

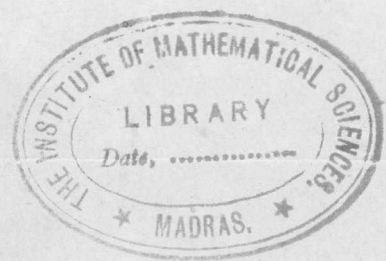
19

MATSCIENCE REPORT 19

FUNCTIONAL ANALYSIS

MARSHALL H. STONE

First Ramanujan visiting professor (1963)  
at Matscience



THE INSTITUTE OF MATHEMATICAL SCIENCES, MADRAS-4, INDIA.

THE INSTITUTE OF MATHEMATICAL SCIENCES

MADRAS - 4 (India)

Lectures on  
PRELIMINARIES TO FUNCTIONAL ANALYSIS

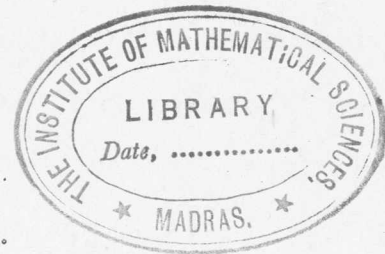
by

Prof. Marshall H. Stone,\*

First Ramanujan Visiting Professor, MATSCIENCE,  
Madras.

Notes by

B. Ramachandran .



---

\* Distinguished Service Professor of Mathematics,  
University of Chicago, Chicago, U.S.A.

## CHAPTER 1.

### SEMI-METRIC AND METRIC SPACES

#### 1. Introduction:-

Semi-metric and metric spaces are obtained by imposing, on the basic set we deal with, a 'distance function' having the properties of Euclidean distance. Thus, let  $X$  be our basic set; suppose that to every pair of points  $x, y \in X$ , there corresponds a real number  $d(x, y)$  such that ( $x, y, z$  are elements of  $X$ ) :

$$(i) \quad d(x, x) = 0$$

$$(ii) \quad d(x, y) \geq 0$$

$$(iii) \quad d(x, y) = d(y, x)$$

$$\text{and} \quad (iv) \quad d(x, z) \leq d(x, y) + d(z, y)$$

The last requirement is the familiar triangle inequality (the sum of two sides of a triangle is not less than the third), while the others have even more obvious interpretations.

We now find that the above set of requirements is equivalent to a subset of itself, namely, just (i) and (iv) taken together. On setting  $x = y$  in (iv), we obtain  $d(y, z) \leq d(z, y)$  ; the reverse inequality is obtained by interchanging  $y$  and  $z$  ; thus we have (iii). We then obtain (ii) by taking  $z = y$  in (iv) and using (i) and (iii). This fact makes it easier for us to verify in a given situation whether the pair  $(X, d)$ , where  $d$  is a real-valued function defined for every pair  $(x, y)$  of points of  $X$ , is indeed a semi-metric or metric space in the sense of the following.

Definition: A space  $(X, d)$  is a semi-metric space if  $d$  satisfies conditions (i) and (iv) above; if, further,  $d$  has the property

$$(v) \quad d(x, y) = 0 \Rightarrow x = y,$$

then  $(X, d)$  is a metric space.

For exhibiting the connection between semi-metric and metric spaces, we shall require the concepts and result that follow, which find application in a wide variety of mathematical problems.

2. Equivalence classes and partitions; conversion of a semi-metric space into a metric space:

Let  $S$  be any set, and let a relation  $\equiv$  between members of  $S$  have the following properties:

(i)  $x \equiv x$  (reflexivity)

(ii)  $x \equiv y \Rightarrow y \equiv x$  (symmetry)

(iii)  $x \equiv y, y \equiv z \Rightarrow x \equiv z$  (transitivity).

Then,  $\equiv$  is called an equivalence relation, and if  $x \equiv y$  we say that  $x$  and  $y$  are equivalent (to each other).

Defining a partition of  $S$  as a collection of (pair-wise) disjoint subsets of  $S$  whose set-union is  $S$ , we have the

Theorem: Every equivalence relation sets up a partition, and conversely.

Proof: Let  $\equiv$  be an equivalence relation. Then, for  $x \in S$ , let  $S_x$  be the set of all  $y$  such that  $y \equiv x$ . It is easy to verify that, for any pair  $x, y \in S$ ,  $S_x$  and  $S_y$  are either identical or disjoint (in other words, if one point of  $S_x$

belongs to  $S_y$ , then  $S_x = S_y$ ). The distinct sets  $S_x, x \in S$ , constitute a partition of  $S$ : we call them the equivalence classes (corresponding to this particular equivalence relation). The elements of  $S$  belonging to the same equivalence class are equivalent to one another; and any two elements taken one each from any two distinct equivalence classes are non-equivalent.

Conversely, given any partition of  $S$ , let us write  $x \equiv y$  if  $x$  and  $y$  are in the same subset of the partition. Then,  $\equiv$  is easily verified to be an equivalence relation. The theorem is proved.

Let now  $(X, d)$  be a semi-metric space. Let us write  $y \equiv x$  if  $d(x, y) = 0$ . Then,  $\equiv$  is an equivalence relation. Denote the set of equivalence classes by  $\bar{X}$ , and the class corresponding to an element  $x$  (the class  $S_x$  above) by  $\bar{x}$ . Then we remark that  $\bar{x}_1 = \bar{x}_2, \bar{y}_1 = \bar{y}_2 \Rightarrow d(x_1, y_1) = d(x_2, y_2)$ ; for  $d(x_1, y_1) \leq d(x_1, x_2) + d(x_2, y_1) \leq d(x_1, x_2) + d(x_2, y_2) + d(y_2, y_1) = d(x_1, y_2)$  and, to obtain the reverse inequality, we have only to interchange the subscripts 1 and 2. Hence, the following definition of  $\bar{d}$  is unambiguous.

$$\bar{d}(\bar{x}, \bar{y}) = d(x, y).$$

It is now easy to verify that  $(\bar{X}, \bar{d})$  is a metric space. Thus, we have "converted" an arbitrary semi-metric space into a metric space, the elements of the latter being the members of a suitably chosen partition of the former.

3. Examples:

1) The most familiar examples of metric spaces are the Euclidean spaces with the usual distance function. If we take the Euclidean plane and define the distance between two elements  $(x_1, y_1)$  and  $(x_2, y_2)$  as  $\max \{ |x_1 - x_2|, |y_1 - y_2| \}$  or as  $|x_1 - x_2|$ , we obtain a semi-metric space in each case.

2) A more sophisticated example, of great interest and importance, is the following: Let  $T$  be an arbitrary set. Consider the set  $X$  of all bounded real-valued (or of all bounded complex-valued) functions  $x$  on  $T$ ; if  $x, y$  be any two such functions, define

$$d(x, y) = \sup_{t \in T} |x(t) - y(t)|.$$

Then  $(X, d)$  is a metric space.

