

SIMPLICITY OF NEAR-RINGS OF TRANSFORMATIONS

GERALD BERMAN AND ROBERT J. SILVERMAN

1. Introduction. Consider a group $\mathfrak{G} = (G, +)$ (not necessarily commutative) and $T(G)$, the set of transformations on G . Define addition $(+)$ and multiplication (\cdot) on $T(G)$ by

$$(1.1) \quad g(A + B) = gA + gB, \quad g(AB) = (gA)B, \quad g \in G, \quad A, B \in T(G).$$

Then $(T(G), +, \cdot) = \mathfrak{T}(\mathfrak{G})$ is a *near-ring, the near-ring of transformations on \mathfrak{G}* . That is (i) $(T(G), +)$ is a group, (ii) $(T(G), \cdot)$ is a semi-group, and (iii) multiplication is left distributive with respect to addition:

$$(1.2) \quad A(B + C) = AB + AC, \quad A, B, C \in T(G).$$

The transformation 0 , where $g0=0$, for all $g \in G$, is the zero of $\mathfrak{T}(\mathfrak{G})$. Let $T_0(G)$ be the set of all transformations which commute with the zero transformation, i.e. $0A = 0, A \in T(G)$. $T_0(G)$ determines a sub-near-ring $\mathfrak{T}_0(\mathfrak{G})$ of $\mathfrak{T}(\mathfrak{G})$.

The main theorem is now stated.

THEOREM 1. *For any group \mathfrak{G} , $\mathfrak{T}(\mathfrak{G})$ and $\mathfrak{T}_0(\mathfrak{G})$ are simple.*

That is, they have no proper nontrivial homomorphic images.

2. Preliminaries. A subset Q of a near-ring \mathfrak{P} determines an *ideal* of \mathfrak{P} if and only if

- (a) $(Q, +)$ is a normal subgroup of $(P, +)$,
- (b) $PQ \subset Q$,
- (c) $(a+q)b - ab$ is in Q for all $a, b \in P, q \in Q$.

As in ring theory, the kernel \mathfrak{Q} of a homomorphism θ from a near-ring \mathfrak{P} to a near-ring \mathfrak{P}' (i.e. the inverse image of the zero of P') is an ideal. Every ideal \mathfrak{Q} is the kernel of the natural homomorphism $\nu: a\nu = a + Q$, from \mathfrak{P} to the difference near-ring $\mathfrak{P} - \mathfrak{Q}$, and every homomorphic image $\mathfrak{P}\theta$ with kernel \mathfrak{Q} is isomorphic to $\mathfrak{P} - \mathfrak{Q}$. Thus a near-ring \mathfrak{P} is simple if and only if its only ideals are itself and the zero ideal.

By way of warning, the following three concepts are introduced. A subset Q of a near-ring \mathfrak{P} determines (α) a *left ideal* if it satisfies (a) and (b), (β) a *right ideal* if it satisfies (a) and (b') $QP \subset Q$, (γ) a *two-sided ideal* if it satisfies (a), (b) and (b'). While an ideal is a left ideal, examples show that ideals need not be two-sided ideals, and

Received by the editors April 17, 1958 and, in revised form, October 27, 1958.

that two-sided ideals need not be ideals.

In the near-ring $\mathfrak{T}(\mathfrak{G})$, denote by Z_g the transformation such that $g'Z_g = g$, $g' \in G$. Clearly $AZ_g = Z_g$, and $Z_gA = Z_{gA}$, for every A in $T(G)$ and g in G . In particular $Z_0 = 0$ in $(T(G), +)$.

LEMMA 1. *If \mathfrak{Q} is an ideal of $\mathfrak{T}(\mathfrak{G})$, then $QT_0(G) \subset \mathfrak{Q}$.*

From (c), letting $a \in \mathfrak{Q}$, $b \in T_0(G)$, $(Z_0 + a)b - Z_0b = ab \in \mathfrak{Q}$. In particular, if \mathfrak{Q} is an ideal of $\mathfrak{T}_0(\mathfrak{G})$, then \mathfrak{Q} is a two-sided ideal of $\mathfrak{T}_0(\mathfrak{G})$.

LEMMA 2. *The only sub-near-ring of $\mathfrak{T}(\mathfrak{G})$ which contains $\mathfrak{T}_0(\mathfrak{G})$ properly is $\mathfrak{T}(\mathfrak{G})$ itself.*

Let \mathfrak{B} be a sub-near-ring of $\mathfrak{T}(\mathfrak{G})$ containing $\mathfrak{T}_0(\mathfrak{G})$. Consider $A \in P$, $A \notin T_0(G)$. Then $A - Z_{0A} \in T_0(G)$. Hence $Z_{0A} \in P$. Since $0A \neq 0$; and $Z_{0A}B = Z_{0(AB)}$, and $T_0(G)$ is transitive on the nonzero elements of G , the set of Z_g 's, $g \in G$ is in P . Thus, $C \in T(G)$, $C = (C - Z_{0C}) + Z_{0C}$ is in P , for $C - Z_{0C}$ is in $T_0(G)$.

