ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Finite Fields and Their Applications 11 (2005) 738–747

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Order of elements in the groups related to the general linear group

M.R. Darafsheh*

Department of Mathematics, Statistics and Computer Science, Faculty of Science, University of Tehran, Tehran, Iran

Received 15 August 2004; revised 6 December 2004
Available online 19 January 2005

Abstract

For a natural number n and a prime power q the general, special, projective general and projective special linear groups are denoted by $GL_n(q)$, $SL_n(q)$, $PGL_n(q)$ and $PSL_n(q)$, respectively. Using conjugacy classes of elements in $GL_n(q)$ in terms of irreducible polynomials over the finite field $GF(q)$ we demonstrate how the set of order elements in $GL_n(q)$ can be obtained. This will help to find the order of elements in the groups $SL_n(q)$, $PGL_n(q)$ and $PSL_n(q)$. We also show an upper bound for the order of elements in $SL_n(q)$.

MSC: primary 20H30; secondary 12E20

Keywords: General linear group; Special linear group; Finite field

1. Introduction and preliminaries

For a finite group G, let $\omega(G)$ denote the set of orders of elements of G and call $\omega(G)$ the spectrum of G. Of course the set $\omega(G)$ is closed and partially ordered by the divisibility relation. Hence $\omega(G)$ is uniquely determined by the set $\mu(G)$ of its maximal elements. One of the recent research problems in finite group theory is that of pure characterization of a finite group G by the set $\omega(G)$. We say that a finite group G is characterizable by $\omega(G)$, in short if every finite group H with $\omega(H) = \omega(G)$ is

* Fax: +98 21 6412178.
E-mail address: daraf@khayam.ut.ac.ir (M.R. Darafsheh).

1071-5797/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2004.12.003

isomorphic to G. One of the first results of this kind is due to Shi [5] who proved that if G is a finite group which contains elements of order $1, 2, 3, 5$ and does not contain elements of any other order, then $G \cong \mathbb{A}_5$.

There are several papers concerning the characterization of the projective special linear groups in low dimensions and for all of them the set of orders for the group in question was already available in the literature, for example in [1]. Now in this paper our intention is to present a method to find $\mu(G)$ for $G = GL_n(q)$, $SL_n(q)$ and $PSL_n(q)$. We used the method of this paper and found $\mu(GL_{14}(2))$ and then characterized this group in [2].

Our method depends on the shape of the conjugacy classes of elements of $GL_n(q)$ described in [3] in terms of polynomials over the Galois field $GF(q)$. Then we find a formula for the order of an element c in a conjugacy class of $GL_n(q)$ and then determine the maximum order of c. Although some results concerning the element orders in $GL_n(q)$ may be known using matrix theory and linear algebra, what makes our investigations interesting is the connection of element orders with polynomials over the Galois field.

Now let us recall some notations and results from [4]. Let $GF(q)$ denote the Galois field with q elements where q is the power of a prime number p. In this paper all polynomials $f(x) \in GF(q)[x]$ have the property that $f(0) \neq 0$, i.e., $f(x)$ is not divisible by x. It is proved in [4, p. 84] that for $f(x) \in GF(q)[x]$ of degree $n \geqslant 1$, there is a positive integer e, $1 \leqslant e \leqslant q^n - 1$, such that $f(x) \mid x^e - 1$. The least positive integer e with the above property is called the order of $f(x)$ and is denoted by $ord(f)$. In particular, it is proved that if $f(x) \in GF(q)[x]$ is irreducible and monic of degree n, then $ord(f) \mid q^n - 1$; moreover, the order of any root of $f(x)$ in the multiplicative group $GF(q^n)^*$ is equal to $ord(f)$.

Order of polynomials is closely related to the order of matrices as follows. Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ be in $GF(q)[x]$ with $a_0 \neq 0$. Then the companion matrix of $f(x)$ is defined to be the $m \times m$ matrix:

$$C(f) = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & 0 \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{bmatrix}.$$

It is easy to verify that $f(x)$ is the characteristic polynomial of $C(f)$, i.e., $\det(xI - C(f)) = f(x)$. Therefore $(-1)^n \det(C(f)) = f(0) = a_0$; hence, $\det(C(f)) = (-1)^n a_0$, so $C(f)$ is an element of $GL_n(q)$. It can be verified that the order of $C(f)$ as an element of $GL_n(q)$ is equal to the order of $f(x)$, i.e., $ord(f) = O(C(f))$. This fact is useful to find the order of elements of $GL_n(q)$.

According to [4], the general formula for the order of a polynomial over $GF(q)$ is Theorem 3.11 in p. 87 which will be stated below.

