AN EQUIVALENCE BETWEEN NONASSOCIATIVE RING THEORY AND THE THEORY OF A SPECIAL CLASS OF GROUPS

KENNETH W. WESTON

Introduction. A. Malcev constructed [1, p. 221] an interesting correspondence \( \mathcal{X} \) between the class \( \mathcal{R}_1 \) of all nonassociative rings with identity and a certain class of groups \( G_6 \), nilpotent of class at most 2. Malcev proved [1, Theorem 1, p. 226] by means of this correspondence that the theories of \( \mathcal{R}_1 \) and \( G_6 \) are equivalent. This theorem is generalized here by showing that all of nonassociative ring theory is equivalent to the theory of a larger class of groups \( \mathcal{S} \).

We prove specifically

**Theorem 1.** (a) There is a one to one mapping \( F \) of the class of all nonassociative rings \( \mathcal{R} \) onto a class of groups \( \mathcal{S} \) where \( \mathcal{S} \) is defined by

\[
G \in \mathcal{S} \iff A_1. \text{ } G \text{ is nilpotent of class at most } 2 \text{ (i.e. } G_3 = 1, G_3 \text{ is the third term of the lower central series).}
\]

\[
\iff A_2. \text{ } G \text{ has 2 operators: } \alpha, \beta \text{ where } \alpha^2 = \beta^2 = \alpha \beta = \beta \alpha = 0.
\]

\[
\iff A_3. \text{ If } K_\alpha \text{ and } K_\beta \text{ are the kernels of } \alpha \text{ and } \beta \text{ respectively then } K_\alpha \cap K_\beta \subseteq Z(G). \text{ (} Z(G) \text{ is the center of } G). \]

\[
\iff A_4. \text{ } K_\alpha \text{ and } K_\beta \text{ are abelian.}
\]

\[
\iff A_5. \text{ There are 2 homomorphisms } \alpha \text{ and } \beta \text{ defined on } K_\alpha \cap K_\beta \to G \text{ satisfying } X^{\alpha \alpha} = X^{\beta \beta} = X \text{ and } X^{\alpha \beta} = X^{\beta \alpha} = 1, \text{ } X \in K_\alpha \cap K_\beta.
\]

(b) If \( T_\mathcal{R} \) and \( T_\mathcal{S} \) denote standard formalization of the theories for \( \mathcal{R} \) and \( \mathcal{S} \) respectively in the sense of Tarski-Mostowski-Robinson, Undecidable theories [2, 1.2] then \( F \) induces a one to one recursive mapping \( \overline{F} \) of all the closed formulas in \( T_\mathcal{R} \) onto those of \( T_\mathcal{S} \). Also if \( R \in \mathcal{R} \) and \( P \) is a closed formula of \( T_\mathcal{R} \) then \( P \) is true in \( R \) if and only if \( \overline{F}(P) \) is true in \( F(R) \). Likewise \( F^{-1} \) induces a one to one recursive mapping \( \overline{F}^{-1} \) of all the closed formulas in \( T_\mathcal{S} \) onto those of \( T_\mathcal{R} \) where \( G \in \mathcal{S} \) and \( Q \) is a closed formula of \( T_\mathcal{S} \) implies that \( Q \) is true in \( G \) if and only if \( \overline{F}^{-1}(Q) \) is true in \( F^{-1}(G) \).

(c) \( F(\mathcal{R}_1) = G_6 \)

The axioms: \( A_1, \cdots, A_5 \) are not in their weakest form.

**Example.** It can be shown that \( A_4 \) can be replaced by the assumption that either \( K_\alpha \) or \( K_\beta \) is abelian.

Received by the editors June 7, 1967 and, in revised form, July 27, 1967.

1356
Proof of Theorem 1 (a). If $R \subseteq \mathbb{R}$ denote by $F(R)$ the collection of unipotent matrices

\[
\begin{pmatrix}
1 & y & z \\
0 & 1 & x \\
0 & 0 & 1
\end{pmatrix}, \quad x, y, z \in R.
\]

It is perfectly straightforward to show that $F(R)$ forms a group with identity

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

and

\[
\begin{pmatrix}
1 & 0 & x \\
1 & 0 & 0 \\
0 & 0 & 1
\end{pmatrix}, \quad x \in R
\]

Therefore by (1) and (2), $F(R)$ is nilpotent of class at most 2 and axiom $A_1$ is satisfied.

