ON GROUPS GENERATED BY ELEMENTS OF PRIME ORDER

L. Grunenfelder, T. Košir, M. Omladič, and H. Radjavi

Abstract. In the first part of the paper we give a characterization of groups generated by elements of fixed prime order p. In the second part we study the group $G_n^{(p)}$ of $n \times n$ matrices with the p-th power of the determinant equal to 1 over a field F containing a primitive p-th root of 1. It is known that the group $G_n^{(2)}$ of $n \times n$ matrices of determinant ± 1 over a field F and the group $SL_n(F)$ are generated by their involutions and that each element in these groups is a product of four involutions. We consider some subgroups G of $G_n^{(p)}$ and study the following problems: Is G generated by its elements of order p ? If so, is every element of G a product of k elements of order p for some fixed integer k ? We show that $G_n^{(p)}$ and $SL_n(F)$ are generated by their elements of order p and that the bound k exists and is equal to 4. We show that every universal p-Coxeter group has faithful two-dimensional representations over many fields F (including $\mathbb{R}$ and $\mathbb{C}$). For a universal p-Coxeter group of rank ≥ 2 for $p \geq 3$ or of rank ≥ 3 for $p = 2$ there is no bound k.

MSC: 15A23, 20F55, 51N30

Keywords: groups, elements of prime order, matrix groups, factorization, special linear group, universal Coxeter group

1. Introduction

The purpose of this paper is twofold. We first give a characterization of general groups generated by elements of fixed prime order p and discuss the consequences for simple, solvable and nilpotent groups. In section 3 we study universal Coxeter groups [H, §5.1] and their generalization to universal p-Coxeter groups, i.e. groups G generated by a set X subject only to relations $x^p = 1$ for all $x \in X$. We show that every universal p-Coxeter group G, of finite or infinite rank r, has a two-dimensional faithful representation over many fields (including $\mathbb{R}$ and $\mathbb{C}$). Note that the standard geometric representation of Coxeter groups is on an r-dimensional vector space [H, §5.4]. Our two-dimensional faithful representation of G for $r \geq 2$ is of minimal dimension since G is not commutative.

In the rest of the paper we concentrate on matrix groups generated by elements of order p. Let $G_n^{(p)}$ be the subgroup of the general linear group $GL_n(F)$ consisting of all matrices A with $(\det A)^p = 1$. The case of matrix groups $G_n^{(2)}$ generated by involutions, i.e. matrices J with $J^2 = I$, has been studied previously. In [GHR] the authors show that $G_n^{(2)}$ is generated by its involutions; moreover, every element in $G_n^{(2)}$ is a product of four involutions

Research supported in part by the NSERC of Canada and by the Ministry of Science and Technology of Slovenia.

but not always a product of three involutions. In [KN] it is shown that the special linear group $SL_n(F)$ is generated by its involutions and that every element is a product of four involutions, but not always a product of three involutions. We further remark that if the underlying space is an infinite dimensional Hilbert space H then the group of all invertible linear operators on H is generated by involutions and every invertible linear operator on H is a product of at most seven involutions [R]. It is an open problem whether each element can be expressed as a product of six involutions; however, four involutions do not suffice in general.

In this paper we consider the following general problem for a subgroup G of $G_n^{(p)}$: Is G generated by its elements of fixed prime order p ? If it is, does there exist an integer k such that every member of G is expressible as a product of k elements of order p from G ? If so, what is the minimal number k ? Not every subgroup of $G_n^{(p)}$ is generated by its elements of order p, of course, as the example of all upper-triangular unipotent matrices (i.e. matrices of the form $I + N$ with N nilpotent) shows. Also, even when the group G is generated by its elements of order p, no finite k may exist. We show that this is the case for universal p-Coxeter groups of rank ≥ 2 for $p \geq 3$ and of rank ≥ 3 for $p = 2$.

Our main subjects of study in sections 4 and 5 are the group $G_n^{(p)}$ and two well-known subgroups, namely the group $T_n^{(p)}$ of all upper-triangular matrices with diagonal entries in the set $\{1, \theta, \theta^2, \ldots, \theta^{p-1}\}$, where θ ($\neq 1$) is a p-th root of 1, and the special linear group $SL_n(F)$. We prove that these groups are generated by their elements of order p, and we show that each element is a product of 4 elements of order p in the group. It remains an open problem if, in general, this bound can be improved.

2. General Remarks on Groups Generated by Elements of Fixed Prime Order

Let p be a fixed prime number. The category of groups generated by elements of order p is closed under quotients, coproducts and finite products. Moreover, it is obvious that a semi-direct product $G = N \ltimes Q$ of groups generated by elements of order p is itself generated by elements of order p.

2.1. Theorem. *Let G be a group and let p be a prime number. Then G is generated by elements of order p if and only if $\eta_* : \mathrm{Hom}(\boldsymbol{Z}_p, G) \to \mathrm{Hom}(\boldsymbol{Z}_p, Q)$ is non-trivial for every non-trivial quotient group $Q = G/H$ with $\eta : G \to Q$ the quotient map.*

Proof. First assume that $\eta_* : \mathrm{Hom}(\boldsymbol{Z}_p, G) \to \mathrm{Hom}(\boldsymbol{Z}_p, Q)$ is non-trivial for every non-trivial quotient map $\eta : G \to Q$. If N is the subgroup of G generated by all elements of order p then $N \neq 1$, since $\mathrm{Hom}(\boldsymbol{Z}_p, G)$ has at least two elements, and N is a normal subgroup of G. Suppose that the quotient group $Q = G/N$ is not trivial. Then by hypothesis $\eta_* : \mathrm{Hom}(\boldsymbol{Z}_p, G) \to \mathrm{Hom}(\boldsymbol{Z}_p, Q)$ is not trivial, so that there is an element x of order p in G such that $\eta(x)$ is an element of order p in Q. But then x is not in N, in contradiction to the assumption that N contains all elements of order p. Conversely, if G is generated by elements of order p, then so is every non-trivial quotient map $\eta : G \to Q$. Hence $\eta_*(x) \neq 1$

for some $x \in \mathrm{Hom}(\boldsymbol{Z}_p, G)$, so that $\eta_* : \mathrm{Hom}(\boldsymbol{Z}_p, G) \to \mathrm{Hom}(\boldsymbol{Z}_p, Q)$ is non-trivial. □