Lemma 1. *Let* $0 \neq f(x) \in GF(q)[x]$, $q = p^r$, $f(0) \neq 0$. *Let* $f(x) = af_1(x)^{k_1} f_2(x)^{k_2} \cdots f_s(x)^{k_s}$ *be the factorization of* $f(x)$ *as the product of distinct irreducible monic polynomials* $f_i(x)$, $1 \leqslant i \leqslant s$, *and* $a \in GF(q)$, $k_1, \ldots, k_s \in \mathbb{N}$. *Then* $ord(f) = ep^t$, *where* e *is the least common multiple of* $ord(f_1), \ldots, ord(f_s)$, *i.e.,* $e = \mathrm{lcm}(ord(f_1), \ldots, ord(f_s))$ *and* t *is the smallest integer such that* $p^t \geqslant \max\{k_1, \ldots, k_s\}$.

By definition $f(x) \in GF(q)[x]$ of degree $n \geqslant 1$ is called primitive over $GF(q)[x]$ if it is the minimal polynomial of a primitive element of $GF(q^n)$ over $GF(q)$. Hence, it is easy to prove that a polynomial $f(x) \in GF(q)[x]$ of degree n is primitive if and only if it is monic and $ord(f) = q^n - 1$. Since primitive elements exist, the group $GL_n(q)$ contains elements of order $q^n - 1$.

Now let us turn to the conjugacy classes of $GL_n(q)$. In what follows we adopt the notations used in [3]. Let $A \in GL_n(q)$ have characteristic polynomial $\det(xI - A) = f_1^{k_1} \ldots f_s^{k_s}$ where $f_i = f_i(x)$, $1 \leqslant i \leqslant s$, are distinct monic irreducible polynomials over $GF(q)$ and $k_i > 0$. The polynomial x is excluded for the reason of invertability of A. Then A is conjugate to a block diagonal matrix of the form $A \sim diag(U_{v_1}(f_1), U_{v_2}(f_2), \ldots, U_{v_s}(f_s))$, where $v_1, v_2, \ldots, v_s$ are certain partitions of $k_1, k_2, \ldots, k_s$, respectively, and $U_{v_i}(f_i)$ is a certain matrix which will be explained later. This conjugacy class of A is denoted by $c = (f_1^{v_1} f_2^{v_2} \ldots f_s^{v_s})$. Since we are interested in the order of A, we observe that $O(A)$ is equal to the least common multiple, *lcm*, of the orders of the matrices $U_{v_i}(f_i)$, $1 \leqslant i \leqslant s$. But for each partition $(\lambda) \equiv l_1 + l_2 + \cdots + l_r$, $l_1 \geqslant l_2 \geqslant \cdots \geqslant l_r > 0$, of a positive integer k and each polynomial $f = f(x) \in GF(q)[x]$, the matrix $U_\lambda(f)$ is defined to be $U_\lambda(f) = diag(U_{l_1}(f), U_{l_2}(f), \ldots, U_{l_r}(f))$. It is clear that the characteristic polynomial of the matrix $U_\lambda(f)$ is $f(x)^k$. But $U_{l_i}(f)$ is defined according to the following.

Let $f(x) = a_0 + a_1 x + \cdots + a_{d-1} x^{d-1} + x^d$ be a monic polynomial of degree d over $GF(q)$ and let

$$U(f) = U_1(f) = \begin{bmatrix} 0 & 1 & 0 \cdots & 0 \\ 0 & 0 & 1 \cdots & 0 \\ \vdots & & & \\ 0 & 0 & \cdots \cdots & 1 \\ -a_0 & -a_1 & \cdots \cdots & -a_{d-1} \end{bmatrix}$$

be its companion matrix. Then for any natural number m the matrix $U_m(f)$ is defined by

$$U_m(f) = \begin{bmatrix} U(f) & I_d & & O \\ O & U(f) & I_d & \\ \vdots & & & \\ \cdots & \cdots & \cdots & U(f) \end{bmatrix}$$

with m diagonal blocks $U(f)$ where I_d is the $d \times d$ identity matrix. It is clear that the characteristic polynomial of $U_m(f)$ is $f(x)^m$.

As we mentioned earlier, the order of an element in the class $c = (f_1^{v_1} f_2^{v_2} \dots f_s^{v_s})$ is equal to the lcm of the orders of the matrices $U_{v_i}(f_i)$, $1 \leqslant i \leqslant s$. But the order of the matrix $U_{v_i}(f_i)$ divides the order of the polynomial $f_i(x)^{k_i}$, $1 \leqslant i \leqslant s$. This is because v_i is a partition of k_i, and if we take k_i alone as the partition of k_i, then the minimal polynomial of $U_{k_i}(f_i)$ is $f_i(x)^{k_i}$.