3. Proof of the theorem. A transformation $A \in T(G)$ has rank $R(A) = R$ if the set $\{gA \mid g \in G\}$ has cardinality R .

LEMMA 3. *A nonzero ideal $\mathfrak{I} \subset \mathfrak{T}_0(\mathfrak{G})$ contains all the elements of rank 2.*

By Lemma 1, \mathfrak{I} is a two-sided ideal, and since $\mathfrak{I} \neq \{0\}$, there exists a $V \in I$ and $g_1, g_1' \in G$, $g_1' \neq 0$ such that $g_1V = g_1'$. Partition G into disjoint sets G_1 and G_2 , $0 \in G_2$. Define $A \in T_0(G)$ such that $gA = g_1$, $g \in G_1$, $gA = 0$, $g \in G_2$. Let g'' be any element of G , and let $B \in T_0(G)$ be such that $g_1'B = g''$. Then $gAVB = g''$, $g \in G_1$, $gAVB = 0$, $g \in G_2$, and $AVB \in I$.

LEMMA 4. *If \mathfrak{G} is finite, $\mathfrak{T}_0(\mathfrak{G})$ is simple.*

Suppose I contains all elements of rank less than or equal to k . Partition G into pairwise disjoint nonempty sets G_0, G_1, \dots, G_k , $0 \in G_0$. Consider $k+1$ elements in G , $g_0 = 0, g_1, \dots, g_k$. Define $A \in I$ such that $gA = g_i$, $g \in G_i$, $i = 0, 1, \dots, k-1$; $gA = 0$, $g \in G_k$. Define $B \in T_0(G)$ such that $gB = 0$, $g \in G_i$, $i = 0, 1, \dots, k-1$, $gB = g_k$, $g \in G_k$. Hence $C = A + B \in I$ and has rank $k+1$. Since the sets G_i , $i = 0, 1, \dots, k$, and the elements g_i , $i = 1, 2, \dots, k$ are arbitrary, $I = T_0(G)$ by induction.

LEMMA 5. *Let \mathfrak{G} have infinite cardinality and let $h \in G$, $h \neq 0$. Then there exists a maximal set $A \subset G$ such that $A \cap (A+h) = \emptyset$. Further, $A \cup (A+h) \cup (A-h) = G$. Hence the cardinality of A , $A+h$, and $A-h$ are each equal to the cardinality of G .*

Consider the collection of subsets of G : $\mathfrak{s} = \{S \mid (S+h) \cap S = \emptyset\}$. The collection \mathfrak{s} is not empty since $\{0\} \in \mathfrak{s}$. Define a partial ordering $S_1 > S_2$, if $S_1 \supset S_2$, and $S_1, S_2 \in \mathfrak{s}$. Consider a linearly ordered sub-collection $\{S_t \mid t \in T, S_t \in \mathfrak{s}\}$. Then, it is asserted that $S' = \bigcup_{t \in T} S_t \in \mathfrak{s}$ and $S' > S_t, t \in T$. Trivially, $S' \supset S_t, t \in T$. Suppose $s' = s'' + h, s', s'' \in S'$. But, $s', s'' \in S_t$ for some t , a contradiction. Hence by Zorn's lemma a maximal set A exists.

Let $k \in G, k \notin A, k \notin A + h$. (If no such element k exists, then $G = A \cup (A + h)$ and the sets A and $A + h$ each have the cardinality of G .) The elements $k + h = a \in A$. For if not, consider $A' = \{A, k\}$. Then $A' + h$ is disjoint from A' , contrary to the maximality of A . Therefore $k = a - h \in A - h$. Since $A, A + h, A - h$ have the same cardinality and their union is G , the lemma is proved.

LEMMA 6. *If I contains a transformation of rank d , then I contains every transformation of rank less than or equal to d .*

Let $\{G_x \subset G \mid x \in X\}$ be any partition of G into pairwise disjoint sets, where X is an index set of cardinality d , with $0 \in G_{x_0}$. Consider any collection $\{g'_x \in G \mid x \in X, g'_{x_0} = 0\}$. Let $V \in I$ have rank d and denote the elements in the image GV of V by $\{g_x \mid x \in X, g_{x_0} = 0\}$. For each $g_x \in GV$, let g''_x be an element such that $g''_x V = g_x$. Define $A \in T_0(G)$ such that $gA = g''_x, g \in G_x, x \in X$. Let B be any element in $T_0(G)$ such that $g_x B = g'_x$. Then AVB is an arbitrary transformation of rank less than or equal to d and is in I .

LEMMA 7. *If \mathfrak{G} has infinite cardinality $\mathfrak{T}_0(\mathfrak{G})$ is simple.*

Define the transformation $D_h \in T_0(G)$ by $gD_h = h, g \neq 0, g \in G$. Then by Lemma 3, $D_h \in I$. Define $C \in T_0(G)$ by $gC = g, g \in A; gC = 0, g \notin A$, where A is a maximal set (Lemma 5) such that $A \cap (A + h) = \emptyset$. Then $T = (1 + D_h)C - C \in I$, where 1 is the identity map. Observe that $gT = (g + h)C - gC = -g, g \in A$. Hence T has rank of the same cardinality as G . Thus, by the previous lemma, $I = T_0(G)$. It is only in Lemma 7 that the invariance property of an ideal is used in proving the simplicity of $\mathfrak{T}_0(\mathfrak{G})$.