2.2. Corollary. *A solvable group G is generated by elements of order p if and only if G_{ab} is an elementary abelian p-group and every epimorphism $\rho : G \to \boldsymbol{Z}_p$ splits.*

Proof. If G is generated by elements of order p then, invoking Theorem 2.1, we see that $\rho_* : \mathrm{Hom}(\boldsymbol{Z}_p, G) \to \mathrm{Hom}(\boldsymbol{Z}_p, \boldsymbol{Z}_p)$ is non-trivial for every epimorphism $\rho : G \to \boldsymbol{Z}_p$. Hence, there is a homomorphism $\kappa : \boldsymbol{Z}_p \to G$ such that $\rho \circ \kappa = 1$. Moreover, G_{ab} is generated by elements of order p, since every quotient of G is. But an abelian group is generated by elements of order p if and only if it is an elementary abelian p-group. Conversely, if $\eta : G \to Q$ is a non-trivial quotient then Q is solvable, Q_{ab} is not trivial and the square of epimorphisms

$$\begin{array}{ccc} G & \xrightarrow{\eta} & Q \\ \downarrow & & \downarrow \\ G_{ab} & \xrightarrow{\eta_{ab}} & Q_{ab} \end{array}$$

commutes. Moreover, Q_{ab} is an elementary abelian p-group, since G_{ab} is, and every epimorphism $\rho : G \to Q \to Q_{ab} \to \boldsymbol{Z}_p$ splits, which implies that $\rho_* : \mathrm{Hom}(\boldsymbol{Z}_p, G) \to \mathrm{Hom}(\boldsymbol{Z}_p, Q)$ is not trivial. By Theorem 2.1 the group G is generated by elements of order p. □

2.3. Corollary. *Let G be a solvable group such that the canonical epimorphism $\eta : G \to G_{ab}$ splits. Then G is generated by elements of order p if and only if G_{ab} is an elementary abelian p-group.*

Proof. Every epimorphism $\rho : G \to \boldsymbol{Z}_p$ has a factorization of the form $\rho = \sigma \circ \eta : G \to G_{ab} \to \boldsymbol{Z}_p$. The epimorphism σ splits, since G_{ab} is an elementary abelian p-group. Moreover, the composite of split epimophisms splits. □

2.4. Corollary. *If a finite nilpotent group G is generated by elements of order p then G is a p-group.*

Proof. The unique Sylow p-subgroup P of G is not trivial and contains all elements of order p, so that $P = G$. □

2.5. Proposition. *A simple group G is generated by elements of order p if and only if it contains an element of order p.*

Proof. The subgroup N of G generated by all elements of order p is not trivial and normal in G. Thus, $N = G$, since G is simple. □

In the following result we assume that $p = 2$.

2.6. Theorem. *If G is generated by involutions then $G^2 = G'$.*

Proof. The identity $(xy)^2 = [x, y]yx^2y$ holds in every group. If G is generated by involutions then every element is of the form $z = x_1x_2 \dots x_n$, where $x_i^2 = 1$ for $i = 1, 2, \dots, n$. The identity $(zx_{n+1})^2 = [z, x_{n+1}]x_{n+1}z^2x_{n+1}$ now shows by induction that every square in G is a product of commutators. To prove the converse, we use the identity $[x, y] = x^2(x^{-1}y)^2y^{-2}$, which holds in every group, and thus we see that every commutator is a product of squares. □

2.7. Examples. Here are some groups generated by involutions. We do not list groups, such as reflection groups or Coxeter groups, that are 'by their very definition' obviously generated by involutions.

(1) An abelian group is generated by involutions if and only if it is an elementary abelian 2-group.
(2) Every non-abelian finite simple group has even order, hence contains an involution. It is therefore generated by involutions by Proposition 2.5.
(3) The symmetric groups S_n are generated by involutions for $n \geq 2$ and so are the alternating groups A_n for $n \geq 5$. The group $A_3 \cong \boldsymbol{Z}_3$ is abelian and $A_4/V \cong \boldsymbol{Z}_3$, so that neither A_3 nor A_4 is generated by involutions.
(4) All the dihedral groups, including the infinite dihedral group, are generated by involutions.

2.8. Examples. Next we list some groups that are generated by their elements of order p. Groups in (2) and (3) will be studied in more detail in the second part of our paper.

(1) An abelian group is generated by elements of order p if and only if it is an elementary abelian p-group.
(2) The projective special linear group $PSL_n(F)$ is a simple group if the characteristic of F is not 2 and F has at least seven elements. Moreover,

$$PSL_n(F) \cong SL_n(F)/Z$$

is the quotient of the special linear group $SL_n(F)$ by its center Z, and Z is the cyclic group of n-th roots of unity in F. Every proper normal subgroup N of $SL_n(F)$ is contained in the center Z since $PSL_n(F)$ is simple and $SL_n(F)$ is perfect.

The authors in [GHR] and [KN] show that $G_n^{(2)} \cong SL_n(F) \ltimes \mathbb{Z}_2$ and $SL_n(F)$ are generated by involutions, i.e. elements of order $p = 2$. Using our results we now give a different proof of their results and moreover we show that $PSL_n(F)$, $SL_n(F)$ and $G_n^{(p)} \cong SL_n(F) \ltimes \mathbb{Z}_p$ are generated by elements of order p for any prime p. For $n \leq p$ we assume there is $\theta \in F$ such that $\theta^p = 1$ but $\theta \neq 1$.

