DEFINITIONS OF A GROUP AND A FIELD BY INDEPENDENT POSTULATES*

BY

LEONARD EUGENE DICKSON†

Introduction.

1. The simple definition here given for a general abstract group relates as to origin and character to Professor MOORE's two definitions, Transactions, vol. 3 (1902), pp. 485–492. A few days before the appearance of the addition, Transactions, vol. 5 (1904), p. 549, to his paper, Professor MOORE remarked to me that one of his postulates relating to an inverse was redundant, meaning postulate ($3''_r$) of his second definition. I thought the reference was to his first definition and attempted to reconstruct the proof of a redundancy, there absent. This attempt led me to alter his postulate (4_l) to read $aa'_r = i_r$ instead of $a'_l a = i_r$ and to note that postulate (3_l) becomes redundant in the altered set, thus obtaining the present definition. Subsequently I learned that Professor MOORE, in his proof of the redundancy of ($3''_r$) in his second definition, had obtained relations ‡ sufficient to establish the present definition but had not applied them to set up the definition itself.

The present postulates for a general group possess the desirable property that they remain independent within sets of postulates for special classes of groups, the specialization being either in the direction of the number ($n > 1$) of elements or their commutativity (§§ 3–5).

The definition of a field (§ 6), based on the present definition of a group, has evident advantages over the earlier definitions. §

The postulates for a field remain independent under an assumption that the set is finite, or forms an enumerable infinitude, or a non-enumerable infinitude.

* Presented to the Society (Chicago) December 30, 1904, under the title "A definition of a group by independent postulates." Received for publication November 19, 1904. The definition of a field was added January 14, 1905.

† Research Assistant to the Carnegie Institution of Washington.

‡ MOORE, this number of Transactions, p. 179.

§ HUNTINGTON and DICKSON, Transactions, vol. 4 (1903), p. 31, p. 13. For the new definitions by HUNTINGTON, with a bibliography, see this number of Transactions, p. 181.

Definition of a group, §§ 2–5.

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

(1_1) For every two † equal or distinct elements a and b of the set, there is a determination of $a \circ b$.

(1_2) For a and b in the set, there is at most one determination of $a \circ b$.

(1_3) If, for a and b in the set, there is at least one determination of $a \circ b$, one determination is an element of the set.

(2) $(a \circ b) \circ c = a \circ (b \circ c)$ whenever a, b, c, and all the determinations of $a \circ b$, $b \circ c$, $(a \circ b) \circ c$, and $a \circ (b \circ c)$ occur in the set.

(3) There occurs in the set an element i such that, for every element a of the set, $a \circ i$ has the determination a.

(4) If such elements i occur, then for a particular i, and for every ‡ a in the set there occurs in the set an element a' such that $a \circ a'$ has the determination i.

Postulates (1_1), (1_2), (1_3) may be combined into the triple statement:

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

In view of (3) and (4), to any element a there correspond elements a' and a'' such that $a \circ a' = i$, $a' \circ a'' = i$, where i is a fixed element such that $e \circ i = e$ for every element e. Applying also (1) and (2), we have

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

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

Hence $a'' \circ a = i$. By this theorem, $a'' \circ a' = i$. Hence

$$i \circ a = (i \circ i) \circ a = [i \circ (a'' \circ a')] \circ a = (i \circ a'') \circ (a' \circ a) = a \circ i = a.$$

Since $a \circ i = a = i \circ a$ for every a, i is called an identity element. If also i_1 is an identity element, then $i_1 = i_1 \circ i = i$. *Hence there is an unique identity element.* Since $a \circ a' = i = a' \circ a$, a' is called an inverse of a. If also a_1' is an inverse of a, then

$$a_1' = a_1' \circ i = a_1' \circ (a \circ a') = (a_1' \circ a) \circ a' = i \circ a' = a'.$$

Hence there is an unique inverse of each element.

* In (2), (6), and (7), we mean by $A = B$ that one of the determinations of A equals one of the determinations of B.

† The assumption need not be made for $a \circ i$ or $a \circ a'$, in view of (3), (4).

‡ The assumption need not be made for $a = i$, in view of (3).

3. We prove that *the postulates* (1_1), (1_2), (1_3), (2), (3), (4), (5_k), $k = 1, 2$, *or* 3, *are consistent and independent*, where

(5_1) The number of distinct elements is a fixed integer n, $n > 1$;*

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

(5_3) The distinct elements form a non-enumerable infinitude.