Now suppose $A \in GL_n(q)$ has characteristic polynomial $m(x) = \det(xI - A) = f_1^{k_1} f_2^{k_2} \dots f_s^{k_s}$ where $f_i = f_i(x)$, $1 \leqslant i \leqslant s$, are distinct monic irreducible polynomials over $GF(q)$ and $k_i > 0$. Then there is a conjugacy class of A with minimal polynomial $m(x)$. This is simply by taking $v_1 = k_1$, $v_2 = k_2, \dots, v_s = k_s$ as partitions of the respective k_i's. It is obvious that if there is a conjugacy class of type A with minimal polynomial $t(x) = f_1^{k_1} f_2^{k_2} \dots f_s^{k_s}$, then $t(x) \mid m(x)$ and therefore $ord(t) \mid ord(m)$. Hence, as far as the maximum order of elements in the conjugacy class of A is concerned we must calculate $ord(m)$ where $m = m(x)$ is given with the condition $\sum_{i=1}^{m} k_i d_i = n$ where $d_i = \deg(f_i)$, $1 \leqslant i \leqslant s$. But as we mentioned earlier, by Lidl and Niederreiter [4], if $f(x) \in GF(q)[x]$ is a monic irreducible polynomial of degree d, then $ord(f) \mid q^d - 1$ and furthermore there is an irreducible polynomial over $GF(q)$ with order $q^d - 1$. Therefore, using Lemma 1 we obtain the following result for the maximum order of elements in the group $GL_n(q)$.

Corollary 1. *Let $m(x) \in GF(q)[x]$, $m(0) \neq 0$, q the power of a prime p, and let $m(x) = f_1^{k_1} f_2^{k_2} \dots f_s^{k_s}$ be the product of distinct monic irreducible polynomials $f_i(x)$ of degree d_i over $GF(q)$, $1 \leqslant i \leqslant s$. Then $ord(m)$ divides $p^t \times \mathrm{lcm}(q^{d_1}-1, q^{d_2}-1, \dots, q^{d_s}-1)$ where t is the smallest non-negative integer such that $p^t \geqslant \max\{k_1, \dots, k_s\}$. Moreover, if $\sum_{i=1}^{s} k_i d_i = n$, then $GL_n(q)$ has an element with the above order.*

Therefore so far as $\mu(GL_n(q))$ is concerned, first we find all the irreducible polynomials of degree up to n over $GF(q)$ and call them $f_1, f_2, \dots, f_s$. Then we consider all the possible factorizations of the form $f_1^{k_1} f_2^{k_2} \dots f_s^{k_s}$ where $k_i > 0$ and $\sum_{i=1}^{s} k_i d_i = n$, $d_i = \deg(f_i)$. Finally, numbers of the form $p^t \times \mathrm{lcm}(q^{d_1} - 1, q^{d_2} - 1, \dots, q^{d_s} - 1)$ are elements of $\mu(GL_n(q))$ where t is explained in Corollary 1.

We will demonstrate some examples at the end of the paper but as the next step we will explain the order of elements in the groups $SL_n(q)$, $PGL_n(q)$ and $PSL_n(q)$. As usual let $A \in GL_n(q)$ have characteristic polynomial $m(x) = \det(xI - A) = f_1^{k_1} f_2^{k_2} \dots f_s^{k_s}$. We have $m(0) = (-1)^n \det A$, hence, $A \in SL_n(q)$ if and only if $m(0) = f_1(0)^{k_1} f_2(0)^{k_2} \dots f_s(0)^{k_s} = (-1)^n$, i.e., the constant term of $m(x)$ is 1 if n is even and it is -1 if n is odd. Therefore, from those $m(x)$ corresponding to maximum order of elements in $GL_n(q)$ we select those with the constant term $(-1)^n$ and find their orders in the same manner.

Now we consider element orders in $PGL_n(q)$. We know that $PGL_n(q) = \frac{SL_n(q)}{Z}$, where $Z = \{\lambda I \mid \lambda^n = 1,\ \lambda \in GF(q)\}$ is the centre of $GL_n(q)$ which is a cyclic group of order $q - 1$. We know that $A \in GL_n(q)$ is a block diagonal matrix of the shape $A = diag(A_1, \dots, A_s)$ where $A_i \in GL_{k_i d_i}(q)$, $1 \leqslant i \leqslant s$. Let $Z_i = \{\lambda_i I_i \mid \lambda_i \in GF(q)^*\}$ where I_i is the $k_i d_i \times k_i d_i$ identity matrix, $1 \leqslant i \leqslant s$. Let $O(AZ) = \alpha$ and $O(A_i Z_i) = \alpha_i$,