If $p = 2$ then the two elements $S, T \in GL_n(F)$

$$S = \begin{pmatrix} 1 & & & & & \\ & & & & & 1 \\ & & & & 1 & \\ & & & \iddots & & \\ & & 1 & & & \\ & 1 & & & & \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} & & & & & 1 \\ & & & & 1 & \\ & & & \iddots & & \\ & & 1 & & & \\ 1 & & & & & \end{pmatrix}$$

are involutions with $\det S = (-1)^{(n-2)(n-1)/2}$ and $\det T = (-1)^{(n-1)n/2}$. Now $T \in SL_n(F)$ if $n = 4k$, $S \in SL_n(F)$ if $n = 4k+1$ or $4k+2$ and $-S \in SL_n(F)$ if $n =$

$4k+3$, but they are not in the center Z of $SL_n(F)$. It follows from Theorem 2.1 and Proposition 2.5 that $PSL_n(F)$ and $SL_n(F)$ are generated by involutions. Moreover, the semi-direct product $G_n^{(2)} \cong SL_n(F) \ltimes \mathbb{Z}_2$ is also generated by involutions.

For $p \geq 3$ and $n \geq p$ the matrix

$$S = \begin{pmatrix} P & 0 \\ 0 & I \end{pmatrix}, \quad \text{where} \quad P = \begin{pmatrix} & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \\ 1 & & & & & \end{pmatrix}$$

is a $p \times p$ cyclic matrix, is an element of $SL_n(F)$ of order p and is not in the center Z. If $2 \leq n < p$ and there is $\theta \in F$ such that $\theta^p = 1$ but $\theta \neq 1$ then the matrix

$$T = \begin{pmatrix} \theta & & & & & \\ & \theta^{-1} & & & & \\ & & 1 & & & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}$$

is in $SL_n(F)$ and $T \notin Z$. In all of the above cases it follows from Theorem 2.1 and Proposition 2.5 that $PSL_n(F)$ and $SL_n(F)$ are generated by their elements of order p. Moreover, the semi-direct product $G_n^{(p)} \cong SL_n(F) \ltimes \mathbb{Z}_p$ is also generated by elements of order p. In section 5 we will show for both groups $G_n^{(p)}$ and $SL_n(F)$ that every element is the product of 4 elements of order p from the group.

(3) Let $T_n^{(p)}$ be the subgroup of $GL_n(F)$ consisting of upper-triangular matrices with spectrum in the set $\{1, \theta, \ldots, \theta^{p-1}\}$, where $\theta^p = 1$ and let $T_n^{(p)+} = T_n^{(p)} \cap SL_n(F)$. Here we assume that $\theta \in F$, $\theta \neq 1$. These groups have the same commutator subgroup, the upper-triangular unimodular group $U_n(F)$, which is nilpotent, and they are therefore solvable. The abelianizations $T_{n\ ab}^{(p)}$ and $T_{n\ ab}^{(p)+}$ are elementary abelian p-groups of rank n and $n-1$, respectively, and the correponding projection maps split. By Corollary 2.3 both groups are generated by elements of order p. In section 4 we will consider the group $T_n^{(p)}$ again and show that each of its elements is a product of 4 of its elements of order p.

3. The Universal Coxeter Groups

A group G generated by a set X, subject only to the relations $x^2 = 1$ for all $x \in X$, is called a universal Coxeter group of rank $|X|$ [H, Chapter 5]. More generally, for a fixed prime p, we call a group G a universal p-Coxeter group if it is generated by a set X, subject only to the relations $x^p = 1$ for all $x \in X$. Such a group is isomorphic to the free product of $|X|$ copies of the cyclic group of order p, or equivalently, a semi-direct product of a free group of rank $|X| - 1$ and a cyclic group of order p. If $|X| = 2$ and $p = 2$ then G is the infinite dihedral group, and every element is a product of two involutions. However, we will show that when $|X| \geq 2$ for $p \geq 3$ or $|X| \geq 3$ for $p = 2$ there is no upper bound on the number of factors required to express each element of G as a product of elements of order

p. If $p = 2$ the group G has a faithful representation of degree $|X|$ over $\mathbb{R}$ (see [H, p. 113]). But we shall see below that every universal Coxeter group has a faithful representation of degree 2 over many fields (including $\mathbb{R}$ and $\mathbb{C}$).

Let (G, X) be a universal p-Coxeter group. Consider X as an alphabet. A word $w = x_1^{j_1} x_2^{j_2} \dots x_k^{j_k}$, with $x_i \in X$ and $k \geq 1$, is called reduced if $x_i \neq x_{i+1}$ for $i = 1, 2, \dots, k-1$, and $1 \leq j_i \leq p-1$ for $i = 1, 2, \dots, k$. We call $l(w) = k$ the length of w. Let $l_x(w)$ be the number of indices i such that $x_i = x$ in the reduced word w, and $l_{x^k y^k}(w)$ the number of occurances of the word $x^k y^k$ in w, i.e. the number of indices i such that $x_i = x$, $x_{i+1} = y$ and $j_i = j_{i+1} = k$. It is an easy observation that each element g in G has a unique presentation which is a reduced word w. We define $l(g) = l(w)$, $l_x(g) = l_x(w)$ and $l_{x^k y^k}(g) = l_{x^k y^k}(w)$.

Lemma 3.1. *A reduced word $w = x_1^{j_1} x_2^{j_2} \dots x_k^{j_k}$ is an element of order p if and only if k is odd, say $k = 2l + 1$ for some integer l, $x_i = x_{k+1-i}$ and $j_i + j_{k+1-i} = p$ for $i = 1, 2, \dots, l$.*

Proof. Suppose that $w = x_1^{j_1} x_2^{j_2} \dots x_k^{j_k}$ is a reduced word. Since the generators $x \in X$ are subject only to relations $x^p = 1$ the relation $w^p = 1$ holds if and only if $x_1 = x_k$, $x_2 = x_{k-1}, \dots, x_l = x_{k+1-l}$ and $j_1 + j_k = p$, $j_2 + j_{k-1} = p, \dots, j_l + j_{k+1-l} = p$, where l is the integer part of $k/2$. Since w is reduced k has to be odd. □

Lemma 3.2. *Let (G, X) be a universal Coxeter group. If $w = q_1 q_2 \dots q_m \in G$, where each q_i is an involution, then*

$$|l_{xy}(w) - l_{yx}(w)| \leq m - 1$$

for each pair $x, y \in X$. If (G, X) is a universal p-Coxeter group, where $p \geq 3$, and $w = q_1 q_2 \dots q_m \in G$, where each q_i is an element of order p, then

$$|l_{xy}(w) - l_{y^{p-1}x^{p-1}}(w)| \leq 2m - 1$$

for each pair $x, y \in X$.