Proof: Clearly,  $d(x, x) = 0$ . If  $d(x, y) = 0$ , then  $x(t) - y(t) = 0$  for every  $t$ , i.e.,  $x = y$ . Finally,

$$|x(t) - z(t)| \leq |x(t) - y(t)| + |z(t) - y(t)|$$

$$\leq \sup |x(t) - y(t)| + \sup |z(t) - y(t)|$$

for every  $t$

$$\Rightarrow \sup |x(t) - z(t)| \leq \sup |x(t) - y(t)| + \sup |z(t) - y(t)|.$$

3) More generally, let  $(X_t, d_t)$  be a metric space for every  $t \in T$ . Consider the set  $X$  of all mappings  $x$  from  $T$  to  $\bigcup_t X_t$  such that  $x_t = x(t) \in X_t$ .

Let us define, for any pair  $x, y \in X$ ,

$$d(x, y) = \sup_{t \in T} d_t(x_t, y_t);$$

where, to avoid the value  $\cdot \infty$  for  $d$ , we assume that  $d(x, x_0) < \infty$  for some fixed  $x_0 \in X$  and for all  $x \in X$ . [Note that, in Ex. 2, every  $(X_t, d_t)$  is the real line with the usual distance, and the zero function plays there the role of the present  $x_0$ .] Then  $(X, d)$  is a metric space, the proof running along lines parallel to those in Ex. 2.

4) Instead of considering functions  $x$  on  $T$  with  $\sup |x(t)| < \infty$  as in Ex. 2, we may consider measurable functions  $x$  on  $T$  such that  $\int |x(t)| dt < \infty$ . If on the set  $X$  of such functions, we define a distance function  $d(x, y) = \int |x(t) - y(t)| dt$ , then  $(X, d)$  is a semi-metric space, In general, it is not already a metric space, since the integral of a non-negative function can be zero without the function being necessarily identically zero.

5) In Ex. 4, we may even replace the integral by an "upper integral". Suppose, for any complex-valued function  $x(t)$ , not necessarily measurable, we define

$$\overline{\int} |x(t)| dt = \inf \left\{ \int \phi(t) dt \mid \phi \text{ is measurable and } \phi(t) \geq |x(t)| \right\}.$$

It follows at once from the definition that if  $|x(t)| \leq |y(t)|$  for (almost) all  $t$ , then  $\overline{\int} |x(t)| dt \leq \overline{\int} |y(t)| dt$  : we shall refer to this property as the monotonicity-property of  $\overline{\int}$ .

In general, the additivity property of the integral is not possessed by  $\overline{\int}$ . It is also clear that if  $|X|$  is measurable, then  $\overline{\int |X|} = \int |X|$ .

Now consider the set  $X$  of all real-valued (or of all complex-valued) functions  $x$  on  $T$  such that  $\overline{\int |x(t)| dt} < \infty$ . Let, for  $x, y \in X$ ,  $d(x, y) = \overline{\int |x(t) - y(t)| dt}$ . Then  $(X, d)$  is a semi-metric space.

Proof: Since the zero-function is measurable,  $\overline{\int 0} = \int 0 = 0$ , and so  $d(x, x) = 0$ .

If  $x_1, x_2$  be any two elements of  $X$ , then, corresponding to any  $\epsilon > 0$ , there exist measurable functions  $\phi_1, \phi_2$  such that  $\phi_j \geq |x_j|$  and  $\overline{\int |x_j|} \geq \int \phi_j - \frac{\epsilon}{2}$ , for  $j = 1, 2$ . Hence,  $\overline{\int |x_1|} + \overline{\int |x_2|} \geq \int (\phi_1 + \phi_2) - \epsilon \geq \overline{\int |x_1 + x_2|} - \epsilon$ , since  $\phi_1 + \phi_2 \geq |x_1| + |x_2| \geq |x_1 + x_2|$ . Since  $\epsilon > 0$  is arbitrary, it follows that

$$\overline{\int |x_1|} + \overline{\int |x_2|} \geq \overline{\int |x_1 + x_2|} \quad (**)$$

The triangle inequality follows at once from this on setting  $x_1 = x - y$ ,  $x_2 = y - z$ .

6) We may generalize the situation in Ex. 5 in the same way as Ex. 2 was generalized to Ex. 3. Let  $(X_t, d_t)$  be a (semi-) metric space for every  $t \in T$ . Consider the set  $X$  of all mappings  $x$  from  $T$  to  $\cup X_t$  such that  $x_t = x(t) \in X_t$ , satisfying

$$\overline{\int d_t(x_t, x_t^0)} dt < \infty$$

for some fixed  $x^0$ . It is clear that  $x^0$  itself belongs to  $X$ .



If we define, for  $x, y \in X$ ,  $d(x, y) = \int d_t(x_t, y_t) dt$ , then  $(X, d)$  is a semi-metric space. (In general, it is not a metric space even if every  $(X_t, d_t)$  is.)

Proof: Since  $d_t(x_t, x_t) = 0$  for every  $t$ , and the zero-function is measurable, it follows that  $d(x, x) = 0$ .

Also, for  $x, y, z \in X$ ,

$$d(x, z) = \int d_t(x_t, z_t) dt \leq \int [d_t(x_t, y_t) + d_t(z_t, y_t)] dt$$

by virtue of the triangle-inequality for each  $d_t$  and the monotonicity-property of  $\int$ ; by (\*\*\*) above, the last expression

$$\leq \int d_t(x_t, y_t) dt + \int d_t(z_t, y_t) dt = d(x, y) + d(z, y).$$

#### 4. Comparison of two metric spaces: Congruences:

A mapping from one metric space  $(X, d)$  to another  $(X', d')$  is called a congruence if it is onto and distance-preserving. It follows that the mapping is also one-one; if two elements  $x, y \in X$  have the same image (i.e.)  $x' = y'$ , then  $d(x, y) = d'(x', y') = 0 \Rightarrow x = y$ . Hence every congruence has an inverse, which is itself a congruence, as is easily verified.

It follows, in particular, that the self-congruences of any given metric space form a group under the usual composition operation. It is, however, not an easy task to determine this group for an arbitrary metric space; in the Euclidean case, linear transformations, i.e. translations, rotations and their combinations, constitute examples of self-congruences.

The following congruence of an arbitrary metric space is of especial interest and importance. Let  $(X, d)$  be any metric space; let  $T \equiv X$ , and, for every  $x \in X$ , define a mapping  $f_x$  from  $T$  into the real number system according to

$$f_x(t) = d(t, x) - d(t, x_0)$$

where  $x_0$  is a fixed element of  $X$ .  $f_x$  is (a continuous function of  $t$ , as we shall see in chapter 3, and is) bounded by  $d(x, x_0)$  on account of the triangle inequality. Let  $F = \{ f_x : x \in X \}$ . For any pair  $f_x, f_y \in F$ , define

$$D(f_x, f_y) = \sup_t | f_x(t) - f_y(t) | = \sup_t | d(x, t) - d(y, t) |$$

Since  $| d(x, t) - d(y, t) | \leq d(x, y)$  by the triangle inequality and attains this value for  $t = x$  (or  $y$ ), it follows that  $D(f_x, f_y) = d(x, y)$ . This immediately implies that  $(F, D)$  is a metric space (a fact which follows directly from the definition of  $D$  also), and that  $x \rightarrow f_x$  is a congruence mapping.

