dobimo znane zanimive rezultate, ki so povzeti v prvem poglavju.

Izrek 0.2 (Burnside) *Če je $\mathbb{F}$ algebraično zaprto polje, je $\mathbb{F}^{n\times n}$ edina nerazcepna podalgebra algebre $\mathbb{F}^{n\times n}$.*

Iz Bursideovega izreka takoj sledi, da je polgrupa matrik nerazcepna natanko tedaj, ko razpenja celotni prostor matrik $\mathbb{F}^{n\times n}$.

V drugem delu prvega poglavja obravnavamo permutabilne funkcije na množicah matrik.

Definicija 0.3 Za funkcijo $\Phi : \mathbb{F}^{n\times n} \to \mathcal{E}$ pravimo, da je *permutabilna* na množici matrik $\mathcal{M} \subset \mathbb{F}^{n\times n}$, če za poljuben nabor matrik $X_1, X_2, \ldots, X_n \in \mathcal{M}$ in poljubno permutacijo $\pi \in S_n$ velja

$$\Phi(X_1X_2\cdots X_n) = \Phi(X_{\pi(1)}X_{\pi(2)}\cdots X_{\pi(n)}).$$

$\diamond$

Izkaže se, da je pojem permutabilnosti tesno povezan z razcepnostjo množic matrik. Lep primer tega je zadnji izrek prvega poglavja.

Izrek 0.4 (Radjavi) *Če je $\mathbb{F}$ algebraično zaprto polje s karakteristiko 0, je množica matrik $\mathcal{M} \subset \mathbb{F}^{n\times n}$ trikotljiva natanko tedaj, ko je sled permutabilna na $\mathcal{M}$.*

Direktna posledica zadnjega izreka je znani Kolčinov izrek.

Izrek 0.5 (Kolčin) *Vsaka polgrupa $\mathcal{S} \subset \mathbb{F}^{n\times n}$ unipotentnih matrik je trikotljiva.*

Iz zgornjetrikotne oblike matrik takoj razberemo njihove lastne vrednosti. Če je $\mathcal{G}$ (pol)grupa zgornjetrikotnih matrik, diagonalni elementi na izbranem mestu diagonale tvorijo pod(pol)grupo multiplikativne grupe $\mathbb{F} \setminus \{0\}$. Ali lahko ta sklep na nek način obrnemo? Eno od možnih vprašanj se glasi: Denimo, da unija spektrov vseh matrik iz $\mathcal{G}$ tvori neko grupo Γ. Ali je tedaj (pol)grupa $\mathcal{G}$ trikotljiva?

V primeru trivialne grupe $\Gamma = \{1\}$ nam Kolčinov izrek da pritrdilen odgovor.

Drug zanimiv primer najdemo v [25]: *Če je $\mathcal{G} \subset \mathbb{C}^{n\times n}$ deljiva grupa matrik in $\Gamma = (0, \infty)$, je grupa $\mathcal{G}$ trikotljiva.*

V drugem poglavju obravnavamo primer, ko je Γ končna grupa. Dokažemo, da lahko pri takem privzetku Kolčinov izrek razširimo le na primer, ko je $\Gamma = \{1, -1\}$.

Izrek 0.6 *Naj bo $\mathbb{F}$ polje s karakteristiko 0. Vsaka polgrupa $\mathcal{S} \subset \mathbb{F}^{n\times n}$ matrik s spektrom vsebovanim v množici $\{1, -1\}$ je trikotljiva.*

Za končne grupe Γ, ki niso vsebovane v $\{1, -1\}$, konstruiramo primere netrikotljivih polgrup matrik s spektri v Γ.

V dokazu izreka 0.6 si pomagamo z algebraičnimi podgrupami grupe $\mathbb{F}^{n\times n}$, tj. grupami matrik, ki jih lahko predstavimo kot množice skupnih ničel nekega nabora polinomov s koeficienti iz $\mathbb{F}$. Algebraične grupe so topološke grupe v topologiji Zariskega. Množica je v tej topologiji zaprta, če sovpada z množico skupnih ničel kakega nabora polinomov s koeficienti iz $\mathbb{F}$. Jasno je, da zaprtje množice zgornjetrikotnih matrik še vedno sestavljajo le zgornjetrikotne matrike. S pomočjo te opazke se lahko omejimo na algebraične grupe.

Topologija Zariskega ima separacijsko lastnost T_1, kar pomeni, da so končne množice zaprte. Ker so spektri matrik iz polgrupe $\mathcal{S}$ vsebovani v končni množici, se ni težko prepričati, da so tudi spektri matrik iz algebraičnega zaprtja polgrupe vsebovani v predpisani končni množici. Po eni od trditev teorije algebraičnih množic je zaprtje polgrupe matrik algebraična grupa, s čimer naš prvotni problem v celoti prevedemo na ekvivalentni problem v okviru algebraičnih grup.

Definicija 0.7 Zaprta podmnožica S algebraične grupe G je *ireducibilna*, če je ni možno zapisati kot netrivialno unijo zaprtih množic; tj. za vsaki zaprti množici $A, B \subset S$, ki zadoščata pogoju

$$S = A \cup B$$

velja bodisi $A = S$, bodisi $B = S$. $\diamond$

Vsako algebraično grupo lahko razbijemo na disjunktno unijo ireducibilnih množic

$$G = G_1 \cup G_2 \cup \cdots \cup G_k,$$

pri čemer je G_1 največja ireducibilna množica, ki vsebuje enoto grupe G. Izkaže se, da je G_1 algebraična podgrupa edinka, ireducibilne množice $G_1, G_2, \ldots, G_k$ pa ravno odseki kvocientne grupe G/G_1.

V algebraični grupi G obstaja taka algebraična unipotentna podgrupa edinka G_u, ki vsebuje vse unipotentne podgrupe edinke grupe G.

Če je $\mathbb{F}$ polje s karakteristiko 0, veljata naslednja izreka.

Izrek 0.8 *Za algebraično grupo G obstaja taka algebraična podgrupa P, da je G poldirektni produkt*

$$G = G_u \rtimes P,$$

tj. vsako matriko $X \in G$ lahko na en sam način zapišemo kot produkt $X = UT$, kjer je $U \in G_u$ in $T \in P$. Sledi $P \approx G/G_u$.

Izrek 0.9 *Vsaka unipotentna podgrupa T algebraične grupe G je ireducibilna.*

Od tod sledi, da je G_u ireducibilna grupa. V dokazu izreka 0.6 najprej dokažemo, da pri danih pogojih velja $G_u = G_1$ in na ta način dokaz prevedemo na primer končne grupe.

V tretjem poglavju iščemo nadaljne posplošitve Kolčinovega izreka in vpeljemo p-lastnost. Privzamemo, da je $\mathbb{F}$ algebraično zaprto polje s karakteristiko 0. Tedaj lahko v polje $\mathbb{F}$ vložimo polje racionalnih števil $\mathbb{Q}$.

Definicija 0.10 Naj bo p neko naravno število in $A \in \mathbb{F}^{n\times n}$ kvadratna matrika s spektrom $\lambda_1, \ldots, \lambda_r, \mu_1, \ldots, \mu_s$ (v tem naboru vsako večkratno lastno vrednost ponovimo z njeno večkratnostjo). Če sta za $i \neq j$ (multiplikativna) reda elementov λ_i in λ_j končni števili, katerih skupna mera deli število p, elementi $\mu_1, \ldots, \mu_s$ pa so algebraično neodvisni nad $\mathbb{Q}$, pravimo, da ima matrika A *p-lastnost*. Množica $\mathcal{M}$ matrik ima p-lastnost, če ima p-lastnost vsaka njena matrika. $\diamond$

Razložimo najprej, od kod definicija p-lastnosti. Naj bo A matrika s spektrom $\lambda_1, \ldots, \lambda_r, \mu_1, \ldots, \mu_s$, kjer sta za $i \neq j$ reda λ_i in λ_j tuji končni števili, elementi $\mu_1, \ldots, \mu_s$ pa so algebraično neodvisni nad $\mathbb{Q}$. Potem velja $\det(A) = 1$ natanko tedaj, ko je A unipotentna matrika, tj. $\sigma(A) = \{1\}$. Privzetek za matriko A je seveda ekvivalenten 1-lastnosti, zato je za matrično grupo $\mathcal{G}$ z 1-lastnostjo preslikava

$$\det : \mathcal{G} \to \mathbb{F} \setminus \{0\}$$

homomorfizem grup z jedrom $\mathcal{K}$, ki ga tvorijo unipotentne matrike. Podgrupa edinka $\mathcal{K}$ je po Kolčinovem izreku trikotljiva. V dokazu glavnega izreka 3.19 tretjega poglavja lahko vidimo, da trikotljivost grupe $\mathcal{K}$ porodi trikotljivost grupe $\mathcal{G}$ (uporabimo komutativnost nerazcepnih komponent grupe $\mathcal{K}$). Vpeljavo p-lastnosti tako motivira

primer $p = 2$. Jedro homomorfizma $(\det)^2 : \mathcal{G} \to \mathbb{F} \setminus \{0\}$ je podgrupa iz matrik s spektrom, vsebovanim v množici $\{1, -1\}$, ki je trikotljiva po izreku 2.8. Pri splošnem p grupa $\mathcal{G}$ ni nujno trikotljiva, v kar nas prepričajo primeri 2.4 na koncu drugega poglavja.

Glavni izrek tretjega poglavja se glasi:

Izrek 0.11 *Naj bo $\mathcal{G} \subset \mathbb{F}^{n\times n}$ grupa matrik nad algebraično zaprtim poljem $\mathbb{F}$ s karakteristiko 0. Če ima grupa $\mathcal{G}$ 2-lastnost, je trikotljiva.*

Del tretjega poglavja je posvečen monomialnim grupam s p-lastnostjo, pri čemer je p praštevilo. Med drugim izpeljemo naslednjo zanimivo trditev:

Trditev 0.12 *Vsaka nerazcepna grupa $\mathcal{G} \subset \mathrm{GL}_9(\mathbb{F})$ eksponenta 3 je konjugirana tenzorskemu produktu $\mathcal{H} \otimes \mathcal{K}$, kjer sta $\mathcal{H}, \mathcal{K}$ podgrupi grupe*

$$\mathcal{P}_3 = \left\{ DC^k \mid k = 0, 1, 2,\ D = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix},\ abc = 1\,,\ a^3 = b^3 = c^3 = 1 \right\}$$

za

$$C = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

V zadnjem poglavju obravnavamo *lokalno permutacijske* grupe matrik $\mathcal{G} \subset \mathbb{C}^{n\times n}$.

Definicija 0.13 Končno grupo matrik $\mathcal{G} \subset \mathbb{C}^{n\times n}$ imenujemo *lokalno permutacijska* grupa, če je vsaka matrika $X \in \mathcal{G}$ podobna neki permutacijski matriki. ⋄

Sprašujemo se, kdaj je lokalno permutacijska grupa simultano podobna kaki grupi permutacijskih matrik. Razni primeri nas prepričajo o tem, da to v splošnem ni res.

Primer 0.14 *Obstaja lokalno permutacijska grupa $\mathcal{G} \subset \mathbb{C}^{4\times 4}$, ki vsebuje cikel dolžine 3 in ni simultano podobna nobeni grupi permutacijskih matrik.*

Dokaz. Naj bo $\omega \in \mathbb{C}$ primitivni tretji koren enote. Označimo

$$B = \begin{bmatrix} \omega & & \\ & \omega^{-1} & \end{bmatrix} \quad \text{in} \quad T_0 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

ter definirajmo bločno zapisani matriki

$$C = \begin{bmatrix} I & \\ & B \end{bmatrix} \quad \text{in} \quad T = \begin{bmatrix} T_0 & \\ & T_0 \end{bmatrix},$$

kjer je I identična matrika velikosti 2×2. Matrika C tedaj ustreza ciklu dolžine 3, matrika T pa produktu dveh tujih transpozicij. Ker velja $TC = C^{-1}T$, je vsak element grupe $\mathcal{G}$, generirane z matrikama T in C, bodisi oblike TC^k bodisi oblike C^k. Ni se težko prepričati, da matrika oblike TC^k ustreza produktu dveh tujih transpozicij, matrika oblike C^k pa neki potenci cikla dolžine 3. Grupa $\mathcal{G}$ je tako res lokalno permutacijska grupa.

Denimo, da je grupa $\mathcal{G}$ simultano podobna kaki grupi permutacijskih matrik, kjer matrika T ustreza permutaciji σ in matrika TC permutaciji σ'. Vsaka izmed permutacij σ in σ' ustreza produktu dveh tujih transpozicij. Produkt $T \cdot (TC) = C$, ki ustreza produktu $\sigma\sigma'$, ustreza po drugi strani nekemu ciklu γ dolžine 3, in ima zato kot permutacija natanko eno negibno točko. Naj bo a negibna točka cikla γ. Ker sta permutaciji σ in σ' brez negibnih točk, permutacija σ' vsebuje neko transpozicijo oblike (ab). Ker je a negibna točka produkta $\sigma\sigma'$, sledi $\sigma(b) = a$. Tedaj tudi permutacija σ vsebuje transpozicijo (ba), od koder sledi, da je b dodatna negibna točka permutacije $\sigma\sigma'$. Prišli smo do protislovja, zato grupa $\mathcal{G}$ res ni simultano podobna nobeni grupi permutacijskih matrik. □

Primer 0.14 lahko razširimo v vse sode dimenzije $n \geq 4$ (glej primer 4.3), poleg tega pa obstajajo protiprimeri za poljubne dimenzije $n \geq 6$. Vsem protiprimerom je skupno, da lokalno permutacijska grupa G ne vsebuje *maksimalnega cikla*, tj. matrike C, podobne matriki oblike

$$\begin{bmatrix} 0 & \cdots & \cdots & 0 & 1 \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{bmatrix}.$$

Konstruirani protiprimeri nas navedejo na naslednjo domnevo:

Domneva: Vsaka lokalno permutacijska grupa, ki vsebuje maksimalni cikel, je simultano podobna grupi permutacijskih matrik.

Naslednje trditve, ki jih dokažemo v četrtem poglavju, potrjujejo domnevo za $n \leq 5$ in v primeru komutativne grupe.

Trditev 0.15 *Vsaka komutativna lokalno permutacijska grupa $\mathcal{G}$, ki vsebuje maksimalni cikel C, je oblike*

$$\mathcal{G} =< C > .$$

Izrek 0.16 *Vsaka lokalno permutacijska grupa $\mathcal{G} \subset \mathbb{C}^{n\times n}$ za $n = 2, 3, 5$ je simultano podobna neki grupi permutacijskih matrik.*

Izrek 0.17 *Vsaka lokalno permutacijska grupa $\mathcal{G} \subset \mathbb{C}^{4\times 4}$, ki vsebuje maksimalni cikel, je simultano podobna neki grupi permutacijskih matrik.*

1 SOME TRIANGULARIZABILITY RESULTS

1.1 About the algebra $\mathbb{F}^{n\times n}$

In this section we recall some well-known results related to triangularizability. For the sake of completeness we include their proofs. We mainly follow the monograph [20] of H. Radjavi and P. Rosenthal.

Definition 1.1 Let $\mathbb{F}$ be a field and $\mathcal{M} \subset \mathbb{F}^{n\times n}$ a set of matrices. The set $\mathcal{M}$ is *irreducible* if the only $\mathcal{M}$-invariant subspaces are $\{0\}$ and $\mathbb{F}^n$. We say that $\mathcal{M}$ is *triangularizable* if there exists a chain of $\mathcal{M}$-invariant subspaces

$$\{0\} = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_n = \mathbb{F}^n \tag{chn}$$

such that $\dim V_i = i$, i.e., the chain (chn) is a maximal chain of linear spaces. $\diamond$

Lemma 1.2 *Let $\mathcal{A} \subset \mathbb{F}^{n\times n}$ be an irreducible algebra. If $\mathcal{A}$ contains a matrix T_0 with rank 1, then*

$$\mathcal{A} = \mathbb{F}^{n\times n}.$$

Proof. Let $(\mathbb{F}^n)^*$ be the space of all functionals on $\mathbb{F}^n$ and pick a vector $y_0 \neq 0$ in the range of T_0. Then we can find a linear functional $\Phi_0 \in (\mathbb{F}^n)^*$ such that $T_0x = \Phi_0(x)y_0$ for all $x \in \mathbb{F}^n$. Since every linear operator is a sum of operators of rank 1, it suffices to show that $\mathcal{A}$ contains every T of the form

$$Tx = \Phi(x)y \tag{rg1},$$

where $\Phi \in (\mathbb{F}^n)^*$ and $y \in \mathbb{F}^n$.

For each $A \in \mathcal{A}$ we have $T_0A \in \mathcal{A}$. But $T_0Ax = \Phi_0(Ax)y_0$, so Φ from (rg1) ranges over all $\Phi_0 \circ A$, with $A \in \mathcal{A}$. If we denote $\mathcal{F} = \{\Phi_0 \circ A \,|\, A \in \mathcal{A}\}$, then $\mathcal{F}$ is a subspace of $(\mathbb{F}^n)^*$. If $\mathcal{F}$ is a proper subspace, then there is $x_0 \neq 0$ such that $\Phi(x_0) = 0$ for all $\Phi \in \mathcal{F}$, i.e., $\Phi_0(\mathcal{A}x_0) = \Phi_0(\mathbb{F}^n) = 0$. This is a contradiction, since $\Phi_0 \neq 0$. Therefore $\mathcal{A}$ contains all T of the form $Tx = \Phi(x)y_0$.

As $\mathcal{A}$ is irreducible, for arbitrary $y \in \mathbb{F}^n$ there is $A \in \mathcal{A}$ such that $Ay_0 = y$. Then for $Tx = \Phi(x)y_0$ we get $AT(x) = \Phi(x)y$, which completes the proof. $\square$

The following result is the well-known Burnside theorem.

Theorem 1.3 *If $\mathbb{F}$ is an algebraically closed field, then $\mathbb{F}^{n\times n}$ is the only irreducible subalgebra of $\mathbb{F}^{n\times n}$.*

PROOF. Let $\mathcal{A} \subset \mathbb{F}^{n\times n}$ be an irreducible algebra of matrices and $T_0 \in \mathcal{A}$ a transformation with minimal nonzero rank in $\mathcal{A}$. We show that T_0 has rank 1.

Assume otherwise. Then we find vectors $x_1, x_2 \in \mathbb{F}^n$ such that T_0x_1, T_0x_2 are linearly independent vectors. Since $\mathcal{A}$ is irreducible we get $\{AT_0x_1 \,|\, A \in A\} = \mathbb{F}^n$ and we can find $A_0 \in \mathcal{A}$ such that $A_0T_0x_1 = x_2$. Then $T_0A_0T_0x_1$ and T_0x_1 are linearly independent. We can find a scalar $\lambda \in \mathbb{F}$ such that the restriction of $(T_0A_0 - \lambda I)$ to $T_0\mathbb{F}^n$ is not invertible. As $T_0A_0T_0x_1 - \lambda T_0x_1 \neq 0$ the operator $(T_0A_0 - \lambda I)T_0$ is nonzero. Since the rank of the operator $(T_0A_0 - \lambda I)T_0$ is strictly smaller then the rank of T_0, this is a contradiction. We conclude that T_0 has rank 1. We use Lemma 1.2 to complete the proof. □

Theorem 1.4 *The only two-sided ideals of the algebra $\mathbb{F}^{n\times n}$ are $\{0\}$ and $\mathbb{F}^{n\times n}$.*

PROOF. For a nonzero $A \in \mathcal{I}$ we can find $B \in \mathbb{F}^{n\times n}$ such that $T_0 = AB \in \mathcal{I}$ has rank 1. By Lemma 1.2 we get $\mathcal{I} = \mathbb{F}^{n\times n}$. □

We will need the next result in establishing a 'block triangularization theorem'.

Theorem 1.5 *For an algebraically closed field $\mathbb{F}$ all the automorphisms of the algebra $\mathbb{F}^{n\times n}$ are inner, i.e., for an automorphism $\Phi : \mathbb{F}^{n\times n} \to \mathbb{F}^{n\times n}$ there exists an invertible matrix $S \in \mathbb{F}^{n\times n}$ such that*

$$\Phi(X) = SXS^{-1}$$

for all $X \in \mathbb{F}^{n\times n}$.

PROOF. Let $\Phi : \mathbb{F}^{n\times n} \to \mathbb{F}^{n\times n}$ be an automorphism. First we note that Φ takes idempotents into idempotents. Let A_0 be an idempotent of rank 1. Then $\{A_0BA_0 \,|\, B \in \mathbb{F}^{n\times n}\}$ is one-dimensional subspace. Its image $\{\Phi(A_0)C\Phi(A_0) \,|\, C \in \mathbb{F}^{n\times n}\}$ is therefore also one-dimensional subspace. Thus $\Phi(A_0)$ is rank-one idempotent whenever A_0 is.

Fix any rank-one idempotent A_0. Clearly any two rank-one idempotents are similar, so $\Phi(A_0)$ is similar to A_0. If we compose this similarity with Φ we can assume that $\Phi(A_0) = A_0$. Let x_0 be a nonzero vector in the range of A_0, i.e., $A_0x_0 = x_0$.

Now we define a transformation that implements Φ. For each $B \in \mathbb{F}^{n\times n}$ we define $S(Bx_0) = \Phi(B)x_0$. We first check that S is a well-defined mapping. If $B_1x_0 = B_2x_0$, then $(B_1 - B_2)A_0x_0 = 0$ and therefore $(B_1 - B_2)A_0 = 0$, since A_0 has rank 1. It follows that

$$(\Phi(B_1) - \Phi(B_2))\Phi(A_0) = (\Phi(B_1) - \Phi(B_2))A_0 = 0,$$

and

$$(\Phi(B_1) - \Phi(B_2))x_0 = 0.$$

Thus S is well-defined.

It is clear that S is linear. If $S(Bx_0) = 0$, then $\Phi(B)x_0 = 0$. This implies $\Phi(B)\Phi(A_0) = \Phi(BA_0) = 0$, so $BA_0 = 0$ and thus $Bx_0 = 0$. This shows that S is injective. Since S is an endomorphism of finite-dimensional space, it is also surjective, and hence invertible.

Now fix $A \in \mathbb{F}^{n\times n}$. Then for each $B \in \mathbb{F}^{n\times n}$ we get

$$S(AB)x_0 = \Phi(AB)x_0 = \Phi(A)\Phi(B)x_0$$

and

$$SBx_0 = \Phi(B)x_0,$$

so

$$SABx_0 = \Phi(A)SBx_0.$$

Each $x \in \mathbb{F}^n$ is of the form $x = Bx_0$ for a suitable $B \in \mathbb{F}^{n\times n}$, therefore we get $SAx = \Phi(A)Sx$, i.e.,

$$\Phi(A) = SAS^{-1}.$$

□

Theorem 1.6 *Let $\mathbb{F}$ be an algebraically closed field. For any subalgebra $\mathcal{A}$ of $\mathbb{F}^{n\times n}$, there is a decomposition*

$$\mathbb{F}^n = \mathcal{N}_1 \oplus \mathcal{N}_2 \oplus \cdots \oplus \mathcal{N}_k,$$

with respect to which every matrix $A \in \mathcal{A}$ has the block upper diagonal form

$$A = \begin{bmatrix} A_{11} & A_{12} & \cdots & & A_{1k} \\ 0 & A_{22} & \cdots & & A_{2k} \\ 0 & 0 & A_{33} & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & & 0 & A_{kk} \end{bmatrix}$$

where the set $\{1, 2, \ldots, k\}$ is a disjoint union of subsets $J_1, J_2, \ldots, J_l$ such that
(1) $\{A_{ii} \mid A \in \mathcal{A}\} = \mathrm{End}_{\mathbb{F}}(\mathcal{N}_i)$ for $i = 1, 2, \ldots, k$;
(2) if $i, j \in J_s$ then

$$A_{ii} = A_{jj}$$

for all $A \in \mathcal{A}$;
(3) if $J_s \neq J_t$ and $i \in J_s, j \in J_t$ then

$$\{(A_{ii}, A_{jj}) \mid A \in \mathcal{A}\} = \mathrm{End}_{\mathbb{F}}(\mathcal{N}_i) \times \mathrm{End}_{\mathbb{F}}(\mathcal{N}_j);$$

(4) for $i \in J_s$ there is an $A \in \mathcal{A}$ such that $A_{ii} = I$ and $A_{jj} = 0$ for all $j \notin J_s$.

Proof. If $\mathcal{A}$ is irreducible, then Burnside's theorem (Theorem 1.3) gives us the desired result, with $k = 1$ and $\mathcal{N}_1 = \mathbb{F}^n$.

Assume that $\mathcal{A}$ is reducible and let

$$\mathcal{M}_0 = \{0\} \subset \mathcal{M}_1 \subset \cdots \subset \mathcal{M}_{m-1} \subset \mathcal{M}_m = \mathbb{F}^n$$

be a maximal chain of distinct $\mathcal{A}$-invariant subspaces. For each $i = 1, \ldots, m$, choose a complementary space $\mathcal{N}_i$ of $\mathcal{M}_{i-1}$ in $\mathcal{M}_i$, so that $\mathcal{M}_i = \mathcal{M}_{i-1} \oplus \mathcal{N}_i$. Then the space $\mathbb{F}^n$ is a direct sum, namely $\mathbb{F}^n = \mathcal{N}_1 \oplus \cdots \oplus \mathcal{N}_m$. Since $\mathcal{M}_i$'s are invariant spaces, all the transformations in $\mathcal{A}$ are clearly block upper triangular with respect to this decomposition. For each i, let $P_i : \mathbb{F}^n \to \mathcal{N}_i$ denote the projection onto $\mathcal{N}_i$ along the sum $\sum_{j \neq i} \mathcal{N}_j$. Then we have $P_1 + P_2 + \cdots + P_m = I$.

For each i, let $\mathcal{A}_i = \{P_i A|_{\mathcal{N}_i} \mid A \in \mathcal{A}\}$ be the 'compression' of the algebra $\mathcal{A}$ on $\mathcal{N}_i$. Then $\mathcal{A}_i$ is an irreducible algebra, since there is no $\mathcal{A}$-invariant subspace 'strictly' between $\mathcal{M}_{i-1}$ and $\mathcal{M}_i$.

