Finite C-Groups

Kazem Mahdavi, Brian Nygen,
Ramona R Ranalli, James Sizemore,
Andrew Stout, Colleen Swanson

June 19, 2007

Abstract

We prove that in a finite group ($p$-group) the number of generators of the center of the group can be arbitrarily large and independent of the number of generators of the group.

1 Introduction

It seems counter–intuitive to think that the center of a group $G$, $Z(G)$, may have an infinite number of generators, while $G$ itself has only a fixed finite number of generators. In [?], H. Abel gave an example of such a group. In this paper, for the case of finite groups, we extend [?] and show the surprising result that in a finite group the number of generators of the center of the group can be arbitrarily large. That is, the number of generators of the center is not bounded by a function of the number of generators of the group.

Theorem 2

For all $m, n \in \mathbb{N}$ such that $m \geq 2$ and $n \geq m$, there exists a finite group $G$ such that the minimal generating set of $G$ has exactly $m$ elements, and the minimal generating set of $Z(G)$ has exactly $n$ elements.

2 Notation and Definitions

Definition 1 (C-Group) If $G$ is a group whose center has more generators than $G$, we say $G$ is a C-Group.

Definition 2 (Commutator) Let $G$ be a group and let $x, y \in G$. Then $[x, y] = xyx^{-1}y^{-1}$ is called the commutator of $x$ and $y$. The subgroup of $G$ generated by the set $\{[x, y] \mid x, y \in G\}$ is called the commutator subgroup of $G$ and will be denoted $G'$.

3 Main Result

We begin by describing, briefly, the group that H. Abel gave, and then we present our result.

3.1 Infinite C-Groups

Here we briefly sketch a class of finitely generated groups whose centers are infinitely generated. One class of such groups is the set of $4 \times 4$ upper-triangular matrices over the ring $Q^{(p)} = \{\frac{n}{p^a} \mid a, n, p \text{ are integers, } n \geq 0,$
p prime, and \((p^n, a) = 1\) \([7]\). Define \(M(Q^{(p)}, 4)\) to be all \(4 \times 4\) matrices over \(Q^{(p)}\) whose elements have the form

\[
\begin{pmatrix}
1 & * & * & *\\
0 & u_1 & * & * \\
0 & 0 & u_2 & * \\
0 & 0 & 0 & 1
\end{pmatrix},
\]

where \(u_i\) denotes a positive unit. It is easy to check that this is a group under matrix multiplication.

It can be shown that \(M(Q^{(p)}, 4)\) is finitely generated by the following elements: matrices where \(u_1 = p\) or \(1/p\) while \(u_2 = 1\) or the reverse, \(u_2 = p\) or \(1/p\) while \(u_1 = 1\) as well as matrices

\[
\begin{pmatrix}
1 & a_1 & a_2 & 0 \\
0 & 1 & a_3 & a_4 \\
0 & 0 & 1 & a_5 \\
0 & 0 & 0 & 1
\end{pmatrix},
\]

where exactly one \(a_i = \pm 1\) and all others are zero.

Now we examine the center of \(M(Q^{(p)}, 4)\). Call it \(Z(M)\). We notice that for an element of \(M(Q^{(p)}, 4)\) to be in \(Z(M)\), the element should be of the form:

\[
\begin{pmatrix}
1 & 0 & 0 & a \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}.
\]

Is \(Z(M)\) finitely generated? No! Assume it is. Then \(Z(M)\) must be generated by a finite number of central matrices. We call a set of such finite matrices \(A\). Then there is an integer \(n\) such that \(p^n\) is the maximum denominator among all the entries of the elements of the set \(A\). Now we notice that the following matrix which is in \(Z(M)\) cannot be generated by elements of \(A\):

\[
\begin{pmatrix}
1 & 0 & 0 & 1/p^{n+1} \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}.
\]

So we see that \(M(Q^{(p)}, 4)\) is an example of a finitely generated group whose center is infinitely generated.

### 3.2 Finite C-groups

First we prove the following Lemma.

**Lemma 1** For all \(a, n, r, p \in \mathbb{N}\) such that \(p\) is a prime and \(r \leq p^n\), we have \(\binom{ap^n}{r} \cdot p^r \equiv 0 \mod p^{n+1}\).

