EXTENDED MALCEV DOMAINS

R. E. JOHNSON

In 1936, Malcev [1] constructed a cancellative monoid \( M \) generated by eight elements which couldn’t be embedded in a group. Later on, Chehata [2] and Vinogradov [3] showed that \( M \) could be ordered. This gave a counterexample to the conjecture that every ordered monoid could be embedded in a group. Since the monoid ring \( F[M] \) of an ordered monoid \( M \) over a (not-necessarily commutative) field \( F \) is a (not-necessarily commutative) integral domain, this also showed that not every integral domain could be embedded in a field. In the present paper, we give a somewhat different construction of an ordered monoid \( N \) generated by six or more elements which cannot be embedded in a group.

Let \( Z \) denote the ring of integers, \( S = \{ x_{ij} \mid i = 1, 2, j \in Z \} \) be a set of indeterminates, and \( A \) be the free monoid generated by \( S \). Each \( a \in S, a \neq 1 \), has the form \( a = a_1 \cdots a_n \) for some \( a_i \in S \). We call \( n \) the degree of \( a \), \( n = \deg a \). As usual, we let \( \deg 1 = 0 \). We order \( A \) by degrees and lexicographically from the assumed ordering:

\[
1 < x_{1i} < x_{ij} < x_{2i} < x_{2j} \quad \text{for all } i, j \in Z \text{ with } i < j.
\]

Thus, if \( a = a_1 \cdots a_m \) and \( b = b_1 \cdots b_n \) with \( a_i, b_i \in S \), then \( a < b \) if either \( \deg a < \deg b \) or \( \deg a = \deg b \) and there exists an integer \( k \) such that \( a_i = b_i \) if \( i < k \) and \( a_k < b_k \).

For any \( i, j \in Z \), let \([i, j]\) and \([i, j]’\) be defined as follows: (1) \([i, j]\) = \([i, j]’\) = \((i+j)/2\) if \( i+j \) is even, (2) \([i, j]\) = \((i+j-1)/2\) and \([i, j]’\) = \((i+j+1)/2\) if \( i+j \) is odd. Also, let \( T \subseteq A \) be defined by

\[
T = \{ x_{ij} x_{kj} \mid i, j \in Z, i > j \}
\]

and \( B \) be the ideal of \( A \) generated by \( T \). Finally, let \( N = A - B \).

We define an operation of multiplication, \( \cdot \), in \( N \) by letting \( a \cdot b = ab \) if \( ab \in B \), and

\[
x_{2i} \cdot x_{1j} = x_{2k} x_{1k}, \quad \text{if } i > j, \quad \text{where } k = [i, j].
\]

Thus, if \( a = a’ x_{2i} \) and \( b = x_{1j}, b’ \in N \), we have \( a \cdot b = a’ x_{2k} x_{1k} b’ \). Since nothing more happens in \( a \cdot b \) than the replacement of one \( x_{2i} \) on the right end of \( a \) by \( x_{2k} \) and one \( x_{1j} \) on the left end of \( b \) by \( x_{1k} \), evidently multiplication in \( N \) is associative and \( \deg a \cdot b = \deg a + \deg b \) for all \( a, b \in N \).

Received by the editors April 19, 1968.

211
Each $a \in \mathbb{N}$, $a \neq 1$, has a unique normal form $a = a_1 \cdots a_n$ where all $a_i \in S$ and $a_i a_{i+1} \in T$, $i = 1, \ldots, n-1$. We order $\mathbb{N}$ by assuming its elements, in normal form, are ordered by the ordering in $A$.

**Theorem 1.** $\{N; \cdot\}$ is an ordered monoid.

**Proof.** Let $a$, $b$, $c \in \mathbb{N}$ with $a < b$. If $\deg a < \deg b$, then clearly $a \cdot c < b \cdot c$ and $c \cdot a < c \cdot b$. So let us assume that $\deg a = \deg b = n$ and $c \neq 1$.

**Case 1.** $n > 1$. By assumption, $a = a_1 \cdots a_n$, $b = b_1 \cdots b_n$, $c = c_1 \cdots c_k$, where $a_i$, $b_i$, $c_i \in S$, and there exists an integer $j$ such that $a_i = b_i$ if $i < j$ and $a_i < b_j$. If $j = 1$, evidently $a \cdot c < b \cdot c$, and we need only check that $c \cdot a < c \cdot b$. If $1 < j < n$, $c \cdot a_1 < c \cdot b_1$ and hence $c \cdot a < c \cdot b$; and obviously $a \cdot c < b \cdot c$. If $j = n$, $c \cdot a_1 = c \cdot b_1$ and $c \cdot a < c \cdot b$; while $a \cdot c < b \cdot c$ provided $c_n \cdot c_1 < b_n \cdot c_1$. This reduces the problem to the following case.

**Case 2.** $n = 1$, with $a$, $b$, $c \in S$. If $a = x_i$ and $b = x_j$, with $i < j$, then $a \cdot c = ac < bc = b \cdot c$. Also, $c \cdot a = ca < cb = c \cdot b$ unless $c = x_{2m}$ and $m > i$. If $i < m \leq j$, then $c \cdot a = x_{2k} x_{1k} \cdot x_{2m} x_{1j} = c \cdot b$ since $k = [m, i] < m$. If $m > j$, $c \cdot a = x_{2k} x_{1k} \cdot x_{2m} x_{1j}$ because either $k = [m, i] < [m, j] = l$ or $k = l$ and $k' < l$ (this is the case only if $j = i + 1$ and $m + i$ is even).