Their consistency follows from the existence of the group of the elements $0, 1, \cdots, n-1$ with $a \circ b = a + b (\text{mod } n)$, and the group of all rational (or real) numbers with $a \circ b = a + b$.

Let I_1 be a set containing i and exactly $n - 1$ further elements b; I_2 or I_3 a set containing i and further elements b forming an enumerable or a non-enumerable infinitude, respectively.

To prove the independence of a postulate (j), we exhibit a set $[j]$ in which postulate (j) fails while each of the remaining postulates hold. In the sets, $a \circ b$ is understood to have a unique determination unless the contrary is stated.

$[1_1]$ Set I_k, $i \circ i = i$, $b \circ b = i$, $b \circ i = b$, no determination of $i \circ b$ or of $b \circ b' (b \neq b')$.

$[1_2]$ Set I_k forming a group under $\odot$; $a \circ c$ with the determinations $a \odot c$ and i.

$[1_3]$ Set I_k; $i \circ i = i$, $b \circ i = b$, $b \circ b' = i$, $i \circ b$ not in the set.

$[2]$ Set I_k; $i \circ i = i$, $b \circ i = b$, $b \circ b' = i$, $i \circ b = i$.

$[3]$ Set I_k; $i \circ i = i$, $b \circ i = i$, $b \circ b' = i$, $i \circ b = i$.

$[4]$ Set I_k; $i \circ i = i$, $b \circ i = b$, $i \circ b = b$, $b \circ b' = b_1$, b_1 a fixed b.

4. We next examine the effect of adding the commutative law:

(6) $a \circ b = b \circ a$ whenever a, b, and all the determinations of $a \circ b$ and $b \circ a$ occur in the set.

The postulates (1_1), (1_2), (1_3), (2), (3), (4), (5_k), (6), *for* $k = 0$, 2, *or* 3, *are consistent and independent.* Here the new postulate is

(5_0) The number of distinct elements is finite but undetermined.

The proof follows from the sets $[1_1]$, $[1_2]$, $[1_3]$, $[3]$, $[4]$ above, and

$[2]'$ Set I_k, $n > 2$; $i \circ i = i$, $i \circ b = b \circ i = b$, $b \circ b = i$, $b \circ b' = b_1 (b \neq b')$, Then, for $b \neq b_1$, $(b \circ b_1) \circ b_1 = b_1 \circ b_1 = i$, $b \circ (b_1 \circ b_1) = b \circ i = b$.

$[6]$ There exist finite and infinite non-commutative groups.†

The question of the independence of the postulates for $k = 1$ is answered by § 5 in connection with the sets $[1_1]$, $[1_2]$, $[1_3]$, $[2]'$, $[3]$, $[4]$.

5. THEOREM.‡ *Let* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_v^{\alpha_v}$, *where* $p_1, \cdots, p_v$ *are distinct primes, and each* $\alpha_j > 0$. *The necessary and sufficient conditions that all existing*

* For $n = 1$, the group may be defined by the independent postulates (1_1), (1_2), (1_3); also by the independent postulates (1_2), (3).

† E. g., that of the transformations $x' = \pm x + b$, where b ranges over all integers, or all real numbers, or the residues modulo m, $m > 2$.

‡ Addition of February 2, 1905.

groups of order n shall be abelian are: (i) each $\alpha_j \leqq 2$; (ii) no $p_j^{\alpha_j} - 1$ is divisible by one of the primes $p_1, \cdots, p_v$.

We first prove that the conditions are necessary. If $\alpha_1 > 2$, a non-abelian G_n is given by the direct product of the cyclic groups $C_{p_k^{\alpha_k}}(k = 2, \cdots, v)$ and a non-abelian $G_{p_1^{\alpha_1}}$, say of the type generated by P and Q where

$$P^{p_1^{\alpha_1-1}} = I, \qquad Q^{p_1} = I, \qquad Q^{-1}PQ = P^{1+p_1^{\alpha_1-2}} \qquad (\alpha_1 > 2).$$