By Burnside's Theorem, we get $\mathcal{A}_i = \mathrm{End}_{\mathbb{F}}(\mathcal{N}_i)$ for each i.

We now show that the algebras $\mathcal{A}_i$ are either pairwise independent or linked in the following sense. Fix distinct i and j. If there is an $A \in \mathcal{A}$ such that $P_i A|_{\mathcal{N}_i} = I$ and $P_j A|_{\mathcal{N}_j} = 0$, then we say that $\mathcal{A}_i$ and $\mathcal{A}_j$ are independent. This relation is symmetric, for $P_i(I - A)|_{\mathcal{N}_i} = 0$ and $P_j(I - A)|_{\mathcal{N}_j} = I$.

If $\mathcal{A}_i$ and $\mathcal{A}_j$ are not independent, we say that they are linked. We justify this terminology by the following. Suppose that for some $A \in \mathcal{A}$ we have $P_i A|_{\mathcal{N}_i} \neq 0$ and $P_j A|_{\mathcal{N}_j} = 0$. Then the set $\{P_i A|_{\mathcal{N}_i} \mid A \in \mathcal{A},\, P_j A|_{\mathcal{N}_j} = 0\}$ is a nonzero two-sided ideal in $\mathcal{A}_i$. Since $\mathcal{A}_i = \mathrm{End}_{\mathbb{F}}(\mathcal{N}_i)$, it follows from Theorem 1.4 that the identity is in this ideal. Thus if $\mathcal{A}_i$ and $\mathcal{A}_j$ are linked, then for $A \in \mathcal{A}$ we have

$$P_i A|_{\mathcal{N}_i} = 0 \Leftrightarrow P_j A|_{\mathcal{N}_j} = 0 \qquad \text{(link)}.$$

Let $\mathcal{A}_i$ and $\mathcal{A}_j$ be linked. Then we can define a mapping $\Phi : \mathcal{A}_i \to \mathcal{A}_j$ by

$$\Phi(P_i A|_{\mathcal{N}_i}) = P_j A|_{\mathcal{N}_j}.$$

It is easy to verify that Φ is indeed a well-defined homomorphism of algebras. By the property (link) Φ is injective. By the definition of the algebra $\mathcal{A}_j$ the map Φ is surjective and therefore it is an isomorphism of algebras.

It follows that $\mathcal{N}_i$ and $\mathcal{N}_j$ have the same dimension. As $\mathcal{A}_i = \mathrm{End}_{\mathbb{F}}(\mathcal{N}_i)$ and $\mathcal{A}_j = \mathrm{End}_{\mathbb{F}}(\mathcal{N}_j)$, we can identify them which gives us an automorphism of the algebra $\mathrm{End}_{\mathbb{F}}(\mathcal{N}_i)$. By Theorem 1.5 we get an invertible linear transformation $S : \mathcal{N}_i \to \mathcal{N}_j$ that implements Φ, i.e.,

$$P_i A|_{\mathcal{N}_i} = S^{-1} P_j A|_{\mathcal{N}_j} S$$

for all $A \in \mathcal{A}$. This justifies the terminology 'linked'.

The proof of the theorem can now be completed by simply identifying linked $\mathcal{A}_i$ with each other. Fix i and define $J(i) = \{j \mid \mathcal{A}_i \text{ and } A_j \text{ are linked}\}$. For each $j \in J(i)$ we choose $S_j : \mathcal{N}_i \to \mathcal{N}_j$ so that

$$P_i A|_{\mathcal{N}_i} = S_j^{-1} P_j A|_{\mathcal{N}_j} S_j$$

for all $A \in \mathcal{A}$. Then we define $T(i) : \mathbb{F}^n \to \mathbb{F}^n$ with respect to the decomposition

$$\mathbb{F}^n = \mathcal{N}_1 \oplus \mathcal{N}_2 \oplus \cdots \oplus \mathcal{N}_m$$

by the block diagonal matrix having $T(i)_{kk} = I$ for $k \notin J$ and $T(i)_{jj} = S_j$ for $j \in J(i)$. Then every element of $T(i)^{-1}\mathcal{A}T(i)$ has the same entries in the positions (j, j) for all $j \in J(i)$.

We define $J_1 = J(1)$ and proceed inductively. Having defined $J_k = J(i_k)$ we take i_{k+1} to be the smallest element of the set $\{1, 2, \ldots, m\} \setminus (J_1 \cup \cdots \cup J_k)$ if this set is not empty (otherwise we are done). We define $J_{k+1} = J(i_{k+1})$. Once we have $\{1, 2, \ldots, m\} = J_1 \cup \cdots \cup J_l$, we finally define $R = T(i_1)T(i_2)\cdots T(i_l)$. Then the algebra $R^{-1}\mathcal{A}R$ has the required properties. □

1.2 Permutable trace and triangularization

Although we will use the following results for groups of matrices, we formulate them in more general context of semigroups.

Definition 1.7 A set $\mathcal{S} \subset \mathbb{F}^{n\times n}$ is called a *matrix semigroup* if it is closed under the matrix multiplication. ◇

The algebra generated by a matrix semigroup $\mathcal{S}$ is just the linear span of $\mathcal{S}$. If $\mathbb{F}$ is an algebraically closed field, then by Theorem 1.3 a semigroup is irreducible if and only if it contains a basis for the space $\mathbb{F}^{n\times n}$.

Definition 1.8 Let Φ be a function from $\mathbb{F}^{n\times n}$ into a set $\mathcal{E}$. We say Φ is *permutable* on a collection $\mathcal{M} \subset \mathbb{F}^{n\times n}$ if for arbitrary $X_1, X_2, \ldots, X_n$ and all permutations $\pi \in S_n$, we have

$$\Phi(X_1X_2\cdots X_n) = \Phi(X_{\pi(1)}X_{\pi(2)}\cdots X_{\pi(n)}).$$

◇

Lemma 1.9 *Let $\mathbb{F}$ be an algebraically closed field and let $\mathcal{M} \subset \mathbb{F}^{n\times n}$ be any collection where $n \geq 2$. If there is a nonzero linear functional f on $\mathbb{F}^{n\times n}$ which is permutable on $\mathcal{M}$, then $\mathcal{M}$ is reducible.*

Proof. Let $\mathcal{S}$ and $\mathcal{A}$ be the semigroup and the algebra generated by $\mathcal{M}$, respectively. Permutability of f on $\mathcal{S}$ follows directly from the hypothesis. However, one can easily verify that f is actually permutable on $\mathcal{A}$.

Suppose that $\mathcal{M}$ is irreducible. Then by Theorem 1.3 we get $\mathcal{A} = \mathbb{F}^{n\times n}$. Pick any pair $A, B \in \mathbb{F}^{n\times n}$ such that $C = AB - BA \neq 0$. Then permutability of f implies that $f(XCY) = 0$ for all $X, Y \in \mathbb{F}^{n\times n}$. It follows that f is zero on a nonzero two-sided ideal $\mathcal{I} = \{XCY \mid X, Y \in \mathbb{F}^{n\times n}\}$. By Theorem 1.4 we get $\mathcal{I} = \mathbb{F}^{n\times n}$ and $f = 0$. This contradiction shows that $\mathcal{M}$ is reducible. □

Corollary 1.10 *Let $\mathbb{F}$ be an algebraically closed field and let $\mathcal{S} \subset \mathbb{F}^{n\times n}$ be a matrix semigroup where $n \geq 2$. If there is a nonzero linear functional f on $\mathbb{F}^{n\times n}$ which is constant on $\mathcal{S}$, then $\mathcal{S}$ is reducible.*

Let $\mathcal{P}$ be a property of collections of square matrices over $\mathbb{F}$. Since we consider the simultaneous similarity of sets of matrices, we assume that the property $\mathcal{P}$ is preserved by the similarities of matrices. This means that the property $\mathcal{P}$ is in fact well defined on collections of linear endomorphisms, since we can choose an arbitrary basis and consider the given property on the corresponding set of matrices. Let $\mathcal{M} \subset \mathbb{F}^{n\times n}$ be a collection of matrices and $U \subset V \subset \mathbb{F}^n$ a pair of invariant subspaces. Then we have a decomposition $\mathbb{F}^n = U \oplus U' \oplus V'$, where $V = U \oplus U'$. If we choose a basis of $\mathbb{F}^n$ according to this decomposition, the matrices from $\mathcal{M}$ have the form

$$X = \begin{bmatrix} X_U & * & * \\ 0 & X_{V/U} & * \\ 0 & 0 & X_{V'} \end{bmatrix}.$$

We denote $\mathcal{M}_{V/U} = \{X_{V/U} \mid X \in \mathcal{M}\}$.

Definition 1.11 Let $\mathcal{P}$ be a property of collections of square matrices over $\mathbb{F}$. We say that the property $\mathcal{P}$ is *inherited by quotients*, if for any $\mathcal{M} \subset \mathbb{F}^{n\times n}$ having property $\mathcal{P}$ and any $\mathcal{M}$-invariant subspaces $U \subset V \subset \mathbb{F}^n$ the set $\mathcal{M}_{V/U}$ still has the property $\mathcal{P}$. ◇

The next lemma is often used when triangularizability is considered.

Lemma 1.12 (Triangularization Lemma) *Let $\mathcal{P}$ be a property of subsets of $\mathbb{F}^{n\times n}$ which is inherited by quotients. If the property $\mathcal{P}$ on a collection $\mathcal{M} \subset \mathbb{F}^{n\times n}$ implies reducibility of $\mathcal{M}$ for $n \geq 2$, then it implies the triangularizability of any collection.*

PROOF. Suppose that $\{0\} = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_m = \mathbb{F}^n$ is a maximal chain of $\mathcal{M}$-invariant subspaces. Then for all i the set $\mathcal{M}_{V_i/V_{i-i}}$ has the property $\mathcal{P}$. By the hypothesis the set consists of 1×1 matrices, which implies triangularizability of $\mathcal{M}$. □

Lemma 1.13 *Let $\mathcal{P}$ be a property of subsets of $\mathbb{F}^{n\times n}$ which is inherited by the quotients, and assume that any $\mathcal{M} \subset \mathbb{F}^{n\times n}$ with the property $\mathcal{P}$ is triangularizable over the algebraic closure $\mathbb{K} = \overline{\mathbb{F}}$ of the field $\mathbb{F}$. If the spectrum $\sigma(X)$ is contained in $\mathbb{F}$ for every $X \in \mathcal{M}$, then we can triangularize $\mathcal{M}$ over the field $\mathbb{F}$.*

PROOF. We prove the lemma by the induction.
For $n = 1$ there is nothing to prove, so we proceed with $n > 1$. In a suitable basis of $\mathbb{K}^n$ all matrices $X \in \mathcal{M}$ transform in the form

$$\Phi(X) = \begin{bmatrix} f_1(X) & * \\ 0 & X' \end{bmatrix},$$

with $f_1(X) \in \mathbb{F}$. If we write the (possibly infinite) system of linear equations defining the intersection of all the kernels $\operatorname{Ker}(X - f_1(X)I)$, it has a nontrivial solution in $\mathbb{K}$. By a rank argument it is clear that we can find a solution in $\mathbb{F}$, so we can assume that $\Phi(X) \in \mathbb{F}^{n\times n}$ for all $X \in \mathcal{M}$. Since the collection $\mathcal{M}' = \{X' \mid X \in \mathcal{M}\}$ still satisfies the assumptions from lemma, we use the inductive hypothesis to finish the proof. □

Theorem 1.14 (Kolchin's theorem) *Let $\mathcal{S} \subset \mathbb{F}^{n\times n}$ be a semigroup of unipotent matrices. Then $\mathcal{S}$ is triangularizable.*

PROOF. By Lemma 1.13 it is enough to consider the case of algebraically closed fields. The spectrum of every matrix $X \in \mathcal{S}$ is $\{1\}$, therefore trace has constant value n on $\mathcal{S}$. By Corollary 1.10 the semigroup is reducible for $n > 1$. Since the unipotency is inherited by the quotiens, we complete the proof using Lemma 1.12.
□

If a collection of matrices $\mathcal{M} \subset \mathbb{F}^{n\times n}$ is triangularizable, it is clear that the trace is a permutable function on $\mathcal{M}$. The following theorem shows that the converse holds provided $\mathbb{F}$ is an algebraically closed field.

Theorem 1.15 (Radjavi) *Let $\mathbb{F}$ be an algebraically closed field with characteristic zero and $\mathcal{M} \subset \mathbb{F}^{n\times n}$ a collection of matrices. Then $\mathcal{M}$ is triangularizable if and only if trace is permutable on $\mathcal{M}$.*

PROOF. Assume that trace is permutable on $\mathcal{M}$ and let $\mathcal{A}$ denote the algebra generated by $\mathcal{M}$. Clearly permutability of trace extends to the algebra $\mathcal{A}$. Let $\{A_{ij}\}$ be the block triangularization of $\mathcal{A}$ obtained in Theorem 1.6. We must show that all the subspaces $\mathcal{N}_i$ are one-dimensional. Assume otherwise. Then one of the subsets $J_k = J$ corresponds to equal diagonal blocks $\{A_{ii} \,|\, i \in J\}$ acting on spaces of dimension at least 2. Let m be the number of elements of J. Then by (1) and (4) of Theorem 1.6 the function f, defined by $f(A) = m \cdot \operatorname{tr}(A)$ is permutable on $\operatorname{End}_{\mathbb{F}}(\mathcal{N}_i)$. Since $m \neq 0$ it follows that trace is permutable on $\operatorname{End}_{\mathbb{F}}(\mathcal{N}_i)$ which is a contradiction. □

The next example shows that in general the field $\mathbb{F}$ has to be algebraically closed to satisfy the previous theorem.

Example 1.16 *Let $\mathcal{G} \subset \mathbb{R}^{2\times 2}$ be the group of all matrices of the form*

$$X = \begin{bmatrix} a & -b \\ b & a \end{bmatrix},$$

$a, b \in \mathbb{R}$. Then trace is permutable on $\mathcal{G}$, but $\mathcal{G}$ is not triangularizable over $\mathbb{R}$.

PROOF. Since $\mathcal{G} = \mathbb{R}\{I, J\}$, where

$$J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

the group $\mathcal{G}$ is commutative and therefore trace is permutable. The matrix J has no real eigenvalues, so the group $\mathcal{G}$ is irreducible over $\mathbb{R}$. □

2 MATRIX GROUPS WITH FINITE SPECTRA

2.1 Algebraic groups

We start with the notion of the algebraic set and the algebraic group. Let $\mathbb{F}$ denote a field with characteristic zero.

Definition 2.1 An ordered pair consisting of a set S and a finitely generated algebra $\mathcal{P}(S) < \mathbb{F}^S$ of $\mathbb{F}$-valued functions on S is called an *algebraic set*, if the following conditions are satisfied:
(a) $\mathcal{P}(S)$ separates the points of S, i.e., for arbitrary $s_1, s_2 \in S$ with $s_1 \neq s_2$ there is a function $f \in \mathcal{P}(S)$ such that

$$f(s_1) \neq f(s_2).$$

(b) For every $\mathbb{F}$-algebra morphism $\Phi : \mathcal{P}(S) \to \mathbb{F}$, there exists an element $s \in S$ such that for all $f \in \mathcal{P}(S)$ we have

$$\Phi(f) = f(s).$$

The elements of $\mathcal{P}(S)$ are called *polynomial functions*. ◇

By the condition (a) the element s from (b) is unique and we write

$$\Phi = s^*.$$

The last correspondence shows us that we may identify the set S and the set $\mathrm{Alg}(\mathcal{P}(S), \mathbb{F})$ of all algebra morphisms from $\mathcal{P}(S)$ to $\mathbb{F}$.
Let $(S, \mathcal{P}(S))$ and $(T, \mathcal{P}(T))$ be algebraic sets and $\alpha : S \to T$ a map. We define the category of the algebraic sets. The objects of this category are algebraic sets, while α is a *morphism* of algebraic sets if

$$\mathcal{P}(T) \circ \alpha \subset \mathcal{P}(S).$$

An algebraic set S becomes a topological space by defining *Zariski topology*. We say that a subset $A \subset S$ is closed or an *algebraic subset* of S whenever there exists a set of functions $U \subset \mathcal{P}(S)$ such that

$$A = \{s \in S \mid f(s) = 0, f \in U\}.$$

It is easy to verify that the pair $(A, \mathcal{P}(S)|_A)$ is again an algebraic set. From the condition (a) in Definition 2.1 it follows that the Zariski topology has property T_1 (i.e., every singleton is a closed set). It is also easy to see that every morphism of algebraic sets is continuous in the Zariski topology.

To define an algebraic group we need the concept of the finite direct product in the category of algebraic sets. Let $(S, \mathcal{P}(S))$ and $(T, \mathcal{P}(T))$ be algebraic sets. We set

$$\mathcal{P}(S \times T) = \mathcal{P}(S) \otimes \mathcal{P}(T)$$

in the sense that $(f \otimes g)(s,t) = f(s)g(t)$, for $f \in \mathcal{P}(S)$, $g \in \mathcal{P}(T)$ and $(s,t) \in S \times T$.

Definition 2.2 Let $(G, \mathcal{P}(G))$ be an algebraic set which also has a structure of a group given by a map $\circ : G \times G \to G$. Let us denote by $\iota : G \to G$ the map, which maps an element $x \in G$ to its inverse x^{-1}. We say that G is an *algebraic group*, if the maps $\circ$ and ι are morphisms of algebraic sets. A subgroup $H \subset G$ is an *algebraic subgroup*, if it is closed in the Zariski topology. $\diamond$

2.2 Some results from the theory of algebraic groups

Let $(S, \mathcal{P}(S))$ be an algebraic set. We call a subset $A \subset S$ *irreducible*, if for every closed sets $C, B \subset A$ such that $A = B \cup C$ it follows that either $B = A$ or $C = A$. We define an *irreducible component* of S to be a maximal irreducible subset of S. Since one can see that the closure of an irreducible set is still an irreducible set, it is clear that the irreducible components of S are algebraic subsets. From the fact that $\mathcal{P}(S)$ is a noetherian ring, it follows (see [14, p. 16]) that there are finitely many irreducible components $S_1, S_2, \ldots, S_n$ and that

$$S = S_1 \cup \cdots \cup S_n.$$

For an algebraic group G in [14, Thm. 1.4, p. 17] it is shown that the irreducible component G_1 containing the unit of G is a normal subgroup of finite index and that the irreducible components of G are exactly the elements of the factor group G/G_1.

Let G be an algebraic group, V a vector space over $\mathbb{F}$ and $\rho : G \to \mathrm{Aut}(V)$ an action of G on the space V. We say that V is a *polynomial G-module* if for every functional $\gamma \in \mathrm{End}(V)^*$ the map $\gamma \circ \rho$ is an element of $\mathcal{P}(G)$.

There exists a natural action of an algebraic group G on the set of polynomial functions $\mathcal{P}(G)$ defined by

$$(\rho(x)(f))(y) = (xf)(y) = f(yx)$$

for $f \in \mathcal{P}(G)$ and $x, y \in G$. This action yields a polynomial G-module where all $\rho(x)$ are automorphisms of the algebra $\mathcal{P}(G)$. We say that a subgroup T of an algebraic group G is *unipotent*, if the action of T on $\mathcal{P}(G)$ is locally unipotent, i.e., $\rho(x)$ restricted to any finite dimensional T-submodule V of $\mathcal{P}(G)$ has the spectrum $\{1\}$ or $\rho(x) - \mathrm{id}_V$ is nilpotent for all $x \in T$. It is shown in [14, p. 65] that for any algebraic group G there exists a maximal unipotent normal algebraic subgroup $G_u < G$ containing every other unipotent normal subgroup of G. In [14] one can also find the following two theorems which hold in characteristic zero.

Theorem 2.3 *Let G be an algebraic group and T a unipotent subgroup of G. Then T is irreducible.*

We will use the consequence that G_u is irreducible.

Theorem 2.4 *For every algebraic group G there exists an algebraic subgroup P such that G is the semidirect product*

$$G = G_u \rtimes P.$$

(Every matrix X from the group G can be uniquely expressed in the form $X = UT$ with $U \in G_u$ and $T \in P$.) We conclude that $P \approx G/G_u$.

2.3 An extension of Kolchin's theorem

For the rest of this section $\mathbb{F}$ will be a field with characteristic zero.

Let us first introduce two examples of the algebraic groups which we will use in the sequel. The first example is the additive group of the field $\mathbb{F}$ with the algebra

$\mathcal{P}(\mathbb{F})$ being $\mathbb{F}[\mathrm{id}]$. The next very important example is the group $G = \mathrm{GL}_n(\mathbb{F})$ of all invertible matrices of order $n \times n$ over the field $\mathbb{F}$. Here, we take $\mathcal{P}(G)$ to be the $\mathbb{F}$-algebra generated by the functionals α_{ij} and $\frac{1}{\det}$, where the functional α_{ij} maps a matrix X to its ij-th entry X_{ij}. We write

$$\mathcal{P}(G) = \mathbb{F}[\alpha_{11}, \ldots, \alpha_{nn}, \frac{1}{\det}].$$

The second example is universal in the sense that every $\mathbb{F}$-algebraic group can be embedded in the group $\mathrm{GL}_n(\mathbb{F})$ for n large enough. It is then easy to see, that $\mathbb{F}^n$ is a polynomial $\mathrm{GL}_n(\mathbb{F})$-module.

Lemma 2.5 *Let H be a subgroup of an algebraic subgroup $G \subset \mathrm{GL}_n(\mathbb{F})$. If H acts unipotently on $\mathbb{F}^n$, then H is a unipotent subgroup of G.*

Proof. By Kolchin's theorem (Theorem 1.14) there exists a basis of $\mathbb{F}^n$ in which all the matrices of the group H take the upper triangular form with diagonal entries all equal to 1. We can clearly take coordinate functionals α_{ij} relative to this basis and $\frac{1}{\det}$ to generate the algebra $\mathcal{P}(G)$. Let us calculate $x\alpha_{ij}$ for an element $x \in H$. For arbitrary $y \in G$ we have

$$(x\alpha_{ji})(y) = \alpha_{ij}(yx) = \sum_{k=1}^{n} \alpha_{ik}(y)\alpha_{kj}(x) = \alpha_{ij}(y) + \sum_{k<j} \alpha_{ik}(y)\alpha_{kj}(x),$$

since $\alpha_{jj}(x) = 1$ and $\alpha_{kj}(x) = 0$ for $k > j$. Next, we have

$$(x(\frac{1}{\det}))(y) = \frac{1}{\det(yx)} = \frac{1}{\det(y)}\frac{1}{\det(x)} = \frac{1}{\det(y)},$$

since $\det(x) = 1$. From the above relations we get

$$x\alpha_{ij} = \alpha_{ij} + \sum_{k<j} \alpha_{kj}(x)\alpha_{ik} \tag{1}$$

and

$$x(\frac{1}{\det^l}) = \frac{1}{\det^l}. \tag{2}$$

If V is a finite dimensional H-polynomial submodule of $\mathcal{P}(G)$, then there exists an integer $N \in \mathbb{N}$ such that

$$V \subset \mathbb{F}\left\{\frac{1}{\det^l}\Pi_{i,j}\alpha^{k_{ij}} \mid k_{ij}, l \leq N\right\}.$$

Now, we show that $\rho(x) - \mathrm{id}_V$ is nilpotent on every element of the form $\frac{1}{\det^l}\Pi_{i,j}\alpha^{k_{ij}}$. From (1) we get

$$(\rho(x) - \mathrm{id}_V)(\alpha_{ij}) = \sum_{k<j}^{n} \alpha_{kj}(x)\alpha_{ik} \tag{3}$$

and from (2)

$$(\rho(x) - \mathrm{id}_V)(\frac{1}{\det^l}) = 0. \tag{4}$$

We define $\alpha_{ij} < \alpha_{uv}$ for $i < u$ or $i = u$ and $j < v$ to get a lexicographic order on the set of monomials $\mathcal{M} = \{\Pi_{i,j}\alpha^{k_{ij}} \mid k_{ij}, l \leq N\}$. By (3) and (1) $\rho(x) - \mathrm{id}_V$ maps α_{ij} into a sum of strictly smaller monomials and that $\rho(x)$ maps α_{ij} into a sum of monomials not greater than α_{ij}. We proceed by induction on the degree of monomials. Assume that $\rho(x) - \mathrm{id}_V$ maps every monomial of degree m into a sum of strictly smaller monomials. Let $f \in \mathcal{M}$ be a monomial of degree m. Then we have

$$(\rho(x) - \mathrm{id}_V)(f\alpha_{ij}) = (\rho(x) - \mathrm{id}_V)(f)\rho(x)(\alpha_{ij}) + f(\rho(x) - \mathrm{id}_V)(\alpha_{ij}).$$

By the induction hypothesis and the base of the induction we conclude that $\rho(x) - \mathrm{id}_V$ strictly decreases the degree of monomials. For $f \in \mathcal{M}$ by (3) and (4) we similarly get

$$(\rho(x) - \mathrm{id}_V)(\frac{f}{\det^l}) = \frac{(\rho(x) - \mathrm{id}_V)(f)}{\det^l}.$$

Clearly this implies that $\rho(x) - \mathrm{id}_V$ is indeed nilpotent on V. □

The following result is well-known; for completeness we present a proof given in [20].

Lemma 2.6 *Let $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in \mathbb{F}$ be elements of the field $\mathbb{F}$ with zero characteristic.*
(1) If $\sum_{i=1}^{n} \alpha_i^k = \sum_{i=1}^{n} \beta_i^k$ for $k = 1, \ldots, n$, then there is a permutation $\pi \in S_n$ such that $\beta_i = \alpha_{\pi(i)}$ for all i.
(2) If $\sum_{i=1}^{n} \alpha_i^k = 0$ for $k = 1, \ldots, n$, then $\alpha_i = 0$ for all i.
(3) If $\sum_{i=1}^{n} \alpha_i^k = c$ with c fixed for $k = 1, \ldots, n+1$, then c is an integer and each $\alpha_i = 0$ is either 0 or 1.