Next define the mappings $\alpha$ and $\beta$ on $F(R)$ by

\[
\begin{pmatrix}
1 & y & z \\
0 & 1 & x \\
0 & 0 & 1
\end{pmatrix}^\alpha = \begin{pmatrix}
1 & 0 & -y \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix},
\]

\[
\begin{pmatrix}
1 & y & z \\
0 & 1 & x \\
0 & 0 & 1
\end{pmatrix}^\beta = \begin{pmatrix}
1 & 0 & x \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}, \quad x, y, z \in R.
\]

It’s trivial to show that $\alpha$ and $\beta$ are operators over $F(R)$ and $\alpha^2 = \beta^2 = \alpha\beta = \beta\alpha = 0$. Thus $A_2$ is satisfied.
If $K_\alpha$ and $K_\beta$ are the kernels of $\alpha$ and $\beta$ respectively then

$$
K_\alpha = \begin{cases}
1 & 0 & y \\
0 & 1 & x \\
0 & 0 & 1
\end{cases}, \quad x, y \in R, \\
K_\beta = \begin{cases}
1 & x & y \\
0 & 1 & 0 \\
0 & 0 & 1
\end{cases}, \quad x, y \in R.
$$

Hence by (1)

$$
K_\alpha \cap K_\beta = \begin{cases}
1 & 0 & x \\
0 & 1 & 0 \\
0 & 0 & 1
\end{cases}, \quad x \in R \subseteq Z(F(R)).
$$

That $K_\alpha$ and $K_\beta$ are abelian follows directly from (4).

Using (5) we can define mappings $\tilde{\alpha}$ and $\tilde{\beta}$ on $K_\alpha \cap K_\beta \rightarrow G$ by

$$
\begin{pmatrix}
1 & 0 & x \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}
= \begin{pmatrix}
1 & -x & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}, \quad x \in R.
$$

Direct calculation shows that $\tilde{\alpha}$ and $\tilde{\beta}$ are homomorphisms of $K_\alpha \cap K_\beta$ into $K_\beta$ and $K_\alpha$ respectively and

$$
\begin{pmatrix}
1 & 0 & x \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}
\begin{pmatrix}
1 & 0 & x \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}
= \begin{pmatrix}
1 & 0 & x \\
0 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}, \quad x \in R.
$$

We have shown thus far that $F(R)$ satisfies axioms: $A_1, \ldots, A_6$.

Now we determine a mapping $H: \emptyset \rightarrow \Re$ such that

$$
\begin{align*}
(a) & \quad F(H(G)) \cong G, \quad G \in \emptyset, \\
(b) & \quad H(F(R)) \cong R, \quad R \in \Re
\end{align*}
$$

and hence $F$ is one to one and onto.

For $G \in \emptyset$ let $H(G) = K_\alpha \cap K_\beta$ where addition $\oplus$ and multiplication $\otimes$ are defined by

$$
\begin{align*}
g_1 \oplus g_2 &= g_1 \cdot g_2, \\
g_1 \otimes g_2 &= \tilde{\beta} \tilde{\alpha}, \\
&= \begin{pmatrix}
g_2 & g_1
\end{pmatrix}, \quad g_1, g_2 \in H(G).
\end{align*}
$$

Obviously $H(G)$ forms an abelian group under addition. $H(G)$ is also closed under multiplication since
\[(g_1 \otimes g_2)^\alpha = [g_2, g_1] = [g_2, g_1] = [1, g_1] = 1\]

and
\[(g_1 \otimes g_2)^\beta = [\tilde{g}_2, \tilde{g}_1] = [\tilde{g}_2, \tilde{g}_1] = [g_2, 1] = 1.\]

The distributive laws also follow.

To prove 7 (b) let \(R \subseteq \mathbb{R}\). By (5)

\[H(F(R)) = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ x \in R.\]

Also, by (8), (6) and (2)
\[
\begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & x \end{pmatrix}^{\tilde{\beta}} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & x \end{pmatrix}^{\tilde{\alpha}} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\end{array}
\]

To prove 7 (a) is somewhat more difficult. Assume that \(G \subseteq \mathcal{G}\) and \(X \in F(H(G))\), i.e.
\[
X = \begin{pmatrix} 1 & h_2 & h_3 \\ 0 & 1 & h_1 \\ 0 & 0 & 1 \end{pmatrix}, \ h_1, h_2, h_3 \subseteq K_{\alpha} \cap K_{\beta}.
\]

Define a mapping \(\tau\) on \(F(H(G)) \to G\) by
\[(9) \quad X' = \tilde{h}_1(h_2)^{-1} h_3.\]

