A NOTE ON NIELSEN EQUIVALENCE IN FINITELY GENERATED ABELIAN GROUPS

DANIEL OANCEA

(Received 16 November 2010)

Abstract

Nielsen transformations determine the automorphisms of a free group of rank \( n \), and also of a free abelian group of rank \( n \), and furthermore the generating \( n \)-tuples of such groups form a single Nielsen equivalence class. For an arbitrary rank \( n \) group, the generating \( n \)-tuples may fall into several Nielsen classes. Diaconis and Graham [“The graph of generating sets of an abelian group”, Colloq. Math. 80 (1999), 31–38] determined the Nielsen classes for finite abelian groups. We extend their result to the case of infinite abelian groups.

Keywords and phrases: Nielsen transformations, abelian groups.

1. Introduction

Let \( G \) be any group of rank \( n \). The following transformations defined on the set \( \Gamma_t(G) \) of all generating \( t \)-tuples of \( G \) (\( t \geq n \)) are called elementary Nielsen transformations:

1. \( \pi : \Gamma_t(G) \to \Gamma_t(G) \), defined by
   \[
   \pi(w_1, w_2, \ldots, w_i, \ldots, w_t) = (w_2, w_1, \ldots, w_i, \ldots, w_t);
   \]

2. \( \sigma : \Gamma_t(G) \to \Gamma_t(G) \), defined by
   \[
   \sigma(w_1, w_2, \ldots, w_t) = (w_2, w_3, \ldots, w_t, w_1);
   \]

3. \( \mu : \Gamma_t(G) \to \Gamma_t(G) \), defined by
   \[
   \mu(w_1, \ldots, w_i, \ldots, w_t) = (w_1 w_2, w_2, \ldots, w_i, \ldots, w_t);
   \]

4. \( \tau : \Gamma_t(G) \to \Gamma_t(G) \), defined by
   \[
   \tau(w_1, \ldots, w_i, \ldots, w_t) = (w_1^{-1}, \ldots, w_i, \ldots, w_t).\]

The elementary Nielsen transformations generate a group, \( N_t(G) \), acting on \( \Gamma_t(G) \). Two \( t \)-tuples from \( \Gamma_t(G) \) are said to be Nielsen equivalent if one can be transformed into the other by means of a finite sequence of elementary Nielsen transformations.
Nielsen [3] showed that every two generating \(t\)-tuples of \(F_n\), the free group of rank \(n\), are Nielsen equivalent, whence it follows in particular that \(N_n(F_n) \cong \text{Aut}(F_n)\).

We are interested here in the case where \(G\) is an arbitrary additively written abelian group \(A\) of rank \(n \geq 1\), that is, in what the Nielsen equivalence classes of \(\Gamma_t(A)\) might be for all \(t \geq n\). We shall use the standard (and unique for the torsion subgroup) direct decomposition of such an \(A\):

\[
A = Z_1 \times \cdots \times Z_k \times Z_{k+1} \times \cdots \times Z_n = \prod_{j=1}^n Z_j,
\]

where for \(1 \leq j \leq k\), \(Z_j \cong \mathbb{Z}\), and for \(k+1 \leq j \leq n\), \(Z_j \cong \mathbb{Z}/m_j\mathbb{Z}\) with the \(m_j\) integers exceeding 1 and satisfying \(m_{j+1}m_j\) (so that \(m_n\) divides all the \(m_j\)).

The following theorem, which in essence extends that of Diaconis and Graham [2] from finite to finitely generated abelian groups, gives the complete answer.

**Theorem 1.1.**

(i) If \(t > n\) then all generating \(t\)-tuples of \(A\) are Nielsen equivalent.

(ii) The case \(t = n\).

(a) If \(k = n\) (so that \(A\) is free abelian) then all generating \(n\)-tuples of \(A\) are Nielsen equivalent. (This case is well known.)

(b) Suppose that \(k < n\) (so that \(A\) has torsion). Let \(z_1, z_2, \ldots, z_n\) be fixed generators of the cyclic summands \(Z_1, Z_2, \ldots, Z_n\) of \(A\). Then every generating \(n\)-tuple of \(A\) is Nielsen equivalent to one and only one \(n\)-tuple of the form \((z_1, z_2, \ldots, z_{n-1}, rz_n)\), where \(1 \leq r < m_n/2\) and \((r, m_n) = 1\). Hence in the case \(m_n > 2\), \(\Gamma_t(A)\) falls into \(\varphi(m_n)/2\) Nielsen classes, while if \(m_n = 2\) there is again just one Nielsen class. (Here \(\varphi\) is the Euler totient function, \(\varphi(m) = |\{i : 0 < i \leq m, \gcd(i, m) = 1\}|\), \(m \in \mathbb{N}^*\).)