PROOF. (1) The functions T_k defined by

$$T_k(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^k$$

are symmetric polynomials. For each k, let S_k denote the elementary symmetric polynomial in variables $x_1, \ldots, x_n$. Then:

$$S_1 = x_1 + \cdots + x_n$$

$$S_2 = x_1x_2 + \cdots + x_{n-1}x_n$$

$$\vdots$$

$$S_n = x_1x_2 \cdots x_n$$

One can verify that

$$T_k - T_{k-1}S_1 + T_{k-2}S_2 - \cdots + (-1)^{k-1}T_1S_{k-1} + (-1)^k kS_k = 0 \qquad \text{(rec)}$$

for $k = 1, \ldots, n$. By this formula we can inductively determine S_k in terms of the T_j's.

The hypothesis that $T_k(\alpha_1, \ldots, \alpha_n) = T_k(\beta_1, \ldots, \beta_n)$ for $k = 1, \ldots, n$, implies $S_k(\alpha_1, \ldots, \alpha_n) = S_k(\beta_1, \ldots, \beta_n)$ for $k = 1, \ldots, n$. This means that the monic polynomial of degree n with zeros at $\alpha_1, \ldots, \alpha_n$ (whose coefficients are the elementary symmetric functions of its roots) coincides with the monic polynomial of degree n with zeros at $\beta_1, \ldots, \beta_n$. It follows that the n-tuples $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are the same except for a permutation.

(2) We take $\beta_i = 0$ for all i and use (1).

(3) We can assume that $c \neq 0$ (otherwise we use (2)). After a permutation, if necessary, assume that $\alpha_1, \ldots, \alpha_m \neq 0$ and $\alpha_i = 0$ for $i > m$. We must now show that $c = m$. It is clear that we can disregard α_i for $i > m$ and assume that $n = m$.

An easy calculation shows that

$$T_{n+1} = T_nS_1 - T_{n-1}S_2 + \cdots + (-1)^{n-1}T_1S_n.$$

Denoting $s_k = S_k(\alpha_1, \ldots, \alpha_n)$ and using the hypothesis $T_k(\alpha_1, \ldots, \alpha_n) = 0$ for $k = 1, \ldots, n+1$, yields

$$1 = s_1 - s_2 + \cdots + (-1)^{n-1}s_n.$$

By the relation (rec), for $k = n$, we also get

$$c(s_1 - s_2 + \cdots + (-1)^{n-1}s_{n-1}) + (-1)^n n s_n = 0.$$

Since $s_n \neq 0$, the last two equations imply $c = n$. By (1) we get $\beta_i = 1$ for all i, proving that $\alpha_i = 1$. □

Lemma 2.7 (Kaplansky) *If $\mathcal{S} \subset \mathbb{F}^{n\times n}$ is a matrix semigroup of invertible matrices and* $\mathrm{tr} : \mathcal{S} \to \mathbb{F}$ *is constant, then every matrix $X \in \mathcal{S}$ has only* 1 *in its spectrum (i.e., $\mathcal{S}$ is unipotent).*

Proof. It follows directly from (3) of Lemma 2.6. □

Let us now recall Radjavi's trace condition (see Theorem 1.15). For an algebraically closed field $\mathbb{F}$ a semigroup $\mathcal{S} \subset \mathbb{F}^{n\times n}$ is triangularizable if and only if for arbitrary $A, B, C \in S$ we have

$$\mathrm{tr}\,(ABC) = \mathrm{tr}\,(CBA),$$

i.e., trace is permutable on the semigroup $\mathcal{S}$. We will use this fact to prove the following theorem.

Theorem 2.8 *Let $\mathcal{S}$ be a semigroup of matrices having their eigenvalues in the set $\{1, -1\}$. Then S is triangularizable.*

Proof. According to Lemma 1.13 we may assume that $\mathbb{F}$ is algebraically closed. We can clearly assume that $\mathcal{S}$ is a submonoid of $\mathrm{GL}_n(\mathbb{F})$. By [14, Prop. 4.1, p.12] the algebraic closure $\mathcal{G}$ of $\mathcal{S}$ is in fact an algebraic subgroup of $\mathrm{GL}_n(\mathbb{F})$. For $\lambda \notin \{1, -1\}$ we define $f_\lambda : \mathcal{G} \to \mathbb{F}$ by $f_\lambda(X) = \det(X - \lambda I)$. It is clear that f_λ is a polynomial function in the coordinate functionals α_{ij}. As the canonical upper diagonal form of any matrix in $\mathcal{S}$ has diagonal entries 1 or -1, it follows that

$$f_\lambda(\mathcal{S}) \subset \{(1-\lambda)^r(-1-\lambda)^s \mid r + s = n\},$$

which implies that $f_\lambda(\mathcal{S})$ is a finite set not containing 0. Since Zariski topology has the property T_1, the set $f_\lambda(\mathcal{S})$ is closed. For f_λ is a continuous map we get

$$f_\lambda(\mathcal{G}) = f_\lambda(\overline{\mathcal{S}}) \subset \overline{f_\lambda(\mathcal{S})} = f_\lambda(\mathcal{S}).$$

It follows that the set $f_\lambda(\mathcal{G})$ does not contain 0, and the spectra of the matrices from $\mathcal{G}$ are also contained in $\{1, -1\}$.

We can now replace the semigroup $\mathcal{S}$ by the group $\mathcal{G}$. Consider the polynomial function $\mathrm{tr} : \mathcal{G} \to \mathbb{F}$. It is clear that it takes only finitely many distinct values. If $\mathcal{G}_1$ is the irreducible component of the unit, the set $\mathrm{tr}\,(\mathcal{G}_1)$ is an irreducible subset of the finite set $\mathrm{tr}\,(\mathcal{G})$. It follows that $\mathrm{tr}\,(\mathcal{G}_1)$ is a singleton, which means that the map tr is constant on $\mathcal{G}_1$. By Lemma 2.7, $\mathcal{G}_1$ is a unipotent group of matrices and by Lemma 2.5 also is an unipotent algebraic subgroup of $\mathcal{G}$. Since $\mathcal{G}_1$ is a normal subgroup of $\mathcal{G}$, we have

$$\mathcal{G}_1 \subset \mathcal{G}_u. \tag{6}$$

For $\mathcal{G}_u$ is irreducible (see Theorem 2.3) and contains the unit of the group $\mathcal{G}$, we have

$$\mathcal{G}_u \subset \mathcal{G}_1. \tag{7}$$

From (6) and (7) it follows that

$$\mathcal{G}_u = \mathcal{G}_1. \tag{8}$$

Therefore, by Theorem 2.4 we get

$$\mathcal{G} = \mathcal{G}_1 \rtimes P. \tag{9}$$

Since $\mathcal{G}_1$ has a finite index and by (9) $P \approx \mathcal{G}/\mathcal{G}_1$, it follows that P is a finite subgroup. As P is finite and $\mathbb{F}$ has characteristic zero, the Jordan from of a matrix $X \in P$ must be diagonal. It follows that for all $X \in P$ we have

$$X = X^{-1}$$

and therefore P is commutative. Now we pick $A, B, C \in \mathcal{G}$. By (9) we can write $A = A'X$, $B = B'Y$ and $C = C'Z$ for some $A', B', C' \in \mathcal{G}_1$ and $X, Y, Z \in P$. Since tr takes only finitely many values and elements of the factor group $\mathcal{G}/\mathcal{G}_1$ are exactly the irreducible components of $\mathcal{G}$ it follows that tr is constant on every coset $\mathcal{G}_1 T$ for $T \in \mathcal{G}$. As P is commutative, we get

$$\mathrm{tr}\,(ABC) \in \mathrm{tr}\,(\mathcal{G}_1 ABC) = \mathrm{tr}\,(\mathcal{G}_1 XYZ) =$$

$$= \mathrm{tr}\,(\mathcal{G}_1 ZYX) = \mathrm{tr}\,(\mathcal{G}_1 CBA) \ni \mathrm{tr}\,(CBA),$$

and thus

$$\operatorname{tr}(ABC) = \operatorname{tr}(CBA).$$

Radjavi's trace condition then implies triangularizability of the group $\mathcal{G}$, and therefore also triangularizability of the semigroup $\mathcal{S} \subset \mathcal{G}$. This completes the proof.

□

2.4 Examples

The following examples shows us that Theorem 2.8 is the best possible extension of Kolchin's theorem under the assumption that the spectra of matrices of a matrix semigroup lies under some finite subgroup of the multiplicative group of the field $\mathbb{F}$.

Let Γ be a finite subgroup of the multiplicative group $\mathbb{F} \setminus \{0\}$ having more than two elements (i.e., $\Gamma \not\subset \{1, -1\}$). We now construct a finite group $\mathcal{P}$ of matrices such that the union of the spectra of its matrices is exactly Γ, but $\mathcal{P}$ is not triangularizable. First we make the next remark.

Assume that a finite matrix group $\mathcal{P}$ is triagularizable and that all of its matrices are upper triangular. Then for any pair $A, B \in \mathcal{P}$ the matrix $ABA^{-1}B^{-1}$ is an upper triangular matrix having all the diagonal entries equal to 1, i.e., is unipotent. Since $\mathcal{P}$ is a finite group the only possible unipotent matrix in $\mathcal{P}$ is the identity matrix and therefore $\mathcal{P}$ has to be a commutative group.

By the above it is enough to construct a noncommutative finite group $\mathcal{P}$ with the desired spectra. First we define

$$\mathcal{P}_2 = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \{1, -1\} \right\} \cup \left\{ \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix} \mid a, b \in \{1, -1\} \right\}.$$

It is easy to verify, that the union of the spectra of the matrices from $\mathcal{P}_2$ is the group $\{1, -1, i, -i\}$ and that $\mathcal{P}_2$ is a noncommutative group with eight elements.

For an odd prime p we denote by $\mathcal{P}_p$ the matrix group generated with the matrices

$$D = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & \lambda & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda^{p-1} \end{bmatrix}$$

and

$$C = \begin{bmatrix} 0 & \cdots & \cdots & 0 & 1 \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{bmatrix}$$

for $\lambda \neq 1$, $\lambda^p = 1$. One can verify that the group $\mathcal{P}_p$ consists of p^3 matrices and the union of the spectra of its matrices is the group $\{\mu \mid \mu^p = 1\}$. For the required group $\mathcal{P}$ we can take

$$\mathcal{P} = \left\{ \begin{bmatrix} \nu & 0 \\ 0 & X \end{bmatrix} \mid \nu \in \Gamma,\ X \in \mathcal{P}_l \right\},$$

with $l = 2$ if the order of Γ is a power of 2 and $l = p$ if p is some prime factor dividing the order of Γ.

3 MATRIX GROUPS WITH INDEPENDENT SPECTRA

3.1 Systems of imprimitivity and Clifford's theorem

In this introduction we consider imprimitivity of the matrix groups and its extreme case, i.e., monomiality. The following facts can be found in [27].

Definition 3.1 Let $\mathcal{G} \subset \mathbb{F}^{n\times n}$ be a matrix group and $\mathcal{W} \subset \mathbb{F}^n$. If $\mathcal{W}$ is a $\mathcal{G}$-invariant space with respect to the left action of $\mathcal{G}$ on $\mathbb{F}^n$, we call $\mathcal{W}$ a $\mathcal{G}$-*module*. $\diamond$

Definition 3.2 A matrix group $\mathcal{G} \subset \mathbb{F}^{n\times n}$ is called *imprimitive* if the space $\mathbb{F}^n$ can be represented as a direct sum of k subspaces ($k > 1$) that are permuted among each other by the elements of $\mathcal{G}$, i.e.,

$$\mathbb{F}^{n\times n} = Q_1 \oplus Q_2 \oplus \cdots \oplus Q_k$$

and for $X \in \mathcal{G}$, $i \leq k$ we find $j \leq k$ such that

$$X(Q_i) = Q_j.$$

The subspaces $Q_1, Q_2, \ldots, Q_k$ are called *systems of imprimitivity* of $\mathcal{G}$. If such a decomposition does not exist, then $\mathcal{G}$ is *primitive*. $\diamond$

Let $\mathcal{G} \subset \mathbb{F}^{n\times n}$ be an irreducible imprimitive matrix group and

$$\mathbb{F}^{n\times n} = Q_1 \oplus Q_2 \oplus \cdots \oplus Q_k$$

a direct sum of systems of imprimitivity. Since $\mathcal{G}$ is irreducible, it is clear that the elements of $\mathcal{G}$ permute the spaces $Q_1, Q_2, \ldots, Q_k$ transitively. Let $\mathcal{H}_i$ be the set of all elements of $\mathcal{G}$ that interchange vectors of Q_i within Q_i. It is easy to verify that $\mathcal{H}_i$ is in fact a subgroup of $\mathcal{G}$ and for $X \in \mathcal{G}$ such that $X(Q_i) = Q_j$ we have

$$X\mathcal{H}_iX^{-1} = \mathcal{H}_j.$$

Let us pick $X_1, X_2, \ldots, X_k \in \mathcal{G}$ such that for all $i \leq k$ we have $X_i(Q_1) = Q_i$. Then for $X \in \mathcal{G}$ we find j such that $X(Q_1) = Q_j$. Since $X_j^{-1}XQ_1 = Q_1$ it follows that $X\mathcal{H}_1 = X_j\mathcal{H}_1$ and therefore $X_1, X_2, \ldots, X_k \in \mathcal{G}$ form a complete system of left representatives of $\mathcal{H}_1$ in $\mathcal{G}$.

Lemma 3.3 *Let $\mathcal{G}$ be an irreducible group. The subgroup $\mathcal{H}_i$ induces an irreducible subgroup $\mathcal{G}_i$ on Q_i.*

PROOF. By symmetry it is sufficient to consider the case $i = 1$. Let $R_1 \subset Q_1$ ba a nontrivial invariant subspace of Q_1 and $X_1, X_2, \ldots, X_k \in \mathcal{G}$ a complete system of left representatives of $\mathcal{H}_1$ in $\mathcal{G}$. We define

$$R = X_1(R_1) \oplus X_2(R_1) \oplus \cdots \oplus X_k(R_1).$$

Since $\mathcal{H}_1(R_1) = R_1$, it is easy to verify that for $X \in \mathcal{G}$ we have $X(R) = R$. As $R \neq 0$ and $\mathcal{G}$ is an irreducible group we get $R = \mathbb{F}^n$. Since $n = \dim(R) = k \cdot \dim(R_1)$, we have

$$\dim(R_1) = \frac{n}{k} = \dim(Q_1)$$

and therefore $Q_1 = R_1$. This completes the proof. □

Proposition 3.4 *For an irreducible group $\mathcal{G}$ there exists a decomposition of $\mathbb{F}^n$ into a direct sum of systems of imprimitivity $Q_1, Q_2, \ldots, Q_k$ such that the groups $\mathcal{G}_i$ (see Lemma 3.3) are primitive.*

PROOF. Let $\mathcal{H}_1$ induce an imprimitive group $\mathcal{G}_1$ on the space Q_1 (see Lemma 3.3), and let

$$Q_1 = Q_{11} \oplus Q_{12} \oplus \cdots \oplus Q_{1l}$$

be a decomposition into systems of imprimitivity. Then $\mathbb{F}^n$ can be represented as the direct sum of kl systems of imprimitivity, namely

$$Q_{ij} = X_i(Q_{1j}),$$

where $X_1, X_2, \ldots, X_k \in \mathcal{G}$ is a complete system of left representatives of $\mathcal{H}_1$ in $\mathcal{G}$. In a finite number of steps we reach the situation described in the proposition. □

The decomposition in Proposition 3.4 is called a *complete decomposition into systems of imprimitivity.*

Theorem 3.5 (Clifford's theorem) *Let $\mathcal{G} \subset \mathbb{F}^{n\times n}$ be an irreducible matrix group and $\mathcal{H} \triangleleft \mathcal{G}$ a normal subgroup of $\mathcal{G}$. Then*
(1) There is a decomposition of $\mathbb{F}^n$,

$$\mathbb{F}^n = L_1 \oplus L_2 \oplus \cdots \oplus L_s,$$

where L_i are irreducible $\mathcal{H}$-modules all having the same dimension.
(2) Let Q_i be the sum of all spaces L_j which are isomorphic to L_i as $\mathcal{H}$-modules. Then all the different spaces Q_i are systems of imprimitivity of the group $\mathcal{G}$. In particular, if $\mathcal{G}$ is a primitive group, then all the spaces L_i are isomorphic $\mathcal{H}$-modules.

Proof. (1) Let L_1 be an irreducible $\mathcal{H}$-submodule of $\mathbb{F}^n$. Since $\mathcal{H}$ is a normal subgroup, for $B_2 \in \mathcal{G}$ we have $\mathcal{H}B_2(L_1) = B_2\mathcal{H}(L_1) = B_2(L_1)$. Therefore the space $L_1 + B_2(L_1)$ either coincides with L_1 or is the direct of two irreducible $\mathcal{H}$-modules. Suppose that for some $B_2, \ldots, B_s \in \mathcal{G}$

$$L = L_1 \oplus B_2(L_1) \oplus \cdots \oplus B_s(L_1)$$

is a direct sum such that for every $G \in \mathcal{G}$ the sum $L + G(L_1)$ is no longer direct. Then $G(L_1) \subset L$ and therefore $G(L) = L$. Since $\mathcal{G}$ is an irreducible group, we get

$$L = L_1 \oplus L_2 \oplus \cdots \oplus L_s = \mathbb{F}^n \tag{hdec}$$

for $L_j = B_j(L_1)$. This proves the first part of the theorem.
(2) Now let Q_1 be the sum of all spaces L_j which are isomorphic to L_1 as $\mathcal{H}$-modules. If R is a $\mathcal{H}$-submodule of $\mathbb{F}^n$ isomorphic to L_1 then $R \subset Q_1$ since the decomposition (hdec) is unique up to some permutation of the sumands. For a pair of isomorphic $\mathcal{H}$-modules $R_1, R_2 \subset \mathbb{F}^n$ and $G \in \mathcal{G}$ it is easy to verify that $G(R_1)$ and $G(R_2)$ are also isomorphic $\mathcal{H}$-modules, since the $\mathcal{H}$ is a normal subgroup.

We now examine $G(Q_1)$, where $G \in \mathcal{G}$. Clearly $G(Q_1)$ contains $G(L_1)$ as a direct summand, and all the other summands are isomorphic to $G(L_1)$. In the decomposition (hdec) we find an $\mathcal{H}$-module L_i isomorphic to $G(L_1)$. Therefore $G(Q_1)$ is contained in a direct sum Q_2 of all L_j isomorphic to L_i. However, the $\mathcal{H}$-modules $G^{-1}(L_i)$ and L_1 are isomorphic, which implies that $G^{-1}(Q_2) \subset Q_1$. Hence $G(Q_1) = Q_2$ and the proof is complete. □

Corollary 3.6 *If $\mathcal{H}$ is a normal subgroup of an irreducible primitive matrix group, then the linear span $\mathbb{F}\mathcal{H}$ is a simple algebra over $\mathbb{F}$.*

PROOF. All the $\mathcal{H}$-modules L_i in the decomposition provided by Theorem 3.5 are isomorphic. Therefore we can find a similarity such that all L_i's are actually the same. By Theorem 1.4, L_1 is a simple algebra, and thus $\mathbb{F}\mathcal{H}$ also is a simple algebra over. □

Lemma 3.7 *Let $\mathcal{G} \subset \mathbb{F}^{n\times n}$ be an irreducible primitive matrix group and $\mathcal{H}$ an abelian normal subgroup of $\mathcal{G}$. Then $\mathcal{H}$ is a subgroup of the multiplicative group of a certain field $\mathbb{K}$ contained in the algebra $\mathbb{F}^{n\times n}$.*

PROOF. We consider the linear span $\mathbb{F}\mathcal{H}$ of $\mathcal{H}$. Since $\mathcal{H}$ is a normal subgroup of a primitive irreducible group, Corollary 3.6 is applicable. Thus $\mathbb{F}\mathcal{H}$ is a simple commutative subalgebra of $\mathbb{F}^{n\times n}$. Therefore $\mathbb{K} = \mathbb{F}\mathcal{H}$ is a field. □

Corollary 3.8 *If $\mathcal{G}$ is an irreducible primitive matrix group over an algebraically closed field $\mathbb{F}$ and $\mathcal{H}$ an abelian normal subgroup of $\mathcal{G}$, then $\mathcal{H}$ is contained in the center $Z(\mathcal{G}) \subset \mathbb{F}\{I\}$.*

PROOF. We apply Lemma 3.7 to conclude that $\mathbb{K} = \mathbb{F}\mathcal{H}$ is a finite extension of the field $\mathbb{F}$. As $\mathbb{F}$ is an algebraically closed field, we get $\mathbb{K} = \mathbb{F}$ and therefore $\mathcal{H} \subset \mathbb{F}\{I\}$. □

The extreme case of imprimitivity is the *monomiality* defined as follows.

Definition 3.9 A matrix A is called *monomial* if it has the form $A = DP$, where D is a diagonal matrix and P a permutation matrix. A group consisting of monomial matrices is called a *monomial group.* ◇

Theorem 3.10 (Taketa) *Let $\mathbb{F}$ be an algebraically closed field and $\mathcal{G} \subset \mathbb{F}^{n\times n}$ an irreducible nilpotent matrix group. Then $\mathcal{G}$ is similar to a monomial group.*

PROOF. By Proposition 3.4 the space $\mathbb{F}^n$ is a direct sum of complete systems of imprimitivity $Q_1, Q_2, \ldots, Q_r$. Then the groups $\mathcal{G}_i$ (see Lemma 3.3) are primitive.

We show that an irreducible nilpotent matrix group $\mathcal{K}$ of degree $m > 1$ is imprimitive. Let $\{I\} = \mathcal{Z}_0 \subset \mathcal{Z}_1 \subset \cdots \subset \mathcal{Z}_l = \mathcal{K}$ be the central series of $\mathcal{K}$ and $G \in \mathcal{Z}_2 \setminus \mathcal{Z}_1$. Then the group generated by $\{G\} \cup \mathcal{Z}_1$ is an abelian normal subgroup of $\mathcal{K}$ not contained in the center $\mathcal{Z}_1 = \mathcal{Z}(\mathcal{K})$. By Corollary 3.8, the group $\mathcal{K}$ is imprimitive.

Since $\mathcal{G}_i$ are irreducible nilpotent primitive groups, the subspaces Q_i are one-dimensional and $\mathcal{G}$ is similar to a monomial group. □

3.2 Matrices with p-property

Let $\mathbb{F}$ be a field of characteristic zero. Then the field of rationals $\mathbb{Q}$ is contained in $\mathbb{F}$. We first show where the definition of the p-property comes from. If every matrix A of an irreducible matrix group $\mathcal{G}$ is similar to a triangular matrix with diagonal entries $\lambda_1, \ldots, \lambda_r, \mu_1, \ldots, \mu_s$ where for $i \neq j$ the orders of λ_i and λ_j are finite numbers without a common divisor and $\mu_1, \ldots, \mu_s$ are transcendently independent over $\mathbb{Q}$, then

$$\det : \mathcal{G} \to \mathbb{F} \setminus \{0\}$$

is a homomorphism of groups with the kernel $\mathcal{K}$ consisting of unipotent matrices. The normal subgroup $\mathcal{K}$ is then triangularizable by the celebrated Kolchin theorem (Theorem 1.14). In the proof of the main theorem (Theorem 3.19) one can see how the triangularizability of $\mathcal{K}$ affects the triangularizability of $\mathcal{G}$ (we use commutativity of the irreducible parts of the group $\mathcal{K}$). The "invention" of the p-property then does not look so odd, because in the case of $p = 2$ we want the kernel of $\det^2$ to be a subgroup consisting of the matrices with eigenvalues 1 and -1 (see Theorem 2.8). Clearly in the case of a general p group $\mathcal{G}$ would not be triangularizable (see Examples 2.4).

Definition 3.11 Let p be a prime number and let matrix A be similar to a triangular matrix with diagonal entries $\lambda_1, \ldots, \lambda_r, \mu_1, \ldots, \mu_s$. If for $i \neq j$ the orders of λ_i and λ_j are finite with greatest common divisor dividing p and $\mu_1, \ldots, \mu_s$ are transcendently independent over $\mathbb{Q}$ we say that the matrix A has *p-property*. We will use this term for a single matrix or a set of matrices all having this property. ⋄

Let us now introduce the following notation. For an element $\lambda \in \mathbb{F}$ with finite multiplicative order, we will denote its order by $|\lambda|$, i.e.,

$$|\lambda| = \min\{t \in \mathbb{N} \mid \lambda^t = 1\}.$$

Lemma 3.12 *Let $q \in \mathbb{N}$ and $\lambda, \mu \in \mathbb{F}$. If the greatest common divisor $d(|\lambda|, |\mu|)$ divides q, then $d(|\lambda^q|, |\mu^q|) = 1$.*

PROOF. Let us denote $|\lambda| = t$, $|\mu| = u$, $|\lambda^q| = r$ and $|\mu^q| = s$. First we determine the numbers r and s. It is easy to verify that

$$r = \frac{t}{d(t, q)},$$

and similarly

$$s = \frac{u}{d(u, q)}.$$

Since $d(u, t)$ divides q, the numbers s and r are co-prime. This completes the proof. □

For a monomial group there is an epimorphism

$$\phi : \mathcal{G} \to P_{\mathcal{G}},$$

where $P_{\mathcal{G}}$ is the group of all permutation matrices P (see Definition 3.9) associated with the matrices from $\mathcal{G}$. We will often use the notation $P_A = \phi(A)$. Let us denote

$$\mathcal{Z}_p = \{\lambda \in \mathbb{F} | \lambda^p = 1\}.$$

Lemma 3.13 *(1) If $\det^p(A) = 1$ for a matrix A with p-property, then $\sigma(A) \subset \mathcal{Z}_p$. (2) If a monomial matrix A, where P_A is a permutation matrix, given by permutation π, has p-property, then the permutation π consists only of transpositions and p-cycles. If $p = 2$ then every transposition in π gives us a block with eigenvalues 1 and -1 in the matrix A. If $p > 2$, then every p-cycle in π gives us a block with eigenvalues $\sqrt[p]{1}$ in the matrix A, and π has at most one transposition.*

PROOF. (1) Let A be a matrix with p-property and $\det^p(A) = 1$. Then

$$\lambda_1^p \cdots \lambda_r^p \mu_1^p \cdots \mu_s^p = 1$$

For $o = |\lambda_1| \cdots |\lambda_r|$ we get

$$\mu_1^{o \cdot p} \cdots \mu_s^{o \cdot p} = 1.$$

As $\mu_1, \ldots, \mu_s$ are transcendently independent, it follows that $s = 0$. Since by Lemma 3.12 orders $|\lambda_1^p|, \ldots, |\lambda_r^p|$ are co-prime, it is easy to see, using the equation $\lambda_1^p \cdots \lambda_r^p = 1$, that in fact $\lambda_1^p = \cdots = \lambda_r^p = 1$ and $\sigma(A) \subset \mathcal{Z}_p$.