Thus, an arbitrary metric space  $(X, d)$  is congruent to a subset of the set of all bounded real-valued functions defined on  $X$ , with the distance function defined in Ex. 2 of § 3.

This example can be refined to cover general topological spaces, leading to a relation between metric spaces and 'compact' topological spaces.

Chapter 2.

METRIC TOPOLOGY AND COMPLETION OF METRIC SPACES

1. Open and closed sets, closure of a set:

Let  $(X, d)$  be a metric space. We call the set  $\{x : d(x, x_0) < r\}$  an open spherical neighborhood of  $x_0$  of radius  $r$ , and denote it by  $S_o(x_0, r)$  -- the subscript of  $S$  standing for 'open'.

Let  $\{x_n\}$  be a sequence of points in  $X$ . We say that  $x$  is a limit of the sequence  $\{x_n\}$  if, given any open spherical neighbourhood of  $x$ ,  $x_n$  belongs to it for all sufficiently large  $n$ . This is obviously equivalent to the requirement that  $d(x_n, x) \rightarrow 0$  as  $n \rightarrow \infty$ . It follows that a limit, if it exists, is unique; for, if  $x$  and  $x'$  are both limits, then  $d(x, x') \leq d(x, x_n) + d(x_n, x') \rightarrow 0$  as  $n \rightarrow \infty$ , so that  $d(x, x') = 0$  or  $x = x'$ .

A subset  $Y$  of  $X$  is said to be open if it is the union of open spheres. In particular, every 'open' sphere is open in this sense.

Theorem 1  $Y$  is open iff every point of  $Y$  has an open spherical neighbourhood  $\subset Y$ .

Proof: If  $Y$  is open, then  $y \in Y \Rightarrow y \in$  some open sphere  $S_o(x_0, r) \subset Y$ . Let  $r' = r - d(x_0, y)$ . Then  $r' > 0$ , and  $S_o(y, r') \subset S_o(x_0, r) \subset Y$ ; for, if  $x \in S_o(y, r')$ , then  $d(x, x_0) \leq d(x, y) + d(y, x_0) < r' + d(y, x_0) = r$ .

Conversely, if every point of  $Y$  has an open spherical neighbourhood contained in  $Y$ , then  $Y$  is just the union of <sup>these</sup> all/open spheres.

A set of the form  $\{x : d(x, x_0) \leq r\}$  is called the closed spherical neighborhood of  $x_0$  of radius  $r$ , and is denoted by  $S_c(x_0, r)$

We introduce the notion of closed sets as complementary to that of open sets in the set-theoretic sense: thus, a set  $Z$  is closed iff its complement  $CZ = X - Z$  is open.

Theorem 2 Every 'closed' sphere is closed (in this sense):

Thus, the difference between sets  $S_o$  and  $S_c$ , apparently due to the absence and presence respectively of the sign of equality in their definitions, is in fact a "topological" difference.

Proof: Let  $y \in Y = C S_c(x, r)$ . Then  $d(x, y) > r$ . If  $r' = d(x, y) - r$ , then  $r' > 0$  and the open sphere  $S_o(y, r')$  is disjoint from  $S_c(x, r)$ ; for, if  $z$  were to belong to both, we have  $d(y, z) < r'$  and  $d(x, z) \leq r$ , so that

$$d(x, y) \leq d(x, z) + d(y, z) < r + r' = d(x, y),$$

a contradiction. Hence every point of  $Y$  has an open spherical neighbourhood  $\subset Y$ , i.e.,  $Y$  is open, by theorem 1.

Theorem 3 (Properties of open sets):

(i) The whole space  $X$  and the empty set  $\phi$  are open.

(ii) An arbitrary union of open sets is open.

(iii) The intersection of two (and so of any finite number of) open sets is open.

Proof: (i)  $X$  is the union of all the open spheres.  $\phi$  contains no points, the "if" condition of Theorem 1 cannot be satisfied, and so  $\phi$  is open.

(ii) The union of unions of open spheres is itself a union of open spheres.

(iii) If  $A_1$  and  $A_2$  are two open sets and  $x \in A_1 \cap A_2$  then  $S_0(x, r_j) \subset A_j$  for some  $r_j > 0$  ( $j = 1, 2$ ), and so, if  $r = \min(r_1, r_2)$ , then  $r > 0$  and  $x \in S_0(x, r) \subset A_1 \cap A_2$ . Hence, by Theorem 1,  $A_1 \cap A_2$  is open.

Note: In general, even a denumerable intersection of open sets need not be open: for example, consider the sequence

$(-\frac{1}{n}, \frac{1}{n})$  of open subsets of the real line.

By set-complementation, we obtain the dual of the above theorem, namely,

Theorem 4 (Properties of closed sets):

(i) The whole space  $X$  and the empty set  $\phi$  are closed.

(ii) An arbitrary intersection of closed sets is closed.

(iii) The union of two (and so of any finite number of) closed sets is closed. Again we note that even a countable union of closed sets need not be closed.

Remark: In considering the implications of the concepts of 'open' and 'closed' sets, it is useful to have the Euclidean picture always in mind.

Let  $Z$  be any subset of  $X$ . By Theorem 4 (ii), the intersection of all the closed sets containing  $Z$  (there exists at least one such set, namely  $X$  itself) is closed. We call this set the closure of  $Z$  and denote it by  $\bar{Z}$ . It is clear that  $\bar{Z} \supset Z$  and is the 'smallest' closed set containing

$Z$  . It is also immediate that if  $Y \subset Z$ , then  $\overline{Y} \subset \overline{Z}$ .

We now discuss two other interpretations of  $\overline{Z}$ , namely, as the set  $aZ$  of all "accumulation points" of  $Z$ , and as the set  $sZ$  of all "sequential limit-points" of  $Z$ .

A point  $x \in X$  is an accumulation-point of  $Z$  iff, for every  $\nu > 0$ ,  $S_0(x, \nu)$  has a non-empty intersection with  $Z$ . It follows at once that every point of  $Z$  is an accumulation-point of  $Z$ , i.e.,  $Z \subset aZ$ . Indeed, we have

Theorem 5:  $aZ = \overline{Z}$ . Pf: : If  $x \in \overline{Z}$  and if, for some  $\nu > 0$ ,  $S_0(x, \nu) \cap Z = \phi$ , then  $Z \subset C[S_0(x, \nu)]$ , a closed set, so that  $\overline{Z} \subset C[S_0(x, \nu)]$ . Hence  $x \in C[S_0(x, \nu)]$ , which is impossible. Hence  $S_0(x, \nu) \cap Z \neq \phi$  for any  $\nu > 0$ , i.e.,  $x \in aZ$ , so that  $\overline{Z} \subset aZ$ .

Conversely, let  $x \notin \overline{Z}$ . Then  $C\overline{Z}$  being open, there exists a sphere  $S_0(x, \nu)$  such that  $S_0(x, \nu) \subset C\overline{Z}$ . But  $C\overline{Z} \subset CZ$ , so that  $S_0(x, \nu) \cap Z = \phi$ . This means that  $x \notin aZ$ , so that  $\overline{Z} \supset aZ$ . Hence the theorem.