In order to first show that \(\tau\) is a homomorphism let
\[
Y = \begin{pmatrix}
1 & k_2 & k_3 \\
0 & 1 & k_1 \\
0 & 0 & 1
\end{pmatrix}, \quad k_1, k_2, k_3 \in K_\alpha \cap K_\beta,
\]

and apply (8) and (9) to get
\[
(X \cdot Y)^r = \begin{pmatrix}
1 & h_2 \oplus k_2 & (h_2 \otimes k_1) \oplus h_3 \oplus k_3 \\
0 & 1 & h_1 \oplus k_1 \\
0 & 0 & 1
\end{pmatrix}^r
\]
\[
= (h_1 k_1)^{\tilde{\beta}} (k_2)^{\tilde{\alpha}} (h_2)^{-1} (k_1)^{\tilde{\alpha}} [k_1, h_2] h_3 k_3.
\]

Since
\[
(X^r)^{-1} = k_3 (k_2^{-1})^{\tilde{\alpha}} (k_1^{-1})^{\tilde{\beta}},
\]

by axioms $A_1$, $A_3$ and $A_4$ we have
\[
(X \cdot Y)^r (X^r)^{-1} = (h_1 k_1)^{\tilde{\beta}} (h_2)^{-1} (k_1)^{\tilde{\alpha}} [k_1, h_2] h_3.
\]

Now every nilpotent group $N$ of class at most 2 satisfies the identity $[u^{-1}, v^{-1}] = [u, v]$, $u, v \in N$ (i.e. observe that $1 = [u, v \cdot v^{-1}] = [u, v] \cdot [u, v^{-1}]$), which in turn implies $[u, v]^{-1} = [u, v^{-1}]$. Consequently
\[
[k_1, h_2] = k_1 h_2 (k_1)^{-1} (h_2)^{-1}.
\]

By (10) and (11) we can see then
\[
(X \cdot Y)^r (X^r)^{-1} = h_1 (h_2)^{-1} h_3 = X^r.
\]

Hence $\tau$ is a homomorphism.

We wish to show now that the kernel of $\tau$ is the identity. Therefore let
\[
X = \begin{pmatrix}
1 & h_2 & h_3 \\
0 & 1 & h_1 \\
0 & 0 & 1
\end{pmatrix}, \quad h_1, h_2, h_3 \in K_\alpha \cap K_\beta,
\]

and
\[
X^r = (h_1)^{\tilde{\beta}} (h_2)^{-1} h_3 = 1.
\]

Thus $h_1 = (h_3)^{\tilde{\beta}} (h_2)^{\tilde{\alpha}}$ and by $A_4$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
\[ h_1 = (h_3)_{-1}^\alpha (h_2)_{-1}^\beta = 1. \]

Likewise

\[ (h_1)_{-1}^\alpha (h_2)_{-1}^\alpha = (h_3)_{-1} (h_2)_{-1} = 1 = h_2. \]

But \( h_1 = h_2 = 1 \) implies \( h_3 = 1 \) and hence \( X \) is the identity.

To show that \( r \) is an onto mapping let \( g \in G \) and \( g_1 = g^a, g_2 = g^b \) and

\[ g_3 = (g_2)_{-1}^\beta g_1 = (g_2)_{-1}^\beta g_1 g_3 = g. \]

Consequently (by \( A_2 \)) \( g_1, g_2, g_3 \in K_a \cap H_\beta \) and

\[ X = \begin{pmatrix} 1 & 1 & 1 \\ 0 & g_1 & g_2 \\ 0 & 0 & 1 \end{pmatrix} \in F(H(G)). \]

Therefore by \( A_3 \), \( X^r = g_3^a g_1 g_2 = g_3^a g_1 \rightarrow g_3 = g. \) Thus \( H \) is the inverse map of \( F \).

**Proof of Theorem 1** (b). We assume that the logical symbolism of \( T_\mathfrak{R} \) and \( T_\mathcal{G} \) is that of [2]. Suppose also that \( T_\mathfrak{R} \) contains among its list of primitive symbols: \( \times, +, 0 \), denoting: multiplication, addition and the additive identity respectively. Let \( T_\mathcal{G} \) contain among its primitive symbols: \( \alpha(), \beta(), [], \cdot, 1 \) to denote: homomorphisms: \( \alpha, \beta \), commutation, multiplication and identity respectively. Suppose also \( K \) denotes a formula in \( T_\mathcal{G} \) representing the predicate \( x \in K_a \cap K_\beta \).