(2) Suppose that π contains a cycle of length n. By permuting the basis we can rearrange π to include the cycle $(123...n)$ and thus A has the form

$$A = \begin{bmatrix} B & 0 \\ 0 & C \end{bmatrix},$$

where

$$B = \begin{bmatrix} 0 & \cdots & \cdots & 0 & d_1 \\ d_2 & \ddots & & & 0 \\ 0 & d_3 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & d_n & 0 \end{bmatrix}.$$

Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of B and denote $d = d_1 \cdots d_n$. Then we get

$$\lambda_i^n = d$$

for all $i = 1, 2, \ldots, n$. If d is transcendental over $\mathbb{Q}$, then λ_i are transcendental and therefore have infinite orders. But on the other hand, λ_i are algebraically dependent ($\lambda_i^n = \lambda_j^n$) and A doesn't have p-property.

We can therefore assume that the orders of λ_i are finite. It follows that

$$d^{|\lambda_i|} = \lambda_i^{n|\lambda_i|} = 1,$$

so that $|d| = m$ divides $|\lambda_i|$ for all $i = 1, 2, \ldots, n$ and therefore $m \in \{1, p\}$. Let ν be a primitive solution of the equation $x^{mn} = 1$. Then ν^n is a primitive solution of the equation $x^m = 1$ and we can write $d = (\nu^n)^k$. Since the order $|d|$ is m, k and m must be co-prime. Let λ be a solution of the equation $x^n = d$. Then $\lambda^{mn} = d^m = 1$, so $\lambda = \nu^s$. Since $\nu^{sn} = \lambda^n = d = \nu^{kn}$, m divides $s - k$ and therefore $s = k + lm$, where l ranges over a complete remainder system modulo n. Let $r = |\lambda|$. As $1 = \lambda^r = \nu^{(k+lm)r}$, mn has to divide $(k + lm)r$. As k and m are co-prime, m divides r, $r = tm$ and n divides $(k + lm)t$.

Let n contain a prime factor q. Then $q|(k+lm)t$ for all l. If $n > 2$, there are $l_1 \neq l_2$, $0 \leq l_1, l_2 < n$ such that q does not divide $(k + l_i m)$, since otherwise we could find l_1, l_2 such that q divides $(k + l_i m)$ and q does not divide $(l_2 - l_1)$. From this we would get $q|(l_2 - l_1)m$ which implies $q|m$ and $q|k$. This is a contradiction, since k and m are co-prime.

From the above we conclude that $n = 2$ or A has two eigenvalues with orders containing the prime factor q. This implies $q = p$ then $n = p^j$. For $j > 1$ we see from the above that p^2 divides t which is again a contradiction.

Thus we have proved that $n = 2$ or $n = p$.

For the second part of (2) let us first deal with the case $p = 2$. If $p = 2$, then $n = 2$. We have already seen that $d^2 = 1$. We have to exclude the possibility $d = -1$. It is obvious since $\lambda_{1,2} = \pm\sqrt{-1}$ have order 4.

Now let $p > 2$ and $n = p$. Then every solution of the equation $\lambda^p = d$ has order dividing p^2. If $d \neq 1$ then the order of λ is neither 1 nor p (as $\lambda^p = d \neq 1$) so that all the solutions have orders p^2 which is a contradiction.

For the last statement of (2) one can easily verify that every transposition gives an eigenvalue with an even order and therefore only one transposition is permitted. □

3.3 On monomial groups with p-property

We restrict our attention now to monomial matrix groups. We state some remarks on the previous results connected to this subject. The letter $\mathcal{G}$ will denote a monomial matrix group with p-property. For a matrix A we will often make no distinction between P_A and its associated permutation π.

Remark 1. If $p \neq 2$ and $\mathcal{G}$ contains a matrix A with a transposition in its P_A, then P_{A^p} is a permutation matrix of the transposition and $-1 \in \sigma(A)$. We got the equivalence:

$$P_{\mathcal{G}} \text{ contains no transposition} \Leftrightarrow -1 \notin \sigma(\mathcal{G})$$

Remark 2. By the discussion given below one could see that transpositions are possible only in the cases $n = 2$ or $n = 3$ with $p = 3$. In both cases we have examples:

Case $n = 2$:

$$\mathcal{G}_2 = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid (ab)^p = 1 \right\} \cup \left\{ \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix} \mid (ab)^p = 1 \right\}$$

Case $n = 3$, $p = 3$:

$$\mathcal{G}_3 = \left\{ DP \mid P \in S_3\,,\ D = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix}\,,\ abc = 1\,,\ a, b, c \in \mathcal{Z}_3 \right\}$$

Let $\mathcal{G} \subset \mathrm{GL}_n(F)$ be irreducible with $n > 2$ and $p > 2$. Assume that $P_\mathcal{G}$ contains a transposition. After a conjugation with a suitable permutation the matrix $P_\mathcal{G}$ contains the transposition $\tau = (12)$. Irreducibility of the group $\mathcal{G}$ implies transitivity of the permutation group $P_\mathcal{G}$ and we can find such a matrix $Y \in \mathcal{G}$ that $P_Y(1) \notin \{1, 2\}$ an thus

$$(12) \neq P_Y \tau P_Y^{-1} \in P_\mathcal{G}.$$

We have found another transposition $\tau' \neq \tau$ in $P_\mathcal{G}$. If τ and τ' are disjoint we get a matrix with two transpositions in $P_\mathcal{G}$ which is a contradiction. The remaining possibility is that the product $\tau\tau'$ is a 3-cycle which means $p = 3$.

Let us now analyze the case $p = 3$ and $n > 3$. We can assume that $P_\mathcal{G}$ contains the transposition $\tau = (12)$ and a permutation π with 3-cycle (otherwise we would need another disjoint transposition for irreducibility). After a conjugation with a suitable permutation from $P_\mathcal{G}$ we can assume that π is of the form $(1bc)$.... If $2 \notin \{b, c\}$ by conjugation with a permutation π we either get $\tau' = (b2) \in P_\mathcal{G}$ (if π fixes 2) and $(12)(b2) = (12b) \in P_\mathcal{G}$ or with τ disjoint transposition τ' which is a contradiction. Thus we can assume that the 3-cycle (123) is contained in $P_\mathcal{G}$. Since $P_\mathcal{G}$ is transitive, we find such a permutation $\rho \in P_\mathcal{G}$ that $\rho(1) = 4$. Otherwise the conjugation with ρ would give us a transposition disjoint with τ' and we have $\rho(2) \in \{1, 2\}$. If $\rho(2) = 1$ then $\rho = (142)...$, $(12)\rho = (14)...$ and thus $(14) \in P_\mathcal{G}$. We get

$$(14)\pi = (1234...)...$$

which is a contradiction by Lemma 3.13. As the assumption $(14) \in P_\mathcal{G}$ yields a contradiction, in the case $\rho(2) = 2$ we get $\rho = (14j)\ldots$, where $j \neq 1, 2$. It follows that

$$(12)\rho = (14j2...)...$$

which again is a contradiction by Lemma 3.13.
We now give a criterion for irreducibility of monomial groups by which one can get irreducibility of the above groups $\mathcal{G}_2$ and $\mathcal{G}_3$. Let us first state a lemma.

Lemma 3.14 *Let $\mathcal{G} \subset \mathbb{F}^{n\times n}$ be a monomial group with transitive group $P_\mathcal{G}$ and let $V \leq \mathbb{F}^n$ be a $\mathcal{G}$-module. Then there exists a vector $v = (v_1, \ldots, v_n) \in V$ with $v_i \neq 0$ for all i.*

Proof. Assume that $v = (v_1, \ldots, v_{k-1}, 0, v_{k+1}, \ldots, v_n) \in V$. Since $P_\mathcal{G}$ is transitive there is a vector $w \in V$ with $w_k \neq 0$. For $n \in \mathbb{N}$ large enough the vector $nv + w$ has at least one more nonzero component as the vector v, so we reach the desired vector inductively. □

For a monomial group $\mathcal{G}$ we denote by $D_\mathcal{G}$ the subgroup of all diagonal matrices.

Proposition 3.15 *Let $\mathcal{G} \subset \mathbb{F}^{n\times n}$ be a monomial group with transitive $P_\mathcal{G}$. If the linear span of $D_\mathcal{G}$ is n-dimensional, then $\mathcal{G}$ is irreducible.*

Proof. If $D_1, \ldots, D_n \in D_\mathcal{G}$ are linearly independent and $v \in \mathbb{F}^n$ a vector with nonzero components (provided by Lemma 3.14), then it is easy to check that $D_1 v, \ldots, D_n v$ span $\mathbb{F}^n$. □

By the Proposition 3.15 the groups $\mathcal{G}_2$ and $\mathcal{G}_3$ from Remark 2 are irreducible.

Lemma 3.16 *Let $\mathbb{F}$ be an algebraically closed field, $\mathcal{G} \subset \mathbb{F}^{n\times n}$ an irreducible group and $\mathcal{K} \triangleleft \mathcal{G}$ an abelian subgroup such that the quotient $\mathcal{G}/\mathcal{K}$ is an abelian group. If $n > 1$, then the group $\mathcal{G}$ is imprimitive.*

Proof. Let $\mathcal{Z}$ be the center of the group $\mathcal{G}$. Since $\mathcal{G}$ is an irreducible group and $\mathbb{F}$ is algebraically closed, we have $Z = \mathcal{G} \cap \mathbb{F}\{I\}$. If $\mathcal{K} \subset \mathcal{Z}$, then $\mathcal{G}$ is nilpotent and by Theorem 3.10 monomial.
If $\mathcal{K} \not\subset \mathbb{F}\{I\}$ then by Corollary 3.8 $\mathcal{G}$ is imprimitive. □

Let $\mathcal{G}$ be a matrix group with p-property. Then $\det^p : \mathcal{G} \to F$ is a homomorphism of groups. Let $\mathcal{K}$ denote the kernel of this homomorphism. By Lemma 3.13

$$\mathcal{K} = \{A \in \mathcal{G} | \sigma(A) \subset \mathcal{Z}_p\}.$$

Proposition 3.17 *Let $\mathcal{G}$ be an irreducible monomial matrix group with p-property. For $p > 2$ we assume in addition that matrices in $P_{\mathcal{G}}$ are without transpositions (the latter assumption is necessary in the cases described in Remark 2.). Then $\mathcal{G} = \mathcal{K}$ or $\mathcal{G}$ is one-dimensional.*

PROOF. If $\mathcal{G}$ is a diagonal matrix group, it is one-dimensional. Thus we assume that $\mathcal{G}$ contains some nondiagonal matrices. Then $P_{\mathcal{G}}$ is a nontrivial group. Since all elements of $P_{\mathcal{G}}$ have order p, the group $P_{\mathcal{G}}$ is a p-group and has nontrivial center $\mathcal{Z}$. If $\mathcal{Z}$ contains a matrix of the form

$$U = \begin{bmatrix} I & 0 \\ 0 & B \end{bmatrix}$$

where I is the identity matrix and B is the permutation matrix of the product of disjoint p-cycles, it is easy to see that the subspace associated with the block I is invariant under $\mathcal{G}$. Though we can find (if we suitably rearrange the basis) a matrix $U \in Z$ of the form

$$U = \begin{bmatrix} C & & & \\ & C & & \\ & & \ddots & \\ & & & C \end{bmatrix}$$

where C is the permutation matrix of the p-cycle. One can easily show that every other matrix $X \in P_{\mathcal{G}}$ has the block-form

$$X = \begin{bmatrix} X_{11} & \cdots & X_{1n} \\ \vdots & & \vdots \\ X_{n1} & \cdots & X_{nn} \end{bmatrix}$$

with $X_{ij} = \varepsilon_{ij} C^{k_{ij}}$, $k_{ij} \geq 0$ where $[\varepsilon_{ij}]_{i,j}$ is a permutation matrix.
Recall the natural homomorphism $\phi : \mathcal{G} \to P_{\mathcal{G}}$ and pick a matrix $\tilde{U} \in \phi^{-1}(U)$. Since $\tilde{U}$ consists of $(p \times p)$-blocks associated with p-cycles in U, by Lemma 3.13 $\tilde{U}$ lies in $\mathcal{K}$. If $A \in \mathcal{G}$ is a diagonal matrix, $A\tilde{U}$ also consists of $(p \times p)$-blocks so $A\tilde{U} \in \mathcal{K}$ and $A \in \mathcal{K}$. As A^p is a diagonal matrix for every $A \in \mathcal{G}$, $A^p \in \mathcal{K}$ and $\sigma(A)^p = \{1\}$. If $A \notin \mathcal{K}$ we can find $\lambda_1 \in \sigma(A)$ with $|\lambda_1| = p^2$. Since every $p \times p$-block in A gives us only eigenvalues in $\mathcal{Z}_p$, eigenvalue λ_1 must be on the diagonal part of the matrix A. According to the block-structure of $P_{\mathcal{G}}$ we can assume the following structures

of matrices A, $\tilde{U}$ and $A\tilde{U}$:

$$A = \begin{bmatrix} \lambda_1 & & & & & \\ & \lambda_2 & & & & \\ & & \ddots & & & \\ & & & \lambda_p & & \\ & & & & \ddots & \end{bmatrix},$$

$$\tilde{U} = \begin{bmatrix} 0 & \cdots & 0 & d_1 & & \\ d_2 & \ddots & & 0 & & \\ & \ddots & & \vdots & & \\ & & d_p & 0 & & \\ & & & & \ddots & \end{bmatrix},$$

$$A\tilde{U} = \begin{bmatrix} 0 & \cdots & 0 & d_1\lambda_1 & & \\ d_2\lambda_2 & \ddots & & 0 & & \\ & \ddots & & \vdots & & \\ & & d_p\lambda_p & 0 & & \\ & & & & \ddots & \end{bmatrix}.$$

By Lemma 3.13 we get $\lambda_1 d_1 \cdots \lambda_p d_p = 1$. As $d_1 \cdots d_p = 1$, we get $\lambda_1 \cdots \lambda_p = 1$ and $\lambda_1^p \cdots \lambda_p^p = 1$. Since the matrix A has p-property, the orders $|\lambda_2|, \ldots, |\lambda_p|$ cannot be p^2. Thus they are all equal to p and we get $\lambda_1^p = 1$, which is a contradiction. This completes the proof. □

Remark 3. Let us now assume that $\mathcal{G}$ is not necessarily irreducible, where $\mathcal{G}$ is not diagonal. If the center $\mathcal{Z}$ of $P_{\mathcal{G}}$, which is again nontrivial, contains a matrix

$$U = \begin{bmatrix} C & & & \\ & C & & \\ & & \ddots & \\ & & & C \end{bmatrix}$$

we proceed as in the proof of Proposition 3.17 to get $\mathcal{G} = \mathcal{K}$. Otherwise, we find a matrix

$$U = \begin{bmatrix} I & 0 \\ 0 & B \end{bmatrix} \in \mathcal{Z}$$

such that B is a product of disjoint p-cycles. We decompose a matrix $M \in P_{\mathcal{G}}$ according to the above block decomposition of U,

$$M = \begin{bmatrix} X & Y \\ Z & W \end{bmatrix}.$$

Since M and U commute, we get the condition

$$(B - I)Z = 0.$$

If $Z \neq 0$, we can find a vector e from the basis such that

$$Be = e$$

which is a contradiction, since B has no fixed points in our basis. Similarly we get $Y = 0$, so the group $\mathcal{G}$ is of the form

$$\mathcal{G} = \left\{ \begin{bmatrix} X_1 & 0 \\ 0 & X_2 \end{bmatrix} | X_1 \in \mathcal{G}^1,\, X_2 \in \mathcal{G}^2 \right\},$$

where $\mathcal{G}^1$ and $\mathcal{G}^2$ are monomial groups of smaller dimension than $\mathcal{G}$.
Now we can see inductively that a monomial group $\mathcal{G}$ with p-property can be put in the form

$$\mathcal{G} = \begin{bmatrix} D & 0 \\ 0 & K \end{bmatrix},$$

where D is a diagonal group and $\sigma(K) \subset \mathcal{Z}_p$.

According to the conclusions of Proposition 3.17 we now consider the case of an irreducible matrix group $\mathcal{G} \subset \mathbb{F}^{n\times n}$ with prime exponent p. In this case $\mathcal{G}$ is a nilpotent group and is therefore automatically monomial (see Theorem 3.10). Since $\mathcal{G}$ is irreducible its degree is a power of p, $n = p^k$. If $p = 2$, then $\mathcal{G}$ is one-dimensional (since it is commutative). What can be said about general p? In Examples 2.4 one can find an example of p-dimensional $\mathcal{G}$. Using tensor product we can construct groups with exponent p and arbitrary degree p^k.
The following proposition shows that in the case $p = 3$ and $k = 2$ this is the only possibility.

Proposition 3.18 *Let $\mathcal{G} \subset \mathrm{GL}_9(\mathbb{F})$ be an irreducible matrix group with exponent 3. Then $\mathcal{G}$ is conjugate to a tensor product $\mathcal{H} \otimes \mathcal{K}$, where $\mathcal{H}, \mathcal{K}$ are subgroups of the group*

$$\mathcal{P}_3 = \left\{ DC^k \mid k = 0, 1, 2,\ D = \begin{bmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{bmatrix},\ abc = 1\,,\ a^3 = b^3 = c^3 = 1 \right\}$$

and

$$C = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

PROOF. The group $\mathcal{G}$ is a monomial group with 3-property. Since $P_{\mathcal{G}}$ is a homomorphic image of the group $\mathcal{G}$, it has exponent 3. From the proof of Proposition 3.17 one can get $P_d = C \otimes I \in Z(P_{\mathcal{G}})$ and all the matrices of $P_{\mathcal{G}}$ are of the form $[\varepsilon_{ij} C^{k_{ij}}]_{i,j}$ where $[\varepsilon_{ij}]_{i,j}$ is a permutation matrix whose order divides 3. We conclude that every matrix $P \in P_{\mathcal{G}}$ takes the form

$$P = \begin{bmatrix} C^{k_1} & & \\ & C^{k_2} & \\ & & C^{k_3} \end{bmatrix} (I \otimes C^l). \tag{1}$$

Since $P_{\mathcal{G}}$ is transitive we find a matrix

$$\begin{bmatrix} & & I \\ C^m & & \\ & C^n & \end{bmatrix} \in P_{\mathcal{G}}.$$

After the conjugation with the matrix

$$\begin{bmatrix} I & & \\ & C^{2m} & \\ & & I \end{bmatrix}$$

we get $P_c = I \otimes C \in P_{\mathcal{G}}$. As $P_d \in P_{\mathcal{G}}$ we find a matrix $X \in \mathcal{G}$ of the form

$$X = \begin{bmatrix} d_1^1 & & & & & & & & \\ & d_2^1 & & & & & & & \\ & & d_3^1 & & & & & & \\ & & & d_1^2 & & & & & \\ & & & & d_2^2 & & & & \\ & & & & & d_3^2 & & & \\ & & & & & & d_1^3 & & \\ & & & & & & & d_2^3 & \\ & & & & & & & & d_3^3 \end{bmatrix} P_d.$$

From $X^3 = I$ we get $d_1 d_2 d_3 = 1$ and thus after the conjugation with the diagonal matrix

$$D = \begin{bmatrix} 1 & & & & & & & & \\ & d_2^1 & & & & & & & \\ & & d_2^1 d_3^1 & & & & & & \\ & & & 1 & & & & & \\ & & & & d_2^2 & & & & \\ & & & & & d_2^2 d_3^2 & & & \\ & & & & & & 1 & & \\ & & & & & & & d_2^3 & \\ & & & & & & & & d_2^3 d_3^3 \end{bmatrix}$$

we assume that $P_d \in \mathcal{G}$. (Note that a conjugation with a diagonal matrix doesn't change the associated group $P_{\mathcal{G}}$.) Using (1) we can write every $X \in \mathcal{G}$ as

$$X = \begin{bmatrix} D_1 C^{k_1} & & \\ & D_2 C^{k_2} & \\ & & D_3 C^{k_3} \end{bmatrix} (I \otimes C^l) \tag{2}$$

for some diagonal matrices D_i.

Assume first that $l = 1$ and denote $A_i = D_i C^{k_i}$. Then $A_3 A_2 A_1 = I$. Since $X P_d^s \in \mathcal{G}$, we see that

$$D_3 C^{k_1+s} D_2 C^{k_2+s} D_3 C^{k_3+s} = I \tag{3}$$

for $s = 0, 1, 2$. Let us define an action of the matrix C on the set of diagonal matrices by $D^C (= CDC^{-1})$. Then the condition (3) is equivalent to

$$D_3 D_2^{C^{m+s}} D_3^{C^{n+2s}} = I \tag{4}$$

where $m = k_3$ and $n = k_2 + k_3$. If we replace s by $s+1$ in the equation (4) and then multiply the resulting equation by the inverse of the equation (4), we get

$$(D_2^C D_2^{-1})^{C^{m+s}} (D_1^{C^2} D_1^{-1})^{C^{n+2s}} = I. \tag{5}$$

This implies

$$(D_2^C D_2^{-1})^{C^{2s}} (D_1^{C^2} D_1^{-1})^{C^{n-m}} = I. \tag{6}$$

Hence $D_2^C D_2^{-1}$ is a scalar matrix $(1/\omega)I$ and thus

$$D_2 = \beta D(\omega)$$

where

$$D(\omega) = \begin{bmatrix} 1 & & \\ & \omega & \\ & & \omega^2 \end{bmatrix}.$$

From the equation (5) we get $D_1 = \alpha D(\omega)$ and finally from (4) $D_3 = \gamma D(\omega)$. It follows that the associated diagonal matrix D_X for a matrix X is of the form

$$D_X = D(\omega) \otimes \begin{bmatrix} \alpha & & \\ & \beta & \\ & & \gamma \end{bmatrix}.$$

Hence

$$X = (D(\omega) \otimes \begin{bmatrix} \alpha & & \\ & \beta & \\ & & \gamma \end{bmatrix}) \begin{bmatrix} C^{k_1} & & \\ & C^{k_2} & \\ & & C^{k_3} \end{bmatrix} (I \otimes C) \qquad (7).$$

If $l \neq 1$ in the form (2) we multiply the matrix X with a matrix of the form (7) and apply our conclusions. It follows that every $X \in \mathcal{G}$ can be written as

$$X = (D(\omega) \otimes \begin{bmatrix} \alpha & & \\ & \beta & \\ & & \gamma \end{bmatrix}) \begin{bmatrix} I & & \\ & C^m & \\ & & C^n \end{bmatrix} (C^k \otimes C^l) \qquad (8).$$

It is now sufficient to show that 3 divides m and n. Assume otherwise. Since $P_d, P_c \in P_{\mathcal{G}}$, we can take $k = 0$ and $l = 0$ and choose

$$A = \begin{bmatrix} \alpha D(\omega) & & \\ & \beta D(\omega) & \\ & & \gamma D(\omega) \end{bmatrix} \begin{bmatrix} I & & \\ & C^m & \\ & & C^n \end{bmatrix} \in \mathcal{G}$$

where $m, n \in \{1, 2\}$. We can also find a matrix $F \in \mathcal{G}$ of the form

$$F = \begin{bmatrix} \delta D(\vartheta) & & \\ & \varepsilon D(\vartheta) & \\ & & \varphi D(\vartheta) \end{bmatrix} \begin{bmatrix} & & I \\ I & & \\ & I & \end{bmatrix}.$$

From $F^3 = I$ we get

$$\delta\varepsilon\varphi = 1. \qquad (9)$$

By Burnside's theorem (Theorem 1.3) a matrix group $\mathcal{G} \subset \mathbb{F}^{n\times n}$ is irreducible if and only if its linear span is $\mathbb{F}^{n\times n}$. The only matrices in $\mathcal{G}$ whose linear combinations have nonzero entries at places $11, 22, 33$ are those of the form

$$X = \begin{bmatrix} \lambda D(\psi) & & \\ & \mu D(\psi) & \\ & & \nu D(\psi) \end{bmatrix} \begin{bmatrix} I & & \\ & C^k & \\ & & C^l \end{bmatrix}. \qquad (10)$$

As $(FA)^3 = I$, we have

$$\alpha\beta\gamma(\omega\vartheta)^m = 1. \tag{11}$$

Similarly $(FA^2)^3 = I$ implies

$$\alpha^2\beta^2\gamma^2(\omega^2\vartheta)^2 m = 1. \tag{12}$$

From equations (12) and (11) then follows $\omega^m = 1$, and hence

$$\omega = 1.$$

If we take a matrix of the form (10), where $m = n = 0$, then the matrix AX has the property established for the matrix A and thus $\psi = 1$. Since all entries at places $11, 22, 33$ are equal for all matrices in the group $\mathcal{G}$, it is not irreducible which is a contradiction. This completes the proof. □

Remark 4. It is easy to see that in the case of an arbitrary prime number p every irreducible group $\mathcal{G} \subset \mathrm{GL}_p(F)$ with exponent p is a subgroup of the group

$$\mathcal{G}_p = \left\{ DP \mid D = \begin{bmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \ddots & \\ & & & \lambda_p \end{bmatrix},\ \lambda_i^p = 1, \lambda_1 \cdots \lambda_p = 1\,,\ P = C^l \right\}$$

where C is the permutation matrix associated with the cycle $(12\ldots p)$.