If each $\alpha_j \leqq 2$ and $p_1^{\alpha_1} - 1$ is divisible by p_2, there exists a non-abelian group of order $p_1^{\alpha_1}p_2^{\alpha_2}$ and hence, as before, one of order n. Indeed, if $\alpha_1 = \alpha_2 = 1$, we use the group generated by P_1 and P_2 where

$$P_1^{p_1} = I, \qquad P_2^{p_2} = I, \qquad P_2^{-1}P_1P_2 = P_1^{\pi} \qquad [p_1 \equiv 1 \pmod{p_2}],$$

where π is an existing primitive root of $x^{p_2} \equiv 1 \pmod{p_1}$. If $\alpha_1 = 1$, $\alpha_2 = 2$, we use the direct product of the preceding group by a cyclic C_{p_2}. If $\alpha_1 = 2$, $\alpha_2 = 1$, the case in which $p_1 - 1$ is divisible by p_2 is disposed of as before, while for $p_1 + 1$ divisible by p_2, $p_2 > 2$, we use the group* generated by S, T_1, T_2, with

$$T_1^{p_1} = T_2^{p_1} = S^{p_2} = I, \quad T_1T_2 = T_2T_1, \quad S^{-1}T_1S = T_2, \quad S^{-1}T_2S = T_1^{-1}T_2^{b},$$

where b is an (existing) integer such that $x^2 + bx + 1 \equiv 0 \pmod{p_1}$ is irreducible, viz., $b = i + i^{p_1}$, i a mark of the $GF[p_1^2]$ belonging to the exponent p_2. Finally, if $\alpha_1 = \alpha_2 = 2$, we use the direct product of one of the preceding groups by C_{p_2}.

It remains to prove that the conditions (i) and (ii) are sufficient to make every G_n abelian. To proceed by induction, we assume that this statement is true for every $n' = p_1^{\beta_1} \cdots p_v^{\beta_v}$, $\beta_1 \leqq \alpha_1, \cdots, \beta_v \leqq \alpha_v$, $n' < n$. Hence every subgroup of G_n is abelian, so that† either G_n is abelian or else n is divisible by at most two distinct primes. But for $n = p$, $n = p^2$, or $n = p_1^{\alpha_1}p_2^{\alpha_2}$, $0 < \alpha_1 \leqq 2$, $0 < \alpha_2 \leqq 2$, $p_1^{\alpha_1} \not\equiv 1 \pmod{p_2}$, $p_2^{\alpha_2} \not\equiv 1 \pmod{p_1}$, G_n is immediately seen to be abelian. Hence the induction is complete.

Definition of a field, §§ 6–9.

6. We employ a set of elements and two functions $a \oplus b$ and $a \otimes b$. For $\circ = \oplus$, postulate (j) of §§ 2, 4, with $j = 1, 2, 3, 4$, or 6, is designated j^+. An element i satisfying 3^+ is designated i_+. For $\circ = \otimes$, (j) is designated $j^\times$; but $4^\times$ is assumed only for elements a distinct from each i_+. An element i satisfying $3^\times$ is designated $i_\times$. As the distributive law we take‡

*Hölder, Mathematische Annalen, vol. 43 (1893), pp. 345–357. We may use the form by Cole and Glover, American Journal of Mathematics, vol. 15 (1893), pp. 207–8.

† Miller and Moreno, Transactions, vol. 4 (1903), p. 398.

‡ If we alter (7) to read $a \otimes (b \oplus c) = (a \otimes c) \oplus (a \otimes b)$, we deduce 6^+ by taking $a = i_\times$ and applying $6^\times$. Then also (7) follows.

(7) $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ whenever a, b, c, and all the determinations of the functions involved occur in the set.

In view of the theorems in §§ 7, 8, we make the definition:* A set of elements forms a field with respect to $\oplus$ and $\otimes$ if postulates 1^+, 2^+, 3^+, 4^+, $1^\times$, $2^\times$, $3^\times$, $4^\times$, $6^\times$, and 7 hold.

7. THEOREM.† *From* 1^+, 2^+, 3^+, 4^+, $1^\times$, $3^\times$, $6^\times$, 7, *follows* 6^+.

We substitute $\beta \oplus \gamma$ for a in (7), apply 1^+, $1^\times$, $6^\times$, 7 and get

$$(\beta \oplus \gamma) \otimes (b \oplus c) = [(b \otimes \beta) \oplus (b \otimes \gamma)] \oplus [(c \otimes \beta) \oplus (c \otimes \gamma)],$$

for every β, γ, b, c in the set. Interchanging b with β, c with γ, and noting that the first member is unaltered in view of $6^\times$, we get by $6^\times$ and 2^+,

$$(b \otimes \beta) \oplus (c \otimes \beta) \oplus (b \otimes \gamma) \oplus (c \otimes \gamma) = (b \otimes \beta) \oplus (b \otimes \gamma) \oplus (c \otimes \beta) \oplus (c \otimes \gamma),$$

Since 1^+, 2^+, 3^+, 4^+ imply an inverse under $\oplus$, we get

$$(c \otimes \beta) \oplus (b \otimes \gamma) = (b \otimes \gamma) \oplus (c \otimes \beta).$$

Taking $\beta = \gamma = i_\times$, we get $c \oplus b = b \oplus c$.

