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 X between the class $\mathfrak{R}_1$ of all nonassociative rings with identity and a certain class of groups G_5, nilpotent of class at most 2. Malcev proved [1, Theorem 1, p. 226] by means of this correspondence that the theories of $\mathfrak{R}_1$ and G_5 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 $\mathfrak{G}$.

We prove specifically

THEOREM 1. (a) *There is a one to one mapping F of the class of all nonassociative rings $\mathfrak{R}$ onto a class of groups $\mathfrak{G}$ where $\mathfrak{G}$ is defined by*

$G\in\mathfrak{G}\Leftrightarrow\mathrm{A}_1$. *$G$ is nilpotent of class at most 2 (i.e. $G_3=1$, G_3 is the third term of the lower central series).*

$\Leftrightarrow\mathrm{A}_2$. *$G$ has 2 operators: α, β where $\alpha^2=\beta^2=\alpha\beta=\beta\alpha=0$.*

$\Leftrightarrow\mathrm{A}_3$. *If K_α and K_β are the kernels of α and β respectively then $K_\alpha\cap K_\beta\subseteq Z(G)$. ($Z(G)$ is the center of G.)*

$\Leftrightarrow\mathrm{A}_4$. *$K_\alpha$ and K_β are abelian.*

$\Leftrightarrow\mathrm{A}_5$. *There are 2 homomorphisms $\tilde{\alpha}$ and $\tilde{\beta}$ defined on $K_\alpha\cap K_\beta\to G$ satisfying $X^{\tilde{\alpha}\alpha}=X^{\tilde{\beta}\beta}=X$ and $X^{\tilde{\alpha}\beta}=X^{\tilde{\beta}\alpha}=1$, $X\in K_\alpha\cap K_\beta$.*

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

(c) $F(\mathfrak{R}_1)=G_5$

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_α or K_β is abelian.

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

PROOF OF THEOREM 1 (a). If $R \in \mathfrak{R}$ denote by $F(R)$ the collection of unipotent matrices

$$\begin{pmatrix} 1 & y & z \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}, \qquad x, y, z \in R.$$

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

$$\left\{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad x \in R \right\} \subseteq Z(F(R)). \tag{1}$$

We shall first verify axioms: $A_1, \cdots, A_5$. In order to do so, assume that g and h are elements of a group G and define the group commutator of g and h to be the product $g^{-1} \cdot h^{-1} \cdot g \cdot h$. If we denote the commutator of g and h by $[g, h]$, then direct calculation yields

$$\left[\begin{pmatrix} 1 & b & c \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & y & z \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 & bx-ya \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad a, b, c, x, y, z \in R. \tag{2}$$

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

Next define the mappings α and β on $F(R)$ by

$$\begin{aligned} \begin{pmatrix} 1 & y & z \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}^{\alpha} &= \begin{pmatrix} 1 & 0 & -y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \\ \begin{pmatrix} 1 & y & z \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}^{\beta} &= \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad x, y, z \in R. \end{aligned} \tag{3}$$

It's trivial to show that α and β are operators over $F(R)$ and $\alpha^2 = \beta^2 = \alpha\beta = \beta\alpha = 0$. Thus A_2 is satisfied.

If K_α and K_β are the kernels of α and β respectively then

$$(4)\qquad K_\alpha = \left\{ \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix},\ x, y \in R \right\},\qquad K_\beta = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ x, y \in R \right\}.$$

Hence by (1)

$$(5)\qquad K_\alpha \cap K_\beta = \left\{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ x \in R \right\} \subseteq Z(F(R)).$$

That K_α and K_β are abelian follows directly from (4).