3.4 Main theorem

Theorem 3.19 *Let $\mathcal{G} \subset \mathbb{F}^{n\times n}$ be a group of matrices over an algebraically closed field $\mathbb{F}$ with characteristic zero. If $\mathcal{G}$ has 2-property, then it is triangularizable.*

Proof. We can assume that $\mathcal{G}$ is irreducible. We now show that $\mathcal{G}$ is one-dimensional.

Let us first show that $\mathcal{G}$ is a monomial group. We have already seen that the natural homomorphism of groups

$$\det{}^2 : \mathcal{G} \to F^*$$

has the kernel $\mathcal{K} = \operatorname{Ker} \det^2$ consisting of matrices with eigenvalues $1, -1$. By Clifford's theorem (Theorem 3.5) we have a decomposition $\mathbb{F}^n = L_1 \oplus \cdots \oplus L_t$, where

each L_i is an irreducible $\mathcal{K}$-module. Since a group of matrices with eigenvalues $1, -1$ is triangularizable (see Theorem 2.8), we get $\dim L_i = 1$, so $\mathcal{K}$ is diagonalizable and therefore commutative. By Proposition 3.4 there exist systems of imprimitivity

$$F^n = Q_1 \oplus \cdots \oplus Q_t$$

where the stabilizers $\mathcal{G}_i$ of Q_i are primitive irreducible groups. Since $\mathcal{G}_i$ satisfy the conditions of the theorem, by the above we can find normal abelian groups $\mathcal{K}_i \triangleleft \mathcal{G}_i$ such that $\mathcal{G}_i/\mathcal{K}_i$ are abelian. Lemma 3.16 implies that $\dim Q_i = 1$ and $\mathcal{G}$ is indeed a monomial group.
By Proposition 3.17 we know that $\mathcal{G} = \mathcal{K}$ or $\mathcal{G}$ is one-dimensional. In both cases $\mathcal{G}$ is commutative and therefore one-dimensional. This completes the proof. □

Proposition 3.20 *Let $\mathcal{G}$ from Theorem 3.19 be without $\mathbb{Q}$-transcendent eigenvalues and assume that $\mathcal{G}$ has already been triangularized. For $X \in \mathcal{G}$ we denote by $d_i(X)$ the i^{th} diagonal entry of the matrix X and $\mathcal{D}_i = d_i(\mathcal{G})$. Then for $i \neq j$ an arbitrary pair $\lambda \in \mathcal{D}_i$ and $\mu \in \mathcal{D}_j$ satisfies the condition $d(\lambda, \mu) \leq 2$, i.e., the condition on orders holds "all over" the group $\mathcal{G}$, not just matrix-wise which was the original assumption.*

Proof. Let us choose $X, Y \in \mathcal{G}$ with $d_i(X) = \lambda$, $d_j(X) = \nu$, $d_i(Y) = \vartheta$, $d_j(Y) = \mu$, $|\lambda| = p$, $|\nu| = q$, $|\vartheta| = r$ and $|\mu| = s$.
We already know that for every matrix $W \in \mathcal{G}$ the eigenvalues of W^2 have pairwise prime orders. As

$$Z = (X^q Y^r)^2,$$

we get $d_i(Z) = (\lambda^2)^q$ and $d_j(Z) = (\mu^2)^r$. Since $|(\lambda^2)^q| = |\lambda^2|$, $|(\mu^2)^r| = |\mu^2|$, $d(d_i(Z), d_j(Z)) = 1$, the orders $|\lambda^2|$ and $|\mu^2|$ are prime, and therefore $d(|\lambda|, |\mu|) \leq 2$.
□

4 PERMUTATION-LIKE MATRIX GROUPS

4.1 Introduction

In previous chapters we discussed various questions of the type: Let $\mathcal{G}$ be a matrix (semi)group and assume that each matrix has a property which reveals the best in some canonical form of this matrix (in our cases we considered the upper triangular form). Can all matrices of $\mathcal{G}$ be simultaneously put in this form, i.e., can we find an invertible matrix $S \in \mathbb{C}^{n\times n}$ such that for all $X \in \mathcal{G}$ the matrix SXS^{-1} is in this canonical form?

In this chapter we discuss this question for permutation matrices.

Definition 4.1 Let $\mathcal{G} \leq \mathbb{C}^{n\times n}$ be a finite group of matrices. If every $X \in \mathcal{G}$ is similar to a permutation matrix, then $\mathcal{G}$ is called a *permutation-like group.* $\diamond$

The central question: Is a permutation-like group equivalent to a group of permutation matrices, i.e., can we find an invertible matrix $S \in \mathbb{C}^{n\times n}$ such that for all $X \in \mathcal{G}$ the matrix SXS^{-1} is a permutation matrix?

In Section 4.2 we familiarize ourselves with the topic by giving various examples of permutation-like groups. These examples shows us that the answer to this question is not always affirmative.

The counterexamples that we construct lead us to the additional assumption that the group $\mathcal{G}$ contains a *maximal cycle*, i.e., a matrix C corresponding to the cycle $\gamma = (123\ldots n) \in S_n$. We can choose a basis $B = \{f_0, f_1, \ldots, f_{n-1}\}$, in which C takes the form

$$C = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & \ddots & & 0 \\ 0 & \ddots & \lambda^2 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & \lambda^{n-1} \end{bmatrix},$$

where λ is a primitive n-th root of the unity. Under this assumption the only possible commutative permutation-like group is the cyclic group

$$\mathcal{G} = < C >$$

which is clearly equivalent to a group of permutation matrices. This is shown in Proposition 4.11.

In Section 4.3 we prove that Sylow p-subgroups of a permutation-like group $\mathcal{G} \subset \mathbb{C}^{n\times n}$ for $p > \frac{n}{2}$ are cyclic which coincides with the property of such Sylow subgroups of the symmetric group S_n (consider the order of S_n).

A useful object that we investigate in Section 4.4 is the *normalizer* $N(< C >)$. If n is a prime number, the subgroup $N(< C >)$ is equivalent to a group of permutation matrices, by Theorem 4.15.

The complete analysis of the cases $n = 2, 3$ is given in Section 4.5.

In Section 4.6 we consider the cases $n = 4, 5$. In the case $n = 4$ the answer to the main question is affirmative provided that the group $\mathcal{G}$ contains a maximal cycle. The first example of Section 4.2 shows the opposite if a maximal cycle is absent. At the end we show that every permutation-like group $\mathcal{G} \subset \mathbb{C}^{5\times 5}$ is equivalent to a group of permutation matrices.

For $n \geq 6$ examples from Section 4.2 show that for an affirmative answer we have to add some assumptions. One of possible conjectures would be:

Conjecture: *A permutation-like group $\mathcal{G} \subset \mathbb{C}^{n\times n}$ containing a maximal cycle is equivalent to a group of permutation matrices.*

This problem turns out to be more difficult as it seemed, so that with the present tools we managed to give the complete answer only for $n \leq 5$.

In the sequel we will use the next notation. Let $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_k > 1$ and $\alpha_1 + \alpha_2 + \cdots + \alpha_k \leq n$. Then the multiindex $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_k)$ determines the cyclic structure of a permutation from the symmetric group S_n. According to this we denote by $\mathcal{C}_\alpha \subset \mathcal{G}$ the subset of all matrices in $\mathcal{G}$ that are similar to the permutation matrix associated with α. Additionally, we define $\mathcal{C}_0 = \{I\}$, $\mathcal{C}_\alpha^0 = \mathcal{C}_\alpha \cup \mathcal{C}_0$, and by m_α we denote the cardinality of $\mathcal{C}_\alpha$.

It is the well-known fact that every finite group is equivalent to a group of unitary matrices, so we can assume in the sequel that our group consists of unitary matrices.

In [1] we find the next proposition which turns out to be very useful for our problem.

Proposition 4.2 *If the sum of all the matrices from some finite matrix group $\mathcal{G} \subset \mathbb{C}^{n\times n}$ is nonzero, then all the matrices from $\mathcal{G}$ have a common fixed point, i.e., there exists a non-zero vector $e \in \mathbb{C}^n$ such that*

$$Xe = e$$

for all $X \in \mathcal{G}$.

Proof. Let

$$S = \sum_{X\in\mathcal{G}} X \neq 0$$

be the sum of all the matrices in $\mathcal{G}$. Then we find a vector f such that $e = Sf \neq 0$. Since $\mathcal{G}$ is a group, for $X \in G$ we have $XS = S$ and therefore

$$Xe = XSf = Sf = e.$$

□

4.2 Examples

We first show that the answer to the central question is negative in general.

Example 4.3 *Let $m \geq l > 1$. There is a permutation-like group $\mathcal{G} \subset \mathbb{F}^{2m\times 2m}$ such that it contains a cycle of length $2l-1$ ($\mathcal{C}_{2l-1} \neq \emptyset$) and is not equivalent to a group of permutation matrices.*

Proof. Let $n = 2m$ and $N = 2l$ be even numbers with $m, l > 1$ and ω a primitive root of degree $N-1$. For $i \in \mathbb{Z}$ we define

$$B_i = \begin{bmatrix} \omega^i & \\ & \omega^{-i} \end{bmatrix}$$

and

$$T_0 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

We construct matrices $C, T \in \mathbb{C}^{n\times n}$

$$C = \begin{bmatrix} I & & & \\ & B_0 & & \\ & & \ddots & \\ & & & B_{l-1} \end{bmatrix}$$

and

$$T = \begin{bmatrix} T_0 & & \\ & \ddots & \\ & & T_0 \end{bmatrix},$$

where I is the $(n-N)\times(n-N)$ identity matrix. Then the matrix C corresponds to an $(N-1)$-cycle and the matrix T to a product of m disjoint transpositions. Since $TC = C^{-1}T$, every element of group $\mathcal{G}$, generated by the matrices T and C, is either of the form TC^k or C^k. It is easy to see that the matrices of the form TC^k correspond to a product of m disjoint transpositions, while the matrices C^k are similar to powers of a cycle of length $(N-1)$. Therefore $\mathcal{G}$ is indeed a permutation-like group.

Suppose that $\mathcal{G}$ is equivalent to a group of permutation matrices, where T corresponds to the permutation σ and TC to the permutation σ'. We have already mentioned that each of σ and σ' is a product of m disjoint transpositions. The product $T\cdot(TC) = C$ then corresponds to the product $\sigma\sigma'$ and is on the other hand clearly similar to a $(N-1)$-cycle γ which has an odd number of fixed points. Let a be a fixed point of the cycle γ. Since the permutations σ and σ' have no fixed points, σ' must contain a transposition (ab). Since a is a fixed point of the product $\sigma\sigma'$, it follows that $\sigma(b) = a$. This yields that σ contains the transposition (ba) which forces b to be another fixed point of the product $\sigma\sigma'$. Therefore fixed points of the product $\sigma\sigma'$ appears in pairs and thus the number of them is even. Since γ has odd number of fixed points, this is a contradiction and $\mathcal{G}$ is not equivalent to a group of permutation matrices. □

Permutation-like groups of exponent 2:

Let $\mathcal{G}$ be a permutation-like group of involutions, i.e., $X^2 = I$ for every matrix $X \in \mathcal{G}$. This assumption implies that $\mathcal{G}$ is a commutative group and each of its matrices is similar to a product of disjoint transpositions.

Consider first a pair of commuting permutations $\tau, \sigma \in S_n$ under the assumption that both of them are products of disjoint transpositions. We assume that τ contains the transposition (12). If 1 and 2 are fixed points of σ, or σ also contains (12), we can restrict ourselves to the set $\{3, 4, \ldots, n\}$.
In the remaining case let σ contain a transposition $(1a)$ with $a \neq 1, 2$. We get $(\tau\sigma)(a) = 2$. The transposition $(2a)$ is therefore contained in $\tau\sigma = \sigma\tau$. From $\tau(a) = b \neq 2$ we get $\sigma(b) = \sigma(\tau(a)) = 2$ which yields that σ contains the transposition $(2b)$. Therefore for some $a \neq b$ we have

$$\tau = (12)(ab)\cdots$$

and

$$\sigma = (1a)(b2)\cdots.$$

We conclude that the transpositions from τ and σ that intersect, but are not equal, appear in pairs which will be called the *conjugated pairs*. We notice that the conjugated pairs commute and their product is the third remaining conjugated pair. We have proved the following lemma.

Lemma 4.4 *Let σ and τ be permutations of order 2, where the disjoint transpositions $P_1, P_2, \ldots$ form σ and the disjoint transpositions $Q_1, Q_2, \ldots$ form τ. We interpret a transposition $T = (ab)$ also as set $\{a, b\}$. Permutations σ and τ commute if and only if for each P_i with property*

$$\emptyset \neq P_i \cap Q_j \neq P_i,$$

for some j, there exist transpositions P_k and Q_l satisfying the condition

$$P_i \cup P_k = Q_j \cup Q_l.$$

Example 4.5 *For $n \geq 8$ there exists four generator group $\mathcal{G} \subset \mathbb{F}^{n\times n}$ of exponent 2, which is not equivalent to a group of permutation matrices.*

Proof. Let $A_0, B_0, C_0, D_0 \in \mathcal{G} \subset \mathbb{C}^{8\times 8}$ be the diagonal matrices with the diagonals

$$d(A_0) = (-1, -1, -1, -1,\ \ 1,\ \ 1,\ \ 1,\ \ 1),$$

$$d(B_0) = (\ 1, -1, -1, -1, -1,\ 1,\ 1,\ 1),$$

$$d(C_0) = (\ 1,\ 1, -1, -1,\ 1,\ 1,\ 1,\ 1)$$

and

$$d(D_0) = (\ 1,\ 1,\ 1, -1, -1,\ 1,\ 1,\ 1).$$

We define the diagonal matrices $A, B, C, D \in \mathcal{G} \subset \mathbb{C}^{n\times n}$,

$$A = A_0 \oplus I_1 \oplus (-I_2),$$

$$B = B_0 \oplus I_1 \oplus (-I_2),$$

$$C = C_0 \oplus I_1 \oplus (-I_2)$$

and

$$D = D_0 \oplus I_1 \oplus (-I_2),$$

where I_2 is the identity matrix of degree $m = [(n-8)/2]$ and I_1 is the identity matrix of degree $n-8-m$. It is easy to verify that $\mathcal{G}$ is a permutation-like group of exponent 2. Suppose that $\mathcal{G}$ is equivalent to a group of permutation matrices, where matrices A, B, C, D correspond to the commuting permutations $\alpha, \beta, \gamma, \delta$, respectively. Clearly the number of $'-1'$ on the diagonal of each of the matrices is equal to the number of the disjoint transpositions that form the corresponding permutation. The permutations α and β are therefore products of $4+m$ disjoint transpositions, while the permutations γ and δ consist of $m+2$ disjoint transpositions. We assume that

$$\alpha = (1,2)(3,4)(5,6)(7,8)(9,10)\cdots(8+2m-1, 8+2m).$$

Since α, β, γ and δ commute, Lemma 4.4 implies that in the case $n = 8+2m+1$ the point n is fixed also by β, γ and δ. Therefore we restrict ourselves to the case of even degree $n = 8+2m$. For the product AB corresponds to a product of two disjoint transpositions, permutation β contains $m+2$ transpositions from α and one conjugate pair of the transpositions from α. By symmetry we can assume that

$$\beta = (1,2)(3,4)(5,7)(6,8)(9,10)\cdots(8+2m-1, 8+2m).$$

The permutation γ is a product of $m+2$ disjoint transpositions and each of the permutations $\alpha\gamma$ and $\beta\gamma$ is a product of two disjoint transpositions. If γ contains

some conjugate pair form α, the product $\gamma\alpha$ has at least four disjoint transpositions. Therefore the set of the transpositions forming γ is contained in the set of the transpositions forming α. In the same fashion we conclude that the set of the transpositions forming γ is contained in the set of the transpositions forming β. It follows that

$$\gamma = (1,2)(3,4)(9,10)\cdots(8+2m-1, 8+2m).$$

Since the matrix BD corresponds to a product of two disjoint transpositions, permutation δ contains exactly $m+2$ transpositions from β. Therefore we get δ by 'erasing' two transpositions, say T_1 in T_2, from β. Let us denote

$$\Gamma = \{(1,2), (3,4), (9,10), \ldots, (8+2m-1, 8+2m)\}.$$

We show that we cannot choose δ satisfying the above conditions.

1. Suppose that $T_1 = (5,7)$ (or $T_1 = (6,8)$). Since α and δ commute we get $T_2 = (6,8)$ (or $T_2 = (5,7)$). Then $\alpha\delta = (5,6)(7,8)$ which is a contradiction, as AD corresponds to a product of four disjoint transpositions.

2. In the remaining case we have $T_1, T_2 \in \Gamma$. This yields

   $$\delta = (5,7)(6,8)P_1P_2\cdots P_m,$$

   where P_i are from set Γ, i.e.,the set of the transpositions forming permutation γ. Then the product $\delta\gamma$ contains four disjoint transpositions which again is a contradiction since CD corresponds to a product of two disjoint transpositions.

□

Proposition 4.6 *Every permutation-like group isomorphic to Klein quadruple is equivalent to a group of permutation matrices.*

Proof. In this case $\mathcal{G}$ is the group of exponent 2, generated by two matrices. Let us write the block decomposition of the two generators of $\mathcal{G}$

$$A = -I_1 \oplus -I_2 \oplus I_3 \oplus I_4 \text{ and } B = -I_1 \oplus I_2 \oplus -I_3 \oplus I_4, \qquad \text{(blk)}$$

where I_1, I_2, I_3 and I_4 are the identity matrices of dimensions k, k', l and $l' = n - k - k' - l$, respectively. Suppose that the matrix A has the smallest trace in the group $\mathcal{G}$ and that the number of '-1' on the diagonal of A is d. Then $k + l \leq d$ and $l \leq d/2$, since otherwise AB would have smaller trace than A.

We now describe the construction of the permutations $\alpha, \beta \in S_n$ corresponding to the matrices A and B. Decompose the standard basis of $\mathbb{C}^n$ into the sets N_1, P_1, N_2, P_2 corresponding to the block decomposition (blk). Then N_2 has the smallest cardinality among the given sets. For $1 \leq i \leq l$ we form the quadruple Q_i consisting of i-th vector from N_1, i-th vector from P_1, i-th vector from N_2 and i-th vector from P_2. It is easy to see that the restriction of A onto the span $\mathbb{C}Q_i$ can be represented by a pair of disjoint transpositions and B with the conjugated pair. Therefore for every i we attach a pair of disjoint transpositions into α and the conjugated pair into β. Finally we join the remaining vectors of the basis into such pairs D_j that A acts on the span $\mathbb{C}D_j$ as transposition while B restricted onto $\mathbb{C}D_j$ either coincides with A or acts as the identity. It the first case we add the same transposition to both permutations α and β while in the later case we add a new transposition only to the permutation α.

This way we get a desired pair of commuting permutations, so that $\mathcal{G}$ is equivalent to a group of permutation matrices. □

Example 4.7 (T. J. Laffey) *For $n \geq 6$ there is a permutation-like group isomorphic to the quaternion group, which is not equivalent to a group of permutation matrices.*

Proof. Let I be the identity matrix of dimension $n-6$. The following representation of the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ consists of matrices individually similar to some permutation matrices.

$$M(i) = \begin{bmatrix} -1 & 0 & & & & & \\ 0 & 1 & & & & & \\ & & -i & 0 & & & \\ & & 0 & i & & & \\ & & & & 1 & 0 & \\ & & & & 0 & 1 & \\ & & & & & & I \end{bmatrix}$$

$$M(j) = \begin{bmatrix} -1 & 0 & & & & & & \\ 0 & 1 & & & & & & \\ & & 0 & 1 & & & & \\ & & -1 & 0 & & & & \\ & & & & 0 & 1 & & \\ & & & & 1 & 0 & & \\ & & & & & & I \end{bmatrix}$$

$$M(k) = \begin{bmatrix} 1 & 0 & & & & & & \\ 0 & 1 & & & & & & \\ & & 0 & -i & & & & \\ & & -i & 0 & & & & \\ & & & & 0 & 1 & & \\ & & & & 1 & 0 & & \\ & & & & & & I \end{bmatrix}$$

The group $\mathcal{G} \subset \mathbb{C}^{n\times n}$ generated by the matrices $M(i), M(j)$ and $M(k)$ is a permutation-like group isomorphic to the group Q. Suppose that $\mathcal{G}$ is equivalent to a group of permutation matrices. Then from the spectra of the matrices we conclude that $M(i)$ corresponds to a 4-cycle, say $\gamma_1 = (1234)$, $M(j)$ corresponds to a disjoint product of a 4-cycle, say γ_2, and a transposition, say τ_2, while $M(k)$ corresponds to a 4-cycle, say γ_3. Since $i^2 = j^2$ the cycles γ_1 and γ_2 act on the same set $\{1, 2, 3, 4\}$. It follows that the product $\gamma_1\gamma_2\tau_2$, corresponding to $ij = k$, contains a transposition τ_2, which is not possible since the matrix $M(k)$ corresponds to a 4-cycle. □

4.3 Sylow subgroups in a permutation-like group

In this section we show that for $p > \frac{n}{2}$ the Sylow p-groups of a permutation-like group are cyclic, which is also the case in the symmetric group S_n. We use the well-known facts which can be found in [23, p. 78-80].

Lemma 4.8 *Let $\mathcal{G} \subset \mathbb{C}^{n\times n}$ be a permutation-like group, $p \leq n$ a prime number and $\mathcal{H} \subset \mathcal{C}_p^0$ a nontrivial subgroup of $\mathcal{G}$. Then $\mathcal{H}$ is a cyclic group.*

Proof. Since $\mathcal{H}$ is a nontrivial group, we can choose a basis for $\mathbb{C}^n$ such that $\mathcal{H}$ contains a matrix of the form

$$A = \begin{bmatrix} I & & & & \\ & \omega & & & \\ & & \omega^2 & & \\ & & & \ddots & \\ & & & & \omega^{p-1} \end{bmatrix},$$

where $\omega \in \mathbb{C}$ is a primitive p-th root of the unity and I the identity matrix of order $n-p+1$. Let us write an arbitrary matrix $X \in H \setminus < A >$ in the form

$$X = \begin{bmatrix} Y & * & * & * \\ * & x_1 & * & * \\ * & * & \ddots & * \\ * & * & * & x_{p-1} \end{bmatrix}.$$

We first show that

$$x_1 = \cdots = x_{p-1} = 0. \qquad \text{(zeros)}$$

Let us denote $y = \operatorname{tr}(Y)$. For $k = 0, 1, \ldots, p-1$ we have $A^k X \in \mathcal{C}_p$ which gives us the system of linear equations

$$\operatorname{tr}(A^k Y) = y + \omega^k x_1 + \omega^{2k} x_2 + \cdots + \omega^{(p-1)k} x_{p-1} = n - p,$$

having the unique solution, namely $y = n - p$ and $x_1 = \cdots = x_{m-1} = 0$.

Since $\mathcal{H}$ is a p-group and has nontrivial center, we may assume that the matrix A commutes with all the matrices from $\mathcal{H}$. Pick a matrix $X \notin < A >$ and decompose the matrices A and X in the fashion

$$A = \begin{bmatrix} I & \\ & D \end{bmatrix} \text{ and } X = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix},$$

where

$$D = \begin{bmatrix} \omega & & & \\ & \omega^2 & & \\ & & \ddots & \\ & & & \omega^{m-1} \end{bmatrix}.$$

Since the matrices A and X commute, we get $X_2 = X_2 D$, $DX_3 = X_3$ and $DX_4 = X_4 D$. As 1 is not an eigenvalue for D, it follows that $X_2 = 0$ and $X_3 = 0$. As D is a diagonal matrix with pairwise different diagonal entries, X_4 is a diagonal matrix. By (zeros) the diagonal entries of X_4 are zero, therefore $X_4 = 0$. The matrix X is then singular which is a contradiction. Therefore

$$\mathcal{H} = < A >$$

is indeed a cyclic group. □

Corollary 4.9 *Let $\mathcal{G} \subset \mathbb{C}^{n\times n}$ be a permutation-like group, $p > \frac{n}{2}$ a prime number and $\mathcal{S} \leq \mathcal{G}$ a Sylow p-subgroup of $\mathcal{G}$. Then:*
(a) The group $\mathcal{S}$ is a cyclic group of order p generated by some $A \in \mathcal{C}_p$.
(b) The group $\mathcal{G}$ has order

$$|\mathcal{G}| = p \cdot l,$$

where p does not divide l.

Proof. (a) Since $p > \frac{n}{2}$, we have $S \subset \mathcal{C}_p^0$ and so we can use (b) from Lemma 4.8.
(b) This is a basic fact following from Sylow's theorems (see [1]). □

4.4 Permutation-like groups with maximal cycles

In this section we consider permutation-like groups $\mathcal{G} \subset \mathbb{C}^{n\times n}$ containing a *maximal cycle*, i.e., a matrix $C \in \mathcal{C}_n$. If $\mathcal{G}$ is a permutation-like group, the sum of its matrices cannot be zero since the traces of all the matrices are nonnegative and the identity matrix $I \in \mathcal{G}$ has positive trace. Therefore by Proposition 4.2 we can write

$$\mathcal{G} = 1 \oplus \mathcal{G}'.$$

We can choose a basis $B = \{f_0, f_1, \ldots, f_{n-1}\}$ in which C takes the form

$$C = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & \ddots & & 0 \\ 0 & \ddots & \lambda^2 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & \lambda^{n-1} \end{bmatrix}, \tag{dia}$$

where λ is a primitive n-th root of the unity. In the same basis we have $\mathcal{G} = 1 \oplus \mathcal{G}'$, since the elements of the basis B are unique up to the scalar factors.

