A solution to Problem No. 11186 of Monthly 112, Nov. 2005

Dinesh Khurana
Department of Mathematics, Panjab University, Chandigarh-160014 (India)

AND

B. Sury
Stat-Math Unit, Indian Statistical Institute, Banglore 560059 (India)

Problem (Proposed by A. J. Christino, Jr. and William C. Waterhouse)
Let \( R \) be a commutative ring and let \( G \) be the set of invertible matrices
\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix}
\]
over \( R \) with \( a + b = c + d \).

(a) Show that \( G \) is a group, and find a more familiar group to which it is isomorphic.

(b) Now suppose further that \( R \) has prime characteristic \( p \), and let \( H \) be the set of invertible matrices
\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix}
\]
over \( R \) with \( a^p + b^p = c^p + d^p \). Prove that \( H \) is a group and that \( H = \{ sg : s \in S, \ g \in G \} \), where \( S \) is a group of invertible \( 2 \times 2 \) matrices over \( R \) that is isomorphic to the group of \( p \)th roots of unity in \( R \) and \( G \) is the group from part (a).

Solution. We shall prove part (a) for an arbitrary ring \( R \) (not necessarily commutative) with identity. We also show that part (a) can be generalized in many directions (see the remark below). We shall denote by \( U(R) \) the group of units of a ring \( R \) and by \( M_2(R) \) the ring of \( 2 \times 2 \) matrices over ring \( R \).

(a). We shall regard elements of \( M_2(R) \) as module endomorphisms of free right \( R \)-module \( R^2 = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a, b \in R \right\} \). Let \( B \) denote the subring of upper triangular matrices of \( M_2(R) \) and let
\[
A = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(R) : a + b = c + d \right\}.
\]
Clearly \( \begin{pmatrix} 1 \\ 1 \end{pmatrix} \) is an eigen-vector of \( T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) in \( A \) and the matrix of \( T \) with respect to the basis \( \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \) is the upper triangular matrix
\[
\begin{pmatrix} a + b & b \\ 0 & d - b \end{pmatrix}.
\]
Thus if \( U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \) then
\[
U^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} U = \begin{pmatrix} a + b & b \\ 0 & d - b \end{pmatrix},
\]
showing that \( U^{-1}AU = B \) and \( U^{-1}\mathcal{U}(A)U = \mathcal{U}(B) \). So \( A \) is a ring isomorphic to ring \( B \) and \( G = \mathcal{U}(A) \) is a group isomorphic to group \( \mathcal{U}(B) \), which is the subgroup of upper triangular matrices of \( \text{GL}(2,R) \).

**Remark.** Note that the above result can be generalized in many directions. For instance, for any \( t \in R \) the set \( G = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : (a + bt)t = c + dt \right\} \) of invertible matrices over \( R \) is a group as \( U^{-1}GU \) is the subgroup of all upper triangular matrices of \( \text{GL}(2,R) \), where \( U = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \). Another obvious direction for generalization is to look at \( \text{GL}(n,R) \) for a general \( n \). Here, for instance, we may take \( G \) to be the set of all matrices \( (a_{ij}) \) in \( \text{GL}(n,R) \) such that for any \( m \in \{1, \ldots, n-1\} \), \( \sum_{k=m}^{n} a_{ik} = \sum_{k=m}^{n} a_{jk} \) for all \( i, j \geq m \). Then \( G \) can easily be shown to be a group by observing that \( U^{-1}GU \) is the subgroup of all upper triangular matrices in \( \text{GL}(n,R) \), where
\[
U = \begin{pmatrix} 1 & 0 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \ldots & 1 \end{pmatrix}.
\]

(b). *(In this part \( R \) will be a commutative ring with characteristic a prime \( p \).) One can easily check that \( H \) is a subgroup of \( \mathcal{U}(M_2(R)) \) (for instance the inverse of \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) \( \in H \) is \( \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \), which clearly is in \( H \).)

Suppose \( h = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) \( \in H \) and let \( h(p) = \begin{pmatrix} a^p & b^p \\ c^p & d^p \end{pmatrix} \). Then \( h(p) \in G \) and \( U^{-1}h(p)U = \begin{pmatrix} (a + b)^p & b^p \\ 0 & (d - b)^p \end{pmatrix} \), where \( U = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \), implying that \( (a + b)^p = (c + d)^p \) is a unit in \( R \) (this can also be seen directly by observing that \( \begin{pmatrix} 1 \\ 1 \end{pmatrix} \) is an eigenvector of \( h(p) \) with eigenvalue \( (a + b)^p \) and \( \begin{pmatrix} 1 \\ 1 \end{pmatrix} \) is
also an eigenvector of $h(p)^{-1}$. Let $r = (c + d)(a + b)^{-1}$. Then $r^p = 1$, 
\[
\begin{pmatrix}
ra & rb \\
c & d
\end{pmatrix} \in G \text{ and }
\]
\[
\begin{pmatrix}
ra & rb \\
c & d
\end{pmatrix} = h.
\]

So let $S = \left\{ \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} : r \in R \text{ with } r^p = 1 \right\}$. Clearly, $S$ is a group isomorphic to the group of $p$th roots of unity in $R$ and we have shown that $H \subseteq SG$. But as $SG \subseteq H$, we get $SG = H$. \(\blacksquare\)