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

$$(6)\qquad \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{\tilde{\alpha}} = \begin{pmatrix} 1 & -x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\quad \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{\tilde{\beta}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix},\quad x \in R.$$

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

$$\begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{\tilde{\alpha}\alpha} = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{\tilde{\beta}\beta} = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{\tilde{\alpha}\beta} = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{\tilde{\beta}\alpha} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We have shown thus far that $F(R)$ satisfies axioms: $A_1, \cdots, A_5$. Now we determine a mapping $H\colon \mathfrak{G} \to \mathfrak{R}$ such that

$$(7)\qquad \begin{array}{ll} \text{(a)} & F(H(G)) \cong G, \quad G \in \mathfrak{G}, \\ \text{(b)} & H(F(R)) \cong R, \quad R \in \mathfrak{R} \end{array}$$

and hence F is one to one and onto.

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

$$(8)\qquad g_1 \oplus g_2 = g_1 \cdot g_2, \qquad g_1 \otimes g_2 = [\overset{\tilde{\beta}}{g_2}, \overset{\tilde{\alpha}}{g_1}], \quad g_1, g_2 \in H(G).$$

Obviously $H(G)$ forms an abelian group under addition. $H(G)$ is also closed under multiplication since

$$(g_1 \otimes g_2)^{\alpha} = [g_2^{\tilde{\beta}}, \ g_1^{\tilde{\alpha}}]^{\alpha} = [g_2^{\tilde{\beta}\alpha}, \ g_1^{\tilde{\alpha}\alpha}] = [1, g_1] = 1$$

and

$$(g_1 \otimes g_2)^{\beta} = [g_2^{\tilde{\beta}}, \ g_1^{\tilde{\alpha}}]^{\beta} = [g_2^{\tilde{\beta}\beta}, \ g_1^{\tilde{\alpha}\beta}] = [g_2, \ 1] = 1.$$

The distributive laws also follow.

To prove 7 (b) let $R \in \mathfrak{R}$. By (5)

$$H(F(R)) = \left\{ \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad x \in R \right\}.$$

Also, by (8), (6) and (2)

$$\begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & x+y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\begin{aligned} \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} &= \left[\begin{pmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{\tilde{\beta}}, \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{\tilde{\alpha}} \right] \\ &= \left[\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right] \\ &= \begin{pmatrix} 1 & 0 & x \cdot y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

To prove 7 (a) is somewhat more difficult. Assume that $G \in \mathfrak{G}$ and $X \in F(H(G))$, i.e.

$$X = \begin{pmatrix} 1 & h_2 & h_3 \\ 0 & 1 & h_1 \\ 0 & 0 & 1 \end{pmatrix}, \qquad h_1, h_2, h_3 \in K_\alpha \cap K_\beta.$$

Define a mapping τ on $F(H(G)) \rightarrow G$ by

(9) $$X^{\tau} = h_1^{\tilde{\beta}} (h_2^{\tilde{\alpha}})^{-1} h_3.$$

In order to first show that τ is a homomorphism let

$$Y = \begin{pmatrix} 1 & k_2 & k_3 \\ 0 & 1 & k_1 \\ 0 & 0 & 1 \end{pmatrix}, \qquad k_1, k_2, k_3 \in K_\alpha \cap K_\beta,$$

and apply (8) and (9) to get

$$\begin{aligned}(X \cdot Y)^\tau &= \begin{pmatrix} 1 & h_2 \oplus k_2 & (h_2 \otimes k_1) \oplus h_3 \oplus k_3 \\ 0 & 1 & h_1 \oplus k_1 \\ 0 & 0 & 1 \end{pmatrix}^\tau \\ &= (h_1 k_1)^{\tilde{\beta}} (k_2^{-1})^{\tilde{\alpha}} (h_2^{-1})^{\tilde{\alpha}} [k_1^{\tilde{\beta}}, h_2^{\tilde{\alpha}}] h_3 k_3.\end{aligned}$$

Since

$$(Y^\tau)^{-1} = k_3^{-1} k_2^{\tilde{\alpha}} (k_1^{-1})^{\tilde{\beta}},$$

by axioms A_1, A_3 and A_4 we have

$$(X \cdot Y)^\tau (Y^\tau)^{-1} = (h_1 k_1)^{\tilde{\beta}} (h_2^{-1})^{\tilde{\alpha}} (k_1^{-1})^{\tilde{\beta}} [k_1^{\tilde{\beta}}, h_2^{\tilde{\alpha}}] h_3. \tag{10}$$