Lemma 4.10 *Let $\{f_0, f_1, \ldots, f_{n-1}\}$ be a basis in which a maximal-cycle matrix C takes the form (dia) and let*

$$e = \sum_{i=0}^{n-1} \beta_i f_i.$$

Then the set

$$B = \{C^k e | k = 0, 1, \ldots n-1\}$$

is a basis of the space $\mathbb{C}^n$ if and only if $\beta_i \neq 0$ for all i.

PROOF. It is clear that the set B is linearly dependent if some β_i is zero. We assume that all the coefficients β_i are nonzero. From

$$\sum_{j=0}^{n-1} \gamma_j C^j e = 0$$

we get

$$\sum_{i,j=0}^{n-1} \beta_i \gamma_j C^j f_i = \sum_{i,j=0}^{n-1} \beta_i \gamma_j \lambda^{ij} f_i = 0.$$

Since the coefficients at f_i vanish for all i, we conclude that

$$\sum_{j=0}^{n-1} \lambda^{ij} \gamma_j = 0.$$

This is possible if and only if all γ_j are zero coefficients. □

Remark: The matrix C takes its 'classical' permutation form in a basis B

$$C = \begin{bmatrix} 0 & \cdots & \cdots & 0 & 1 \\ 1 & \ddots & & & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{bmatrix} \qquad \text{(cyc)}$$

if and only if the basis B is given as $B = \{C^k e | k = 0, 1, \ldots n-1\}$ for some $e \in \mathbb{C}^n$.

We now show that every commutative permutation-like group containing a maximal cycle is equivalent to a group of permutation matrices.

Proposition 4.11 *Let $\mathcal{G}$ be a commutative permutation-like group containing a maximal cycle C. Then*

$$\mathcal{G} = < C > .$$

PROOF. Let $\lambda \in \mathbb{C}$ be a primitive n-th root of unity and pick any $X \in \mathcal{G}$. As C has no multiple eigenvalues and X commutes with C, X is a circulant, i.e.,

$$X = p(C),$$

for some polynomial $p(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$. Since each matrix from $\mathcal{G}$ is similar to a permutation matrix, for every $k \leq n-1$ we have

$$n a_k = \mathrm{tr}\,(C^{-k} X) = m_k,$$

where $m_k \leq n$ are nonnegative integers. It follows that $a_k = \frac{m_k}{n} \geq 0$. As X is a unitary matrix, we get

$$a_0 + a_1 + \ldots + a_{n-1} = |p(1)| = 1 = |p(\lambda)| = |a_0 + a_1\lambda + \ldots + a_{n-1}\lambda^{n-1}|.$$

It is easy to see that this is only possible in the case where $a_l = 1$ for some l, while for $k \neq l$ we have $a_k = 0$. Therefore

$$\mathcal{G} = \{I, C, C^2, \ldots, C^{n-1}\},$$

and it is clearly equivalent to a group of permutation matrices. □

Recall that the multiplicative group $\mathcal{Z}_n = \{\lambda^k | k \in \mathbb{Z}\}$ is isomorphic to the cyclic group $Z_n = \{0, 1, \ldots, n-1\}$. This group affords the structure of a commutative ring which is a field if n is a prime number.

Let C be a maximal cycle in a permutation-like group $\mathcal{G}$ and $X \in \mathcal{G} \backslash < C >$ a matrix with property $XC = C^k X$, or equivalently

$$XCX^{-1} = C^k.$$

Therefore C and C^k are similar matrices which means that C^k also represents a maximal cycle. This is possible if and only if k is a unit of the ring $\mathbb{Z}_n$.

Lemma 4.12 *Let $X \in \mathcal{G}$ be a matrix satisfying*

$$XC = C^k X,$$

for some unit $k \neq 1$ of the ring Z_n and let $l = k^{-1}$ be its inverse. Then $\pi(i) = il$ defines a permutation on the set Z_n. Let

$$\pi = \gamma_0 \cdot \gamma_1 \cdots \gamma_r$$

be a disjoint cycle decomposition for π and choose a basis in which C takes the form (dia). Then X is a monomial matrix of the form

$$X = D_0 P_0 \oplus D_1 P_1 \oplus \cdots \oplus D_r P_r,$$

where D_i are diagonal matrices and P_i the permutation matrices corresponding to the cycles γ_i. The multiplicative order of l coincides with the order of the permutation π.

PROOF. Let $f_0, f_1, \ldots, f_{n-1}$ be a basis such that C has the form (dia). From $(\lambda^k)^l = \lambda$ it follows that

$$C^k X f_i = XC f_i = \lambda^i X f_i = (\lambda^{il})^k X f_i,$$

therefore we find a scalar α such that

$$X f_i = \alpha f_{il}, \tag{mon}$$

since the eigenvalues $1, \lambda^k, \lambda^{2k}, \ldots, \lambda^{(n-1)k}$ of the matrix C^k are distinct. The multiplication by l defines a permutation π on the set $Z_n = \{0, 1, \ldots, n-1\}$ which fixes 0.

Let o be the multiplicative order of element l. The group $\{1, l, l^2, \ldots, l^{o-1}\}$ acts on the set Z_n, while the 'ordered' orbits of this action are exactly the disjoint cycles of π. Since the length of each orbit divides the degree of the acting group, we have $\pi = \gamma_0 \cdot \gamma_1 \cdots \gamma_r$, where γ_i are the cycles of lengths dividing o. It follows that

$$\pi^o = id.$$

The cycle corresponding to the orbit containing 1 has clearly length o which implies that o is exactly the order of the permutation π. Let P_i be the permutation matrix associated with the cycle γ_i. Then the permutation matrix P corresponding to the permutation π has the form

$$P = P_0 \oplus P_1 \oplus \cdots \oplus P_r.$$

By (mon) matrix X is monomial and we can write it as

$$X = D_0 P_0 \oplus D_1 P_1 \oplus \cdots \oplus D_r P_r.$$

□

Lemma 4.13 *Let*

$$X = \begin{bmatrix} 0 & \cdots & \cdots & 0 & a_1 \\ a_2 & \ddots & & & 0 \\ 0 & a_3 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_n & 0 \end{bmatrix} \in \mathbb{C}^{n \times n}$$

be a matrix similar to a permutation matrix P. Then we can choose a basis such that P is equal to C in the form (cyc). If we define

$$Q = \begin{bmatrix} \mu_1 & & & \\ & \mu_2 & & \\ & & \ddots & \\ & & & \mu_n \end{bmatrix},$$

with

$$\mu_i = \frac{1}{a_1 a_2 \cdots a_i},$$

it holds

$$QXQ^{-1} = C.$$

PROOF. We can write $X = DC$, where D is a diagonal matrix with the diagonal entries $(a_1, a_2, \ldots, a_n)$. Write $a = a_1 a_2 \cdots a_n$. Then the matrix X has the spectrum

$$\sigma(X) = \{z \in \mathbb{C} \mid z^n = a\}.$$

Since X is similar to a permutation matrix, its spectrum contains 1, and so $a = 1$. It follows that the matrix X is indeed similar to C. For $a = 1$ we get $\mu_n = 1$ and therefore $QXQ^{-1} = C$. □

Corollary 4.14 *Let n be a prime number, $\mathcal{G} \subset \mathbb{C}^{n\times n}$ a permutation-like group containing a maximal cycle C, and let $X \in \mathcal{G} \setminus < C >$ be a matrix satisfying*

$$XC = C^k X$$

for some $k \in \mathbb{N}$. Then there exist a basis B_{dia} and a basis B_{cyc} in which X takes the permutation form, while C has the form (dia) in the basis B_{dia} and the form (cyc) in the basis B_{cyc}. In the basis B_{dia} X corresponds to the permutation on Z_n given by the multiplication with k^{-1}, while in the basis B_{cyc} it corresponds to the multiplication by k. The order o of the element k is equal to the order of the permutation matrix X which is a product of, say p, disjoint cycles of length o and

$$p \cdot o = n - 1.$$

We can express the basis B_{cyc} in the form $B_{cyc} = \{e, Ce, C^2e, \ldots, C^{n-1}e\}$ for some $e \in \mathbb{C}^n$.

PROOF. Since $C \neq I$ we have $k \neq 0$. If $k = 1$ the group $< X, C >$ is commutative; therefore by Proposition 4.11 it follows that $X \in < C >$ which is a contradiction.
As n is a prime number, each $k \neq 0$ is a unit of the field Z_n and the group of units Z_n^* is a cyclic group. Let us write $l = k^{-1}$ and denote by o the order of l which is clearly equal to the order of k. By Lemma 4.12 it follows that the multiplication by l is a permutation $\pi = \gamma_0 \cdot \gamma_1 \cdots \gamma_r$ on the set Z_n having the fixed point 0. We can assume that $\gamma_0 = (0)$. Since Z_n^* is a group, it is easy to see that all the cycles $\gamma_1, \ldots, \gamma_r$ have length o.
Choose a basis B in which C takes the form (dia) and $\mathcal{G} = 1 \oplus \mathcal{G}'$. By Lemma 4.12 we can write X as

$$X = 1 \oplus D_1 P_1 \oplus \cdots \oplus D_r P_r.$$

Since P_i corresponds to the cycle γ_i, it holds $(P_i)^o = I$, and therefore

$$(X^o)' = (\det D_1) I \oplus (\det D_2) I \oplus \cdots \oplus (\det D_r) I,$$

where I is the identity matrix of dimension $o \times o$. As X^o is a diagonal matrix, it commutes with C and therefore by Proposition 4.11 we have $X^o = C^s$. From the block $(\det D_1)I$ of the matrix $(X^o)'$ we see that $\det D_1 = \lambda^s = \lambda^{ls}$ and therefore $s = ls$ which yields $s = 0$. We have proved that

$$X^o = I,$$

or $\det D_i = 1$ for all i. By Lemma 4.13 we can transform the matrix $D_i P_i$ into P_i using a diagonal similarity. Therefore there exists a diagonal similarity of the matrix X and the matrix $P = P_0 \oplus P_1 \oplus \cdots \oplus P_r$. Since a diagonal similarity doesn't change diagonal matrix C, the new basis satisfies the conditions for B_{dia}.
Let us write $B_{dia} = \{f_0, f_1, \ldots, f_{n-1}\}$. Then for $e = f_0 + f_1 + \cdots + f_{n-1}$ we have $Xe = e$, while the set $B = \{C^i e | i = 0, 1, \ldots n-1\}$ is a basis by Lemma 4.10. Since

$$X(C^i e) = C^{ki} X e = C^{ki} e,$$

X is a permutation matrix, therefore the basis B can be taken as B_{cyc}. □

Theorem 4.15 (**Normalizer theorem**) *Let n be a prime number, $\mathcal{G} \subset \mathbb{C}^{n \times n}$ a permutation-like group containing a maximal cycle C, and $\mathcal{N} = N(< C >)$ the*

normalizer of the group $< C >$. Then in a suitable basis $\mathcal{N}$ consists of permutation matrices. If $\mathcal{N} \neq < C >$ the group $\mathcal{N}$ is generated by C and some matrix $X_0 \in \mathcal{N} \setminus < C >$, therefore all the elements $X \in \mathcal{N}$ are of the form

$$X = C^r X_0^s.$$

The matrix X_0 corresponds to a product of disjoint cycles of length o, where o divides $n-1$.

PROOF. For arbitrary $X \in \mathcal{N}$ there is a uniquely determined $k \in Z_n^*$ with the property $XCX^{-1} = C^k$ which is equivalent to the already mentioned relation $XC = C^k X$. Pick $X_1, X_2 \in \mathcal{N}$. Then for $i = 1, 2$ we get $X_i C X_i^{-1} = C^{k_i}$ from what follows $X_1 X_2 C = C^{k_1 k_2} X_1 X_2$, so Z_n^* is in fact a homomorphic image of the group $\mathcal{N}$. Let $X_0 \in \mathcal{N} \setminus < C >$ be an element with the maximal order o and

$$X_0 C = C^k X_0.$$

Let for $X \in \mathcal{N} \setminus < C >$ be $XC = C^l X$. We write o for the order of k and r for the order of l. By the choice of X_0 we have $r \leq o$. Since Z_n^* is a cyclic group with the order $m = n - 1$, we get $k = a^p$, where $l = a^q$. Then

$$o = \frac{m}{d(p, m)}$$

and

$$r = \frac{m}{d(q, m)}.$$

We investigate the condition

$$l = k^t \tag{1},$$

which is equivalent to the condition

$$a^q = a^{pt} \tag{1'}.$$

The equation (1′) is satisfied if and only if $q - pt$ is divisible by m. Since $o \geq r$, we get $d = d(p, m) \leq d(q, m)$ and therefore we can write $m = m'd$, $p = p'd$ and $q = q'd$. Now (1′) holds if and only if $q' - p't$ is divisible by m'. As m' and p' have no common divisor, we can find numbers t and u such that $q' = p't + m'u$ what confirms our

hypothesis.
We denote by $P(\sigma)$ the permutation matrix associated with a permutation σ. Let π be the permutation on the set Z_n corresponding to the multiplication by k^{-1}. Pick a basis B_{dia} such that C has the form (dia) and $X_0 = P(\pi)$. Then we have

$$X = DP(\sigma),$$

where σ is the multiplication by $l^{-1} = k^{-t}$ and D a diagonal matrix. By (1) we get $\sigma = \pi^t$. It follows that $P(\sigma) = P(\pi)^t = X_0^t$, and therefore

$$D = XX_0^{-t} \in \mathcal{N}.$$

In the basis B_{dia} all the diagonal matrices of $\mathcal{N}$ are contained in $< C >$, and so $X \in \mathcal{N}X_0 \subset \mathcal{N}$ what implies

$$\mathcal{N} \subset < C, X_0 > .$$

If we choose a basis B_{cyc}, where matrices C and X_0 are both permutation matrices, then the group $\mathcal{N}$ consists of permutation matrices. By Corollary 4.14 we get the last claim of our theorem. □

4.5 Cases $n = 2, 3$

Recall that $\mathcal{C}_\alpha$ denotes the set of matrices from a permuation-like group corresponding to the permutation with cyclic structure given by multiindex α.
Case n=2: We assume that $\mathcal{G}$ is not a trivial group. It this case each nonidentity matrix corresponds to a transposition. For all $X \in \mathcal{G}$ we have $X^2 = I$. Therefore $\mathcal{G}$ is an abelian group and by Proposition 4.11 it is equivalent to a group of permutation matrices.

Case n=3:

Proposition 4.16 *Let $\mathcal{G} \subset \mathbb{C}^{3\times 3}$ be a permutation-like group. Then $\mathcal{G}$ is equivalent to a group of permutation matrices.*

PROOF. The group $\mathcal{G}$ is the union of the sets $\mathcal{C}_3$, $\mathcal{C}_2$ and $\mathcal{C}_0$.
Suppose that $\mathcal{C}_3 \neq \emptyset$. Since $3 > \frac{3}{2}$, the order of $\mathcal{G}$ can be written in the form

$$|\mathcal{G}| = 3 \cdot 2^l$$

by Corollary 4.9. If $\mathcal{C}_2 = \emptyset$, we get $|\mathcal{G}| = 3$ and $\mathcal{G} =< C >$. If $\mathcal{C}_2 = \emptyset$, it follows from Corolary 4.9 that $|\mathcal{G}| = 6$. Let $S =< C >$ be a Sylow 3-subgroup for some $C \in \mathcal{C}_3$. Since the number $1 + 3k$ of Sylow 3-subgroups divides the order $|\mathcal{G}|$, we get $k = 0$. It follows that Sylow subgroup $< C >$ is a normal subgroup of $\mathcal{G}$. Therefore

$$\mathcal{G} = N(< C >)$$

is equivalent to a group of permutation matrices by Theorem 4.15.
In the case $\mathcal{C}_3 = \emptyset$ the group $\mathcal{G} = \mathcal{C}_2^0$ is either trivial or $\mathcal{G} =< T >$ for some $T \in \mathcal{C}_2$. □

4.6 Cases $n = 4, 5$

Some tools for the case $\mathcal{C}_n \neq \emptyset$
Let $\mathcal{G} \subset \mathbb{C}^{n\times n}$ be a permutation-like group and let $C \in \mathcal{C}_n$ be a maximal cycle. Choose a basis in which C has the form (cyc). Since all the matrices from $\mathcal{G}$ have a common fixed point and each fixed point of the matrix C has to be a scalar multiple of the vector

$$e_0 = [1, \ldots, 1]^T$$

for each matrix $X \in \mathcal{G}$, we have $Xe_0 = e_0$. Therefore for arbitrary i we get

$$\sum_{k=1}^{n} x_{ik} = 1. \qquad \text{(row)}$$

For an integer k we define

$$s_k(X) = \operatorname{tr}(C^k X).$$

Then

$$\sum_{k=0}^{n-1} s_k(X) = \sum_{i,j=1}^{n} x_{ij},$$

and the property (row) implies

$$\sum_{k=0}^{n-1} s_k(X) = n. \tag{sum}$$

Since in permutation-like groups each matrix Y is similar to its inverse Y^{-1}, it follows that

$$s_{-k}(X^{-1}) = \mathrm{tr}\,(C^{-k}X^{-1}) = \mathrm{tr}\,(XC^k) = \mathrm{tr}\,(C^kX) = s_k(X)$$

If $X \in \mathcal{C}_{2,2,\ldots,2}$, i.e., X is a matrix satisfying $X^2 = I$ or $X^{-1} = X$, we get

$$s_k(X) = s_{-k}(X). \tag{sym}$$

Let the cyclic group $< C >$ act on $\mathcal{G}$ by the left multiplication, and write $\mathcal{O}(X)$ for the orbit of $X \in \mathcal{G}$. Then

$$\mathcal{O}(X) = \{X, CX, C^2X, \ldots C^{n-1}X\}.$$

If we choose a fixed point of the group $\mathcal{G}$ as the first vector of our basis, each subgroup $\mathcal{H} \leq \mathcal{G}$ decomposes as

$$\mathcal{H} = 1 \oplus \mathcal{H}'.$$

According to this we write the matrix $X \in \mathcal{G}$ as $X = 1 \oplus X'$ and for an integer k we define *reduced traces* by

$$s'_k(X) = \mathrm{tr}\,((C^kX)') = s_k(X) - 1.$$

Since the fixed point of C is determined up to a scalar multiple, the group $\mathcal{G}'$ is without fixed points, which gives us

$$\sum_{X \in \mathcal{G}} s'_0(X) = 0, \tag{sumg}$$

by Proposition 4.2. Let $\mathcal{G}_S$ be the subgroup of the 'even' (meant as similar to a permutation matrix associated with an even permutation) matrices in $\mathcal{G}$, and $\mathcal{G}_L$ be the subset of the 'odd' matrices. If n is an odd number, the matrix C corresponds to

an 'even' permutation and therefore the group $\mathcal{G}'_S$ has no fixed point. By Proposition 4.2 it follows that

$$\sum_{X \in \mathcal{G}_S} s'_0(X) = 0 \qquad \text{(evn)}$$

and consequently

$$\sum_{X \in \mathcal{G}_L} s'_0(X) = 0. \qquad \text{(odd)}$$

For $X \in \mathcal{G}$ we denote the unordered list of its traces by

$$\mathcal{T}r(X) = [s_0(X), s_1(X), \ldots, s_{n-1}(X)]$$

and the ordered list of its traces by

$$\mathrm{Tr}(X) = (s_0(X), s_1(X), \ldots, s_{n-1}(X)).$$

The properties (sum) and (sym) will in some cases help us to reduce the possibilities for the lists $\mathcal{T}r(X)$ and $\mathrm{Tr}(X)$.

Case n=4: Let $\mathcal{G} \subset \mathbb{C}^{4\times 4}$ be a permutation-like group containing a maximal cycle $C \in \mathcal{C}_4$. The set of the 'even' matrices is then the union of sets $\mathcal{C}_3$, $\mathcal{C}_{2,2}$ and $\mathcal{C}_0$, while the set of the 'odd' matrices splits into the sets $\mathcal{C}_4$ and $\mathcal{C}_2$. Let us write the table of the traces in the group $\mathcal{G}$

TYPE	$\mathcal{C}_2$	$\mathcal{C}_{2,2}$	$\mathcal{C}_3$	$\mathcal{C}_4$
s_0	2	0	1	0
s'_0	1	-1	0	-1

Table 1

Property (sumg) in this case implies

$$3 + m_2 - m_{2,2} - m_4 = 0, \qquad \text{(sum}')$$

where m_α denotes the cardinality of the set $\mathcal{C}_\alpha$. Let us denote $\mathcal{C}'_{2,2} = \mathcal{C}_{2,2} \setminus < C >$ and $\mathcal{C}'_4 = \mathcal{C}_4 \setminus < C >$ and consider the lists $\mathcal{T}r(X)$ and $\mathrm{Tr}(X)$ for a chosen matrix X knowing that the matrices X and CX have different parity.

1) $X \in \mathcal{C}_2$: We have $s_0(X) = 2$ and by (sym) $s_1(X) = s_3(X)$. If the list $\mathcal{T}r(X)$ contains 1, then

$$\mathrm{Tr}(X) = (2, 1, 0, 1), \tag{T1}$$

otherwise

$$\mathrm{Tr}(X) = (2, 0, 2, 0). \tag{T2}$$

We join the matrices of the type (T1) into the set $\mathcal{C}_2^{(1)}$ and the matrices of the type (T2) into the set $\mathcal{C}_2^{(0)}$.

2) $X \in \mathcal{C}'_{2,2}$: In view of (sym), the only possibility in this case is

$$\mathrm{Tr}(X) = (0, 2, 0, 2).$$

3) $X \in \mathcal{C}_3$: Since $s_0(X) = 1$ and CX is an odd matrix, we can exclude the possibility that $\mathrm{Tr}(X) = (1, 1, 1, 1)$. Therefore our list contains 2 and the orbit of X coincides with the orbit of an element from $\mathcal{C}_2$. This gives us

$$\mathrm{Tr}(X) \in \{(1, 2, 1, 0), (1, 0, 1, 2)\}.$$

4) $X \in \mathcal{C}'_4$: As $s_0(X) = 0$ the list $\mathcal{T}r(X)$ contains 2. Since $CX, C^3X \in \mathcal{G}_S$, we get $s_1(X), s_3(X) \leq 1$ and

$$\mathrm{Tr}(X) = (0, 1, 2, 1).$$

We construct the *table of the orbits* in the following fashion. The column under a chosen type (given in the first row) shows the numbers of elements of the given type (in the first column) contained in the orbit. For instance, the orbit of a matrix $X \in \mathcal{C}_3$ (5^{th} column) contains 1 element from $\mathcal{C}_2$, 2 elements from $\mathcal{C}_3$ and 1 element from $\mathcal{C}_4$.

TYPE	$\mathcal{C}_2^{(0)}$	$\mathcal{C}_2^{(1)}$	$\mathcal{C}'_{2,2}$	$\mathcal{C}_3$	$\mathcal{C}'_4$
$\mathcal{C}_2$	2	1	2	1	1
$\mathcal{C}_{2,2}$	2		2		
$\mathcal{C}_3$		2		2	2
$\mathcal{C}_4$		1		1	1

Table 2

Lemma 4.17 *Let $\mathcal{G} \subset \mathbb{C}^{4\times 4}$ be a permutation-like group containing a maximal cycle C. Let $S \subset \mathcal{G}_S$ be a Sylow 2-subgroup in the 'even' part $\mathcal{G}_S$ of $\mathcal{G}$, and $X_1 \in S$. Then one of the following cases occurs:*
(1) The group S has order 2 and

$$\mathcal{G} =< C > .$$

(2) The group S can be written as

$$S_C = \{X_1, X_2, X_3 = X_1X_2, I\},$$

where $X_2 \in \mathcal{C}_{2,2}$ is a matrix commuting with $X_1 = C^2$. The set

$$S_{\mathcal{G}} = \{C, C^3, CX_2, CX_3, X_1, X_2, X_3, I\}$$

is a Sylow 2-subgroup in $\mathcal{G}$, and we have

$$\mathcal{C}_{2,2} = \{X_1, X_2, X_3\}. \tag{3c22}$$

Proof. The Sylow 2-subgroup S of the group $\mathcal{G}_S$ is contained in $\mathcal{C}^0_{2,2}$, and therefore for all $X \in S$ we get $X^2 = I$ which implies that S is a commutative group.
(1) Assume that $|S| = 2$ and $\mathcal{C}_3 \neq \emptyset$. By Corollary 4.9 the Sylow 3-subgroups have order 3 and we have $|\mathcal{G}_S| = 6$. The number $1 + 3k$ of Sylow 3-subgroups divides $|\mathcal{G}_S|$ from what follows that $k = 0$ and $m_3 = 2$. As $6 = |\mathcal{G}_S| = m_3 + m_{2,2} + 1$, we have $m_{2,2} = 3$ and by applying (sum') we get $m_2 = m_4$. The group $\mathcal{G}_S$ is a normal subgroup with index 2 in $\mathcal{G}$, therefore $|\mathcal{G}| = 12$ and the number of the 'odd' matrices is $m_2 + m_4 = 6$. This gives us $m_4 = 3$ and $\mathcal{C}_4 = \{C, C^3, Z\}$ for some $Z \in \mathcal{C}_4 \setminus < C >$. Then $Z \neq Z^3 \in \mathcal{C}_4$ and therefore $Z^3 \in < C >$, from what follows $Z \in < C >$. This is a contradiction which means that

$$\mathcal{C}_3 = \emptyset,$$

$|\mathcal{G}_S| = 2$ and $|\mathcal{G}| = 4 = | < C > |$. It follows that

$$\mathcal{G} =< C > .$$

(2) Let $|S| \geq 4$ and pick a matrix $X_1 \in S$, $X_1 \neq I$. Since S is a commutative group of matrices, it can be transformed by a common similarity into a diagonal group of matrices with

$$X_1 = \begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix}, \qquad (*)$$

where I is the identity matrix of dimension 2×2. Each nonidentity matrix in S is a diagonal matrix whose diagonal is the unordered quadruple $[1, 1, -1, -1]$. It is easy to see that the only possibility is then

$$S = \{X_1, X_2, X_1X_2, I\},$$

with

$$X_2 = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{bmatrix}.$$

Therefore $|S| = 4$.