A point  $x \in X$  is called a sequential limit-point of  $Z$  if it is the limit of a sequence of points in  $Z$ . We then have

Theorem 6:  $sZ = \overline{Z}$

By theorem 5, it suffices to show that  $sZ = aZ$ . Let  $x = \lim z_n$ , where every  $z_n \in Z$ . Then every open spherical neighbourhood of  $x$  contains a point  $z_n$  for some  $n$ , by definition of limit, so that it follows that  $x \in aZ$ , i.e.,  $sZ \subset aZ$ .

To prove the converse relation, we require the Zermelo Axiom of choice: Given any collection of non-empty sets, we can select one element from each of these sets; in other words, a function  $f$  can be defined on a collection of non-empty sets,  $\{S_t : t \in T, \text{ an index set}\}$  such that, for each  $t \in T$ ,  $f(S_t) \in S_t$ . (While the legitimacy of such an assumption in our logical apparatus has been questioned in some quarters, the axiom of choice plays a crucial role in many developments in modern mathematics.)

Let now  $x \in a \mathbb{Z}$ . Then every one of the sets  $S_0(x, \frac{1}{n}) \cap \mathbb{Z}$  is non-empty, and, by the axiom of choice, we can pick a sequence  $\{x_n\}$  of elements of  $X$  such that  $x_n \in S_0(x, \frac{1}{n}) \cap \mathbb{Z}$ . It is clear that  $x = \lim x_n$ , i.e., a sequential limit-point of  $\mathbb{Z}$ . Hence  $a \mathbb{Z} \subset s \mathbb{Z}$ , and the theorem is proved.

2. Completeness: For historical reasons, a sequence  $\{x_n\}$  of points in  $(X, d)$  is said to be a Cauchy-sequence if  $d(x_m, x_n) \rightarrow 0$  as  $m, n \rightarrow \infty$ . While every sequence with a limit is a Cauchy-sequence (if  $x = \lim x_n$ , then  $d(x_m, x_n) \leq d(x_m, x) + d(x_n, x) \rightarrow 0$  as  $m, n \rightarrow \infty$ ), it is not necessarily true that every Cauchy-sequence converges to a limit. The set of rational numbers, with the usual distance function, is a metric space in which not every Cauchy-sequence has a limit (take, for example, a sequence of rationals converging to  $\sqrt{2}$ ). Thus we are led to the

Definition: A metric space  $(X, d)$  in which every Cauchy-sequence has a limit is said to be complete.

We now proceed to show that any metric space can be 'completed', that is, embedded, in a certain sense, in a complete metric space. For this purpose, we require the following definition and lemma.

Definition:  $Y \subset X$  is said to be dense in  $X$  if  $\bar{Y} = X$ .

Lemma: Every closed subset of a complete metric space is complete.

Proof: If  $Y$  is closed, and  $\{y_n\}$  is a Cauchy-sequence of elements in  $Y$ , then  $\{y_n\}$  has a limit  $y$  in  $X$ . But, since  $Y = \bar{Y} = \bar{Y}$ , it follows that  $y \in Y$  (i.e.)  $(Y, d)$  is complete.

Theorem 7: Every metric space  $(X, d)$  can be 'completed' in the sense that there exists a congruence map of  $(X, d)$  onto a dense subset of a complete metric space.

Proof: We have seen (Chapter 1, § 3, Ex. 2) that the set  $\mathcal{F}$  of all bounded real-valued functions  $f$  on a set  $X$  constitute a metric space under the distance function

$$D(f, g) = \sup_{x \in X} |f(x) - g(x)|, \quad f, g \in \mathcal{F}.$$

This metric space is, further-more, complete: If  $\{f_n\}$  be a Cauchy-sequence in  $\mathcal{F}$ , then

$$D(f_m, f_n) = \sup_{x \in X} |f_m(x) - f_n(x)| \rightarrow 0 \text{ as } m, n \rightarrow \infty \quad (*)$$

This implies that, for every  $x \in X$ ,  $|f_m(x) - f_n(x)| \rightarrow 0$  as  $m, n \rightarrow \infty$ , so that, by the completeness of the real number system, there exists a real number  $f(x)$  for every  $x$  such that  $f(x) = \lim_{n \rightarrow \infty} f_n(x)$ . We now assert that  $f$ , as a function



of  $X$ , is also bounded: on account of  $(*)$ , there exists an integer  $N$  such that for  $m, n \geq N$ ,  $\sup_x |f_m(x) - f_n(x)| < \frac{1}{2}$ , so that  $|f_m(x) - f_n(x)| < \frac{1}{2}$  for all  $x \in X$ . Setting  $n = N$  and letting  $m \rightarrow \infty$  in this relation, we have, since  $\lim f_n(x) = f(x)$ , that  $|f(x) - f_N(x)| \leq \frac{1}{2}$ . Also  $f_N$  is bounded, so that we have

$$|f(x)| \leq |f(x) - f_N(x)| + |f_N(x)| \leq \frac{1}{2} + \sup_x |f_N(x)| < \infty.$$

Now, we have seen that  $(X, d)$  has a congruence-mapping onto a subset  $F$  of the set of all bounded, (continuous) real-valued functions with the same distance function as  $D$  above (Chapter 1, § 4). But  $(F, D)$  is a subspace of the metric space  $(\mathcal{F}, D)$  above which is complete. By the lemma above,  $(\bar{F}, D)$  is also complete. Thus we have a complete metric space of which  $(F, D)$  is a dense subset congruent to the given metric space  $(X, d)$ . The theorem is proved.

The question now arises as to whether the process of completion is unique in some sense. The answer, in the affirmative is given by

Theorem 8: If  $(X, d)$  and  $(X', d')$  be two metric spaces and  $Y, Y'$  are subsets of  $X, X'$  respectively such that  $\bar{Y} = X, \bar{Y}' = X'$ , and  $Y \cong Y'$ , then  $X \cong X'$ .

We shall prove this by showing that every completion (in particular, the completion given in the proof of theorem 7) is equivalent to the canonical completion which we describe now.

Let  $(X, d)$  be a metric space, and let  $\mathcal{C}$  be the set of all Cauchy-sequences  $\{x_p\}$ . On  $\mathcal{C}$ , define a distance-function according to

$$D(\{x_p\}, \{y_p\}) = \lim_{p \rightarrow \infty} d(x_p, y_p).$$

The limit on the right exists because  $|d(x_p, y_p) - d(x_q, y_q)| \leq d(x_p, x_q) + d(y_p, y_q) \rightarrow 0$  as  $p, q \rightarrow \infty$ , so that  $d(x_p, y_p)$  is a Cauchy-sequence of real numbers and so has a real limit. It is easy to verify that  $(\mathcal{C}, D)$  is a semi-metric space. In what follows, we shall take it to have been converted into a metric space in the usual way (so that all equivalent Cauchy-sequences in  $X$  are identified; two Cauchy-sequences  $\{x_p\}$  and  $\{y_p\}$  being equivalent if  $\lim_{p \rightarrow \infty} d(x_p, y_p) = 0$ ), and shall continue to denote the derived metric space also by  $(\mathcal{C}, D)$ .

