ON SEMI-GROUPS AND THE GENERAL ISOMORPHISM BETWEEN INFINITE GROUPS*

BY

LEONARD EUGENE DICKSON†

1. When there exists a correspondence between the elements of two finite groups such that the product of two elements of one corresponds to the product of the corresponding elements of the other, then the elements of either which correspond to the identity of the other group form themselves a group. It is somewhat surprising that this familiar theorem fails in general for infinite groups, as shown by definite examples in §§ 7–8. Nevertheless, DE SÉGUIER ‡ has attempted to establish the theorem for any groups; the error § in his argument is quite subtile. The correct theorem involves the concept || *semi-group*, which reduces to a group when there is a finite number of elements, but not in general for an infinitude of elements.

2. Given a function $a \circ b$ of two arguments and a set of elements, we say that the elements form a semi-group with respect to $\circ$ when the following postulates hold:

(1) For every two elements a and b of the set, $a \circ b$ is uniquely determined as an element of the set.

(2) $(a \circ b) \circ c = a \circ (b \circ c)$, in the sense of Transactions, p. 199.

(3) If a, x, x' occur in the set, and if there are equal determinations in the set of $a \circ x$, $a \circ x'$, then $x = x'$.

(4) If there are equal determinations of $x \circ a$, $x' \circ a$, then $x = x'$.

We may replace the triple statement (1) by the three postulates (1_1), (1_2), (1_3) of Transactions, p. 199.

* Presented to the Society (Chicago) December 30, 1904. Received for publication December 9, 1904.

† Research Assistant to the Carnegie Institution of Washington.

‡ *Éléments de la théorie des groupes abstraits* (1904), p. 66. In this text a group is any finite or infinite group unless a limitation is explicitly given. The theorem in question is expressly applied to infinite groups in § 66; cf. top of p. 68.

§ *Ibid.*, p. 66, l. 9: "tous les éléments $\cdots$ répondent d'ailleurs à a_i^{-1}."

|| Otherwise defined by DE SÉGUIER, *ibid.*, p. 8. Cf. the writer's review in the Bulletin of the American Mathematical Society, vol. 11 (1904), pp. 159–164. The postulates (3) and (4) there given by the writer are here replaced by the equivalent but more desirable postulates (3) and (4). The proof of the independence of the new postulates applies as well to the former, whose independence was stated without proof.

Semi-groups fall naturally into three classes, according as

(5_1) The number of elements is a fixed integer n;

(5_2) The elements of the set form an enumerable infinitude;

(5_3) The elements of the set form a non-enumerable infinitude.

To establish the independence of the postulates of the system

$$S_k = (1, 2, 3, 4, 5_k) \qquad (k = 1, 2, \text{or } 3),$$

with $n > 2$ in (5_1), we exhibit, for $j = 1, 2, 3, 4, 5_k$, a set Σ_j of elements and a rule of combination $\circ$ such that the jth postulate fails while the remaining four hold. According as $k = 1, 2$, or 3, we employ as

Σ_1: N, R with 2 omitted, P with 2 omitted, with $a \circ b = a + b$;

Σ_2: C; R, with $a \circ b = a^{-1} \times b^{-1}$; P, with $a \circ b = a^{-1} \times b^{-1}$;

Σ_3: N, R, P, with $a \circ b = a$;

Σ_4: N, R, P, with $a \circ b = b$;

Σ_{5k}: R, P, R, with $a \circ b = a \times b$;

where N is the set of the first n positive integers, R the set of all positive rational numbers, P the set of all positive real numbers; and where C is any group of order n modified by interchanging two rows of its multiplication-table; for example, having the elements $0, 1, \cdots, n-1$, such that for any element b,

$$0 \circ b = (b + 1), \qquad 1 \circ b = b, \qquad a \circ b = (a + b) \text{ if } a > 1,$$

(d) denoting the least positive residue of d modulo n. Then

$$(0 \circ 0) \circ 0 = 1 \circ 0 = 0, \qquad 0 \circ (0 \circ 0) = 0 \circ 1 = 2.$$

A finite semi-group is a group. Indeed, the system* S_1 is precisely the definition of a finite group given by WEBER.† The corresponding definition of a finite commutative group was given earlier by KRONECKER.‡ Every infinite group is a semi-group, but not inversely.

3. THEOREM. *A set of elements belonging to a group and such that the product of any two occurs in the set forms a semi-group.*

---

* Not until I had written out the independence proof for S_1 did I notice that a similar proof had been given by HUNTINGTON at the end of his paper in the Bulletin of the American Mathematical Society, vol. 8 (1902), pp. 296–300.