1. If $\mathcal{C}_3 = \emptyset$ then $\mathcal{G}_S = \mathcal{C}^0_{2,2}$ and therefore $|\mathcal{G}_S| = 4$. It follows that $m_{2,2} = 3$.

2. Assume now that $\mathcal{C}_3 \neq \emptyset$. Then $|\mathcal{G}_S| = 12$. The number of Sylow 3-subgroups in $\mathcal{G}_S$ is $1 + 3k$ and it divides 12. This gives us $k = 0, 1$. If there is only one Sylow 3-subgroup in $\mathcal{G}$, we get $\mathcal{C}_3 = \{A, A^2\}$. Table 2 shows us that the orbit $\mathcal{O}(A)$ coincides with an orbit $\mathcal{O}(Z)$ for a suitable $Z \in \mathcal{C}'_4$ and contains both 3-cycles A, A^2. Therefore $\mathcal{C}_4 = \{C, C^3, Z\}$. Then $Z \neq Z^3 \in \mathcal{C}_4$ which means that $Z^3 \in < C >$ and $Z \in < C >$. This contradiction shows that we have 4 Sylow 3-subgroups. Since a pair of Sylow 3-subgroups have trivial intersection, we get $m_3 = 4 \cdot 2 = 8$. As $12 = |\mathcal{G}_S| = m_3 + m_{2,2} + 1$, we conclude that $m_{2,2} = 3$.

In both cases we have got $m_{2,2} = 3$ which means that

$$\mathcal{C}_{2,2} = \{X_1, X_2, X_3\}.$$

Since $CX_2C^{-1} \in \mathcal{C}_{2,2}$ and by Proposition 4.11 the matrix X_2 does not commute with C, we have $CX_2 = X_3C$. In the same way we get $CX_3 = X_2C$ therefore the set $S_{\mathcal{G}}$ is closed under multiplication and it is indeed a group. Since the order of a Sylow 2-subgroup in $\mathcal{G}_S$ is 4, a Sylow 2-subgroup in $\mathcal{G}$ has order 8. Therefore $S_{\mathcal{G}}$ is a Sylow 2-subgroup of $\mathcal{G}$. □

Theorem 4.18 *Let $\mathcal{G} \subset \mathbb{C}^{4\times 4}$ be a noncommutative permutation-like group containing a maximal cycle, $\mathcal{S}_4 \subset \mathbb{C}^{4\times 4}$ the group of all permutation matrices, and $S_{\mathcal{G}}$ the Sylow 2-subgroup from Lemma 4.17. Then:*

(1) For $\mathcal{C}_3 = \emptyset$ we have

$$\mathcal{G} = S_{\mathcal{G}}$$

and $\mathcal{G}$ is equivalent to the group of permutation matrices isomorphic to the group of symmetries of a square.

(2) For $\mathcal{C}_3 \neq \emptyset$ the group $\mathcal{G}$ is equivalent to the group $\mathcal{S}_4$.

Proof. We pick a maximal cycle $C \in \mathcal{C}_4$ and fix a basis such that

$$C = \begin{bmatrix} 1 & & & \\ & i & & \\ & & -1 & \\ & & & -i \end{bmatrix}.$$

Then

$$X_1 = C^2 = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}.$$

By the property (3c22) from Lemma 4.17 we can find a matrix $X_2 \in \mathcal{C}_{2,2}$ which does not commute with C. This gives us $X_2 C X_2^{-1} \in \mathcal{C}_4 \setminus \{C\}$.
Assume first that $\mathcal{G} = S_{\mathcal{G}}$. Then $\mathcal{C}_4 = \{C, C^3\}$. As $X_2 C X_2^{-1} \neq C$ it follows that $X_2 C = C^3 X_2$. By Lemma 4.12 we get

$$X_2 = \begin{bmatrix} 1 & & & \\ & & & a \\ & & b & \\ & c & & \end{bmatrix}.$$

Table 2 shows us that $T = CX_2 \in \mathcal{C}_2$. From the spectrum of T we conclude that $[\sqrt{ac}, -\sqrt{ac}, -b] = [1, 1, -1]$ which means that $b = -1$ and $ac = 1$. By Lemma 4.13 we can find a diagonal similarity which gives us $a = c = 1$. It is easy to see that $\mathcal{G}$ is then equivalent to a group of permutation matrices, where the cycle C corresponds to cycle (1234) and X_2 corresponds to the permutation (12)(34). The group $\mathcal{G}$ is then isomorphic to the group of symmetries of a square.

Assume now that $\mathcal{G}$ is a general permutation-like group satisfying the conditions of the theorem. Since $\mathcal{G}$ is noncommutative, its Sylow 2-subgroups has order 8 by Lemma 4.17.

1. Suppose that $\mathcal{C}_3 = \emptyset$. Then $\mathcal{G}$ is a 2-group and therefore $\mathcal{G} = S_{\mathcal{G}}$.

2. Assume that $\mathcal{C}_3 \neq \emptyset$ and pick $A \in \mathcal{C}_3$. By Corollary 4.9 Sylow 3 groups have order 3. Therefore $|\mathcal{G}| = 3 \cdot 8 = 24$. We can choose a basis $\overline{B}$ such that $\mathcal{G} = 1 \oplus \mathcal{G}'$, $A = 1 \oplus A'$ and $X_1, X_2, X_3 = X_1X_2$ from $S_{\mathcal{G}}$ are diagonal matrices, where

$$X_1' = \begin{bmatrix} -1 & & \\ & 1 & \\ & & -1 \end{bmatrix}, \; X_2' = \begin{bmatrix} -1 & & \\ & -1 & \\ & & 1 \end{bmatrix} \text{ and } X_3' = \begin{bmatrix} 1 & & \\ & -1 & \\ & & -1 \end{bmatrix}.$$

Then $S = \{X_1, X_2, X_3, I\}$ is a Sylow subgroup in $\mathcal{G}_S$. Since $A \notin S$ for all $i = 1, 2, 3$, we get $AX_i \in \mathcal{G}_S \setminus S = \mathcal{C}_3$ yielding $s_0'(AX_i) = 0$ and

$$A' = \begin{bmatrix} 0 & a & b \\ c & 0 & d \\ e & f & 0 \end{bmatrix}.$$

We also have $AX_1A^{-1} \in \{X_2, X_3\}$. Assume first that $AX_1A^{-1} = X_2$. It follows that $AX_2A^{-1} = A^2X_1A^{-2} = X_3$. It means that $X_2A = AX_1$ and $X_3A = AX_2$. This gives us

$$\begin{bmatrix} 0 & -a & -b \\ -c & 0 & -d \\ e & f & 0 \end{bmatrix} = (X_2A)' = (AX_1)' = \begin{bmatrix} 0 & a & -b \\ -c & 0 & -d \\ -e & f & 0 \end{bmatrix}$$

and

$$\begin{bmatrix} 0 & a & b \\ -c & 0 & -d \\ -e & -f & 0 \end{bmatrix} = (X_3A)' = (AX_2)' = \begin{bmatrix} 0 & -a & b \\ -c & 0 & d \\ -e & -f & 0 \end{bmatrix}.$$

The above relations imply $a = d = e = 0$. Therefore A' is of the form

$$A' = \begin{bmatrix} 0 & 0 & b \\ c & 0 & 0 \\ 0 & f & 0 \end{bmatrix}. \tag{c3m}$$

If $AX_1A^{-1} = X_3$ then $A^2X_1A^{-2} = X_2$ and the matrix $(A^2)'$ is of the form (c3m). As shown before we can find a basis $B = \{e_1, e_2, e_3, e_4\}$ such that $S_{\mathcal{G}}$ is a group of permutation matrices and C the permutation matrix corresponding to the cycle (1243).

Then $X_1 = C^2$, X_2 and X_3 correspond to the permutations (14)(23), (12)(34) and (13)(24), respectively. Conjugation by the orthogonal matrix

$$Q = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix}$$

transforms our group into $\mathcal{G} = 1 \oplus \mathcal{G}'$, where X_1, X_2 and X_3 have the previously prescribed diagonal form and C is of the form

$$C = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 0 & 1 \\ & & -1 & 0 \end{bmatrix}.$$

Then a cycle $A \in \mathcal{C}_3$ satisfies (c3m) and we have

$$(CA)' = \begin{bmatrix} 0 & 0 & -b \\ 0 & f & 0 \\ -c & & 0 \end{bmatrix}.$$

The ordered list of traces $\mathrm{Tr}(A)$ shows us that $CA \in \mathcal{C}_4 \cup \mathcal{C}_2$, so that we consider two cases:

1. If $CA \in \mathcal{C}_4$ then $s'_0(CA) = f = -1$ and $bc = -1$ or $c = -\frac{1}{b}$. Let us denote

$$P = \begin{bmatrix} 1 & & & \\ & \frac{1}{b} & & \\ & & -1 & \\ & & & 1 \end{bmatrix}.$$

Then

$$PAP^{-1} = \begin{bmatrix} 1 & & & \\ & 0 & 0 & 1 \\ & 1 & 0 & 0 \\ & 0 & 1 & 0 \end{bmatrix} \qquad \text{(c3p)}$$

and $PCP^{-1} = C^3$. The group $P\mathcal{G}P^{-1}$ then contains a matrix A in the form (c3p) and matrix C^3. Conjugation by the matrix $Q^{-1} = Q^T$ preserves the matrix A in the form (c3p) and transforms C^3 into the permutation matrix corresponding to the cycle (1342). After these conjugations $\mathcal{G}$ contains permutation matrices associated with (234) and (1342). Since $\mathcal{C}_3 \neq \emptyset$, the group of permutation matrices $\mathcal{G}_P$, generated with these two matrices, has 24 elements. It follows that $\mathcal{G} = \mathcal{G}_P$, which completes

the proof of this case.

2. If $CA \in \mathcal{C}_2$ then $s_0'(CA) = f = 1$ and $bc = 1$, i.e., $2c = \frac{1}{b}$. Then for

$$P = \begin{bmatrix} 1 & & & \\ & \frac{1}{b} & & \\ & & 1 & \\ & & & 1 \end{bmatrix}$$

we get

$$PAP^{-1} = \begin{bmatrix} 1 & & & \\ & 0 & 0 & 1 \\ & 1 & 0 & 0 \\ & 0 & 1 & 0 \end{bmatrix}$$

and $PCP^{-1} = C$. The group $P\mathcal{G}P^{-1}$ contains a matrix A of the form (c3p) and matrix C. The conjugation by $Q^{-1} = Q^T$ preserves A and changes C into the permutation matrix associated with the permutation (1243). Once these conjugations are applied the group $\mathcal{G}$ contains permutation matrices corresponding to the permutations (234) and (1243). Since $\mathcal{C}_3 \neq \emptyset$, the group $\mathcal{G}_P$ generated by these two matrices has 24 elements, and therefore

$$\mathcal{G} = \mathcal{G}_P$$

which means that $\mathcal{G}$ consists of permutation matrices. □

Case n=5: If $n = 5$, the set of 'even' matrices is the union of the sets $\mathcal{C}_5$, $\mathcal{C}_3$, $\mathcal{C}_{2,2}$ and $\mathcal{C}_0$ while the set of the 'odd' matrices is the union of the sets $\mathcal{C}_4$, $\mathcal{C}_{3,2}$ and $\mathcal{C}_2$. The table of traces is the following

TYPE	$\mathcal{C}_2$	$\mathcal{C}_{2,2}$	$\mathcal{C}_3$	$\mathcal{C}_{3,2}$	$\mathcal{C}_4$	$\mathcal{C}_5$
s_0	3	1	2	0	1	0
s_0'	2	0	1	-1	0	-1

Table 3

Consider an orbit for $X \in \mathcal{C}_\alpha$. As C is an even matrix, the product $C^k X$ has the same parity as X. Table 3 shows that the trace separates the elements in $\mathcal{G}_S$ and also in $\mathcal{G}_L$. Therefore we can reconstruct the structure of the orbit $\mathcal{O}(X)$ knowing

just the (unordered) list $\mathcal{T}r(X)$.

1) $X \in \mathcal{C}_2$: Since $s_0(X) = 3$, the only possible list is

$$\mathcal{T}r(X) = [3, 1, 1, 0, 0].$$

From (sym) we conclude that $s_3(X) = s_{-2}(X) = s_2(X)$ and $s_4(X) = s_{-1}(X) = s_1(X)$, and so

$$\mathrm{Tr}(X) = (3, 1, 0, 0, 1), (3, 0, 1, 1, 0).$$

2) $X \in \mathcal{C}_{2,2}$: This case gives us the possibilities

$$\mathcal{T}r(X) = [1, 1, 1, 1, 1], [1, 1, 1, 2, 0], [1, 2, 2, 0, 0],$$

where we can eliminate the second one using the property (sym). Let us decompose the set $\mathcal{C}_{2,2}$ as union of the sets

$$\mathcal{C}_{2,2}^{(fix)} = \{X \in \mathcal{C}_{2,2} | \mathcal{O}(X) \subset \mathcal{C}_{2,2}\}$$

and

$$\mathcal{C}_{2,2}^{(var)} = \{X \in \mathcal{C}_{2,2} | \mathcal{O}(X) \not\subset \mathcal{C}_{2,2}\}.$$

For $X \in \mathcal{C}_{2,2}^{(var)}$ we have

$$\mathrm{Tr}(X) = (1, 2, 0, 0, 2), (1, 0, 2, 2, 0).$$

3) $X \in \mathcal{C}_3$: As $s_0(X) = 2$ is an even number, the list $\mathcal{T}r(X)$ must contain the number 1 and therefore the orbit $\mathcal{O}(X)$ coincides with the orbit of an element $Y \in \mathcal{C}_{2,2}^{(var)}$. It follows that

$$\mathrm{Tr}(X) = (2, 1, 2, 0, 0), (2, 0, 1, 0, 2).$$

4) $X \in \mathcal{C}_{3,2}$: Since $s_0(X) = 0$ and $\mathcal{O}(X) \subset \mathcal{G}_L$ the list $\mathcal{T}r(X)$ contains 3. The orbit $\mathcal{O}(X)$ then coincides with the orbit of an element $Y \in \mathcal{C}_2$ which gives the possibilities

$$\mathrm{Tr}(X) = (0, 3, 0, 1, 1), (0, 1, 3, 1, 0).$$

5) $X \in \mathcal{C}_4$: We get two cases. If the list $\mathcal{T}r(X)$ contains 3, the orbit $\mathcal{O}(X)$ coincides with the orbit of an element $Y \in \mathcal{C}_2$ and therefore

$$\mathcal{T}r(X) = [1, 1, 3, 0, 0],$$

while in the second case we have $\mathcal{T}r(X) = [1, 1, 1, 1, 1]$ which means that $\mathcal{O}(X) \subset \mathcal{C}_4$. We decompose the set $\mathcal{C}_4$ into the sets

$$\mathcal{C}_4^{(fix)} = \{X \in \mathcal{C}_4 | \mathcal{O}(X) \subset \mathcal{C}_4\}$$

and

$$\mathcal{C}_4^{(var)} = \{X \in \mathcal{C}_4 | \mathcal{O}(X) \not\subset \mathcal{C}_4\}.$$

6) $X \in \mathcal{C}_5$: Let us assume that $X \notin < C >$. As $s_0(X) = 0$, the list $\mathcal{T}r(X)$ contains 1 with 'odd multiplicity. Then the orbit $\mathcal{O}(X)$ coincides with the orbit of an element $Y \in \mathcal{C}_{2,2}$ and therefore

$$\mathrm{Tr}(X) = (0, 1, 0, 2, 2), (0, 2, 1, 2, 0).$$

We denote $\mathcal{C}_5' = \mathcal{C}_{2,2} \setminus < C >$ and resume the structure of the orbits for the matrices $X \notin < C >$.

TYPE	$\mathcal{C}_2$	$\mathcal{C}_{2,2}^{(fix)}$	$\mathcal{C}_{2,2}^{(var)}$	$\mathcal{C}_3$	$\mathcal{C}_{3,2}$	$\mathcal{C}_4^{(fix)}$	$\mathcal{C}_4^{(var)}$	$\mathcal{C}_5'$
$\mathcal{C}_2$	1				1		1	
$\mathcal{C}_{2,2}$		5	1	1				1
$\mathcal{C}_3$			2	2				2
$\mathcal{C}_{3,2}$	2				2		2	
$\mathcal{C}_4$	2				2	5	2	
$\mathcal{C}_5$			2	2				2

Table 4

Proposition 4.19 *Let $C \in \mathcal{C}_5$ be a maximal cycle and $\mathcal{C}_3 = \emptyset$. Then the group $\mathcal{G}$ coincides with $N(< C >)$ and is equivalent to a group of permutation matrices.*

PROOF. If $\mathcal{C}_3 = \emptyset$, table 4 shows that

$$\mathcal{C}_{2,2} = \mathcal{C}_{2,2}^{(fix)},$$

since the orbits of the elements of $\mathcal{C}_{2,2}^{(var)}$ intersect $\mathcal{C}_3$. As the orbit of an element of $\mathcal{C}_4^{(var)}$ contains a matrix $Y \in \mathcal{C}_{3,2}$, and $Y^2 \in \mathcal{C}_3$, we get $\mathcal{C}_4^{(var)} = \emptyset$. Since the orbit of an arbitrary element from $\mathcal{C}_2$ intersects $\mathcal{C}_3$, we have $\mathcal{C}_2 = \emptyset$. This gives us

$$\mathcal{G} = \mathcal{C}_5 \cup \mathcal{C}_4^{(fix)} \cup \mathcal{C}_{2,2}^{(fix)} \cup \mathcal{C}_0.$$

Since the orbit of a matrix $X \in \mathcal{C}_5'$ intersects $\mathcal{C}_3$, we get

$$\mathcal{C}_5^0 =< C > .$$

For $X \in \mathcal{G}$ we have $X < C > X^{-1} \subset \mathcal{C}_5^0 =< C >$. It follows that

$$\mathcal{G} = N(< C >)$$

and $\mathcal{G}$ is by Theorem 4.15 equivalent to a group of permutation matrices. □

Remark: If $\mathcal{G} = N(< C >) \neq < C >$ Theorem 4.15 implies $\mathcal{C}_3 = \emptyset$. It follows that $\mathcal{G} \neq N(< C >)$ holds if and only if $\mathcal{C}_3 \neq \emptyset$.

Lemma 4.20 *Let $\mathcal{G} \subset \mathbb{C}^{5\times 5}$ be a permutation-like group. Then:*
(1) If $\mathcal{C}_3 \neq \emptyset$, then Sylow 3-subgroups of $\mathcal{G}$ are cyclic.
(2) If $\mathcal{C}_{2,2} \neq \emptyset$, then Sylow 2-subgroups of the group $\mathcal{G}_S \leq \mathcal{G}$ have orders 2 or 4.

We assume now that $\mathcal{C}_5, \mathcal{C}_3 \neq \emptyset$ and $C \in \mathcal{C}_5$ is a maximal cycle.
(3) We have

$$m_5 = 24 \text{ and } m_3 = 20$$

and Sylow 2-subgroups of $\mathcal{G}$ have orders 4 or 8.
(4) The order of the group $\mathcal{G}$ is 60 or 120. If $|\mathcal{G}| = 60$ then $\mathcal{G} = \mathcal{G}_S$.
(5) The set $\mathcal{C}_{2,2}^{(fix)}$ is contained in $N(< C >)$ and has 5 elements.

PROOF. (1) This follows from Corollary 4.9.
(2) Let S be a Sylow 2-subgroup of the group $\mathcal{G}_S = 1 \oplus \mathcal{G}_S'$. Assume that $\mathcal{G} = \mathcal{G}_S$.

Then $S \subset \mathcal{C}^0_{2,2}$ and therefore for $X \in S$ we get $X^2 = I$. It follows that S is a commutative group.

Let us pick a matrix $X_1 \in S$, $X_1 \neq I$. Since S is a commutative group, it is equivalent to a group of diagonal matrices and we can write

$$X_1 = 1 \oplus \begin{bmatrix} I & 0 \\ 0 & -I \end{bmatrix},$$

where I is the identity matrix of order 2×2. Each matrix from S is a diagonal matrix with diagonal equal to (unordered) five-tuple $[1, 1, 1, -1, -1]$. It is easy to verify that in this situation

$$S \subset \{X_1, X_2, X_1X_2, I\},$$

with

$$X_2 = 1 \oplus \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{bmatrix}.$$

We conclude that $|S| \leq 4$.

(3) First we assume that $\mathcal{G} = \mathcal{G}_S$. By Corollary 4.9 Sylow 5-sugroups of $\mathcal{G}$ are cyclic. According to (1) and (2) we get $|\mathcal{G}| \leq 60$. Since $\mathcal{G} \neq N(< C >)$, the Sylow subgroup $< C >$ is not a normal subgroup. The number $1 + 5k$ of Sylow 5-subgroups is then at least 6. As the intersection of two Sylow 5-subgroups is trivial, the number of elements of the set $\mathcal{C}_5$ is

$$m_5 = 4(1 + 4k) \geq 24.$$

By the property (evn) we get $-m_5 + m_3 + 4 = 0$, i.e.,

$$m_5 = m_3 + 4.$$

It follows that $m_3 \geq 20$ and $|\mathcal{G}| \geq 24 + 20 > 30$. Since $|S| = 2$ would imply that $|\mathcal{G}| = 30$, we actually have $|S| = 4$ and $S = \{X_1, X_2, X_1X_2, I\}$. For $k > 1$ the numbers m_5 and m_3 are too big, therefore we have

$$m_5 = 24 \text{ and } m_3 = 20.$$

We now assume that $\mathcal{G}$ is a general permutation-like group. Then an arbitrary subgroup $H \leq \mathcal{G}$ splits into the 'even part' H_S, which is a normal subgroup of H,

and the 'odd part' H_L which is either empty set or it has the same cardinality as H_S. For a Sylow 2-subgroup S its 'even part' has order 4 which gives us the last claim of (3).
(4) From Corollary 4.9 it follows that the Sylow 5-subgroups have order 5. By (1) and (3) it follows that the order of $\mathcal{G}$ is either $5 \cdot 3 \cdot 4 = 60$ or $5 \cdot 3 \cdot 8 = 120$,

$$|\mathcal{G}| = 60, 120 \qquad \text{(or5)}.$$

(5) The orbit of a matrix $X \in \mathcal{C}_3$ contains exactly one matrix $Y \in \mathcal{C}_{2,2}^{(var)}$. Since the orbit $\mathcal{O}(Y)$ contains exactly two elements from $\mathcal{C}_3$, the cardinality of $\mathcal{C}_{2,2}^{(var)}$ is $m_{2,2}^{(var)} = \frac{m_3}{2} = 10$. Then we get

$$60 = |\mathcal{G}_S| = m_5 + m_3 + m_{2,2}^{(var)} + m_{2,2}^{(fix)} + m_0 = 55 + m_{2,2}^{(fix)},$$

which gives us

$$m_{2,2}^{(fix)} = 5.$$

Pick a matrix $X \in \mathcal{C}_{2,2}^{(fix)}$. Then $CX \in \mathcal{C}_{2,2}$ and $(CX)^2 = I$ which implies

$$XCX^{-1} = XCX = C^{-1},$$

and therefore $X \in N(< C >)$. □

Lemma 4.21 *Let $\mathcal{G} = 1 \oplus \mathcal{G}'$ be a permutation-like group and $X_1 = 1 \oplus T$, where*

$$T = \begin{bmatrix} & & & 1 \\ & & 1 & \\ & 1 & & \\ 1 & & & \end{bmatrix}.$$

Suppose that $X_2 \in \mathcal{G}$ commutes with X_1 and denote $X_3 = X_1 X_2$.
(1) Then

$$X_2 = 1 \oplus \begin{bmatrix} \alpha & \beta & \gamma & \delta \\ \beta' & \alpha' & \delta' & \gamma' \\ \gamma' & \delta' & \alpha' & \beta' \\ \delta & \gamma & \beta & \alpha \end{bmatrix}. \qquad \text{(c22)}$$

If $X_2 \in \mathcal{C}_{2,2} \setminus \{X_1, I\}$ we additionally get $\alpha' = -\alpha$ in $\delta' = -\delta$.
(2) There exists a basis B_{cyc} such that C has the form (cyc), $X_1 = 1 \oplus T$ and $X_2 = 1 \oplus X_2'$. We have $X_1 \in \mathcal{C}_{2,2}^{(fix)}$ and for $X_2 \in \mathcal{C}_{2,2} \setminus \{X_1, I\}$ we get $X_2, X_3 \in \mathcal{C}_{2,2}^{(var)}$.