$1 \leqslant i \leqslant s$. Then there exist λ and λ_i in $GF(q)^*$ such that $A^\alpha = \lambda I$ and $A_i^{\alpha_i} = \lambda_i I_i$, where I_i is the identity element of $GL_{k_i d_i}(q)$, $1 \leqslant i \leqslant s$. From $A^\alpha = \lambda I$ we obtain $A_i^\alpha = \lambda I_i$, $1 \leqslant i \leqslant s$, hence $\alpha_i \mid \alpha$, for all $1 \leqslant i \leqslant s$. If we set $l = \mathrm{lcm}(\alpha_1, \ldots, \alpha_s)$, then clearly $l \mid \alpha$. We also have $A_i^l = \mu_i I_i$ for some $\mu_i \in GF(q)^*$. Since $GF(q)^*$ is a cyclic group of order $q-1$, we set $GF(q)^* = \langle a \rangle$ and let $\mu_i = a^{m_i}$, $1 \leqslant i \leqslant s$, $0 \leqslant m_i < q-1$. If γ is the least positive integer for which $\mu_1^\gamma = \mu_2^\gamma = \cdots = \mu_s^\gamma$, then $l\gamma = \alpha$ would be the order of ZA. But from the last identities we obtain $a^{\gamma m_1} = a^{\gamma m_2} = \cdots = a^{\gamma m_s}$. Hence $q-1 \mid \gamma(m_1 - m_i)$, $1 \leqslant i \leqslant s$. we may disregard equal m_i's and assume $q-1 \mid \gamma(m_1 - m_i)$, $m_1 \neq m_i$, for $2 \leqslant i \leqslant s'$. Therefore $q-1 \mid \gamma \gcd(m_1 - m_2, \ldots, m_1 - m_{s'})$ where gcd denotes the greatest common divisor. Hence, the least γ is $\gamma = \frac{q-1}{\gcd(q-1, |m_1-m_2|, \ldots, |m_1-m_{s'}|)}$. Therefore, the order of ZA is $\alpha = \frac{(q-1)\mathrm{lcm}(\alpha_1, \ldots, \alpha_s)}{\gcd(q-1, |m_1-m_2|, \ldots, |m_1-m_{s'}|)}$. The same formula applies for the order of elements in the group $PSL_n(q)$.

2. Bounds for element orders

First we deal with the order of elements in the group $GL_n(q)$. In the introduction we mentioned that $GL_n(q)$ contains elements of order $q^n - 1$. We will show this is the largest number for the order of an element in $GL_n(q)$.

Corollary 2. *If $A \in GL_n(q)$, then $O(A) \leqslant q^n - 1$.*

Proof. Let $c = (f_1^{\nu_1} \ldots f_s^{\nu_s})$ represent a conjugacy class in $GL_n(q)$. Then we know $f(x) = f_1(x)^{k_1} \ldots f_s(x)^{k_s}$ has the property that $\sum_{i=1}^s k_i d_i = n$ and ν_i is a partition of k_i, $1 \leqslant i \leqslant s$, and $f_i(x)$ are distinct monic irreducible polynomials over $GF(q)$ of degree d_i, $1 \leqslant i \leqslant s$. It is obvious that for any matrix A representing class c we have $m(x) \mid f(x)$, where $m(x)$ is the minimal polynomial of A. But then $ord(m) \leqslant ord(f)$ and consequently $ord(A) \leqslant ord(f)$. By Theorem 3.9, in [4, p. 86] we have

$$ord(f) = \mathrm{lcm}(ord(f_1^{k_1}), \ldots, ord(f_s^{k_s})).$$

But being a polynomial of order $k_i d_i$ we have $ord(f_i^{k_i}) \leqslant q^{k_i d_i} - 1$, $1 \leqslant i \leqslant s$. Hence $ord(f) \leqslant \mathrm{lcm}(q^{k_1 d_1} - 1, q^{k_2 d_2} - 1, \ldots, q^{k_s d_s} - 1) \leqslant (q^{k_1 d_1} - 1)(q^{k_2 d_2} - 1) \cdots (q^{k_s d_s} - 1) \leqslant q^{k_1 d_1 + k_2 d_2 + \cdots + k_s d_s} - 1 = q^n - 1$.

This proves that $O(A) \leqslant q^n - 1$. □

Next we investigate an upper bound for the order of elements in $SL_n(q)$, but some of the results are also true for $GL_n(q)$. We remind that a polynomial of degree n over $GF(q)$ is the characteristic polynomial of a matrix in $SL_n(q)$ if and only if $(-1)^n f(0) = 1$.