Given a formula \( P \) in \( T_\mathfrak{R} \) we construct a new formula \( B \) of \( T_\mathcal{G} \) by replacing each occurrence of: \( x_i \times x_j, x_i + x_j \) and 0 in \( P \) by: \([\beta(x_i), \alpha(x_i)]\), \( x_i \cdot x_j, 1 \) respectively. Let \( B^K \) denote the formula obtained by relativizing \( B \) to \( K \), [2, p. 25]. The map \( F \) is defined by \( F(P) = B^K \). It's clear from the construction of \( H \) that \( P \) is true in \( R \) if and only if \( B^K \) is true in \( F(R) \).

For the converse assume that \( P \) is a formula in \( T_\mathcal{G} \). Transform \( P \) recursively into prenex form [3, Theorem 19, p. 167] \( Q_1 x_1, \ldots, Q_n x_n S(x_1, \ldots, x_n, 1) \) where \( Q_i \) represents a quantifier and \( S(x_1, \ldots, x_n, 1) \) is a formula in \( T_\mathcal{G} \) with all of its variables: \( x_1, \ldots, x_n \), occurring free. We may assume without generality that each variable \( x_i \) occurs with positive exponent. From this we construct a formula \( C \) in \( T_\mathfrak{R} \) defined by

\[ Q_1 x_1 Q_1 y_1 Q_1 z_1, \ldots, Q_n x_n Q_n y_n Q_n z_n S'(x_1, y_1, z_1, \ldots, x_n, y_n, z_n, 0) \]

where \( S'(x_1, y_1, z_1, \ldots, x_n, y_n, z_n, 0) \) results from \( S(x_1, \ldots, x_n, 1) \) by replacing every equation of the form: \( x_{i_1} \cdots x_{i_k} = 1 \) by

\[ (x_{i_1} + x_{i_2} + \cdots + x_{i_k} = 0) \land (y_{i_1} + y_{i_2} + \cdots + y_{i_k} = 0) \]

\[ \land ((y_{i_1} + y_{i_2} + \cdots + y_{i_{k-1}})x_{i_k} + (y_{i_1} + \cdots + y_{i_{k-2}})x_{i_{k-1}} + \cdots + y_{i_1}x_{i_2} + z_{i_1} + \cdots + z_{i_k} = 0) \]

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
and every equation of the form: 
\( x_{j_1}x_{j_2} \cdots x_{j_m} = x_{l_1}x_{l_2} \cdots x_{l_q} \) by
\[
(x_{j_1} + x_{j_2} + \cdots + x_{j_m} = x_{l_1} + x_{l_2} + \cdots + x_{l_q})
\]
\[
\land (y_{j_1} + y_{j_2} + \cdots + y_{j_m} = y_{l_1} + y_{l_2} + \cdots + y_{l_q})
\]
\[
\land (y_{j_1} + y_{j_2} + \cdots + y_{j_{m-1}}x_{j_m} + y_{j_1}x_{j_2} + z_{j_1} + \cdots + z_{j_m}) = (y_{l_1} + y_{l_2} + \cdots + y_{l_{q-1}}x_{l_q} + (y_{l_1} + y_{l_2} + \cdots + y_{l_{q-2}}x_{l_{q-1}} + \cdots + y_{l_1}x_{l_2} + z_{l_1} + \cdots + z_{l_m}).
\]

Define the map \( \bar{F}^{-1} \) by \( \bar{F}^{-1}(P) = C \). As is obvious from the construction of \( F, P \) is true in \( G \) if and only if \( C \) is true in \( F^{-1}(G) \).

**Proof of Theorem 1 (c).** The correspondence \( \mathcal{X} \) in [1] is the following.

If \( R \in \mathcal{R}_1 \) let \( \mathcal{X}(R) \) denote the collection of ordered triples \((x_1, x_2, x_3)\) of elements from \( R \) and define multiplication by
\[
(x_1, x_2, x_3) \cdot (y_1, y_2, y_3) = (x_1 + y_1, x_2 + y_2, x_2y_1 + x_3 + y_3).
\]

One has only to make the correspondence
\[
\begin{bmatrix} 1 & x_2 & x_3 \\ 1 & 0 & x_1 \\ 0 & 0 & 1 \end{bmatrix} \leftrightarrow (x_1, x_2, x_3)
\]
between \( F(R) \) and \( \mathcal{X}(R) \) to see \( F(R) \cong \mathcal{X}(R) \). Since \( G_6 = \mathcal{X}(\mathcal{R}_1) \), the proof is complete.

The proof of the following statement follows from (2).

**Theorem 2.** The operators \( \alpha \) and \( \beta \) in \( A_2 \) are left commutation by matrices:
\[
\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}
\]
respectively.

**References**


University of Notre Dame