Now, we know by theorem 7 that there exists at least one completion of  $(X, d)$ . Let  $(\bar{X}, d')$  be any completion of  $(X, d)$ , with  $(\bar{X}, d') \stackrel{f}{\cong} (X, d)$ , where  $f$  is the congruence-mapping. Given  $\{x_p\} \in \mathcal{C}$ , let  $z_p = f(x_p)$  for every  $p$ ; then  $d'(z_p, z_q) = d(x_p, x_q) \rightarrow 0$  as  $p, q \rightarrow \infty$ , so that  $\{z_p\}$  is a Cauchy-sequence in  $\bar{X}$  and so has a limit  $z \in \bar{X}$ . Consider the mapping  $F$  from  $\mathcal{C}$  to  $\bar{X}$  given by  $\{x_p\} \xrightarrow{F} z$ . The mapping is onto; for given  $z \in \bar{X}$ , by Theorem 6,  $z = \lim z_n$ , where  $z_n \in \bar{X}$ , and if  $x_n = f^{-1} z_n$  for every  $n$ , then  $\{x_n\} \in \mathcal{C}$  is such that  $F(\{x_n\}) = z$ . Also, it is distance-preserving, since  $D(\{x_p\}, \{y_p\}) = \lim d(x_p, y_p) = \lim d'(z_p, w_p) = d'(z, w)$ , where  $w_p = f(y_p)$  and  $w = \lim w_p \in \bar{X}$ . Hence,  $(\mathcal{C}, D) \xrightarrow{F} (\bar{X}, d')$  is a congruence. Thus, every completion of  $(X, d)$  is equivalent to

$(\mathcal{C}, \mathcal{D})$ , and so any two completions are equivalent. This proves Theorem 8. (Note that  $\mathcal{C}$  is now the set of all non-equivalent Cauchy-sequences, the members of the sequences being elements of  $X$ ), and we have incidentally shown that  $(\mathcal{C}, \mathcal{D})$  is a complete metric space.

Remark: In our procedure above, the completeness of the real number system plays a vital role. Our proof of the existence of a completion (Theorem 7) makes essential use of this; again, if we had to prove directly that the space  $(\mathcal{C}, \mathcal{D})$  above is complete -- instead of making use of the fact that at least one completion of  $(X, d)$  exists -- then we would have to consider Cauchy-sequences of Cauchy-sequences of elements of  $X$  and thus repeat the fairly involved argument for the completeness of the real number system for the present situation.

Our discussions above indicate that questions of convergence depend on what sets are 'open' rather than on the metric underlying them. This suggests the generalization of the notion of convergence of sequences to spaces, where there exists a system of "open" sets with properties abstracted out of the metric case, but not necessarily defined through a metric -- the "topological" spaces. We shall refer to these spaces again in the next chapter.

Chapter 3:

CONTINUITY AND GENERAL TOPOLOGICAL SPACES

Let  $f$  be a mapping of a metric space  $(X, d)$  into another  $(X', d')$ . We say that  $f$  is continuous at a point  $x_0 \in X$  if the images of points close to  $x_0$  are close to  $f(x_0)$ ; precisely, if, given any  $\epsilon > 0$ , there exists a  $\delta = \delta(\epsilon, x_0) > 0$  such that  $d(x, x_0) < \delta \Rightarrow d'[f(x), f(x_0)] < \epsilon$ . In other words, we require that the inverse image of any given open sphere around  $f(x_0)$  should contain some open sphere around  $x_0$ .

We say that  $f$  is continuous if it is continuous at every point of  $X$ . It follows that, if  $f$  is continuous, then the inverse image of any open set is open: for, let  $F' \subset X'$  be open and let  $F = f^{-1}(F')$ ; if  $x \in F$ , then  $x' = f(x) \in F'$ , and so there exists an open sphere round  $x'$  contained in  $F' \Rightarrow$  by continuity of  $f$ , that there exists an open sphere round  $x$  contained in the inverse image of the former open sphere and so in  $F \Rightarrow F$  is open.

Conversely, if the inverse image of any open set is open, then  $f$  is continuous. For, let  $x_0$  be any point of  $X$  and let us consider any open sphere round  $f(x_0)$ . Its inverse image is open, by assumption, and since  $x_0$  belongs to this inverse image, there exists an open sphere round  $x_0$  contained in it, i.e.,  $f$  is continuous at  $x_0$ .

Thus, the (global) continuity of  $f$  implies and is implied by the inverse image of every open set being open. Since this property makes no reference to the underlying metrics, we find

that the notion of continuity can be generalized to mappings from one 'topological' space into another, where a 'topological' space is a set with a distinguished family of subsets called 'open' sets, satisfying the conditions given in the statement of Theorem 3 of Chapter 2. (By duality, it follows that we may equally well start from a distinguished family of subsets given by 'closed sets' with properties as in the statement of Theorem 4 of Chapter 2.)

Continuity properties of the metric: Let  $a$  be any fixed element of  $X$ . Then the mapping  $X \rightarrow d(x, a)$  of  $(X, d)$  into the real-number system (with the usual metric) is a continuous mapping. For, by the triangle inequality,

$$|d(x, a) - d(x_0, a)| \leq d(x, x_0).$$

It is even uniformly continuous in the **sense** that, given any  $\epsilon > 0$ , the inverse image of an 'open sphere' (reducing to an open interval) around  $d(x_0, a)$  of radius  $\epsilon$  contains an open sphere of radius  $\delta$  independent of  $x_0$  around  $x_0$ . (We may take  $\delta = \epsilon$  in this particular case.)

Again, consider the Cartesian product of the basic set of the given metric space with itself, and define  $D [(x, y), (x', y')] = \max [d(x, x'), d(y, y')]$ , for  $(x, y), (x', y') \in (X \times X)$ . Then  $(X \times X, D)$  is a metric space, and the mapping  $(x, y) \rightarrow d(x, y)$  of  $(X \times X, D)$  into the real number system is continuous, and uniformly so, because of the relation

$$|d(x, y) - d(x_0, y_0)| \leq d(x, x_0) + d(y, y_0).$$

In the course of the proof of Theorem 7 in Chapter 2, we have seen that the set  $\mathcal{F}$  of all bounded real-valued functions  $f$  on a set  $X$  constitute a complete metric space under the distance-function  $D(f, g) = \sup_x |f(x) - g(x)|$ . We shall now show that the subset  $\mathcal{C}$  of  $\mathcal{F}$ , consisting of all bounded continuous functions on  $X$ , is closed, so that  $(\mathcal{C}, D)$  is itself a complete metric space. The proof is the same as that of the classical result that the limit function of a uniformly convergent sequence of continuous functions is itself continuous.