Proof. Suppose (G, X) is a universal p-Coxeter group. If $p = 2$ then it is easy to observe using Lemma 3.1 that $l_{xy}(q) = l_{yx}(q)$ for every involution $q \in G$. Also, if $p \geq 3$ then it is not difficult to show that $\left|l_{xy}(q) - l_{y^{p-1}x^{p-1}}(q)\right| \leq 1$ for every element $q \in G$ of order p. Suppose that $w \in G$ can be expressed in the form $w = q_1 q_2 \dots q_m$, where each q_i is an element of order p. We want to bring w to reduced form. A pair xy is cancelled completely only by a pair $y^{p-1}x^{p-1}$, since $(xy)^{-1} = y^{p-1}x^{p-1}$. The number of subwords xy can change without the number of subwords $y^{p-1}x^{p-1}$ changing, or conversely, only when just one of the letters x or y is cancelled. This can happen in w at most once for each pair $q_i q_{i+1}$ of consecutive elements of order p. There are $m - 1$ such pairs. If $p = 2$ it follows that $|l_{xy}(w) - l_{yx}(w)| \leq m - 1$ and if $p \geq 3$ it follows that $\left|l_{xy}(w) - l_{y^{p-1}x^{p-1}}(w)\right| \leq 2m - 1$. □

Theorem 3.3. *If G is a universal p-Coxeter group with $p \geq 3$ and rank ≥ 2 or $p = 2$ and rank ≥ 3 then there is no bound on the number of elements of order p required to express each element of G as a product of elements of order p.*

Proof. Assume first that $p = 2$. Since elements in X are subject only to relations $x^2 = 1$ for all $x \in X$ it suffices to prove the assertion for a universal Coxeter group of rank 3. Namely, if $|X| \geq 4$ then any triple of elements of X generates a subgroup of G which is a universal Coxeter group of rank 3. So let $X = \{x, y, z\}$ be the alphabet. Now for each positive integer n consider the word $w_n = (xyz)^n$. If $w_n = q_1 q_2 \dots q_m$, where each q_i is an involution, then Lemma 3.2 implies that $n \leq m - 1$, i.e. $m \geq n + 1$, since $l_{xy}(w_n) = n$ and $l_{yx}(w_n) = 0$.

If $p \geq 3$ then it suffices to consider the universal p-Coxeter group of rank 2. So let $X = \{x, y\}$. For each positive integer n consider the word $w_n = (xy)^n$. If $w_n = q_1 q_2 \dots q_m$, where each q_i is an element of order p, then Lemma 3.2 implies that $n \leq 2m - 1$, i.e. $m \geq \frac{n+1}{2}$, since $l_{xy}(w_n) = n$ and $l_{y^{p-1}x^{p-1}}(w_n) = 0$. □

For $p = 2$ a (universal) Coxeter group of rank r has a faithful linear representation in $GL_r(\boldsymbol{R})$ (see [H]). The next result shows that every universal p-Coxeter group has faithful two-dimensional representations over various fields, including $\mathbb{R}$ and $\mathbb{C}$.

Theorem 3.4. *Every universal p-Coxeter group (G, X) has faithful two-dimensional matrix representations over any field F containing a subset of cardinality $|X|$ which is algebraically independent over the prime subfield (e.g. $F = \mathbb{R}$ or $\mathbb{C}$).*

Proof. First we consider the case $p = 2$. Let Ω be a subset of F of cardinality $|X| = rank(G)$ which is algebraically independent over the prime subfield. Let H be the subgroup of $GL_2(F)$ generated by the set of involutions

$$S = \left\{ \begin{pmatrix} \omega & 1 - \omega^2 \\ 1 & -\omega \end{pmatrix} | \omega \in \Omega \right\}.$$

Choose a bijection $\phi : X \to S$. We will show that the induced group homomorphism $\Phi : G \to H$, determined by $\Phi(x) = \phi(x)$ for $x \in X$, is bijective. We prove that $\Phi(g)$ cannot be upper-triangular for any reduced word $g \in G \backslash \{1\}$, so in particular $\Phi(g) \neq 1$. Proceed by induction on the length $l(g)$ of the reduced word g. The assertion is obvious if $l(g) = 1$. Let $g = x_1 x_2 \dots x_m$ in G be a reduced word with $l(g) = m$ and let $s_i = \phi(x_i)$. Then $\Phi(g) = s_1 s_2 \dots s_m$ in H. We may write $g = x_1 w_1 x_1 w_2 \dots x_1 w_k$ if $x_m \neq x_1$ or $g = x_1 w_1 x_1 w_2 \dots x_1 w_k x_1$ if $x_m = x_1$, where each w_i is reduced, $l_{x_1}(w_i) = 0$ and $1 \leq l(w_i) < l(g)$. Let $b_i = \Phi(w_i)$ for $i = 1, 2, \dots, k$. If we write

$$s_1 = \begin{pmatrix} \omega & 1 - \omega^2 \\ 1 & -\omega \end{pmatrix} \quad \text{and} \quad b_i = \begin{pmatrix} b_{11}^i & b_{12}^i \\ b_{21}^i & b_{22}^i \end{pmatrix}$$

then by the induction hypothesis none of the b_i is upper-triangular, i.e. $b_{21}^i \neq 0$ for $i = 1, 2, \dots, k$. Moreover, it follows by induction on k that the entries $p_{11}(\omega)$ and $p_{21}(\omega)$ of the matrix

$$h = s_1 b_1 s_1 b_2 \dots s_1 b_k = \begin{pmatrix} p_{11}(\omega) & p_{12}(\omega) \\ p_{21}(\omega) & p_{22}(\omega) \end{pmatrix}$$

are polynomials in ω of degree $2k$ and $2k - 1$, respectively, both with leading coefficient $(-1)^k b_{21}^1 b_{21}^2 \dots b_{21}^k$, while the polynomials $p_{12}(\omega)$ and $p_{22}(\omega)$ have at most degree $2k$ and $2k - 1$, respectively. Thus, neither the matrix h nor the matrix hs_1 is upper-triangular. It

follows that $\Phi(g) = 1$ only for $g = 1$.