Our proof follows that of [2] closely. What is new is the inclusion of the case where \(A\) is infinite \((k \geq 1\) and the use of matrices from \(\text{GL}_t(\mathbb{Z})\). Note also that in [2] only transformations generated by the first three types of elementary Nielsen transformations are used, so that in case (ii)(b) (with, in addition, \(k = 0\)) they obtain \(\varphi(m_n)\) classes.

### 2. Preliminaries

Any \(t\)-tuple \(g := (g_1, \ldots, g_t)\) of elements of \(A\) can be written as a \(t \times n\) matrix,

\[
g = \begin{pmatrix}
g_{11} & g_{12} & \cdots & g_{1n} \\
g_{21} & g_{22} & \cdots & g_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
g_{t1} & g_{t2} & \cdots & g_{tn}
\end{pmatrix},
\]

where \(g_{ij} \in Z_j, 1 \leq i \leq t, 1 \leq j \leq n,\) and \(g_j = g_{j1} \cdots g_{jn}\). Using this representation of \(t\)-tuples of \(A\) together with the \(\mathbb{Z}\)-module structure of the subgroups \(Z_j\) of \(A\), we have an action of \(\text{GL}_t(\mathbb{Z})\) on the set \(\Gamma_t(A)\) of generating \(t\)-tuples of elements of \(A\),
namely that given by multiplication of the above matrix $g$ on the left by the matrices of $\text{GL}_t(\mathbb{Z})$.

Consider the following matrices in $\text{GL}_t(\mathbb{Z})$:

$$M_1 = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

$$M_3 = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \quad M_4 = \begin{pmatrix} -1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

These matrices in fact generate $\text{GL}_t(\mathbb{Z})$ [1] and we have an epimorphism $\Phi : \text{N}(F_t) \to \text{GL}_t(\mathbb{Z})$, induced by the natural epimorphism $F_t \to \mathbb{Z}^t$. Thus $\Phi(\pi) = M_1$, $\Phi(\sigma) = M_2$, $\Phi(\mu) = M_3$, and $\Phi(\tau) = M_4$, taking $G = F_t$ in the definitions of $\pi$, $\sigma$, $\mu$, $\tau$ above.

The following lemma is immediate from the fact that on the one hand $M_1$, $M_2$, $M_3$, $M_4$ act on the $t$-tuples of $\Gamma(A)$ like $\pi$, $\sigma$, $\mu$, $\tau$ respectively, and on the other they generate $\text{GL}_t(\mathbb{Z})$.

**Lemma 2.1.** Let $A$ be, as above, a finitely generated abelian group of rank $n$, and let $g$ and $h$ be generating $t$-tuples of $A$, written, as above, as $t \times n$ matrices. Then $g$ is Nielsen equivalent to $h$ if and only if there exists a matrix $S \in \text{GL}_t(\mathbb{Z})$ such that $Sg = h$.

The next lemma is key.

**Lemma 2.2.** Let $C$ be an (additively written) nontrivial cyclic group and $(a_1, \ldots, a_t)$ a generating $t$-tuple of $C$, $t \geq 2$. Then for any generator $z$ of $C$, there exists $S \in \text{GL}_t(\mathbb{Z})$ such that $S(a_1, \ldots, a_t)^T = (z, 0, \ldots, 0)^T$. (Here $T$ denotes the transpose.) Equivalently, there exists a sequence of elementary Nielsen transformations taking $(a_1, \ldots, a_t)$ to $(z, 0, \ldots, 0)$ for any generator $z$ of $C$.

**Proof.** We use induction on $t$. We identify $C$ with the additive group of the ring $\mathbb{Z}/m\mathbb{Z}$, where $m = |C|$ (including the case $m = \infty$, $C \cong \mathbb{Z}$).