Lemma 2. *Let $0 \neq f(x) \in GF(q)[x]$ with degree n has order $\frac{q^n-1}{q-1}, n \geqslant 1$. Then $f(x)$ is irreducible over $GF(q)$ and $(-1)^n f(0) = 1$.*

Proof. Let q be the power of a prime number p. Since $ord(f) = \frac{q^n-1}{q-1}$ we have $(ord(f), p) = 1$. Therefore, by Lemma 1, $f(x) = f_1(x)\cdots f_s(x)$, $s \geqslant 1$, where $f_i(x)$ are distinct monic irreducible polynomials over $GF(q)$. If deg $f_i(x) = m_i$, then $ord(f_i) \mid q^{m_i} - 1$, $1 \leqslant i \leqslant s$. If we set $d = \frac{(q^{m_1}-1)\cdots(q^{m_s}-1)}{(q-1)^{s-1}}$, then for all i we have $ord(f_i) \mid d$, which implies $f_i(x) \mid x^d - 1$, hence $f(x) \mid x^d - 1$. Therefore $ord(f) \leqslant d$.

But if $s \geqslant 2$, then we have $d < \dfrac{q^{m_1+\cdots+m_s} - 1}{q-1} = \dfrac{q^n - 1}{q-1} = ord(f)$, which contradicts the above inequality. Hence $s = 1$ and $f(x)$ must be irreducible.

Now let α be a root of $f(x)$ in $GF(q^n)$. Then the multiplicative order of α is $\frac{q^n-1}{q-1}$. The roots of $f(x)$ are α^{q^j}, $0 \leqslant j < n$; hence, the constant term of $f(x)$ is $(-1)^n f(0) = N_{GF(q^n)/GF(q)}(\alpha) = \alpha\alpha^q \ldots \alpha^{q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}} = 1$ implying $(-1)^n f(0) = 1$ and the lemma is proved. □

On the other hand, polynomials of degree n and order $\frac{q^n-1}{q-1}$, $n \geqslant 1$, exist. Because if $f(x)$ is a primitive polynomial of degree n over $GF(q)$, then the roots $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ of $f(x)$, which all lie in $GF(q^n)$, each have order $q^n - 1$ in $GF(q^n)^*$; hence, $\beta = \alpha^{q-1}$ has order $\frac{q^n-1}{q-1}$ and the conjugates $\beta, \beta^q, \ldots, \beta^{q^{n-1}}$ are distinct and $g(x) = (x-\beta)(x-\beta^q)\cdots(x-\beta^{q^{n-1}}) \in GF(q)[x]$ is the minimal polynomial of β of degree n, which is therefore irreducible over $GF(q)$. Now by Theorem 3.3, in [4, p. 84] the order of $g(x)$ is equal to the order of β and our claim is proved. From the above and Lemma 2 we obtain the following corollary.

Corollary 3. *The group* $SL_n(q)$, $n \geqslant 1$, *has an element of order* $\frac{q^n-1}{q-1}$.

Lemma 3. *Let* $0 \neq f(x) \in GF(q)[x]$, $f(0) \neq 0$, *be a monic irreducible polynomial of degree n with the property* $(-1)^n f(0) = 1$. *Then* $ord(f) \mid \frac{q^n-1}{q-1}$.

Proof. Let α be a root of $f(x)$ in $GF(q^n)$. Then the multiplicative order of α is equal to $ord(f)$. But $1 = (-1)^n f(0) = N_{GF(q^n)/GF(q)}(\alpha) = \alpha\alpha^q \ldots \alpha^{q^{n-1}} = \alpha^{\frac{q^n-1}{q-1}}$ which implies $\alpha^{\frac{q^n-1}{q-1}} = 1$, hence $o(\alpha) \mid \frac{q^n-1}{q-1}$ and the lemma is proved. □

As a consequence of the above lemma if the characteristic polynomial of $A \in SL_n(q)$ is irreducible over $GF(q)$, then $O(A) \mid \frac{q^n-1}{q-1}$.

Lemma 4. *Let* $0 \neq f(x) \in GF(q)[x]$, $f(0) \neq 0$ *be a polynomial of degree* $n \geqslant 1$ *and* $f(x) = f_1(x)f_2(x)\cdots f_s(x)$ *be the factorization of* $f(x)$ *in terms of distinct monic irreducible polynomials over* $GF(q)$. *If* $s \geqslant 2$, *then* $ord(f) < \frac{q^n-1}{q-1}$.

Proof. Suppose $ord(f_i) = m_i$, $1 \leqslant i \leqslant s$. Then we know that $ord(f_i) \mid q^{m_i} - 1$. If we define $d = \frac{(q^{m_1}-1)\cdots(q^{m_s}-1)}{(q-1)^{s-1}}$, then with the same reasoning as in the proof of Lemma 2, we will obtain $f(x) \mid x^d - 1$ which implies $ord(f) \leqslant d$. But for $k \geqslant 2$ we have $d < \frac{q^n-1}{q-1}$, hence $ord(f) < \frac{q^n-1}{q-1}$ and the lemma is proved. □

Lemma 5. *The following inequality*

$$x^{yz} - 1 \geqslant zx(x-1)(x^y - 1)$$

holds for natural numbers x, y, z with the conditions $(y, z) \neq (1, 2), (1, 3), (2, 2)$ or $z \neq 1$. (The inequality holds in the cases $(x, y, z) = (2, 2, 2)$, $(x, y, z) = (2, 1, 3)$ and $(x, z) = (1, 1)$.)