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

$$[\tilde{k}_1, h_2^{\tilde{\alpha}}] = k_1^{\tilde{\beta}} h_2^{\tilde{\alpha}} (k_1^{\tilde{\beta}})^{-1} (h_2^{\tilde{\alpha}})^{-1}. \tag{11}$$

By (10) and (11) we can see then

$$(X \cdot Y)^\tau (Y^\tau)^{-1} = h_1^{\tilde{\beta}} (h_2^{\tilde{\alpha}})^{-1} h_3 = X^\tau.$$

Hence τ is a homomorphism.

We wish to show now that the kernel of τ is the identity. Therefore let

$$X = \begin{pmatrix} 1 & h_2 & h_3 \\ 0 & 1 & h_1 \\ 0 & 0 & 1 \end{pmatrix}, \qquad h_1, h_2, h_3 \in K_\alpha \cap K_\beta,$$

and

$$X^\tau = h_1^{\tilde{\beta}} (h_2^{\tilde{\alpha}})^{-1} h_3 = 1.$$

Thus $h_1^{\tilde{\beta}\beta} = (h_3^{\beta})^{-1} (h_2^{\tilde{\alpha}})^{\beta}$ and by A_5

$$h_1 = \left(h_3^{\beta}\right)^{-1}\left(h_2^{\tilde{\alpha}}\right)^{\beta} = 1.$$

Likewise

$$\left(h_1^{\tilde{\beta}}\right)^{\alpha} = \left(h_3^{\alpha}\right)^{-1}\left(h_2^{\tilde{\alpha}}\right)^{\alpha}, \qquad 1 = h_2.$$

But $h_1 = h_2 = 1$ implies $h_3 = 1$ and hence X is the identity.

To show that τ is an onto mapping let $g \in G$ and $g_1 = g^{\alpha}$, $g_2 = g^{\beta}$ and $g_3 = (g_2^{\tilde{\beta}})^{-1} g (g_1^{\tilde{\alpha}})^{-1}$. Consequently (by A_2) $g_1, g_2, g_3 \in K_{\alpha} \cap H_{\beta}$ and

$$X = \begin{pmatrix} 1 & g_1^{-1} & g_3 \\ 0 & 1 & g_2 \\ 0 & 0 & 1 \end{pmatrix} \in F(H(G)).$$

Therefore by A_3, $X^{\tau} = g_2^{\tilde{\beta}} g_1^{\tilde{\alpha}} g_3 = g_2^{\tilde{\beta}} g_3 g_1^{\tilde{\alpha}} = g$. Thus H is the inverse map of F.

PROOF OF THEOREM 1 (b). We assume that the logical symbolism of $T_{\mathfrak{R}}$ and $T_{\mathfrak{G}}$ 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 $T_{\mathfrak{G}}$ contain among its primitive symbols: $\tilde{\alpha}(\ )$, $\tilde{\beta}(\ )$, $[\ ,\ ]$, $\cdot$, 1 to denote: homomorphisms: $\tilde{\alpha}$, $\tilde{\beta}$, commutation, multiplication and identity respectively. Suppose also K denotes a formula in $T_{\mathfrak{G}}$ representing the predicate $x \in K_{\alpha} \cap K_{\beta}$.