Let $t = 2$, and let $(a_1, a_2)$ be any pair generating $C$. Since $z$ is a generator of $C$, we have $a_1 = n_1z$, $a_2 = n_2z$, for some $n_1, n_2 \in \mathbb{Z}$. Let $d = \gcd(n_1, n_2)$, let $k, l \in \mathbb{Z}$ be such that $kn_1 + ln_2 = d$, and define $S_1 \in \text{GL}_2(\mathbb{Z})$ by

$$S_1 = \begin{pmatrix} k & l \\ -n_2/d & n_1/d \end{pmatrix}.$$

One verifies directly that $S_1(a_1, a_2)^T = (dz, 0)^T$. Since $(dz, 0)$ is a generating pair,
we have \((d, m) = 1\) \((d = \pm 1\) if \(m = \infty\)), and so for some \(c \in \mathbb{Z}\) we have \(cd \equiv 1 \mod m\). A possible two further \(S_2\) and \(S_3\) are defined as follows: first
\[
\begin{pmatrix}
1 & 0 \\
c & 1
\end{pmatrix}
\begin{pmatrix}
dz \\
0
\end{pmatrix}
= 
\begin{pmatrix}
dz \\
z
\end{pmatrix}
,
\]
and then
\[
\begin{pmatrix}
0 & 1 \\
1 & 0
\end{pmatrix}
\begin{pmatrix}
1 & -d \\
0 & 1
\end{pmatrix}
\begin{pmatrix}
dz \\
z
\end{pmatrix}
= 
\begin{pmatrix}
z \\
0
\end{pmatrix}
.
\]

Taking the product of the matrices \(S_1, S_2, S_3\) (right to left) we obtain a matrix \(S \in \text{GL}_2(\mathbb{Z})\) such that
\[
S \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = 
\begin{pmatrix} z \\ 0 \end{pmatrix}
.
\]

The inductive step from \(t\) to \(t + 1\) proceeds as follows: if \((a_1, \ldots, a_t, a_{t+1})\) is a generating \((t + 1)\)-tuple of \(C\), then by the induction hypothesis there exists \(M \in \text{GL}_t(\mathbb{Z})\) such that
\[
M(a_1, \ldots, a_t)^T = (u, 0, \ldots, 0)^T,
\]
where \(u\) is any generator of the subgroup \(\langle a_1, \ldots, a_t \rangle\). Define the \((t + 1) \times (t + 1)\) matrix \(W\) by
\[
W := \begin{pmatrix}
M & 0^T \\ 0 & 1
\end{pmatrix}
.
\]
Then \(W \in \text{GL}_{t+1}(\mathbb{Z})\), and
\[
W
\begin{pmatrix}
a_1 \\ a_2 \\ \vdots \\ a_t \\ a_{t+1}
\end{pmatrix}
= 
\begin{pmatrix}
u \\ 0 \\ \vdots \\ 0 \\ a_{t+1}
\end{pmatrix}
,
\]
where now \((u, 0, \ldots, 0, a_{t+1})\) is a generating \((t + 1)\)-tuple for \(C\). Defining \(Q_{(t+1) \times (t+1)}\) by
\[
Q := 
\begin{pmatrix}
1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0
\end{pmatrix}
,
\]
we have
\[
Q
\begin{pmatrix}
u \\ 0 \\ \vdots \\ a_{t+1}
\end{pmatrix}
= 
\begin{pmatrix}
u \\ 0 \\ \vdots \\ 0
\end{pmatrix}
.
\]
Let $S \in \text{GL}_2(\mathbb{Z})$ be obtained as in the case $t = 2$ above, that is, such that
\[ S(u, a_{t+1})^T = (z, 0)^T, \]
where $z$ is our chosen arbitrary generator of $C$. If we define the matrix $R \in \text{GL}_{t+1}(\mathbb{Z})$
by
\[ R := \begin{pmatrix} S & \circ \\ \circ & I_{t-1} \end{pmatrix}, \]
then $RQW(a_1, \ldots, a_t, a_{t+1})^T = (z, 0, \ldots, 0)^T$. \hfill \Box

3. Proof of the theorem

PROOF. The proof follows that for finite abelian groups given by Diaconis and Graham [2], except that we present it in a somewhat modified form, using matrices in $\text{GL}_t(\mathbb{Z})$ to execute the Nielsen transformations. We may assume without loss of
generality that $t \geq 2$ since the case $t = 1$ (implying $n = 1$) is obvious.