Suppose next that $p \geq 3$. Let Ω be a subset of F of cardinality $|X| = rank(G)$ which is algebraically independent over the prime subfield. Let H be the subgroup of $GL_2(F)$ generated by the set

$$S = \left\{ \begin{pmatrix} \omega & \omega^2 - t\omega + 1 \\ -1 & t - \omega \end{pmatrix} | \omega \in \Omega \right\},$$

where θ ($\neq 1$) is a p-th root of 1 and $t = \theta + \theta^{-1}$. Observe that the characteristic polynomial of the matrix

$$s = \begin{pmatrix} \omega & \omega^2 - t\omega + 1 \\ -1 & t - \omega \end{pmatrix}$$

is equal to $\lambda^2 - t\lambda + 1$, so the eigenvalues are θ and θ^{-1}, and s is an element of order p. Furthermore, we find for $k = 2, 3, \dots$, that

$$s^k = \begin{pmatrix} t_k\omega - t_{k-1} & t_k\omega^2 - (t_{k+1} + t_{k-1})\omega + t_k \\ -t_k & -t_k\omega + t_{k+1} \end{pmatrix},$$

where $t_k = \sum_{i=0}^{k-1} \theta^{2i-k+1}$. Note that $t = t_2$ and that $t_k \neq 0$ for $k = 1, 2, \dots , p-1$. Choose a bijection $\phi : X \to S$. We will show that the induced group homomorphism $\Phi : G \to H$, determined by $\Phi(x) = \phi(x)$ for $x \in X$, is bijective. We prove that $\Phi(g)$ cannot be upper-triangular for any reduced word $g \in G \backslash \{1\}$, so in particular $\Phi(g) \neq 1$. Proceed by induction on the length $l(g)$ of the reduced word g. The assertion is obvious if $l(g) = 1$. Let $g = x_1^{j_1} x_2^{j_2} \dots x_m^{j_m}$ in G be a reduced word with $l(g) = m$ and let $s_i = \phi(x_i)$. Then $\Phi(g) = s_1^{j_1} s_2^{j_2} \dots s_m^{j_m}$ in H. We may write $g = x_1^{l_1} w_1 x_1^{l_2} w_2 \dots x_1^{l_k} w_k$ if $x_m \neq x_1$ or $g = x_1^{l_1} w_1 x_1^{l_2} w_2 \dots x_1^{l_k} w_k x_1^{l_{k+1}}$ if $x_m = x_1$, where each w_i is reduced, $l_{x_1}(w_i) = 0$ and $1 \leq l(w_i) < l(g)$. Let $b_i = \Phi(w_i)$ for $i = 1, 2, \dots , k$. If we write

$$s_1^{l_i} = \begin{pmatrix} t_{l_i}\omega - t_{l_i-1} & t_{l_i}\omega^2 - (t_{l_i+1} + t_{l_i-1})\omega + t_{l_i} \\ -t_{l_i} & -t_{l_i}\omega + t_{l_i+1} \end{pmatrix} \quad \text{and} \quad b_i = \begin{pmatrix} b_{11}^i & b_{12}^i \\ b_{21}^i & b_{22}^i \end{pmatrix}$$

then by the induction hypothesis none of the b_i is upper-triangular, i.e. $b_{21}^i \neq 0$ for $i = 1, 2, \dots , k$. Moreover, it follows by induction on k that the entries $p_{11}(\omega)$ and $p_{21}(\omega)$ of the matrix

$$h = s_1^{l_1} b_1 s_1^{l_2} b_2 \dots s_1^{l_k} b_k = \begin{pmatrix} p_{11}(\omega) & p_{12}(\omega) \\ p_{21}(\omega) & p_{22}(\omega) \end{pmatrix}$$

are polynomials in ω of degree $2k$ and $2k-1$, with leading coefficient $t_{l_1} t_{l_2} \dots t_{l_k} b_{21}^1 b_{21}^2 \dots b_{21}^k$ and $-t_{l_1} t_{l_2} \dots t_{l_k} b_{21}^1 b_{21}^2 \dots b_{21}^k$, respectively, while the polynomials $p_{12}(\omega)$ and $p_{22}(\omega)$ have degrees at most $2k$ and $2k-1$, respectively. Thus, neither the matrix h nor the matrix $hs_1^{l_{k+1}}$ is upper-triangular. It follows that $\Phi(g) = 1$ only for $g = 1$. □

4. Upper-Triangular Groups

Let p be a fixed prime number and let θ ($\neq 1$) be a p-th root of 1. We denote by $T_n^{(p)}$ the group of all upper-triangular matrices over the field F with spectrum contained in the set $\{1, \theta, \theta^2, \dots , \theta^{p-1}\}$. In the rest of the paper we assume that $\theta \in F$. In Example 2.8(3) we showed that the group $T_n^{(p)}$ is generated by its elements of order p. We now consider some special elements of the group that are products of 2 elements of order p from the group.