Note that to prove that  $\mathcal{C}$  is closed, it is (necessary and) sufficient to prove that its 'sequential-limit-points' belong to it. Let  $\{f_n\}$  be a sequence in  $\mathcal{C}$  converging to  $f$  (in  $\mathcal{F}$ ) in the sense that  $D(f_n, f) \rightarrow 0$  as  $n \rightarrow \infty$ . Given any  $\epsilon > 0$ , there exists  $N = N(\epsilon)$  such that  $D(f_n, f) < \epsilon$  for  $n \geq N$ . Hence, for all  $x$ , and for any given  $x_0$ , we have

$$|f_N(x) - f(x)| < \epsilon,$$

$$|f_N(x_0) - f(x_0)| < \epsilon.$$

Since  $f_N$  is continuous, we have, for all  $x$  such that  $d(x, x_0) < \delta = \delta(x_0, \epsilon)$  that  $|f_N(x) - f_N(x_0)| < \epsilon$ . Hence it follows from these three inequalities that  $|f(x) - f(x_0)| < 3\epsilon$  if  $d(x, x_0) < \delta$ . Since  $\epsilon > 0$  is arbitrary, it follows that  $f$  is continuous at  $x_0$ , and, since  $x_0 \in X$  is arbitrary, that  $f$  is continuous.

We saw in § 4 of Chapter 1, that a metric space  $(X, d)$  is congruent to a certain subspace  $(\mathcal{F}, D)$  of the metric space  $(\mathcal{F}, D)$  of all bounded real-valued functions on  $X$  itself

with  $D(f, g) = \sup_x |f(x) - g(x)|$  for  $f, g \in \mathcal{F}$ .

The elements of  $\mathcal{F}$  were the functions  $\{f_x, x \in X\}$ , where

$$f_x(t) = d(t, x) - d(t, x_0), \quad x_0 \in X \text{ fixed, } t \in X.$$

We now know that every  $f_x$  is in fact continuous, so that we can assert that every metric space is congruent to a certain set of bounded continuous real-valued functions defined on it.

The mapping  $X \rightarrow \mathcal{F}$  of  $(X, d)$  onto  $(\mathcal{F}, D)$  is itself a continuous mapping, as indeed any congruence mapping of one metric space onto another is.

#### Chapter 4:

#### MONOIDS, GROUPS AND MORPHISMS.

In what follows, we shall work under the general set-up of a 'monoid' and, as occasion arises, specialize our results to groups.

A monoid is an algebraic system consisting of a basic set  $X$  and a binary operation defined on it. (A binary operation on  $X$  is a mapping of  $X \times X$  into  $X$ , i.e., an association, with every pair  $x, y$  -- in that order -- of elements of  $X$ , an element  $z$  of  $X$ ). We shall usually call the binary operation as multiplication (if we use additive terminology, we may call it summation).

If the multiplication is associative, i.e., if, for all  $x, y, z \in X$ , we have  $(xy)z = x(yz)$ , then the monoid is an associative monoid.

There are certain mappings of a monoid into itself which are definable in terms of the multiplication operation. We shall

denote by  $\lambda_x$  the mapping given by  $y \rightarrow xy$  and call it left-multiplication by  $x$ ; similarly,  $\rho_x$  will denote the mapping  $y \rightarrow yx$  and is called right-multiplication by  $x$ . Certain questions which may be posed immediately concerning these mappings are: when is  $\lambda_x$  one-one and when is  $\lambda_x$  onto? And similarly for  $\rho_x$ . We have:

$\lambda_x$  is one-one iff  $xy = xy' \Rightarrow y = y'$  for all  $y$ .

A sufficient condition for this is that left-cancellation of  $x$  be possible;

$\lambda_x$  is onto iff  $xy = z$  has a solution  $y$ , for every  $z \in X$ , and similar (dual) results hold for  $\rho_x$ . The two questions posed above are thus linked to equations in one unknown in the multiplicative system. [In the first case, we require that the only solution of  $xy' = xy$  (in the unknown  $y'$ ) be  $y' = y$ ; in the second, that  $xy = z$  be solvable.] We also note that, in the presence of left-cancellation of  $x$ , if a solution for the equation  $xy = z$  exists (given  $x, z \in X$ ), then it is unique: for,  $xy = xy' (= z) \Rightarrow y = y'$ .

A group may be defined as an associative monoid  $X$  in which, for any  $x, z \in X$ , the equations  $xy = z$  and  $yx = z$  are solvable in  $X$ . Then, we have:

(1) there exists a unique element  $e$  (the identity or neutral element) such that

$$xe = ex = x$$

for all  $x \in X$ ;

(2) to every  $x \in X$ , there corresponds a unique element  $x^{-1}$  called the inverse of  $x$  such that



$$x x^{-1} = x^{-1} x = e \quad ; \quad \text{and}$$

(3) the solutions for  $xy = z$  and  $yx = z$  are unique (in fact, the left- and right-cancellation laws hold).

Proof: (1) Let  $a$  be an arbitrary but fixed element of  $X$ . The equation  $ea = a$  has a solution  $e$ . Also, for any  $x$ , there exists a  $y$  such that  $ay = x$ . Then  $ex = e(ay) = (ea)y = ay = x$ , so that  $ex = x$  for all  $x$ . Also the equation  $ae' = a$  has a solution  $e'$ , and, for any  $x$ , there exists a  $z$  such that  $za = x$ . Then  $xe' = (za)e' = z(ae') = za = x$ , so that  $xe' = x$  for all  $x$ . Then

$$e = e e' \quad (\text{since } xe' = x \text{ for all } x)$$

$$= e' \quad (\text{since } ex = x \text{ for all } x)$$

so that there exists an element  $e$  such that  $xe = ex = x$  for all  $x$ . The same argument shows that  $e$  is unique.

(2) The equations  $xy = e$  and  $zx = e$  have solutions. Then, we have  $y = ey = (zx)y = z(xy) = ze = z$  so that  $xy = yx = e$ . If  $y'$  be any element with this property, then  $y' = y'e = y'(xy) = (y'x)y = ey = y$ . Hence there exists a unique inverse for  $x$ .

(3)  $xy = z$  and  $yx = z$  have unique solutions because the cancellation laws hold: if  $xy = xy'$ , then left-multiplying by  $x^{-1}$ , we have  $y = y'$ ; similarly, right-multiplication by  $x^{-1}$  in the relation  $yx = y'x$  gives  $y = y'$ .

Conversely, in an associative monoid with properties (1) and (2) above, we have that  $xy = z$  has the solution  $y = x^{-1}z$  and  $yx = z$  has the solution  $y = zx^{-1}$ . Thus

we obtain two equivalent definitions of a group.

In the calculation of inverses, we note two points of importance: (1)  $(x^{-1})^{-1} = x$  itself and (2)  $(xy)^{-1} = y^{-1}x^{-1}$ .

The associate monoid of transformations of a set: If  $f$  be a mapping from a set  $S_1$  into a set  $S_2$ ,  $g$  from  $S_2$  into  $S_3$ , then we define the composition  $g \times f$  as the mapping of  $S_1$  to  $S_3$  given by  $(g \times f)(x) = g(f(x))$ . If  $h$  be a mapping of  $S_3$  into  $S_4$ , then we have  $h \times (g \times f) = (h \times g) \times f$  in the sense that each maps  $x \in S_1$  into the same element  $h(g(f(x)))$  of  $S_4$ . In particular, this is true of transformations of a given set  $X$  (mappings of  $X$  into itself) which thus constitute an associative

monoid under the composition operation. In the case where  $X$  is itself a monoid, this monoid contains all the left- and right-multiplications. We find that if  $X$  is an associative monoid, then

$\lambda_{xx'} = \lambda_x \times \lambda_{x'}$  and  $\rho_{xx'} = \rho_{x'} \times \rho_x$  (we may thus say that, in this case, the  $\lambda_x$ 's combine like their indices and the  $\rho_x$ 's like their indices reversed).