As above, we write an arbitrary generating $t$-tuple of $A$ in the form of a $t \times n$ matrix:
\[
g = \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ g_{t1} & g_{t2} & \cdots & g_{tn} \end{pmatrix},
\]
with $g_{ij} \in \mathbb{Z}$, $1 \leq i \leq t$, $1 \leq j \leq n$.

We show by induction on $s$, $1 \leq s < t$, that for any choice of generators $z_1$, $z_2$, \ldots, $z_s$ of $Z_1$, $Z_2$, \ldots, $Z_s$ respectively, there is a matrix $R_s \in \text{GL}_t(\mathbb{Z})$ such that
\[
R_s g = \begin{pmatrix} z_1 & 0 & \cdots & 0 & f_{1,s+1} & \cdots & f_{1n} \\ 0 & z_2 & \cdots & 0 & f_{2,s+1} & \cdots & f_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & z_s & f_{s,s+1} & \cdots & f_{sn} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & f_{t,s+1} & \cdots & f_{tn} \end{pmatrix}.
\tag{3.1}
\]

The initial step: $s = 1$.

Since $g$ is a generating $t$-tuple, it follows that $(g_{1j}, g_{2j}, \ldots, g_{tj})$ is a generating
$t$-tuple for $Z_j$, $1 \leq j \leq n$. Consider the first column of $(g_{ij})$, whose entries are in $Z_1$. By Lemma 2.2, there exists a matrix $R_1 \in \text{GL}_t(\mathbb{Z})$ such that
\[
R_1 \begin{pmatrix} g_{11} \\ g_{21} \\ \vdots \\ g_{t1} \end{pmatrix} = \begin{pmatrix} z_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},
\]
where $z_1$ is the arbitrarily chosen generator of the cyclic group $Z_1$ ($z_1 = \pm 1$ if $Z_1 \cong \mathbb{Z}$). Thus

$$R_1g = \begin{pmatrix} z_1 & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{t2} & \cdots & a_{tn} \end{pmatrix},$$

for some $a_{ij} \in Z_j$. As always, since $R_1 \in \text{GL}_t(\mathbb{Z})$, $R_1g$ is still a generating $t$-tuple of $A$.

The inductive step from $s$ to $s + 1 \leq n$.

We assume inductively that there is a matrix $R_s$ such that $R_sg$ has the form (3.1) above. Consider the $(t-s)$-tuple $f_{s+1} := (f_{s+1,s+1}, \ldots, f_{s+1,t})$ consisting of the entries in (3.1) below $f_{s,s+1}$. This generates a subgroup $\langle d \rangle$ of the cyclic group $Z_{s+1}$. Thus by Lemma 2.2 there exists a $(t-s) \times (t-s)$ matrix $P \in \text{GL}_{t-s}(\mathbb{Z})$ such that

$$P \begin{pmatrix} f_{s+1,s+1} \\ f_{s+2,s+1} \\ \vdots \\ f_{t,s+1} \end{pmatrix} = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$ 

Hence defining the $t \times t$ matrix

$$S := \begin{pmatrix} I_s & \bigcirc & P \end{pmatrix}, \quad S \in \text{GL}_t(\mathbb{Z}),$$

where $I_s$ is the $s \times s$ identity matrix, we have

$$S = \begin{pmatrix} z_1 & 0 & \cdots & 0 & f_{1,s+1} & \cdots & f_{1n} \\ 0 & z_2 & \cdots & 0 & f_{2,s+1} & \cdots & f_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & z_s & f_{s,s+1} & \cdots & f_{sn} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & f_{t,s+1} & \cdots & f_{tn} \end{pmatrix}$$

$$= \begin{pmatrix} z_1 & 0 & \cdots & 0 & f_{1,s+1} & f_{1,s+2} & \cdots & f_{1n} \\ 0 & z_2 & \cdots & 0 & f_{2,s+1} & f_{2,s+2} & \cdots & f_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & z_s & f_{s,s+1} & f_{s,s+2} & \cdots & f_{sn} \\ 0 & 0 & \cdots & 0 & d & h_{s+1,s+2} & \cdots & h_{s+1,n} \\ 0 & 0 & \cdots & 0 & h_{s+2,s+2} & h_{s+2,n} & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & h_{t,s+2} & \cdots & h_{tn} \end{pmatrix}.$$ 