**Proof** Write \(r! = p^k \cdot m\), where \(k \in \mathbb{Z}\), \(k \geq 0\), \(m \in \mathbb{N}\) and \(p \nmid m\).

Now, as there are \(\left\lfloor \frac{r}{p} \right\rfloor\) numbers less than or equal to \(r\) which are divisible by \(p\), \(\left\lfloor \frac{r}{p^2} \right\rfloor\) which are divisible by
\[ p^2, \text{ and in general, } \left\lfloor \frac{r}{p^i} \right\rfloor \text{ which are divisible by } p^i, \text{ we have } k = \sum_{i=1}^{\infty} \left\lfloor \frac{r}{p^i} \right\rfloor. \] So,

\[ k = \sum_{i=1}^{\infty} \left\lfloor \frac{r}{p^i} \right\rfloor \leq \frac{r}{p} + \cdots + \frac{r}{p^{\log_p r}} < \sum_{i=0}^{\infty} \frac{r}{p \left( \frac{1}{p} \right)^i} = \frac{r}{p-1} \leq r. \]

Now, let \( s = r - k. \) Clearly, \( s \in \mathbb{Z} \), where \( s \geq 1. \) Since \( \frac{ap^n \cdots (ap^n - r + 1)}{m \cdot p^k} \equiv \left( \frac{ap^n}{r} \right) \in \mathbb{N} \) and \((m, p^n) = 1, \) then \( a \) \( \left( \frac{ap^n}{r} \right) \cdot p^r = \frac{ap^n \cdots (ap^n - r + 1)}{m} \cdot p^{r-k} = t \cdot p^{n+s} \equiv 0 \mod p^{n+1}. \)

The main results of this paper, as stated in Theorem 2 in the introduction, are a corollary of the next theorem.

**Theorem 1** The set

\[ G_{p,n} = \left\{ \left( \begin{array}{c} a_1 \mod p^{n+1} \\ \vdots \\ p^{n+1} a_{n+1} \mod p^{n+1} \end{array} \right) \right\} \bigg| h, a_1, a_2, \ldots, a_{n+1} \in \mathbb{Z}_{p^{n+1}}, p \text{ prime} \]

together with the binary operation

\[
\begin{pmatrix}
 a_1 \\
 p a_2 \\
 \vdots \\
p^{n+1} a_{n+1}
\end{pmatrix}
\bigg| h, a_1, a_2, \ldots, a_{n+1} \in \mathbb{Z}_{p^{n+1}}, p \text{ prime}
\end{pmatrix}
\bigg| h_1, h_2 \bigg| h_1 + h_2 \mod p^{n+1},
\begin{pmatrix}
 a_1 \\
 p a_2 \\
 \vdots \\
p^{n+1} a_{n+1}
\end{pmatrix}
+ \begin{pmatrix}
 1 & 0 & \cdots & 0 \\
p & 1 & 0 & \cdots \\
\vdots & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & p
\end{pmatrix}
\begin{pmatrix}
 b_1 \\
 p b_2 \\
 \vdots \\
p^{n+1} b_{n+1}
\end{pmatrix}
\] is a C-group. It has two generators while its center has \( n + 2 \) generators.

**Proof** In order to save space, we set

\[ M = \begin{pmatrix}
 1 & 0 & \cdots & 0 \\
p & 1 & 0 & \cdots \\
0 & p & \cdots & \cdots \\
\vdots & \ddots & \ddots & \ddots \\
0 & \cdots & 0 & p
\end{pmatrix}
\]

Since \( G_{p,n} \) is a semidirect product, it is a group.
Consider \( g_0 = \left( 1, \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right) \) and \( g_1 = \left( 0, \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right) \). We will show that \( g_0 \) and \( g_1 \) are the generators of \( G_{p,n} \).

Note that

\[
g_2 = \left( 0, \begin{bmatrix} 0 \\ p \\ \vdots \\ 0 \end{bmatrix} \right) = g_1^{-1} g_0 g_1 g_0^{-1}
\]

and, using induction, we can show that

\[
g_k = \left( 0, \begin{bmatrix} 0 \\ p^{k-1} \\ \vdots \\ 0 \end{bmatrix} \right) = g_{k-1}^{-1} g_0 g_k g_0^{-1},
\]

with \( p^{k-1} \) in the \( k^{th} \) position.