Proof. We may assume $x > 1$. If $z > 3$, then for any $a \in \mathbb{N}$ we have $a^z = (1+a-1)^z = 1 + z(a-1) + \frac{z(z-1)}{2}(a-1)^2 + \cdots \geqslant 1 + z(a-1)^3$, hence $a^z - 1 > z(a-1)^3$. Now setting $a = x^y$ we will obtain $x^{yz} - 1 \geqslant z(x^y - 1)^3 \geqslant zx(x-1)(x^y - 1)$ and the inequality holds.

If $z = 3$, then the above inequality simplifies to $x^{zy} + x^y + 1 \geqslant 3x(x-1)$ which obviously holds for $y \neq 1$. If $y = 1$, then the inequality holds only if $x = 2$. Therefore, if $(y, z) \neq (1, 3)$, then the inequality stated in the lemma holds.

If $z = 2$, then the inequality becomes $x^y + 1 \geqslant 2x(x-1)$. If $y = 1$, the inequality does not hold, and if $y = 2$, $x \neq 2$, again the inequality holds. For $y \geqslant 3$, the inequality holds for any x.

If $z = 1$, then the inequality stated in the Lemma holds only if $x = 1$. The Lemma is proved now. □

Lemma 6. *Let $f(x) = g(x)^b$, where $g(x)$ is a monic irreducible polynomial of degree $d \geqslant 1$ over $GF(q)$. Then*
(a) *$ord(f) \leqslant q^{bd} - 1$,*
(b) *if $b \geqslant 2$, then $ord(f) \leqslant \frac{q^{bd}-1}{q-1}$ holds when $(d, b) \neq (1, 2)$.*

Proof. (a) Since $f(x)$ is a polynomial of degree bd, by Lemma 3.1, in [4, p. 84] the order of $f(x)$ is at most $q^{bd} - 1$.

(b) By Lemma 1 we have $ord(f) = p^t\, ord(g)$ where q is a power of p and t is the least positive integer such that $p^t \geqslant b$. By [4, Corollary 3.4, p. 84] we have $ord(g) \leqslant q^d - 1$, hence $ord(f) \leqslant p^t(q^d - 1)$. But by the definition of t we have $p^{t-1} < b$, thus $p^t < pb$ and $ord(f) < pb(q^d - 1) \leqslant qb(q^d - 1)$.

Now by Lemma 5, taking $x = q$, $y = d$, $z = b$, we have $q^{bd} - 1 \geqslant bq(q-1)(q^d - 1)$ except for $(d, b) = (1, 2), (1, 3), (2, 2)$. Note that by assumption $b \geqslant 2$. Therefore $qb(q^d - 1) \leqslant \frac{q^{bd}-1}{q-1}$ implying $ord(f) < \frac{q^{bd}-1}{q-1}$.

If $(d, b) = (1, 3)$, then $ord(f) \leqslant p(q-1)$ if p is odd and $ord(f) \leqslant 4(q-1)$ if $p = 2$. Since we have $p(q-1) \leqslant q(q-1) < \frac{q^3-1}{q-1}$ and $4(q-1) < \frac{q^3-1}{q-1}$, the inequality in (b) holds in this case. If $(d, b) = (2, 2)$, then $ord(f) \leqslant p(q^2 - 1) \leqslant q(q^2 - 1) < \frac{q^4-1}{q-1}$ and again the inequality holds. Therefore the lemma is proved. □

Example 1. In this example we will compute $\mu(G)$ where $G = GL_2(q)$ or $SL_2(q)$, q a power of prime p. The conjugacy classes of G are of the shape $c = (f_1 f_2), (f_1^2)$ or (f_3), where f_1 and f_2 are distinct monic irreducible polynomials of degree 1 and f_3 is an irreducible polynomial of degree 2. According to Corollary 1, the maximum order of c is $q-1$, $p(q-1)$ or q^2-1, respectively. Therefore $\mu(GL_2(q)) = \{p(q-1), q^2-1\}$.