Example 4.1. Let

$$J = \begin{pmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & \ddots & \ddots & \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix}$$

be the $n \times n$ Jordan cell with eigenvalue 1. Then we claim that $J = J_1 J_2$, where the $n \times n$ upper-triangular matrices

$$J_1 = \begin{pmatrix} 1 & \theta & \theta^2 & \theta^3 & \dots & \binom{n-1}{0}\theta^{n-1} \\ & \theta & 2\theta^2 & 3\theta^3 & \dots & \binom{n-1}{1}\theta^{n-1} \\ & & \theta^2 & 3\theta^3 & \dots & \binom{n-1}{2}\theta^{n-1} \\ & & & \theta^3 & \dots & \binom{n-1}{3}\theta^{n-1} \\ & & & & \ddots & \vdots \\ & & & & & \binom{n-1}{n-1}\theta^{n-1} \end{pmatrix}$$

with (i,j)-entry $\binom{j-1}{i-1}\theta^{j-1}$, and

$$J_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ & \theta^{-1} & -\theta^{-1} & \theta^{-1} & \dots & (-1)^{n+2}\theta^{-1}\binom{n-2}{0} \\ & & \theta^{-2} & -2\theta^{-2} & \dots & (-1)^{n+3}\theta^{-2}\binom{n-2}{1} \\ & & & \theta^{-3} & \dots & (-1)^{n+4}\theta^{-3}\binom{n-2}{2} \\ & & & & \ddots & \vdots \\ & & & & & \theta^{-n+1}\binom{n-2}{n-2} \end{pmatrix}$$

with (i,j)-entry $(-1)^{i+j}\theta^{-i+1}\binom{j-2}{i-2}$, are elements of order p. The relation $J = J_1 J_2$ is proved by straightforward calculation if we note that

$$J_1 = \sum_{m=0}^{n-1} \theta^m J^m E_{m+1} \quad \text{and} \quad J_2 = \sum_{m=0}^{n-1} \theta^{-m}(I - \theta N)^{m-1} E_{m+1},$$

where I is the $n \times n$ identity matrix, $N = J - I$ and E_i is the projection on the i-th component, i.e. the $n \times n$ matrix with the only nonzero entry on the i-th place on the diagonal equal to 1. Next we show by induction on k that

$$J_1^k = \sum_{m=0}^{n-1} \theta^m \left(\theta^{k-1} I + (1 + \theta + \ldots + \theta^{k-1})N\right)^m E_{m+1}$$

and

$$J_2^k = \sum_{m=0}^{n-1} \theta^{-km} \left(I - \theta(1 + \theta + \ldots + \theta^{k-1})N\right)^{m-1} E_{m+1}.$$

Relations $J_1^p = I$ and $J_2^p = I$ follow for $k = p$.

In a similar way, for $j = 1, 2, \ldots, p-1$, the Jordan matrix

$$J(\theta^j) = \begin{pmatrix} \theta^j & 1 & & & \\ & \theta^j & 1 & & \\ & & \ddots & \ddots & \\ & & & \theta^j & 1 \\ & & & & \theta^j \end{pmatrix}$$

with eigenvalue θ^j is a product of upper-triangular matrices

$$K_{1j} = G_j J_1 G_j^{-1} \quad \text{and} \quad K_{2j} = \theta^j G_j J_2 G_j^{-1},$$

where G_j is the diagonal matrix

$$G_j = \begin{pmatrix} 1 & & & & \\ & \theta^j & & & \\ & & \theta^{2j} & & \\ & & & \ddots & \\ & & & & \theta^{(n-1)j} \end{pmatrix}.$$

Note that K_{1j} and K_{2j} are also matrices of order p and thus all the Jordan matrices $J(\theta^j)$, $j = 0, 1, \dots, p-1$, are products of two upper-triangular matrices of order p. □

Theorem 4.2. *Every element in $T_n^{(p)}$ is a product of four elements of order p from $T_n^{(p)}$.*

(Here and later we assume that the identity matrix I is an element of order p for any prime p.)

Proof. We use the matrices from Example 4.1. Let A be an arbitrary element of $T_n^{(p)}$. For any given set $\{x_1, x_2, \dots, x_{n-1}\}$ of nonzero elements of F there is a matrix L diagonally similar to the matrix J_1 from 4.1 and such that the entries on the first diagonal above the main diagonal of L are equal to $x_1, x_2, \dots, x_{n-1}$. This can be checked directly if we conjugate J_1 by the diagonal matrix

$$\begin{pmatrix} 1 & & & & \\ & y_1 & & & \\ & & y_2 & & \\ & & & \ddots & \\ & & & & y_{n-1} \end{pmatrix},$$

where $y_i = (i+1)!\,\theta^{\binom{i+1}{2}}(x_1 x_2 \cdots x_i)^{-1}$. As soon as the field has more then 2 elements we can choose the set $\{x_1, x_2, \dots, x_{n-1}\}$ of nonzero elements so that all the entries on the first diagonal above the main diagonal of the product AL are also nonzero. This can be observed easily by direct calculation. Let D denote the diagonal matrix with the diagonal entries equal to the diagonal entries of AL. Then the product ALD^{-1} is similar via an upper-triangular similarity to the matrix J of 4.1. Therefore it is a product of 2 upper-triangular matrices of order p. Our Theorem now follows since L and D are also elements of order p. □

4.3. Question. We do not know whether the bound 4 in Theorem 4.2 is best possible. It follows easily from example 4.1 that each matrix with the spectrum in the set $\{1, \theta, \dots, \theta^{p-1}\}$ is product of 2 elements of order p. However it is not clear whether for $A \in T_n^{(p)}$ these 2 elements can be chosen to be upper-triangular.

5. The Group $G_n^{(p)}$ and the Special Linear Group

Theorem 5.1. *The group $G_n^{(p)}$ is generated by elements of order p. Moreover each element of $G_n^{(p)}$ is a product of 4 elements of order p from $G_n^{(p)}$.*

Proof. The theorem for $p = 2$ is proved in [GHR]. Let $p \geq 3$. We first assume that $A \in G_n^{(p)}$ is not a scalar matrix. By [S, Thm. 1] we can find a lower-triangular matrix L and an upper-triangular matrix U such that A is similar to LU, L is unipotent and

$$U = \begin{pmatrix} \det A & & & & & \\ & 1 & & * & & \\ & & 1 & & * & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & 1 \end{pmatrix}.$$

By Example 4.1 (and its counter-part for lower-triangular matrices) it follows that each of the two matrices L and U is a product of two matrices of order p from $G_n^{(p)}$. The spectra of L and U are contained in $\{1, \det A\}$ and in their Jordan canonical form all the blocks of sizes greater than 1 correspond to the eigenvalue 1. By 4.1 each of these blocks is a product of two blocks of the same size and order p.