It can then be easily shown that any element in the group is expressible as

\[
\begin{pmatrix} x_1 \\ px_2 \\ \vdots \\ p^n x_{n+1} \end{pmatrix} = g_{a_{n+1}} \cdots g_{a_2} g_{a_1} h
\]

and so \( g_0 \) and \( g_1 \) generate the group. Since the group is not abelian, it cannot be cyclic; therefore its minimal generating set must have exactly two elements.

Now, let \( x \in Z(G_{p,n}) \). Then \( xg_0 = g_0 x \) and \( xg_1 = g_1 x \).

We have

\[
xg_0 = g_0 x
\]

\[
\iff \left( h, \begin{bmatrix} x_1 \\ px_2 \\ \vdots \\ p^n x_{n+1} \end{bmatrix} \right) \left( 1, \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right) = \left( 1, \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right) \left( h, \begin{bmatrix} x_1 \\ px_2 \\ \vdots \\ p^n x_{n+1} \end{bmatrix} \right)
\]

\[
\iff \left( (h + 1) \mod p^{n+1}, \begin{bmatrix} x_1 \\ px_2 \\ \vdots \\ p^n x_{n+1} \end{bmatrix} \right) = \left( (h + 1) \mod p^{n+1}, M \begin{bmatrix} x_1 \\ px_2 \\ \vdots \\ p^n x_{n+1} \end{bmatrix} \right)
\]

\[
\iff \begin{bmatrix} x_1 \\ px_2 \\ \vdots \\ p^n x_{n+1} \end{bmatrix} = M \begin{bmatrix} x_1 \\ px_2 \\ \vdots \\ p^n x_{n+1} \end{bmatrix}
\]

\[
\iff px_1 \mod p^{n+1} = \cdots = p^n x_n \mod p^{n+1} = 0
\]

\[
\iff \exists a_1, \ldots, a_{n+1} \in \mathbb{Z}_p \text{ such that } x_1 = p^n a_1, px_2 = p^n a_2, \ldots, p^n x_{n+1} = p^n a_{n+1}.
\]
Also,

\[ xg_1 = g_1x \]

\[ \iff \left( h, \begin{bmatrix} x_1 \\ px_2 \\ \vdots \\ p^n x_{n+1} \end{bmatrix} \right) \left( \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \right) = \left( \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \right) \left( h, \begin{bmatrix} x_1 \\ px_2 \\ \vdots \\ p^n x_{n+1} \end{bmatrix} \right) \]

\[ \iff \left( h, \begin{bmatrix} x_1 \\ px_2 \\ \vdots \\ p^n x_{n+1} \end{bmatrix} \right) + M^h \left( \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \right) = \left( h, \begin{bmatrix} x_1+1 \\ px_2 \\ \vdots \\ p^n x_{n+1} \end{bmatrix} \right) \]

\[ \iff M^h \left( \begin{bmatrix} 1 \\ \vdots \\ 0 \end{bmatrix} \right) = \left( \begin{bmatrix} 1 \\ \vdots \\ 0 \end{bmatrix} \right). \]

Therefore,

\[ x \in Z(G_{p,n}) \iff x = \left( h, \begin{bmatrix} p^{a_1} \\ p^{a_2} \\ \vdots \\ p^{a_{n+1}} \end{bmatrix} \right) \text{ for some } a_1, a_2, \ldots, a_{n+1} \in \mathbb{Z}_p, \text{ and } M^h \left( \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \right) = \left( \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \right). \]

By induction on \( h \), we will show that for all \( i \) such that \( i \leq \min(h, n+1) \), the \( i \)th entry of \( M^h \left( \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \right) \) is \( p^{i-1} \mod (h-1) \), and that the rest are 0:

For \( h = 1 \),

\[ M^1 \left( \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right) = \left( \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right) = \left( \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right). \]

Let it hold for \( h \). Then for \( h + 1 \) we have,

\[ M^{h+1} \left( \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \right) = M \left( \begin{bmatrix} \frac{h}{1} \\ \frac{h}{2} \\ \vdots \\ \frac{h}{k} \\ \frac{h}{k+1} \\ \vdots \\ \frac{h}{h+1} \\ \frac{h}{h+1} \end{bmatrix} \right) \left( \begin{bmatrix} \frac{h}{1} \\ \frac{h}{2} \\ \vdots \\ \frac{h}{k} \\ \frac{h}{k+1} \\ \vdots \\ \frac{h}{h+1} \\ \frac{h}{h+1} \end{bmatrix} \right) = \left( \begin{bmatrix} \frac{h}{1} \\ \frac{h}{2} \\ \vdots \\ \frac{h}{k} \\ \frac{h}{k+1} \\ \vdots \\ \frac{h}{h+1} \\ \frac{h}{h+1} \end{bmatrix} \right). \]