LEMMA 8. $\mathfrak{T}(\mathfrak{G})$ is simple.

If G has order 2, then the theorem is easily checked directly. Assume therefore that G has order greater than 2. If \mathfrak{J} is a nonzero ideal in $\mathfrak{T}(\mathfrak{G})$, and if there exists a $C \in I \cap T_0(G), C \neq 0$, then $T_0(G) \subset I$ by Lemmas 1, 4, 7. In addition, since an ideal is a left ideal, $Z_g C = Z_g C \in I, g \in G$. Choose $g \in G$ so that $gC \neq 0$. Then, since the smallest near-ring properly containing $\mathfrak{T}_0(\mathfrak{G})$ is $\mathfrak{T}(\mathfrak{G})$, the lemma follows. Finally if the ideal contains no nonzero element of $T_0(G)$, consider $B \neq 0 \in I$ and

$g \in G$ such that $gB = g_1 \neq 0$. Then $Z_g B = Z_{g_1} \in I$. Let $C \in T_0(G)$ such that $g_1 C = 0$ and $(g_2 + g_1)C \neq g_2 C$ for some $g_2 \in G$, $g_2 \neq g_1$, $g_2 \neq 0$. Then $D = (1 + Z_{g_1})C - C \in I$. Further $D \in T_0(G)$ and $g_2 D \neq 0$, contrary to the assumption.

The theorem follows from Lemmas 4, 7, 8.

4. Two-sided invariant sub-near-rings. A sub-near-ring \mathfrak{Q} of a near-ring \mathfrak{B} is *two-sided invariant* if conditions (b) and (b') of §2 hold.

LEMMA 9. *The sets (i) $T_z(G) = \{A \in T(G) \mid R(A) = 1\}$, (ii) $T_f(G) = \{A \in T(G) \mid R(A) < \aleph_0\}$, (iii) $T_{\aleph_k}(G) = \{A \in T(G) \mid R(A) \leq \aleph_k\}$, where \aleph_k is an infinite cardinal number, determine two-sided invariant sub-near-rings of $\mathfrak{T}(\mathfrak{G})$. Further $T_{\aleph_{k_1}}(G) \supsetneq T_{\aleph_{k_2}}(G)$ provided $d \geq \aleph_{k_1} > \aleph_{k_2}$, where d is the cardinality of $T(G)$.*

The proof of this lemma is straight forward and depends on very simple properties of cardinal numbers. The theorem which follows shows that these near-rings determine the two sided invariant sub-near-rings of $\mathfrak{T}(\mathfrak{G})$ and $\mathfrak{T}_0(\mathfrak{G})$.

THEOREM 2. (i) *The two-sided invariant sub-near-rings of $\mathfrak{T}(\mathfrak{G})$ are $\mathfrak{T}_z(\mathfrak{G})$, $\mathfrak{T}_f(\mathfrak{G})$, and $\mathfrak{T}_{\aleph_k}(\mathfrak{G})$ for any infinite cardinal number \aleph_k less than or equal to the cardinality of \mathfrak{G} . (ii) *The two-sided invariant sub-near-rings of $\mathfrak{T}_0(\mathfrak{G})$ are $\{0\}$ and the intersection of the two-sided invariant sub-near-rings of $\mathfrak{T}(\mathfrak{G})$ with $\mathfrak{T}_0(\mathfrak{G})$.**

Let \mathfrak{B} be a two-sided invariant sub-near-ring of $\mathfrak{T}(\mathfrak{G})$ which has an element C of maximal infinite rank \aleph_k . Then, for suitable choices of $A, B \in T(G)$, ACB represents any transformation whose rank is less than or equal to \aleph_k . (See proof of Lemma 6.) Thus $\mathfrak{B} = \mathfrak{T}_{\aleph_k}(\mathfrak{G})$. If P contains no element of infinite rank, suppose P contains an element C of rank greater than 1. Then as above it follows that every element of rank less than or equal to the rank of C is in P . The argument used in the proof of Lemma 4 is now valid to show that $\mathfrak{B} = \mathfrak{T}_f(\mathfrak{G})$. If the rank of every element of P is 1, then $P \subset T_z(G)$ and it is immediate that $\mathfrak{B} = \mathfrak{T}_z(\mathfrak{G})$. The proof of (ii) is similar.

REFERENCES

1. Gerald Berman and Robert J. Silverman, *Near-rings*, Amer. Math. Monthly vol. 66 (1959) pp. 23-34.
2. D. W. Blackett, *Simple and semi-simple near-rings*, Proc. Amer. Math. Soc. vol. 4 (1953) pp. 772-785.
3. L. E. Dickson, *On finite algebras*, Nachr. Akad. Wiss. Göttingen (1905) pp. 358-393.
4. H. Zassenhaus, *Über enliche Fastkörper*, Abh. Math. Sem. Univ. Hamburg. vol. 11 (1936) pp. 187-220.