8. THEOREM. *Let* i_+ *be chosen so that* 4^+, *as well as* 3^+, *is satisfied. Then* $a \otimes i_+ = i_+ \otimes a = i_+$ *for every element* a. *If* $a \otimes b = i_+$ *and* $b \neq i_+$, *then* $a = i_+$. *Hence* i_+ *has the ordinary properties of zero under* $\oplus$ *and* $\otimes$.

By 7 for $b = c = i_+$, $e = e \oplus e$, where $e = a \otimes i_+$. Hence (§ 2), $a \otimes i_+ = i_+$ for every a. By $1^\times$, $6^\times$, $i_+ \otimes a = i_+$.

By $2^\times$, from $a \otimes b = i_+$ follows $i_+ = a \otimes (b \otimes c)$ for every c. Let $i_\times$ be chosen so that $4^\times$, as well as $3^\times$, holds. Taking c such that $b \otimes c = i_\times$, we get $i_+ = a \otimes i_\times = a$.

9. THEOREM. *Postulates* 1^+, 2^+, 3^+, 4^+, $1^\times$, $2^\times$, $3^\times$, $4^\times$, $6^\times$, 7, 5_k $(k = 0$, 2, *or* $3)$ *are independent.*

For $k = 0$, i. e., for a finite number of elements, we employ the sets:

[1^+] Elements $0, 1, -1$; $a \oplus b = a + b$, $a \otimes b = a \times b$.

[2^+] $0, 1, -1$; $0 \oplus a = a \oplus 0 = a$, $a \oplus b = 0 (a \neq 0, b \neq 0)$, $\otimes = \times$.

[3^+] $0, 1, \cdots, n-1 (n > 1)$; $a \oplus b = b$, $a \otimes b = a + b (\mathrm{mod}\ n)$.

* If the set is finite, we may omit 3^+ and insert 6^+. Then if 3^+ fails, all the elements form a group with respect to $\otimes$. It cannot contain an element a of period α, $\alpha > 1$. Indeed, if we set $y = i_\times \oplus a \oplus a^2 \oplus \cdots \oplus a^{\alpha-1}$, we get $a \otimes y = y$, whence $a = i_\times$. The single element in the set necessarily satisfies 3^+.

† Some months after devising this proof I learned that a similar proof had been given by HILBERT, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 8 (1899-1900), p. 183. But earlier writers have noted the essential point in the proof; viz., that the uniqueness of the expansion of $(\beta + \gamma)(b + c)$ depends upon the validity of the commutative law for addition.

$[4^+]$

$\oplus$	0	1
0	0	1
1	1	1

$\otimes$	0	1
0	0	0
1	0	1

$[1^\times]$ $0, 1$; $a \oplus b = a + b \pmod 2$, $0 \otimes a = 0$, $1 \otimes 1 = 1$, $1 \otimes 0$ not in the set.

$[2^+]$ Eight * elements (ξ, η, ζ), ξ, η, ζ taken modulo 2;

$$(\xi, \eta, \zeta) \oplus (x, y, z) = (\xi + x, \eta + y, \zeta + z),$$

$$(\xi, \eta, \zeta) \otimes (x, y, z) = (z\xi + x\zeta, (x + y)\xi + (x + z)\eta + y\zeta, y\xi + x\eta + z\zeta).$$

The latter equals $i_\times = (0, 0, 1)$ if $D \equiv \xi + \zeta + \xi\zeta \not\equiv 0 \pmod 2$ and

$$x \equiv \xi(1 + \zeta)/D, \; y \equiv (\xi + \xi\eta + \eta\zeta)/D, \; z \equiv \zeta(1 + \xi)/D.$$

But $D \equiv 0$ only when $\xi \equiv \zeta \equiv 0$; while if $\xi \equiv \zeta \equiv 0$, $\eta \equiv 1$, we have

$$(0, 1, 0) \otimes (x, y, z) = (0, x + z, x) = i_\times \text{ if } x \equiv z \equiv 1.$$

Finally, $2^\times$ fails for $a = (0, 1, 0)$, $b = (0, 1, 0)$, $c = (1, 1, 1)$.