† Mathematische Annalen, vol. 20 (1882), p. 302; *Lehrbuch der Algebra*, 2d ed., vol. 2, pp. 3–4.

‡ KRONECKER, Berliner Monatsbericht, 1870, pp. 882–883.

Indeed, postulates (1)–(4) hold for the set. For example, the elements $a^{cn}(n=1, 2, \cdots)$ of the infinite cyclic group $\{a, a^{-1}\}$ form a semi-group.

4. THEOREM. *In a semi-group any right-hand identity is a left-hand identity, and conversely; there is at most one identity.*

If i is a right-hand identity, then for every a and b,

$$a \circ (i \circ b) = (a \circ i) \circ b = a \circ b,$$

whence $i \circ b = b$ by (3), so that i is a left-hand identity. The converse follows from $(b \circ i) \circ a = b \circ (i \circ a) = b \circ a$ and (4). Finally, if i and i_1 are identities, $i = i \circ i_1 = i_1$.

5. THEOREM. *In a semi-group containing the identity, any right-hand inverse of a is a left-hand inverse of a, and conversely; there is at most one inverse of a.*

If $a \circ a' = i$, then

$$a \circ (a' \circ a) = (a \circ a') \circ a = i \circ a = a = a \circ i,$$

whence $a' \circ a = i$ by (3). The converse follows similarly from (4).

6. A correspondence between the elements of two sets A and B is called *mutual* when, if a is one of the elements corresponding to b, b is one of the elements corresponding to a. We write $a \sim b$.

Two groups A and B are called *isomorphic* if there exists a mutual correspondence between their elements such that to each element of A corresponds one or more elements of B and to each element of B corresponds one or more elements of A, and such that $a_i a_j \sim b_i b_j$ if $a_i \sim b_i$, $a_j \sim b_j$.

Let A' denote the set of elements of A corresponding to the identity I_B of B, and B' the set of elements of B corresponding to I_A.

If $a_i' \sim I_B$, and $a_j' \sim I_B$, then $a_i' a_j' \sim I_B$. From § 3 follows the

THEOREM. *Each of the sets A' and B' is a semi-group.*

7. As an example in which neither of the semi-groups A' and B' is a group, consider the two infinite cyclic groups

$$A = \{a, a^{-1}\}, \qquad B = \{b, b^{-1}\}. \tag{6}$$

To a^i we make correspond b^{-i+j} $(j = 0, 1, 2, \cdots)$, for every integer i positive, negative, or zero. Then to $a^i a^l$ correspond

$$b^{-(i+l)+r} = b^{-i+j} b^{-l+k} \qquad (r = j + k = 0, 1, 2, \cdots).$$

Moreover for any integer i, it follows that to b^i correspond a^{-i+j} $(j = 0, 1, 2, \cdots)$ and no further elements of A. Thus

$$A' = (I, a, a^2, \cdots), \qquad B' = (I, b, b^2, \cdots),$$

neither being a group. But the correspondence obeys the definition in § 6.

8. As an example in which neither A' nor B' contains the identity, consider groups (6) and the correspondences

$$I_A \sim b^{1+j}, a \sim b^j, a^{2i} \sim b^{-i+j}, a^{2i+1} \sim b^{-i+j}, a^{-i} \sim b^{i+j} \quad (j=0, 1, 2, \cdots),$$

i being any positive integer. Then, inversely,

$$I_B \sim a^{1+j}, b^i \sim a^{-i+j}, b^{-i} \sim a^{2i+j} \qquad (j=0, 1, 2, \ldots),$$

while any element of B corresponds only to the indicated elements of A. The correspondence obeys the definition in § 6.

9. THEOREM. *If one of the semi-groups A' and B' is a group, the other is.*

Suppose that B' is a group. Let a' be any element of A', and let b be one of the elements of B which correspond to a'^{-1}. Since $I_B \sim a'$, then $bI_B \sim a'^{-1}a' = I_A$. Hence b is in B'. Then b^{-1} lies in the group B'. Hence

$$b^{-1} \sim I_A, \; I_B = b^{-1}\, b \sim I_A\, a'^{-1} = a'^{-1},$$

so that a'^{-1} lies in A'. Hence A' is a group.

COROLLARY I. If A' or B' includes only a finite number of elements, A' and B' are groups.

COROLLARY II. If the groups A and B are isormorphic in the usual special sense so that there exists a mutual correspondence between their elements such that to each element of A corresponds an unique element of B and to each element of B corresponds one or more elements of A, and such that $a_i a_j \sim b_i b_j$ if $a_i \sim b_i$, $a_j \sim b_j$, then the elements of A which correspond to the identity of B form a group.

THE UNIVERSITY OF CHICAGO,
November 30, 1904.