Let us examine when the mapping  $x \rightarrow \lambda_x$ , from a monoid into its monoid of transformations, is one-one. We must have that for  $x \neq x'$ , there exists at least one  $y$  such that  $xy \neq x'y$ , i.e., that the  $\{\rho_y\}$  form a separating family of transformations.

[A family  $\mathcal{F}$  of mappings of a given set  $S$  into a given set  $S'$  is a separating family if, for any pair of distinct elements  $s_1, s_2$  of  $S$ , there exists at least one member  $f \in \mathcal{F}$  such that  $f(s_1) \neq f(s_2)$ .] A sufficient condition for this is that the right cancellation law hold for some particular element of  $X$ .

In the case of a group, it follows that  $x \rightarrow \lambda_x$  is a one-one mapping (The mappings  $\lambda_x$  of  $X$  into itself are all one-one and onto), and  $xy$  corresponds to  $\lambda_x \cdot \lambda_y$ .  $\lambda_e$  is the identity mapping and  $(\lambda_x)^{-1}$ , the inverse mapping of the one-one, onto mapping  $\lambda_x$ , is the same as  $\lambda_{(x^{-1})}$ . In other words,  $\{\lambda_x\}$  is itself a group, which is isomorphic to the given group in the sense of the definition which shortly follows.

MORPHISMS OF MONOIDS: Suppose we have two monoids, the operation in each being called multiplication, and that there exists a mapping  $\phi$  from one into the other such that it preserves products (i.e.)  $\phi(xy) = \phi(x) \cdot \phi(y)$  for all  $x, y$  in the domain-monoid of  $\phi$ . Then  $\phi$  is called a morphism.

If  $\phi$  is an onto mapping, in addition, we call it a homomorphism. A one-one homomorphism is called an isomorphism: it is clear that an isomorphism has an inverse mapping which itself is an isomorphism. Thus the relation of 'isomorphism' is a symmetric one.

A morphism of a monoid into itself is called an endomorphism. An endomorphism-isomorphism is called an automorphism.

It is clear that the composition of two morphisms is a morphism; of two endomorphisms, an endomorphism; and of two homomorphisms, a homomorphism.

Defining a sub-monoid of a monoid as a subset closed under the operation of the monoid (the 'product' of any two elements of the subset should again be in the subset), we see that the image of a monoid under a morphism to another monoid is a

submonoid of the latter. (We remark that in the case of a group, a sub-monoid need not be a sub-group: for instance, in the group of all real numbers under addition, the positive numbers form a submonoid but not a subgroup.)

Theorem: The homomorphic image of a group is a group.  
(If we map a group into a monoid by means of a morphism, the image-set is itself a group).

Proof: If  $\phi$  be the morphism, then  $e' = \phi(e)$  plays the role of the identity and  $\phi(x^{-1})$  is the inverse of  $\phi(x)$ .

In what follows, we examine homomorphic images in greater detail.

The structure of the homomorphic image of a monoid and of a group: Let  $X, X'$  be two monoids and let  $X'$  be the homomorphic image under  $\phi$  of  $X$ . Consider the relation  $\equiv$  on  $X$  given by  $x \equiv y$  iff  $\phi(x) = \phi(y)$ . This is an equivalence relation with the further property that  $x \equiv x', y \equiv y' \Rightarrow xy \equiv x'y'$ . This property enables us to define, in an un-ambiguous manner, a product between equivalence classes according to  $[x][y] = [xy]$ . The mapping  $\phi(x) \rightarrow [x]$  is also one-one, and so defines an isomorphism between  $X'$  and the set of all equivalence classes  $[x]$ . Thus, every homomorphic image of a monoid is isomorphic to the set of equivalence classes (with a suitable binary operation defined on it) corresponding to a certain equivalence relation.

This result applies to a group, of course. But we can then say something more about the equivalence classes above. We need the concept of an invariant or normal subgroup: a subgroup  $Y$  of a group  $X$  is said to be invariant if  $x \in X, y \in Y \Rightarrow xyx^{-1} \in Y$ .

Now, in the case of a group, consider  $[e]$ , the equivalence class containing the identity  $e$ . If  $x \equiv e$ ,  $y \equiv e$ , then  $y^{-1}y \equiv y^{-1}$  or  $y^{-1} \equiv e$  and so  $xy^{-1} \equiv e^2 = e$ , showing that  $[e]$  is a subgroup. [Here we use the fact that  $Y \subset X$  is a sub-group if and only if for any  $x, y \in Y$ ,  $xy^{-1} \in Y$  also.] Again if  $x \in X$  and  $y \equiv e$  then  $xy \equiv x$ ,  $xyx^{-1} \equiv xx^{-1} = e$  shows that  $[e]$  is invariant.  $[e]$  is called the 'Kernel' of the homomorphism. Furthermore,  $x \equiv y$  iff  $xy^{-1} \in [e]$ , and  $[x] = [e] * [x] = [x]$ , where  $xA$  (respectively  $Ax$ ) denotes the set obtained by left-(right-)multiplying the elements of  $A$  by  $x$ . Thus every homomorphic image of a group is isomorphic to the set of equivalence classes defined by a certain equivalence relation, where, moreover, the kernel of the homomorphism,  $[e]$  is an invariant subgroup. We shall call the latter set the quotient-group of  $X$  relative to  $[e]$ .

Conversely, given any invariant subgroup  $Y$  of  $X$ , we can define an equivalence relation on  $X$  compatible with the group product. Let  $x \equiv y$  iff  $xy^{-1} \in Y$ ; then,  $\equiv$  is an equivalence relation such that  $x \equiv x', y \equiv y' \Rightarrow xy \equiv x'y'$ . For,  $(xy)(x'y')^{-1} = xy(y')^{-1}(x')^{-1} = x(x')^{-1} \cdot (x)y(y')^{-1}(x')^{-1}$ ; Now,  $x(x')^{-1} \in Y$ , and, since  $y(y')^{-1} \in Y$ ,  $x' \in X$ ,  $Y$  invariant  $\Rightarrow x'y(y')^{-1}(x')^{-1} \in Y$ , we have that  $xy \equiv x'y'$  from the above. Hence we can define a product on the set of equivalence classes unambiguously according to;  $[x][y] = [xy]$ , and  $x \rightarrow [x]$  is a homomorphism of  $X$  onto this set of equivalence classes (with this operation).

Thus, every homomorphic image of a group  $X$  is isomorphic to the 'quotient-group' of  $X$  relative to some invariant sub-group of  $X$ , and, conversely, every such 'quotient-group' is a homomorphic image of  $X$ .

Chapter 5:

RINGS, AND ENDOMORPHISMS OF ABELIAN GROUPS; HOMOMORPHIC IMAGES OF A RING

Endomorphisms of Abelian groups, and rings with unit:

For the mappings  $\phi, \psi, \dots$  of an arbitrary set  $X$  into a monoid, we can define a composition operation according to

$$(\phi \psi)(x) = \phi(\psi(x)),$$

so that the set of all such mappings becomes a monoid with this operation.