It remains to consider the scalar case $A = \alpha I$, where $\alpha^{np} = 1$ as $\omega = \det A = \alpha^n$ is such that $\omega^p = 1$. Observe that for $a \in F,\ a \notin \{0, 1, -1\}$, the matrix

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$$

is the product of two matrices

$$J_1(a) = \begin{pmatrix} \frac{at}{a+1} & a - \left(\frac{at}{a+1}\right)^2 \\ -\frac{1}{a} & \frac{t}{a+1} \end{pmatrix} \quad \text{and} \quad J_2(a) = \begin{pmatrix} \frac{at}{a+1} & a\left(\frac{t}{a+1}\right)^2 - 1 \\ 1 & \frac{t}{a+1} \end{pmatrix},$$

where $t = \theta + \theta^{-1}$, $\theta^p = 1$ and $\theta \neq 1$. Note that $J_1(a)^p = J_2(a)^p = I$, since both $J_1(a)$ and $J_2(a)$ have the characteristic polynomial equal to $\lambda^2 - t\lambda + 1$, and thus θ and θ^{-1} are the eigenvalues. Now if n is even then

$$\alpha I = \begin{pmatrix} \alpha & & & & & \\ & \alpha^{-1} & & & & \\ & & \alpha^3 & & & \\ & & & \ddots & & \\ & & & & \alpha^{n-1} & \\ & & & & & \alpha^{-n+1} \end{pmatrix} \begin{pmatrix} 1 & & & & & \\ & \alpha^2 & & & & \\ & & \alpha^{-2} & & & \\ & & & \ddots & & \\ & & & & \alpha^{-n+2} & \\ & & & & & \omega \end{pmatrix}$$

and if n is odd then

$$\alpha I = \begin{pmatrix} \alpha & & & & & \\ & \alpha^{-1} & & & & \\ & & \alpha^3 & & & \\ & & & \ddots & & \\ & & & & \alpha^{-n+2} & \\ & & & & & \omega \end{pmatrix} \begin{pmatrix} 1 & & & & & \\ & \alpha^2 & & & & \\ & & \alpha^{-2} & & & \\ & & & \ddots & & \\ & & & & \alpha^{n-1} & \\ & & & & & \alpha^{-n+1} \end{pmatrix}.$$

Each 2×2 block of the form

$$\begin{pmatrix} \alpha^i & 0 \\ 0 & \alpha^{-i} \end{pmatrix}$$

is the product of 2 matrices $J_1(\alpha^i)$ and $J_2(\alpha^i)$ of order p. Since $\omega^p = 1$ it follows for both cases n even and n odd that $A = \alpha I$ is a product of 4 matrices of order p. □

Lemma 5.2. *Suppose that $A \in SL_n(F)$ is unipotent. If n is odd or divisible by 4 then A is a product of two involutions from $SL_n(F)$. If $n = 4k + 2$ for some integer $k \geq 1$ then A is a product of 3 involutions from $SL_n(F)$. If $p \geq 3$ then A is a product of two elements of order p from $SL_n(F)$.*

Proof. Without loss we may assume that

$$A = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_k \end{pmatrix}$$

is in Jordan canonical form. By Example 4.1 each J_i is a product of 2 elements J_{i1} and J_{i2} of order p. Then A is a product of two upper-triangular elements H_1 and H_2 of order p.

Suppose that $p = 2$. Since $\det A = 1$ it follows that $\det H_1 = \det H_2 = \pm 1$. If the latter is equal to 1 then $H_1, H_2 \in SL_n(F)$. It remains to consider the case $\det H_i = -1$ for $i = 1, 2$. If n is odd then $\det(-H_i) = 1$ and therefore $A = (-H_1)(-H_2)$ is a product of two involutions $-H_1, -H_2 \in SL_n(F)$. If $n = 4k$ for some $k \geq 1$ then observe that in the proof one can choose the $(1, 1)$ entry in each J_{i1} so that the diagonal entries in H_1 are alternating 1 and -1. This is achieved by multiplying some of the pairs J_{i1}, J_{i2} by -1. Now $\det H_1 = 1$ and since $\det A = 1$, we have $\det H_2 = 1$. So $A = H_1 H_2$ is a product of two involutions $H_1, H_2 \in SL_n(F)$.

Consider next the case $n = 4k + 2$ for some $k \geq 1$. First assume that one of the blocks, say J_l, is of odd size. By multiplying both J_{l1} and J_{l2} by -1, if necessary, we are able to change H_1 so that $\det H_1 = 1$. If all of the blocks in A are of even size then multiply A by

$$G = \begin{pmatrix} -1 & 1 & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & 1 & & \\ & & & & -1 & 1 \\ & & & & & 1 \end{pmatrix}$$

which is an involution of determinant 1. The product

$$GA = \begin{pmatrix} -1 & 0 & 1 & & & \\ & 1 & 1 & & & \\ & & \ddots & & & \\ & & & 1 & 1 & 0 \\ & & & & -1 & 0 \\ & & & & & 1 \end{pmatrix}$$

has a Jordan chain of length 1 corresponding to 1 and hence it is a product of two upper-triangular involutions K_1, K_2 with $\det K_i = 1$ as shown above if one block is of odd size. Then it follows that A is a product of 3 involutions G, K_1 and K_2 from $SL_n(F)$.