For $SL_2(q)$ we must consider those f_i's for which $f_1(0)f_2(0) = (-1)^2 = 1$, $f_1^2(0) = (-1)^2 = 1$ or $f_3(0) = (-1)^2 = 1$. By Lemma 3 the maximum order of f_3 is $\frac{q^2-1}{q-1} = q+1$. If $c = (f_1^2)$, then $f_1(x) = x + a$, $a^2 = 1$. If p is odd, we have $ord(f_1) = 2p$ and if $p = 2$, $ord(f) = p = 2$. If $c = (f_1 f_2)$, then we may take $f_1(x) = x + a$ and $f_2(x) = x + a^{-1}$ where $a \in GF(q)^*$. Then the maximum order of c is $q-1$. Therefore, for q odd we have $\mu(SL_2(q)) = \{2p, q-1, q+1\}$ and for q even $\mu(SL_2(q)) = \{p, q-1, q+1\}$. Hence, we have the following corollary.

Corollary 4. *The largest number for an element of the group $SL_2(q)$* is $q+1$ *except when $q = p$ is an odd prime and in this case $2p$ is the largest number for the order of an element in the group $SL_2(p)$.*

Lemma 7. *Let q be a power of prime p and $0 \neq f(x) \in GF(q)[x]$, $f(0) \neq 0$, have the factorization $f(x) = f_1(x)^{k_1} f_2(x)^{k_2} \dots f_s(x)^{k_s}$, where $f_i(x)$ are distinct monic irreducible polynomials. Let $\deg f(x) = n \geqslant 1$ and at least for one of the k_i's we have $k_i \geqslant 2$. Further assume that in the case $n = 2$, p odd, we have $q \neq p$. Then $ord(f) < \frac{q^n-1}{q-1}$.*

Proof. We may assume $k_1 \geqslant 2$. Let $\deg f_i(x) = m_i$, $1 \leqslant i \leqslant s$. Therefore, by Lemma 6 we can write

$$\begin{aligned} ord(f) &= \operatorname{lcm}(ord(f_1^{k_1}), ord(f_2^{k_2}), \dots, ord(f_s^{k_s})) \\ &\leqslant ord(f_1^{k_1}) ord(f_2^{k_2}) \dots ord(f_s^{k_s}) \\ &\leqslant \frac{q^{m_1k_1}-1}{q-1}(q^{m_2k_2}-1)\cdots(q^{m_sk_s}-1) \\ &\leqslant \frac{(q^{m_1k_1}-1)(q^{m_2k_2}-1)\cdots(q^{m_sk_s}-1)}{q-1} \\ &\leqslant \frac{q^{m_1k_1+m_2k_2+\cdots+m_sk_s}-1}{q-1} \\ &= \frac{q^n-1}{q-1}. \qquad \square \end{aligned}$$

Theorem 1. *The largest order of an element in the group* $SL_n(q)$ *is* $\frac{q^n-1}{q-1}$ *except in the case of the group* $SL_2(q)$, p *odd, where this number is* $2p$.

Proof. Suppose $c = (f_1^{\nu_1} f_2^{\nu_2} \dots f_s^{\nu_s})$ represents a conjugacy class in $SL_n(q)$. Then ν_i is a partition of k_i, f_i's are distinct monic irreducible polynomials of degree d_i, $1 \leqslant i \leqslant s$, and furthermore $\sum_{i=1}^{s} k_i d_i = n$ and $(-1)^n f(0) = 1$, where $f(x) = f_1(x)^{k_1} \dots f_s(x)^{k_s}$. If $s = 1$, then by Lemma 3 the theorem follows. If $s \geqslant 2$, then from Lemmas 4 and 7 the result holds. □

3. Computing $\mu(G)$ where $G = GL_6(5)$, $SL_6(5)$, $PGL_6(5)$ and $PSL_6(5)$

As an illustration for our methods we will find the maximal elements of $\omega(G)$, where G is one of the groups $GL_6(5)$, $SL_6(5)$ or $PSL_6(5)$. Each conjugacy class in $GL_6(5)$ with maximum order is represented by a polynomial $f(x) = f_1(x)^{k_1} \dots f_s(x)^{k_s}$, where $f_i(x)$ are distinct monic irreducible polynomials over the field $GF(5)$, so that each of them has maximum order and $\sum_{i=1}^{s} k_i d_i = 6$, $d_i = \deg f_i(x)$, $1 \leqslant i \leqslant s$. For simplicity we write $[d]$ for a polynomial of degree d and when it is raised to a power k we will write $[d^k]$. The symbol $[d^k]$ also may represent the product of different polynomials of degree d as well. Therefore in the following table, using our previous results, we will write the maximum orders of elements in each class of $GL_6(5)$ and $SL_6(5)$. In the case of $SL_6(5)$ we write a typical polynomial, the order of which is maximal. We will use this to find the order of elements in $PSL_6(5)$. We also use the list of irreducible polynomials over $GF(5)$ given in [4].

Therefore, by Table 1 we obtain $\mu(GL_6(5)) = \{100, 620, 3120, 3124, 15624\}$ and $\mu(SL_6(5)) = \{50, 620, 624, 744, 1560, 3124, 3906\}$.