Now since the elements of $A$ represented by the rows of the submatrix
Nielsen equivalence in finitely generated abelian groups

\[
\begin{pmatrix}
  z_1 & 0 & \ldots & 0 & f_{1,s+1} \\
  0 & z_2 & \ldots & 0 & f_{2,s+1} \\
  \vdots & \vdots & \ddots & \vdots & \vdots \\
  0 & 0 & \ldots & z_s & f_{s,s+1} \\
  0 & 0 & \ldots & 0 & d
\end{pmatrix}
\]

generate \(Z_1 \times Z_2 \times \cdots \times Z_{s+1}\), there must exist integers \(v_1, v_2, \ldots, v_{s+1}\) such that

\[
v_1(z_1, 0, \ldots, 0, f_{1,s+1}) + v_2(0, z_2, 0, \ldots, 0, f_{2,s+1}) + \cdots + v_{s+1}(0, \ldots, 0, d) = (0, \ldots, 0, z_{s+1}),
\]

where \(z_{s+1}\) is the arbitrarily chosen generator of \(Z_{s+1}\). It follows that \(v_j \equiv 0 \pmod{m_j}\) for \(j = 1, \ldots, s\) (where, as usual, we interpret this to mean \(v_j = 0\) for those \(j\), if any, for which \(Z_j \cong \mathbb{Z}\)). In view of the ordering of the \(Z_j\) so that \(m_{j+1}|m_j\), we also have that all of \(v_1, \ldots, v_s \equiv 0 \pmod{m_{s+1}}\) (or are all zero if \(Z_{s+1} \cong \mathbb{Z}\)). Hence \(v_{s+1}d = z_{s+1}\), so that in fact \(d\) generates \(Z_{s+1}\). Thus there exist integers \(a_i, 1 \leq i \leq s\), such that \(f_{i,s+1} = a_id\). We now proceed in three steps.

- **Step 1** (valid also if \(s+1 = t\)). Let \(W_s\) be the matrix in \(\text{GL}_t(\mathbb{Z})\) obtained from the identity matrix by replacing the \((i, s+1)\) entries with \(a_i\) for \(1 \leq i \leq s\). Then

\[
W_s \begin{pmatrix}
  z_1 & 0 & \ldots & 0 & * & * & \cdots & * \\
  0 & z_2 & \ldots & 0 & * & * & \cdots & * \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  0 & 0 & \ldots & z_s & * & * & \cdots & * \\
  0 & 0 & \ldots & 0 & d & * & \cdots & * \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  0 & 0 & \ldots & 0 & * & \cdots & * \\
\end{pmatrix}
\]

The \(*\) entries are placeholders and their values are not important for the argument; we are using them to simplify notation.

The next two steps require \(s+1 < t\).

- **Step 2.** Let \(X_s\) be the matrix in \(\text{GL}_t(\mathbb{Z})\) obtained from the identity matrix by replacing the \((s+2, s+1)\) entry with \(v_{s+1}\). Then

\[
\begin{pmatrix}
  z_1 & 0 & \ldots & 0 & 0 & * & \cdots & * \\
  0 & z_2 & \ldots & 0 & 0 & * & \cdots & * \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  0 & 0 & \ldots & z_s & 0 & * & \cdots & * \\
  0 & 0 & \ldots & 0 & d & * & \cdots & * \\
  \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
  0 & 0 & \ldots & 0 & 0 & * & \cdots & * \\
\end{pmatrix}
\]
Step 3. Let $Y_s$ be the matrix in $\text{GL}_t(\mathbb{Z})$ obtained from the identity matrix by modifying four of the entries as follows: $(s + 1, s + 1) : 0$, $(s + 1, s + 2) : 1$, $(s + 2, s + 1) : 1$, $(s + 2, s + 2) : -b$, where $b$ is an integer such that $bz_{s+1} = d$. An immediate calculation gives

$$X_s = \begin{pmatrix}
    z_1 & 0 & \cdots & 0 & 0 & * & \cdots & * \\
    0 & z_2 & \cdots & 0 & 0 & * & \cdots & * \\
    \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
    0 & 0 & \cdots & z_s & 0 & * & \cdots & * \\
    0 & 0 & \cdots & 0 & d & * & \cdots & * \\
    \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
    0 & 0 & \cdots & 0 & 0 & * & \cdots & * \\
\end{pmatrix}$$