To conclude the proof consider the case $p \geq 3$. Fix an integer k. Observe that by multiplying the $(1,1)$ entries of the blocks J_{1i} and J_{2i} by θ^{j_i} and θ^{-j_i}, respectively, for an appropriate integer j_i we can assume that the diagonal entries of H_1 form a sequence $\theta^k, \theta^{k+1}, \ldots, \theta^{k+n-1}$. Note that after these multiplications the new matrices H_1' and H_2' are still elements of order p. The proof will be complete if we choose the integer k in such a way that $\det H_1' = 1$. Then also $\det H_2' = 1$ since $\det A = 1$. If n is odd, say $n = 2l+1$, then for $k = -l$ it follows that $\det H_1' = 1$. If n is even, say $n = 2l$, then for some integers a and b we have $-2a + pb = n - 1$, since 2 and p are relatively prime. For $k = a$ it follows that $\det H_1' = \Pi_{i=0}^{n-1} \theta^{n+i} = \theta^{l(2a+n-1)} = \theta^{lpb} = 1$. □

Remark 5.3. If $p = 2$ and $n = 4k+2$ then the number 3 in Lemma 5.2 cannot, in general, be replaced by 2. For example if $n = 6$ and A is the 6×6 Jordan cell with eigenavalue 1, then A has a 1-dimensional eigenspace at the eigenvalue 1. Consider a product $J_1 J_2$ of two involutions $J_1, J_2 \in SL_6(F)$. Since $\det J_i = 1$, it follows that both $\dim \ker(J_i - I)$ and $\dim \ker(J_i + I)$ are even, equal to $0, 2, 4$ or 6. If we assume that 1 is the only eigenvalue of $J_1 J_2$ then it is easy to observe that at least one of $\dim(\ker(J_1 - I) \cap \ker(J_2 - I))$ and $\dim(\ker(J_1 + I) \cap \ker(J_2 + I))$ is ≥ 2. This is a consequence of the fact that the intersection of two subspaces of dimension ≥ 4 has dimension at least 2. Therefore the eigenspace at 1 for $J_1 J_2$ is always of dimension ≥ 2, i.e. it is never 1-dimensional. So A is not a product of two involutions from $SL_6(F)$. □

Theorem 5.4. *The special linear group $SL_n(F)$ is generated by elements of order p. Moreover each element of $SL_n(F)$ is a product of 4 elements of order p from $SL_n(F)$.*

Proof. The case $p = 2$, i.e. the case of generation of $SL_n(F)$ by involutions, is proved in [KN]. Suppose that $p \geq 3$. We first assume that $A \in G_n^{(p)}$ is not a scalar matrix and we argue as in the first part of the proof of Theorem 5.1. By [S, Thm. 1] we can find a lower-triangular matrix L and an upper-triangular matrix U such that A is similar to LU, and both L and U are unipotent. By Lemma 5.2 it follows that each of the matrices L and U is a product of two matrices from $SL_n(F)$ of order p.

It remains to consider the scalar case $A = \alpha I$, where $\alpha^n = 1$. We argue as in the second part of the proof of Theorem 5.1. We use the same notation as in that proof. Note that now $\omega = 1$. Since the matrices $J_1(\alpha^i)$ and $J_2(\alpha^i)$ both have determinant 1, it follows that $A = \alpha I$ is a product of 4 elements of order p from $SL_n(F)$. □

Remark 5.5. If $n \leq p$ then each non-scalar matrix in $SL_n(F)$ is a product of two elements of order p in $SL_n(F)$. This follows from the fact that in [S, Thm. 1] we can choose the diagonal entries in L and U to be all different powers of ω. If $n = p$ then each matrix in $SL_n(F)$ is a product of two elements of order p in $SL_n(F)$. If $n < p$ then each matrix in $SL_n(F)$ is a product of three elements of order p, since $\alpha I = D(\alpha D^{-1})$, where $D = \mathrm{diag}(\omega, 1, \ldots, 1, \omega^{-1})$. We can adapt the above remark to the case of $G_n^{(p)}$ and show that for $n \leq p$ each non-scalar matrix in $G_n^{(p)}$ is a product of two matrices of order p in $G_n^{(p)}$ and that $\alpha I \in G_n^{(p)}$ is a product of three elements of order p in $G_n^{(p)}$.

Questions 5.6. Several questions arise naturally at this point. We indicate some but do not pursue them further.

One can study the problems of our paper under fewer assumptions. First, what if F does not contain a primitive p-th root of 1. Then $G_n^{(p)}(F) = SL_n(F)$. The case $p = 2$ was studied in [KN]; for $p \geq 3$ we do not know whether Theorem 5.4 holds for such a field. Even more generally, one can drop the assumption that p is a prime and study these problems for p an arbitrary integer ≥ 2.

Acknowledgement. The authors wish to thank Professor Carlos A.M. André for pointing out an error in an earlier draft of the paper.

References

[GHR] W. H. Gustafson, P. R. Halmos, H. Radjavi. *Products of Involutions.* Linear Alg. Appl. **13**, 157–162, 1976.

[H] J. E. Humphreys. *Reflection Groups and Coxeter Groups.* Cambridge Univ. Press, 1990.

[KN] F. Knüppel and F. Nielsen, $SL(V)$ *is* 4*-reflectional.* Geometriae Dedicata **38**, 301–308, 1991.

[R] H. Radjavi. *The Group Generated by Involutions.* Proc. Royal Irish Acad. **81A**, 9–12, 1981.

[S] A.R. Sourour. *A Factorization Theorem for Matrices.* Lin. Multilin. Alg. **19**, 141–147, 1986.

L. Grunenfelder and H. Radjavi : Department of Mathematics, Statistics and Computing Science, Dalhousie University, Halifax, Nova Scotia, Canada, B3H 3J5
e-mail: luzius@mscs.dal.ca, radjavi@mscs.dal.ca

T. Košir and M. Omladič : Department of Mathematics, University of Ljubljana, Jadranska 19, 1000 Ljubljana, Slovenia
e-mail: tomaz.kosir@fmf.uni-lj.si, matjaz.omladic@uni-lj.si