To obtain $\mu(PSL_6(5))$ we use the formula found at the end of Section 1. Note that here the centre of the group $SL_6(5)$ is $Z = \{\pm I\}$. We denote the image of $A \in PSL_6(5)$ by $\overline{A}$. If A is a 6×6 matrix over $GF(5)$ with minimal polynomial $(x+1)^6$, then it is easy to see that $A^{25} = -I$, hence $O(\overline{A}) = 25$. If A corresponds to the polynomial $(x+2)^5(x+3)$, then $A = \begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}$, where A_1 is a 5×5 matrix with minimal polynomial $(x+2)^5$ and A_2 is a 1×1 matrix with minimal polynomial $x+3$. We have $A_1^5 = -2I$ and $A_2 = -3I$, hence $l = \operatorname{lcm}(5,1) = 5$. Therefore $A_1^5 = -2I = \mu_1 I$ and $A_2^5 = -3I = \mu_2 I$, where $\mu_1 = -2$ and $\mu_2 = -3$. If we set $GF(5)^* = \langle 2 \rangle$, then $\mu_1 = 2^3$, $\mu_2 = 2$, thus $m_1 = 3$ and $m_2 = 2$. Now for the order of A, α, we have : $\alpha = \frac{(5-1)\times 5}{\gcd(5-1,1)} = 20$.

Therefore the matrix corresponding to $(x+2)^5(x+3)$ has order 20 in $PSL_6(5)$. Continuing in this way we are able to find the maximum order of elements of the group $PSL_6(5)$ as follows:

$\mu(PSL_6(5)) = \{25, 620, 624, 744, 1560, 1562, 1953\}$.

The set of orders of elements in $PGL_6(5)$ can be obtained similarly. The result of our computation is

$\mu(PGL_6(5)) = \{25, 620, 744, 3120, 3124, 3906\}$.

Table 1

	c	Maximum order in $GL_6(5)$	A typical element in $SL_6(5)$ with maximum order	Maximum order in $SL_6(5)$	Maximum order in $PSL_6(5)$
1	$[1^6]$	$5^2.(5-1)=100$	$(x+1)^6$, $(x+2)^5(x+3)$	$5^2.2=50, 5.4=20$	25, 20
2	$[1^4][2]$	$5.(5^2-1)=120$	$(x+1)(x+2)^3(x^2+x+2)$	120	120
3	$[1^3][3]$	$5.(5^3-1)=620$	$(x+3)(x+4)^2(x^3+x^2+2)$	620	620
4	$[1^2][4]$	$5.(5^4-1)=3120$	$(x+1)(x+3)(x^4+x^2+2x+2)$, $(x+2)^2(x^4+x+4)$	$624, 5.312=1560$	624, 1560
5	$[1^2][2^2]$	$5.(5^2-1)=120$	$(x+2)^2(x^2+x+2)^2$	120	120
6	$[1][5]$	$5^5-1=3124$	$(x+3)(x^5+4x+2)$	3124	1562
7	$[1][2][3]$	$\mathrm{lcm}(5-1, 5^2-1, 5^3-1)=744$	$(x+4)(x^2+x+2)(x^3+3x+2)$	744	744
8	$[2][4]$	$5^4-1=624$	$(x^2+2x+3)(x^4+x^2+2x+2)$	624	624
9	$[2^3]$	$5.(5^2-1)=120$	$(x^2+x+2)^2(x^2+2x+4)$	120	120
10	$[3^2]$	$5.(5^3-1)=620$	$(x^3+x+1)^2$, (x^3+3x+2) (x^3+3x+3)	$5.62=310, 124$	155, 62
11	$[6]$	$5^6-1=15624$	$x^6+x^4+x^3+1$	3906	1953

Acknowledgments

I would like to thank the research council of the University of Tehran for financial support. I also would like to express my deep gratitude to Dr. Y. Farjami of the mathematics department of the University of Tehran for many useful discussions during the preparation of this paper specially in computing Table I.

References

[1] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, Atlas of Finite Groups, Clarendon Press, Oxford, 1985.

[2] M.R. Darafsheh, Y. Farjami, A. Mahmiani, Recognition of the linear groups over the binary field by the set of their element orders, submitted for publication.

[3] J.A. Green, The characters of the finite general linear groups, Trans. Amer. Math. Soc. 80 (1955) 402–447.

[4] R. Lidl, H. Niederreiter, Finite fields, Addison–Wesly Publishing Company Inc., 1983.

[5] W.J. Shi, A characteristic property of $\mathbb{A}_5$, J. Southwest-China Teachers Univ. 11 (3) (1986) 11–14 (Chinese).