(3) If B_{cyc} is a basis such that C has the form (cyc), $X_1 = 1 \oplus T$ and $X_2 = 1 \oplus X_2'$, then

$$\begin{bmatrix} 1 & & & & \\ & 0 & 1 & & \\ & 1 & 0 & & \\ & & & 0 & 1 \\ & & & 1 & 0 \end{bmatrix} \in \{X_2, X_3\}.$$

PROOF. (1) By comparing the second and third rows in the products X_1X_2 and X_2X_1 we get the desired results.
Since $X_2 \in \mathcal{C}_{2,2}$, we have $\operatorname{tr} X_2 = 1$ and therefore $\alpha' = -\alpha$. As $X_3^2 = (X_1X_2)^2 = I$ and $X_1X_2 \neq I$, we conclude that $X_3 \in \mathcal{C}_{2,2}$ and get $\delta' = -\delta$.
(2) We first check that $X_2 \notin \mathcal{C}_{2,2}^{(fix)}$. By (5) of Lemma 4.20 it follows that $\mathcal{C}_{2,2}^{(fix)} = \mathcal{O}(X_1)$. Suppose that

$$X_2 = C^p X_1.$$

Since $4 = -1$ is the only element of the multiplicative group Z_5^* with order 2, we get

$$X_1 C = C^{-1} X_1$$

by Corollary 4.14 and therefore

$$X_1X_2 = X_1C^pX_1 = C^{-p} \neq C^p = X_2X_1.$$

It follows that $X_2 \in \mathcal{C}_{2,2}^{(var)}$. For X_3 also commutes with X_1, we get $X_3 \in \mathcal{C}_{2,2}^{(var)}$. From the list $\operatorname{Tr}(X_2)$ we see that $\{CX_2, C^2X_2\} \cap \mathcal{C}_3 \neq \emptyset$. Assume that $CX_2, CX_3 \in \mathcal{C}_3$. Then

$$I = (CX_3)^3 = X_1C^{-1}X_2CX_2C^{-1}X_2.$$

By the left multiplication with C^2X_1 we get

$$C^2X_1 = (CX_2)^2C^{-1}X_2 = (CX_2)^{-1}C^{-1}X_2 = X_2C^{-2}X_2$$

and

$$C^2X_3 = X_2C^{-2}.$$

Therefore

$$C^2X_3C^2 = X_2.$$

Then $CX_2 = C^3X_3C^2 = C^{-2}X_3C^2 \in \mathcal{C}_{2,2}$ which contradicts the fact that $X_2 \in \mathcal{C}_{2,2}^{(var)}$. It follows that exactly one of the matrices CX_2 and CX_3 is contained in $\mathcal{C}_3$. We can assume that $CX_2 \in \mathcal{C}_3$ and $CX_3 \in \mathcal{C}_5$. By (1) we can write

$$X_2 = 1 \oplus \begin{bmatrix} \alpha & \beta & \gamma & \delta \\ \beta' & -\alpha & -\delta & \gamma' \\ \gamma' & -\delta & -\alpha & \beta' \\ \delta & \gamma & \beta & \alpha \end{bmatrix}.$$

Since $CX_2 \in \mathcal{C}_3$, we get

$$s_0'(CX_2) = \alpha(\lambda - \lambda^2 - \lambda^3 + \lambda^4) = 1.$$

It follows that

$$\alpha = \frac{1}{\lambda - \lambda^2 - \lambda^3 + \lambda^4}.$$

For $C^2X_3 \in \mathcal{C}_3$ we can use the same argument to show that

$$\delta = \frac{1}{\lambda^2 - \lambda^4 - \lambda^6 + \lambda^8} = -\alpha.$$

This gives us

$$\alpha + \delta = 0. \qquad (*)$$

Let $B_{dia} = \{f_0, f_1, f_2, f_3, f_4\}$ be a basis such that C has the form (dia) and $X_1 = 1 \oplus T$. We define $g_1 = f_1 + f_4$, $g_2 = f_2 + f_3$, $V_1 = \mathcal{L}\{g_1, g_2\}$ in $V_{-1} = V_1^{\perp}$. Then $X_1|_{V_1} = I$ and $X_1|_{V_{-1}} = -I$ which implies that V_1 and V_{-1} are invariant subspaces for X_2. If $X_2|_{V_1} = -I$ we get $X_2' = -X_1'$ which means that -1 is an eigenvalue for X_3 with multiplicity 4. This is clearly impossible in our group. We can therefore find a vector $g \in V_1$ such that

$$X_2(g) = g.$$

Let us write $g = \mu_1 g_1 + \mu_2 g_2$.

If $\mu_1 = 0$, we have $X_2 g_2 = g_2$ from what follows that $-\alpha - \delta = 1$.

If $\mu_2 = 0$, we have $X_2 g_1 = g_1$ which gives us $\alpha + \delta = 1$ and by (*) $\mu_2 \neq 0$.

Since both cases contradict (*), we have $\mu_1, \mu_2 \neq 0$.

For

$$e = f_0 + g,$$

we get

$$X_1 e = e \text{ and } X_2 e = e,$$

By Lemma 4.10 $B_{cyc} = \{e, Ce, C^2e, C^3e, C^4e\}$ is a basis such that the matrices C, X_1 in X_2 have the prescribed forms.

(3) Let B_{cyc} be a basis satisfying the assumptions. By (1) we can write X_2 as

$$X_2 = 1 \oplus \begin{bmatrix} \alpha & \beta & \gamma & \delta \\ \beta' & -\alpha & -\delta & \gamma' \\ \gamma' & -\delta & -\alpha & \beta' \\ \delta & \gamma & \beta & \alpha \end{bmatrix}.$$

If necessary we interchange the matrices X_2 and X_3 and assume that $CX_2 \in \mathcal{C}_3$. Then

$$(CX_2)^2 = \begin{bmatrix} 0 & \delta & \gamma & \beta & \alpha \\ 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha & \beta & \gamma & \delta \\ 0 & \beta' & -\alpha & -\delta & \gamma' \\ 0 & \gamma' & -\delta & -\alpha & \beta' \end{bmatrix}^2 = \begin{bmatrix} * & * & * & * & * \\ 0 & \delta & \gamma & \beta & \alpha \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \end{bmatrix}.$$

It follows that

$$\begin{bmatrix} * & * & * & * & * \\ 0 & \delta & \gamma & \beta & \alpha \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \end{bmatrix} = (CX_2)^2 = (CX_2)^{-1} = X_2 C^{-1} = \begin{bmatrix} * & * & * & * & * \\ \delta & 0 & \alpha & \beta & \gamma \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \end{bmatrix}$$

and therefore $\delta = 0$. As $CX_2 \in \mathcal{C}_3$, we get

$$2 = s_1(X_2) = \beta + \beta'.$$

Since X_2 is a unitary matrix, we have $|\beta| = |\beta'| = 1$ and therefore $\beta = \beta' = 1$. We have shown that the matrix X_2 has the prescribed permutation form. □

Corollary 4.22 *Let $\mathcal{G} \subset \mathbb{C}^{5\times 5}$ be a permutation-like group such that $\mathcal{C}_5 \neq \emptyset$. Then its subgroup $\mathcal{G}_S$ of 'even' matrices is equivalent to a group of permutation matrices.*

Proof. If $\mathcal{C}_3 = \emptyset$, we use Proposition 4.19. Otherwise pick a matrix $C \in \mathcal{C}_5$. By (5) of Lemma 4.20 we can find a matrix $X_1 \in \mathcal{C}_{2,2}^{(fix)}$. By Lemma 4.21 we can find a

matrix $X_2 \in \mathcal{C}_{2,2}^{(var)}$ and a basis B such that C, X_1 and X_2 are permutation matrices. The group H generated by these three matrices therefore consists of permutation matrices. By Lemma 4.20 the group H has 60 elements and same holds for the group $\mathcal{G}_S$. Since $\mathcal{G}_S$ contains group H, the two groups actually coincide and $\mathcal{G}_S$ itself is a group of permutation matrices. □

Lemma 4.23 *Let $\mathcal{G} \subset \mathbb{C}^{5\times 5}$ be a permutation-like group such that $\mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_5 \neq \emptyset$. Then there exists a matrix $Z \in N(< C >) \cap \mathcal{C}_4$.*

Proof. We pick a matrix $Y \in \mathcal{C}_4$. Then $S = Y < C > Y^{-1}$ is a Sylow 5-subgroup contained in $\mathcal{G}_S$. Therefore S is conjugated to the Sylow subgroup $< C >$ within the group $\mathcal{G}_S$. This means that we can find a matrix $A \in \mathcal{G}_S$ such that $Y < C > Y^{-1} = A^{-1} < C > A$, i.e.,

$$(AY) < C > (AY)^{-1} =< C > .$$

Then $Z = AY \in N(< C >)$ is an 'odd' matrix and we can find a number k such that

$$ZC = C^k Z.$$

By Corollary 4.14 we know that $Z \notin \mathcal{C}_2$, thus $Z \in \mathcal{C}_4$ and Z is a required matrix from $\mathcal{C}_4$. □

Theorem 4.24 *Let $\mathcal{G} \subset \mathbb{C}^{5\times 5}$ be a permutation-like group such that $\mathcal{C}_5 \neq \emptyset$. Then $\mathcal{G}$ is equivalent to a group of permutation matrices.*

Proof. If $\mathcal{G} = \mathcal{G}_S$, our claim follows from 4.22. We assume that $\mathcal{G}_L \neq \emptyset$. Then $\mathcal{C}_4 \neq \emptyset$ and we can pick a matrix $Z \in N(< C >)$ by Lemma 4.23. Then

$$ZC = C^k Z,$$

where $k = 2, 3$, since 2 and 3 are the only elements of order 4 in the multiplicative group Z_5^*. If necessary we change matrix Z with Z^3 and assume that

$$ZC = C^2 Z.$$

By Corollary 4.14 we can find a basis $B_{mon} = \{f_0, f_1, f_2, f_3, f_4\}$ such that C has the form (dia) and

$$Z = \begin{bmatrix} 1 & & & & \\ & & 1 & & \\ & & & & 1 \\ & 1 & & & \\ & & & 1 & \end{bmatrix}.$$

It follows that

$$Z^2 = X_1 = \begin{bmatrix} 1 & & & & \\ & & & & 1 \\ & & & 1 & \\ & & 1 & & \\ & 1 & & & \end{bmatrix}.$$

Let $S = \{Z, Z^3, X_1, X_2, X_3, T_1, T_2, I\}$ be a Sylow 2-subgroup containing the matrix Z. We denote $g_1 = \frac{f_1+f_4}{\sqrt{2}}$, $g_2 = \frac{f_2+f_3}{\sqrt{2}}$, $h_1 = \frac{f_1-f_4}{\sqrt{2}}$ and $h_2 = \frac{f_2-f_3}{\sqrt{2}}$. Then $B = \{f_0, g_1, g_2, h_1, h_2\}$ is an orthonormal basis such that

$$Z = \begin{bmatrix} 1 & & & & \\ & 0 & 1 & & \\ & 1 & 0 & & \\ & & & 0 & 1 \\ & & & -1 & 0 \end{bmatrix},$$

$X_1 = 1 \oplus I \oplus (-I)$ and therefore

$$X_2 = \begin{bmatrix} 1 & & & & \\ & a & b & & \\ & \overline{b} & -a & & \\ & & & c & d \\ & & & \overline{d} & -c \end{bmatrix},$$

where a and c are real numbers. It follows that

$$T = ZX_2 = \begin{bmatrix} 1 & & & & \\ & \overline{b} & -a & & \\ & a & b & & \\ & & & \overline{d} & -c \\ & & & -c & d \end{bmatrix}.$$

Since $T \in S$ is an 'odd matrix' and $T \neq Z, Z^3$, we have $T \in \mathcal{C}_2$. We get $T = T^{-1} = T^*$, $a = 0$ and $|b| = 1$. The matrix T has real diagonal entries, thus b is a real number which means that $b = \pm 1$. As -1 is a simple eigenvalue of T, we conclude

that $b = 1$ which implies that

$$X_2(g_1 + g_2) = g_1 + g_2.$$

If we define $e = f_0 + g_1 + g_2 = f_0 + f_1 + f_2 + f_3 + f_4$, we get $Ze = X_1e = X_2e = e$. The set $B_{per} = \{e, Ce, C^2e, C^3e, C^4\}$ is by Lemma 4.10 a basis such that C has the form (cyc),

$$X_1 = \begin{bmatrix} 1 & & & & \\ & & & & 1 \\ & & & 1 & \\ & & 1 & & \\ & 1 & & & \end{bmatrix}$$

and $X_2 = 1 \oplus X_2'$. By (3) of Lemma 4.21 the group $\mathcal{H} = \{X_1, X_2, X_3, I\}$ is a permutation group. Since C and Z are permutation matrices it follows that the group $\mathcal{G}_0$ generated by $\mathcal{H}$, C and Z consists of permutation matrices and intersects sets $\mathcal{C}_5$, $\mathcal{C}_4$ and $\mathcal{C}_3$. As such it has the order 120. Since the group $\mathcal{G}$ has the same order we get

$$\mathcal{G} = \mathcal{G}_0,$$

and $\mathcal{G}$ itself is a permutation group. □

Let $\mathcal{G} \subset \mathbb{C}^{5\times 5}$ be a permutation-like group. Since Theorem 4.24 gives the affirmative answer in the case $\mathcal{C}_5 \neq \emptyset$, we consider now the case $\mathcal{C}_5 = \emptyset$.

Lemma 4.25 *We pick a matrix $A \in \mathcal{C}_3$ and write*

$$A = \begin{bmatrix} I & \\ & D \end{bmatrix}, \tag{c3d}$$

where

$$D = \begin{bmatrix} \alpha & \\ & \alpha^2 \end{bmatrix}.$$

Assume that the matrix

$$X = \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix}$$

satisfies the condition $XA = A^kX$. Then $B_2 = 0$ and $B_3 = 0$. There exists a unitary matrix $U = V \oplus I$ such that $UAU^{-1} = A$ and VB_1V^{-1} is a diagonal matrix. Additionally we have:

(1) For $k = 1$ the matrix B_4 is diagonal.

(2) For $k = 2$ the matrix B_4 is of the form

$$B_4 = \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix}.$$

PROOF. Since the spectrum of D does not contain 1, the matrix $D - I$ is invertible. It follows that $B_2 = 0$ and $B_3 = 0$. We also get $DB_4 = D^k B_4$ which yields the desired form for B_4. It is clear that the conjugation by U does not change A, while for a suitable V block B_1 changes into a diagonal matrix. □

Theorem 4.26 *Let $\mathcal{G} \subset \mathbb{C}^{5\times 5}$ be a permutation-like group such that $\mathcal{C}_5 = \emptyset$. Then $\mathcal{G}$ is equivalent to a group of permutation matrices.*

PROOF.

1. $\mathcal{C}_3 \neq \emptyset$:

First we explore the case $\mathcal{G} = \mathcal{G}_S$. Then the order of $\mathcal{G}$ is 3, 6 or 12, since its Sylows 2-subgroups again contain at most 4 elements.

- $|\mathcal{G}| = 3$: In this case we have

$$\mathcal{G} =< A >$$

for a matrix $A \in \mathcal{C}_3$ and $\mathcal{G}$ is clearly equivalent to a group of permutation matrices.

- $|\mathcal{G}| = 6$: Then the number of Sylow 3-subgroups is equal to $1 + 3k$ and divides 6. It follows that $k = 0$ and $< A >$ is a normal Sylow subgroup for arbitrary $A \in \mathcal{C}_3$. This yields $m_3 = 2$, $m_{2,2} = 6 - m_3 - 1 = 3$ and therefore

$$\mathcal{C}_{2,2} = \{X_1, X_2, X_3\}.$$

For $i \neq j$ we get $X_i X_j \notin \mathcal{C}^0_{2,2}$, since otherwise we would have $X_i X_j = X_j X_i$ and $\{I, X_i, X_j, X_i X_j\}$ would be a subgroup of order 4. The group $\mathcal{G}$ can be realized by permutations

$$X_1 = (12)(34)\,,\ X_2 = (12)(35) \text{ and } X_3 = (12)(45),$$

where $A = X_1 X_2 = (345)$.

• $|\mathcal{G}| = 12$: The number of Sylow 3-subgroups is $1 + 3k$ and divides 12 therefore we get $k = 0, 1$. The Sylow 2-subgroups are of the form $\{I, X, Y, XY\}$, for some $X, Y \in \mathcal{C}_{2,2}$.

If $k = 0$ there is only one Sylow 3-subgroup, and therefore $m_3 = 2$. Since it follows that $m_{2,2} = 9$ we have at least 3 Sylow 2-subgroups. As the number of Sylow 2-subgroups is $1 + 2l$ and it divides 12, we actually have 3 Sylow 2-subgroups with pairwise trivial intersections. Let $S = \{I, X, Y, XY\}$ and $S' = \{I, X', Y', X'Y'\}$ be two Sylow subgroups. Then $XX' \notin \mathcal{C}^0_{2,2}$, since otherwise we would get a Sylow subgroup $\{I, X, X', XX'\}$ having nontrivial intersection with S. Similarly we show that $XY', XX'Y' \notin \mathcal{C}^0_{2,2}$ therefore $XX', XY', XX'Y' \in \mathcal{C}_3 = \{A, A^2\}$. It follows that the list $[XX', XY', XX'Y']$ has at least two equal element which is clearly a contradiction.

In the remaining case we get $k = 1$ therefore there are 4 Sylow 3-subgroups and $m_3 = 8$. It follows that $m_{2,2} = 3$ and

$$S = \mathcal{C}^0_{2,2} = \{I = X_0, X_1, X_2, X_1X_2 = X_3\}$$

is the unique Sylow 2-subgroup. The matrices X_i and X_j commute for arbitrary i and j. Let us pick a matrix $X \in \mathcal{C}_{2,2}$ and a matrix $A \in \mathcal{C}_3$. Since $A \notin S$, we get $XA \in \mathcal{C}_3$. By lemma 4.25 the condition $XA = AX$ implies that in a suitable basis we get $B_2 = 0$ and $B_3 = 0$, while B_1 is a diagonal matrix. If $B_4 = -I$, then the spectrum of matrix XA contains $-\alpha$ which is impossible therefore -1 is in the spectra of B_1 and XA. Since the spectra of the matrices from $\mathcal{C}_3$ do not contain -1, matrices X and A do not commute. We pick a matrix $A \in \mathcal{C}_3$ and a matrix $X_1 \in \mathcal{C}_{2,2}$ and define $X_2 = A^{-1}X_1A$, $X_3 = A^{-1}X_2A$. Then

$$\mathcal{G} = \{A^kX_i \mid k = 0, 1, 2\,,\ i = 0, 1, 2, 3\}.$$

It follows that the group $\mathcal{G}$ can be realized by setting $A = (123)$ and $X_1 = (12)(34)$.

Let $\mathcal{G}$ be a general permutation-like group without a maximal cycle.

• $|\mathcal{G}_S| = 3$: In this case we get $\mathcal{G}_S =< A >$ and $\mathcal{C}_{2,2} = \emptyset$ therefore $\mathcal{C}_4 = \emptyset$. The order of $\mathcal{G}$ is then 6 which implies the existence of a matrix $T \in \mathcal{C}_2$. We must treat two cases:

(a) If $AT = TA$ the matrix $B = AT \in \mathcal{C}_{3,2}$ is an element of order 6 and

$$\mathcal{G} =< B > .$$

(b) If $AT = A^2T$ the group $\mathcal{G}$ can be realized by $A = (123)$ and $T = (12)$.

• $|\mathcal{G}_S| = 6$: Let $< A >$ be the unique Sylow 3-subgroup, where A has the form (c3d). We write $\mathcal{C}_{2,2} = \{X, X_2, X_3\}$ and assume that

$$X = \begin{bmatrix} 1 & & & & \\ & -1 & & & \\ & & 1 & & \\ & & & 0 & 1 \\ & & & 1 & 0 \end{bmatrix}, \tag{p22}$$

where $X_2 = AX$ and $X_3 = A^2X$. Let $\{I, X_1, T, T'\}$ be a Sylow 2-subgroup. Suppose that $AT = TA$. Then by Lemma 4.25 we can find a basis such that X has the form (p22), A has the form (c3d) and T is a diagonal matrix. We get $T_{22} = -1$, since otherwise the spectrum of the product AT would either contain $-\alpha$ or $-\alpha^2$, or -1 would be a triple eigenvalue for the product XT. It follows that $T' = XT$ is of the form

$$T' = \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 0 & 1 \\ & & & 1 & 0 \end{bmatrix},$$

which give us $T'A = A^2T'$. By changing the roles of T and T' we cover the remaining case.

We have found out that the matrices A, X and T generate a group which can be represented by the following permutations $A = (345)$, $X = (12)(34)$ and $T = (12)$.

• $|\mathcal{G}_S| = 12$: In this case we have the unique Sylow 2-subgroup $\{I, X_1, X_2, X_3\}$ in $\mathcal{G}_S$ therefore all the Sylow 2-subgroups in $\mathcal{G}$ have the form

$$S = \{I, X_1, X_2, X_3, T_1, T_2, Z_1, Z_2\}.$$

We write $S = 1 \oplus S'$. It is easy to verify that at least one of matrices T_1, T_2, Z_1, Z_2 lies in the set $\mathcal{C}_4$. Case $n = 4$ shows that S' is equivalent to a group of permutation matrices, where Z_1 corresponds to cycle (1234), X_1 to permutation (13)(24), and

T_1, T_2 respectively to transpositions (12) and (24). Therefore each matrix $T \in \mathcal{C}_2$ commutes with exactly one of the matrices X_1, X_2, X_3.
Suppose that we can find a matrix $B \in \mathcal{C}_{3,2}$. Then matrices $T = B^3 \in \mathcal{C}_2$ and $A = B^2 \in \mathcal{C}_3$ commute. From the structure of 'even part' $\mathcal{G}_S$ we see that T commutes, say, with the matrix X_1. Since $X_2 = A^{-1}X_1A$ and $X_3 = A^{-2}X_1A^2$, matrix T also commute with matrices X_2 and X_3. For this is impossible we conclude that

$$\mathcal{C}_{3,2} = \emptyset.$$

We can therefore write $\mathcal{G} = 1 \oplus \mathcal{G}'$, where $\mathcal{G}'$ satisfies the assumptions of Theorem 4.18. It follows that $\mathcal{G}'$ and $\mathcal{G}$ are equivalent to some groups of permutation matrices.

2. $\mathcal{C}_3 = \emptyset$: In this case we clearly get $\mathcal{C}_{3,2} = \emptyset$ and $\mathcal{G}_S = \mathcal{C}^0_{2,2}$.

• $\mathcal{C}_4 \neq \emptyset$: If we write $\mathcal{G} = 1 \oplus \mathcal{G}'$ then $\mathcal{G}'$ satisfies the assumptions of Theorem 4.18. As before this completes the proof.

• $\mathcal{C}_4 = \emptyset$: Under this assumption, $\mathcal{G}$ is a commutative group. If $\mathcal{G}_S$ has order 4, the order of group $\mathcal{G}$ is 8 and $\mathcal{G} = \{I, X_1, X_2, X_3, T_1, T_2, T_3, T_4\}$ where $X_i \in \mathcal{C}_{2,2}$ and $T_j \in \mathcal{C}_2$. The diagonal form of $\mathcal{G}$ shows us that this is impossible, since otherwise -1 is a triple eigenvalue of at least one of the products X_1T_j. In the remaining case we have $\mathcal{G}_S = \{I, X\}$, where $X \in \mathcal{C}_{2,2}$ and $\mathcal{G} = \{I, X, T_1, T_2\}$. We can realize the group $\mathcal{G}$ by setting $X = (12)(34)$, $T_1 = (12)$ in $T_2 = (34)$. As we have checked all the cases, the proof is complete. □

Combining the last two theorems we get the following main result of this section.

Theorem 4.27 *Every permutation-like group $\mathcal{G} \subset \mathbb{C}^{5\times5}$ is equivalent to a group of permutation matrices.*

References

[1] J. Bernik, R. Drnovšek, T. Košir, M. Omladič, H. Radjavi, *Irreducible semigroups of matrices with eigenvalue one*, Semigroup forum **67** (2003), 271–287.

[2] A. Borel, *Linear algebraic groups,* Springer-Verlag, New York 1991.

[3] J. V. Brawley, *Scalar polynomial functions on the nonsingular matrices over a finite field*, Linear Algebra and Applications **174** (1992), 1–12.

[4] G. Birkhoff, S. MacLane, *A survey of modern algebra*, Macmillan, New York, 1965.

[5] M. Burrow, *Representation theory of finite groups*, Academic press, New York, 1971.

[6] G. Cigler, *On matrix groups with finite spectrum*, Linear Algebra and Applications **286** (1999), 287–295.

[7] G. Cigler, *Matrix groups with independent spectra*, Linear Algebra and Applications **327** (2001), 27–40.

[8] G. Cigler, *Permutation-like matrix groups*, in preparation.

[9] D. Ž. Djokovič, *Exponential map and automorphism group of a connected Lie group*, American Journal of Mathematics **99** (1977), 973–984.

[10] L. Dornhoff, *Group Representation Theory (part A)*, Marcel Dekker, New York, 1971.

[11] W. Feit, *Characters of Finite Groups*, W. A. Benjamin, New York, 1967.

[12] W. Feit, *The Representation Theory of Finite Groups*, North-Holland Publishing Company, Amsterdam-New York-Oxford, 1982.

[13] M. Fried, *Irredicibility results for separated equations*, Journal of Pure and Applied Algebra **48** (1987), 1–23.

[14] G. P. Hochschild, *Basic theory of algebraic groups and Lie algebras*, Springer-Verlag, New York 1981.

[15] S.-T. Hu, *Elements of modern algebra*, Holden-Day, San Francisco, 1965.

[16] I. Kaplansky, *Lie algebras and locally compact groups,* The University of Chicago press, 1971.

[17] S. Lang, *Algebra,* Addison-Wesley, 1965.

[18] M. Omladič, H. Radjavi, *Irreducible semigroups with multiplicative spectral radius*, Linear Algebra and Applications **251** (1997), 59–72.

[19] B. Peterson, E. Taft, *Hopf algebra of linearly recursive sequences*, Aequationes Mathematicae **20** (1980), 1–17.

[20] H. Radjavi, P. Rosenthal, *Simultaneous triangularization*, Springer-Verlag, New York, 2000.

[21] H. Radjavi, P. Rosenthal, *Invariant Subspaces*, Springer-Verlag, New York 1973.

[22] R. W. Richardson, P. J. Slodowy, *Minimum vectors for real reductive algebraic groups*, J. London Math. Soc. **42** (1990), 409–429.

[23] J. J. Rotman, *The Introduction to the Theory of Groups*, Springer-Verlag, New York, 1991.

[24] J. P. Serre, *Algebraic groups and class fields*, Springer-Verlag, New York 1988.

[25] A. Simonič, *Matrix Groups With Positive Spectra*, Linear Algebra and Applications **173** (1992), 57–76.

[26] D. A. Suprunenko, *Matrix Groups*, AMS Providence, Rhode Island, 1976.

[27] D. A. Suprunenko, *Solvable and Nilpotent Linear Groups*, AMS Providence, Rhode Island, 1963.

[28] M. E. Sweedler, *Hopf Algebras*, Benjamin, New York 1969.

[29] W. C. Waterhouse, *Introduction to affine group schemes,* Springer-Verlag, New York 1979.

Izjava

Izjavljam, da je to delo rezultat lastnega raziskovalnega dela.

Gregor Cigler