If $a = x_i$ and $b = x_j$, with $i < j$, then a similar analysis shows that $c \cdot a < c \cdot b$ and $a \cdot c < b \cdot c$ for all $c \in S$.

Finally, we might have $a = x_i$ and $b = x_j$. Then $a \cdot c < b \cdot c$ for all $c \in S$. If $c = x_m$ then clearly $c \cdot a = ca < cb = c \cdot b$. If $c = x_{2m}$, then $c \cdot a = ca < cb = c \cdot b$ if $m \leq i$, whereas, if $m > i$, $c \cdot a = x_{2k} x_{1k} \cdot x_{2m} x_{1j} = c \cdot b$ because $k = [m, i] < m$. This proves the theorem.

For any $m, n \in \mathbb{Z}$, with $m < n$, let $S(m, n) = \{x_i | i = 1, 2, m \leq i \leq n\}$ and $N(m, n)$ be the submonoid of $\mathbb{N}$ generated by $S(m, n)$. Since $S(i, j) \subseteq S(i, j)$ for all $i, j \in \mathbb{Z}$ with $i < j$, evidently each element of $N(m, n)$ when expressed in normal form is a product of elements of $S(m, n)$. If $m < n$, $m' < n'$, and $n - m = n' - m'$, then it is clear that $N(m, n) \cong N(m', n')$.

**Theorem 2.** The monoid $N(1, 3)$ generated by six elements cannot be embedded in a group.

The standard proof of Malcev can be used. Thus, assume that $N(1, 3)$ is a submonoid of some group $G$. Since $x_{12} \cdot x_{11} = x_{21} \cdot x_{12}$, $x_{23} \cdot x_{11} = x_{23} \cdot x_{13}$, and $x_{23} \cdot x_{12} = x_{25} \cdot x_{13}$, we have in $G$ that $x_{22}^{-1} x_{21} = x_{11}^{-1} x_{12}^{-1} = x_{23}^{-1} x_{22}$ = $x_{23}^{-1} x_{13}^{-1}$. Hence, $x_{25} \cdot x_{13} = x_{25} \cdot x_{13}$ contrary to the definition of the monoid $N$. Therefore, $N(1, 3)$ cannot be embedded in a group.

A consequence of Theorem 2 and our remarks above is that the monoid $N(m, n)$ with $n > m + 1$ cannot be embedded in a group.
If $F$ is any integral domain, then the monoid ring $F[N]$ generated by $N$ over $F$ is also an integral domain. For if $f = f_1a_1 + \cdots + f_m a_m$ and $g = g_1b_1 + \cdots + g_n b_n$ are elements of $F[N]$, with $f_i, g_i \in F, f_m \neq 0,$ $g_n \neq 0$, and $a_i, b_i \in N$ such that $a_1 < \cdots < a_m$ and $b_1 < \cdots < b_n$, then $fg$ is nonzero with highest term $f_m g_n a_m b_n$. Since $N$ cannot be embedded in a group, $F[N]$ cannot be embedded in a field. This is also true of each subdomain $F[N(m, n)]$ for which $n > m + 1$.

For any integral domain $D$ and its associated ring $(D)_n$ of $n \times n$ matrices over $D$, the poset $P$ of annihilating right ideals of $(D)_n$ has dimension at least $n$. If $D$ is a field, or a subring of a field, the dimension of $P$ is exactly $n$. For other domains, the dimension of $P$ might be considerably different as the following result shows.

**Theorem 3.** If $F$ is a field, $R = F[N]$, and $P$ is the poset of annihilating right ideals of $(R)_2$, then $P$ satisfies neither the dcc nor the acc.

**Proof.** Let $\{e_{ij} | i, j = 1, 2\}$ be the usual unit matrices in $(R)_2$. If $i + 1 \geq j$ and $r + 1 \geq s$, then $x_{2i} \cdot x_{ij} = x_{2r} \cdot x_{is}$ iff $i + j = r + s$. For each $n \in \mathbb{Z}$, let $a_n = x_{2n} e_{11} - x_{2n+1} e_{12}$ and $b_{nj} = x_{1n} e_{1j} + x_{1n} e_{2j}$, $j = 1, 2$. Then the right annihilator of $a_n$ in $(R)_2$ is given by

\[
(a_n)^r = \sum_{k=-\infty}^{n} \sum_{j=1}^{2} b_{kj}(R)_2.
\]

For if $\sum_{ij} f_{ij} e_{ij} \in (a_n)^r$, then $x_{2n} f_{11} = x_{2n+1} f_{12}$ and $x_{2n} f_{12} = x_{2n+1} f_{22}$. If $f_{ij} = p_{ij} e_{ij} + p_{ij} e_{ij} + \cdots$, with $p_{ijk} \in F$, $e_{ijk} \in N$, and $c_{ijk} < c_{ij}$, necessarily $p_{11k} = p_{21k}$, $p_{12k} = p_{22k}$, $x_{2n} \cdot c_{11k} = x_{2n+1} \cdot c_{11k}$, $x_{2n} \cdot c_{12k}$ $= x_{2n+1} \cdot c_{12k}$ for each $k$. Thus, it is clear that $c_{11k} = c_{11k}$, $c_{12k} = x_{1j} \cdot c_{21k}$ with $i \leq n + 1$, $j = i - 1$, and $c_{11k} = c_{12k}$ for each $k$; and similarly for $c_{22k}$ and $c_{22k}$. Thus, $\sum_{ij} f_{ij} e_{ij}$ has the form given in (1). Since $(a_n)^r < (a_{n+1})^r$ for all $n \in \mathbb{Z}$, $P$ satisfies neither the dcc nor the acc. This proves the theorem.

**Bibliography**


**University of New Hampshire**