Given a formula P in $T_{\mathfrak{R}}$ we construct a new formula B of $T_{\mathfrak{G}}$ by replacing each occurrence of: $x_i \times x_j$, $x_i + x_j$ and 0 in P by: $[\tilde{\beta}(x_j), \tilde{\alpha}(x_i)]$, $x_i \cdot x_j$, 1 respectively. Let B^K denote the formula obtained by relativizing B to K, [2, p. 25]. The map $\overline{F}$ is defined by $\overline{F}(P) = B^K$. 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 $T_{\mathfrak{G}}$. Transform P recursively into prenex form [3, Theorem 19, p. 167] $Q_1x_1, \cdots, Q_nx_n\, S(x_1, \cdots, x_n, 1)$ where Q_i represents a quantifier and $S(x_1, \cdots, x_n, 1)$ is a formula in $T_{\mathfrak{G}}$ with all of its variables: $x_1, \cdots, x_n$, 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

$$Q_1x_1Q_1y_1Q_1z_1, \cdots, Q_nx_nQ_ny_nQ_nz_nS'(x_1, y_1, z_1, \cdots, x_n, y_n, z_n, 0)$$

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

$$\begin{aligned}(x_{i_1} + x_{i_2} + \cdots + x_{i_k} = 0) \wedge (y_{i_1} + y_{i_2} + \cdots + y_{i_k} = 0)&\\ \wedge ((y_{i_1} + y_{i_2} + \cdots + y_{i_{k-1}})x_{i_k}&\\ + (y_{i_1} + \cdots + y_{i_{k-2}})x_{i_{k-1}} + \cdots&\\ + y_{i_1}x_{i_2} + z_{i_1} + \cdots + z_{i_k} = 0)&\end{aligned}$$

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

$$\begin{aligned}
&(x_{j_1}+x_{j_2}+\cdots+x_{j_m}=x_{l_1}+x_{l_2}+\cdots+x_{l_q})\\
&\wedge(y_{j_1}+y_{j_2}+\cdots+y_{j_m}=y_{l_1}+y_{l_2}+\cdots+y_{l_q})\\
&\wedge(y_{j_1}+y_{j_2}+\cdots+y_{j_{m-1}})x_{j_m}\\
&\quad+(y_{j_1}+y_{j_2}+\cdots+y_{j_{m-2}})x_{j_{m-1}}+\cdots+y_{j_1}x_{j_2}+z_{j_1}+\cdots+z_{j_m}\\
&\quad=(y_{l_1}+y_{l_2}+\cdots+y_{l_{q-1}})x_{l_q}+(y_{l_1}+y_{l_2}+\cdots+y_{l_{q-2}})x_{l_{q-1}}\\
&\qquad\qquad+\cdots+y_{l_1}x_{l_2}+z_{l_1}+\cdots+z_{l_m}).
\end{aligned}$$

Define the map $\overline{F}^{-1}$ by $\overline{F}^{-1}(P)=C$. 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 $\mathbf{X}$ in [**1**] is the following.

If $R\in\mathfrak{R}_1$ let $\mathbf{X}(R)$ denote the collection of ordered triples (x_1, x_2, x_3) of elements from R and define multiplication by

$$(x_1, x_2, x_3)\cdot(y_1, y_2, y_3) = (x_1+y_1, x_2+y_2, x_2\cdot y_1+x_3+y_3).$$

One has only to make the correspondence

$$\begin{pmatrix}1 & x_2 & x_3\\ 0 & 1 & x_1\\ 0 & 0 & 1\end{pmatrix}\leftrightarrow(x_1, x_2, x_3)$$

between $F(R)$ and $\mathbf{X}(R)$ to see $F(R)\cong\mathbf{X}(R)$. Since $G_5=\mathbf{X}(\mathfrak{R}_1)$, the proof is complete.

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

THEOREM 2. *The operators α and β in A_2 are left commutation by matrices*:

$$\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix}\quad \textit{and}\quad \begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$$

respectively.

REFERENCES

1. A. Malcev, *On a correspondence between rings and groups*, Amer. Math. Soc. Transl. (2) **45** (1960), 221–231.

2. A. Tarski, A. Mostowski and R. Robinson, *Undecidable theories*, North-Holland, Amsterdam, 1953.

3. S. Kleene, *Introduction to metamathematics*, Van Nostrand, Princeton, N. J., 1952.

UNIVERSITY OF NOTRE DAME