Since \( \left( \begin{bmatrix} \frac{h}{1} \\ \frac{h}{2} \\ \vdots \\ \frac{h}{k} \\ \frac{h}{k+1} \\ \vdots \\ \frac{h}{h+1} \\ \frac{h}{h+1} \end{bmatrix} \right) = h \),

\[ p^h \mod p^{n+1} = 0 \iff h \mod p^n = 0, \]

where \( p^h \) is the second entry of \( M^h \left( \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \right) \). By Lemma ??, the rest of the entries (after the first entry) will be equal to 0 mod \( p^{n+1} \) if \( h \mod p^n = 0 \) as well.
So $x$ must be of the form
\[
\begin{pmatrix}
(p^n h) \mod p^{n+1}, \\
\frac{p^n a_1}{p^n a_2} \\
\vdots \\
\frac{p^n a_{n+1}}{p^n a_{n+1}}
\end{pmatrix},
\]
where $h, a_1, \ldots, a_{n+1} \in \mathbb{Z}_p$. Note that
\[
\begin{pmatrix}
(p^n h_1) \mod p^{n+1}, \\
\frac{p^n a_1}{p^n a_2} \\
\vdots \\
\frac{p^n a_{n+1}}{p^n a_{n+1}}
\end{pmatrix} \cdot \begin{pmatrix}
(p^n h_2) \mod p^{n+1}, \\
\frac{p^n b_1}{p^n b_2} \\
\vdots \\
\frac{p^n b_{n+1}}{p^n b_{n+1}}
\end{pmatrix} = \begin{pmatrix}
(p^n (h_1 + h_2)) \mod p^{n+1}, \\
\frac{p^n (a_1 + b_1)}{p^n (a_2 + b_2)} \\
\vdots \\
\frac{p^n (a_{n+1} + b_{n+1})}{p^n (a_{n+1} + b_{n+1})}
\end{pmatrix},
\]
thus there exists an isomorphism
\[
\varphi : Z(G_{p,n}) \to \prod_{i=1}^{n+2} \mathbb{Z}_p
\]
(the direct product of $n + 2$ copies of $\mathbb{Z}_p$), defined by
\[
\begin{pmatrix}
(p^n h) \mod p^{n+1}, \\
\frac{p^n a_1}{p^n a_2} \\
\vdots \\
\frac{p^n a_{n+1}}{p^n a_{n+1}}
\end{pmatrix} \mapsto (h, a_1, a_2, \ldots, a_{n+1}).
\]
Since the minimal generating set of $\prod_{i=1}^{n+2} \mathbb{Z}_p$ has exactly $n + 2$ elements, so does that of $Z(G_{p,n})$. As the minimal generating set of $G_{p,n}$ has 2 elements, and the minimal generating set of $Z(G_{p,n})$ has $n + 2$ elements, $G_{p,n}$ is a C-group.

This brings us to our main theorem

**Theorem 2** For all $m, n \in \mathbb{N}$ such that $m \geq 2$ and $n \geq m$, there exists a finite group $G$ such that the minimal generating set of $G$ has exactly $m$ elements, and the minimal generating set of $Z(G)$ has exactly $n$ elements.

**Proof** The group $G_{p,n-m} \times \prod_{i=1}^{m-2} \mathbb{Z}_p$, for a prime $p > 2$, is an example of such a group.

**References**


**4 Authors Contact Information**

Khazem Mahdavi, University of Texas at Tyler (kmahdavi@uttyler.edu); Brian Nguyen, University of California, San Diego (brianjnguyen@gmail.com); Ramona Ranalli, University of Texas at Tyler (ranalli@uttyler.edu); James Sizemore, University of California, Los Angeles (sizemmore@math.ucla.edu); Andrew Stout, University of California, San Diego (astout@math.ucsd.edu); Colleen Swanson, Mt. Holyoke College (cm-swanso@mtholyoke.edu)