$$= \begin{pmatrix}
    z_1 & 0 & \cdots & 0 & 0 & * & \cdots & * \\
    0 & z_2 & \cdots & 0 & 0 & * & \cdots & * \\
    \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
    0 & 0 & \cdots & z_s & 0 & * & \cdots & * \\
    0 & 0 & \cdots & 0 & d & * & \cdots & * \\
    \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
    0 & 0 & \cdots & 0 & 0 & z_{s+1} & * & \cdots & * \\
\end{pmatrix}$$

$$Y_s = \begin{pmatrix}
    z_1 & 0 & \cdots & 0 & 0 & * & \cdots & * \\
    0 & z_2 & \cdots & 0 & 0 & * & \cdots & * \\
    \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
    0 & 0 & \cdots & z_s & 0 & * & \cdots & * \\
    0 & 0 & \cdots & 0 & d & * & \cdots & * \\
    \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
    0 & 0 & \cdots & 0 & 0 & z_{s+1} & * & \cdots & * \\
    0 & 0 & \cdots & 0 & 0 & * & \cdots & * \\
\end{pmatrix} = \begin{pmatrix}
    z_1 & 0 & \cdots & 0 & 0 & * & \cdots & * \\
    0 & z_2 & \cdots & 0 & 0 & * & \cdots & * \\
    \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
    0 & 0 & \cdots & z_s & 0 & * & \cdots & * \\
    0 & 0 & \cdots & 0 & z_{s+1} & * & \cdots & * \\
    \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
    0 & 0 & \cdots & 0 & 0 & * & \cdots & * \\
\end{pmatrix}$$
We have thus reached the form required by the induction step, completing the induction.

Part (i) of the theorem (the case \( t > n \)) now follows, since for \( s = n \) (<\( t \)) the matrix on the right of Equation (3.2) becomes

\[
\begin{bmatrix}
z_1 & 0 & \cdots & 0 & 0 \\
0 & z_2 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & z_{n-1} & 0 \\
0 & 0 & \cdots & 0 & z_n \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & 0 \\
\end{bmatrix}
\]

For part (ii) of the theorem (the case \( t = n \)), the above argument (up to and including Step 1) shows that for \( s = n - 1 \) our initial generating \( t \)-tuple can be transformed by means of matrices from \( \text{GL}_n(\mathbb{Z}) \) to

\[
\begin{bmatrix}
z_1 & 0 & \cdots & 0 & 0 \\
0 & z_2 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & z_{n-1} & 0 \\
0 & 0 & \cdots & 0 & d \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & 0 \\
\end{bmatrix}
\]

and the generator \( d \) of \( Z_n \) can be written as \( r z_n \) for a unique \( r \) with \( 1 \leq r < m_n \) satisfying \( (r, m_n) = 1 \). If \( r \geq m_n/2 \), then premultiplication by the matrix

\[
\begin{bmatrix}
I_{n-1} & 0^T \\
0 & -1 \\
\end{bmatrix} \in \text{GL}_n(\mathbb{Z})
\]

will cause \( r z_n \) to be replaced by \(-r z_n = r' z_n \) for \( r' \) satisfying \( 0 < r' < m_n/2 \).

Finally, we show that if \( \mathbf{h}_1, \mathbf{h}_2 \) are as in (3.3) with entries \( d_1 = r_1 z_n, d_2 = r_2 z_n \) in place of \( d \), where \( 0 < r_1 < r_2 < m_n/2 \), then \( \mathbf{h}_1, \mathbf{h}_2 \) cannot be transformed into one another by any matrix from \( \text{GL}_n(\mathbb{Z}) \). If \( A \in \text{GL}_n(\mathbb{Z}) \), with \( A \mathbf{h}_1 = \mathbf{h}_2 \), one can easily see that modulo \( m_n \), \( A \) is a diagonal matrix, with entries \( a_{ii} = 1 \) for \( 1 \leq i \leq n - 1 \), and with \( a_{nn} r_1 = r_2 \). Since \( \det(A) \in \{-1, 1\} \), \( A \in \text{GL}_n(\mathbb{Z}) \), then also modulo \( m_n \), \( \det(A) = a_{nn} \in \{-1, 1\} \). It follows that \( r_1 = r_2 \) or \( r_1 = -r_2 \).

**Acknowledgement**

This work formed part of the author’s PhD dissertation (York University, 2010). The author thanks his supervisor R. G. Burns for help with the presentation of this paper.
References


DANIEL OANCEA, 1549 Victoria St. E, Whitby, Ontario, Canada L1N 9E3
e-mail: daniel.oancea@opg.com