$[3^\times]$ $0, 1$; $a \oplus b = a + b \pmod 2$, $a \otimes b = 0$.

$[4^\times]$ $0, 1, \cdots, n - 1$, n composite; $a \oplus b = a + b \pmod n$, $a \otimes b = a \times b \pmod n$

$[6^\times]$ Nine elements $a + bj$, $a, b \equiv 0, 1, -1 \pmod 3$;

$$(a + bj) \oplus (c + dj) = a + c + (b + d)j,$$

$$(a + bj) \otimes (c + dj) = ac - (-1)^{ab} bd + \{bc + (-1)^{ab} ad\} j,$$

where the exponent ab is taken in the form $0, 1$, or -1. Then $j \otimes j = -1$,

$$j \otimes (1 + j) = -1 + j, \qquad (1 + j) \otimes j = 1 - j,$$

so that $6^\times$ and the right-hand distributive law fail. For $4^\times$,

$$(a + bj) \otimes \left(\frac{a - (-1)^{ab} bj}{a^2 + b^2} \right) = 1 = i_\times,$$

since $a^2 + b \equiv 0$ only when $a \equiv b \equiv 0 \pmod 3$. Computation shows that $2^\times$ holds.

$[7]$ Any finite group of order > 1; $a \oplus b = a \otimes b = a \circ b$.

$[5_0]$ All rational numbers; $\oplus = +$, $\otimes = \times$.

* A much simpler statement of Σ_7, Transactions, vol. 4 (1903), p. 20.

For $k=2\,(k=3)$, *i. e.*, for an enumerable (a non-enumerable) infinitude of elements, we employ the following sets $[j]$, R denoting the set of all rational (real) numbers, R_+ that of all positive rational (positive real) numbers:

$[1^+]$ R; $\otimes = \times$, $a \oplus 0 = 0 \oplus a = a$, $a \oplus a = 0$, $a \oplus b$ not in R if $a \neq b$, $a \neq 0$ or $b \neq 0$.

$[2^+]$ R; $\otimes = \times$, $a \oplus a = 0$, $a \oplus b = a + b\,(a \neq b)$.

$[3^+]$ R_+; $\oplus = +$, $\otimes = \times$.

$[4^+]$ R_+ and zero; $\oplus = +$, $\otimes = \times$.

$[1^\times]$ R; $\oplus \equiv +$, $a \otimes b = ab$ (if $a=1$, $b=1$, or $ab=1$), otherwise $a \otimes b$ not in R.

$[2^\times]$ Hypercomplex numbers $\alpha + \beta i + \gamma j$, α, β, γ arbitrary in R;

$\otimes$	1	i	j
1	1	i	j
i	i	-1	1
j	j	1	-2

Then $(ii)j = -j$, $i(ij) = i$; $(\alpha + \beta i + \gamma j)(x + yi + zj) = 1$ if

$$x = \alpha/\Delta, \quad y = -\beta/\Delta, \quad z = -\gamma/\Delta, \quad \Delta = \alpha^2 + \gamma^2 + (\beta - \gamma)^2.$$

$[3^\times]$ R; $a \oplus b = a + b$, $a \otimes b = 0$.

$[4^\times]$ Positive and negative integers and zero; $\oplus = +$, $\otimes = \times$. (All $a_1e_1 + a_2e_2$ with a_1 and a_2 real, $e_1^2 = 0$, $e_1e_2 = e_2e_1 = e_1$, $e_2^2 = e_2$; $\oplus = +$, $\otimes = \times$; then $e_1 \otimes y = i_\times = e_2$ is impossible since $e_1(y_1e_1 + y_2e_2) = y_2e_1$.)

$[6^\times]$ All quaternions $ai + bj + ck + d$, a, b, c, d in R; $\oplus = +$, $\otimes = \times$

$[7]$ R_+; $\oplus = \otimes = \times$.

$[5_k$, $k = 2$ or $3]$ Any finite field, *e. g.*, the classes of residues modulo p.

THE UNIVERSITY OF CHICAGO.