In particular, consider the mappings of a monoid  $X$  into itself; let us examine conditions under which the composition of two endomorphisms of  $X$  will again be an endomorphism.

If  $\phi$  and  $\psi$  be two endomorphisms, then we have

$$(\phi \psi)(xy) = \phi(\psi(xy)) = [\phi(x) \phi(y)] \cdot [\psi(x) \psi(y)] \text{ while}$$

$$(\phi \psi)(x) \cdot (\phi \psi)(y) = [\phi(x) \psi(x)] \cdot [\phi(y) \psi(y)]$$

so that we can assert that  $\phi \psi$  is also an endomorphism if the (operation on the) given monoid is associative and commutative; in general, however, we cannot do so.

Relations between the operations  $\cdot$  and  $\circ$ : Let  $\phi, \psi, \chi$  be transformations of the monoid  $X$ . Consider  $\phi \circ (\psi \cdot \chi)$ . We have

$$[\phi \circ (\psi \cdot \chi)](x) = \phi[(\psi \cdot \chi)(x)] = \phi[\psi(x) \cdot \chi(x)]$$

In case  $\phi$  is an endomorphism, the last expression

$$= \phi(\psi(x)) \cdot \phi(\chi(x)) = (\phi \circ \psi)(x) \cdot (\phi \circ \chi)(x) = [(\phi \circ \psi) \cdot (\phi \circ \chi)](x)$$

so that

$$\phi \circ (\psi \cdot \chi) = (\phi \circ \psi) \cdot (\phi \circ \chi) \quad \text{in the case where } \phi \text{ is an endomorphism.} \tag{1}$$

On the other hand, without any restrictions on  $\phi, \psi, \chi$ , we have

$$\begin{aligned} [(\psi \cdot \chi) \circ \phi](x) &= (\psi \cdot \chi)(\phi(x)) = \psi(\phi(x)) \cdot \chi(\phi(x)) \\ &= [(\psi \circ \phi)(x)] \cdot [(\chi \circ \phi)(x)] \\ &= [(\psi \circ \phi) \cdot (\chi \circ \phi)](x) \end{aligned}$$

so that

$$(\psi \cdot \chi) \circ \phi = (\psi \circ \phi) \cdot (\chi \circ \phi) \tag{2}$$

(1) and (2) are distributive laws; in particular they are valid on the set of endomorphisms of  $X$ .

Let now  $X$  be an Abelian group; we shall find it convenient to write it in additive notation and correspondingly to use  $+$  instead of  $\cdot$  to denote the operation, introduced above, on mappings: thus  $(\phi + \psi)$  is defined according to:

$(\phi + \psi)(x) = \phi(x) + \psi(x)$ , for transformations  $\phi, \psi$  of  $X$ .

We shall call  $\phi \times \psi$  the product of  $\phi$  and  $\psi$ .

Since  $(X, +)$  is associative and commutative, it follows, from what we saw above, that the sum of two endomorphisms, on  $X$  is an endomorphism; so is the 'product' of two, since

$$\begin{aligned} (\phi \times \psi)(x+y) &= \phi(\psi(x+y)) = \phi(\psi(x) + \psi(y)) \\ &= \phi(\psi(x)) + \phi(\psi(y)) = (\phi \times \psi)(x) + (\phi \times \psi)(y). \end{aligned}$$

Thus, the set  $\mathcal{E}$  of endomorphisms of an Abelian group  $(X, +)$  form an algebraic system with two binary operations  $+$  and  $\times$  -- a diploid. Indeed we can assert something more, namely,

Theorem:  $(\mathcal{E}, +, \times)$  is a ring with unit:

Proof: (1)  $(\mathcal{E}, +)$  is an Abelian group:  $(\mathcal{E}, +)$  is associative and commutative since  $(X, +)$  is. Also, if  $\theta$  denotes the endomorphism which maps every element of  $X$  into the neutral element of  $X$ , we find that  $(\phi + \theta)(x) = \phi(x) + \theta(x) = \phi(x) = (\theta + \phi)(x)$ , so that  $\phi + \theta = \theta + \phi$ , for all  $\phi \in \mathcal{E}$ . Also, for  $\phi \in \mathcal{E}$ , if  $-\phi$  is defined according to  $(-\phi)(x) = -\phi(x)$ , then  $-\phi \in \mathcal{E}$  also and is the 'negative' of  $\phi$  in the sense that  $\phi + (-\phi) = (-\phi) + \phi = \theta$ .

We have already seen that

(2)  $\times$  is associative, and

(3) the two distribution laws hold (where  $\times$  distributes over  $+$ ).



Finally,

(4) if  $\epsilon$  be the identity-mapping of  $X$  onto itself, then, for all  $\phi \in \mathcal{E}$ ,  $\epsilon \chi \phi = \phi \times \epsilon = \phi$

Thus,  $(\mathcal{E}, +, \times)$  is a ring with unit.

We now proceed to show that the converse is also true, i.e., every ring with unit is isomorphic to a ring of endomorphisms (not necessarily the ring of endomorphisms i.e., the ring of all the endomorphisms) of an Abelian group, namely, the additive group of the ring. Let  $(X, +, \cdot)$  be a ring with unit; consider the set of mappings  $\{ \phi_x : x \in X \}$ , where  $\phi_x$  is given by:  $\phi_x(y) = xy$  (left-multiplication by  $x$ ). We note the following facts:

(1)  $\phi_x$  is an endomorphism since

$$\phi_x(y+z) = x(y+z) = xy + xz = \phi_x(y) + \phi_x(z)$$

(2)  $\phi_{x+x'} = \phi_x + \phi_{x'}$ , since

$$\begin{aligned} \phi_{x+x'}(y) &= (x+x')y = xy + x'y = \phi_x(y) + \phi_{x'}(y) \\ &= (\phi_x + \phi_{x'})(y) \end{aligned}$$

(3)  $\phi_{xx'} = \phi_x \times \phi_{x'}$ , since

$$\begin{aligned} \phi_{xx'}(y) &= xx'y = x(x'y) = x(\phi_{x'}(y)) \\ &= \phi_x(\phi_{x'}(y)) = (\phi_x \times \phi_{x'})(y) \end{aligned}$$

Thus the mapping  $x \rightarrow \phi_x$  is a morphism of the given ring into the ring of endomorphisms of the Abelian group  $(X, +)$ . We now show that this mapping is one-one (though not necessarily onto). Since the given ring has a unit  $e$ , if  $\phi_x = \phi_{x'}$ , then

$\chi = \phi_{\chi}(\epsilon) = \phi_{\chi'}(\epsilon) = \chi'$ . Thus the mapping is an isomorphism onto a ring of endomorphisms of  $(X, +)$ , and our assertion is proved.

The case of a ring without unit: We shall now show that an arbitrary ring can be embedded in a ring with unit, whence it will follow from the above that any ring is isomorphic to a ring of endomorphisms of an Abelian group. We first take a few preliminary remarks.

In a monoid (using additive notation), we can define positive integral multiples of any element  $\chi$  recursively according to  $1\chi = \chi$ ,  $(n+1)\chi = n\chi + \chi$ . We may then define  $0\chi = \theta$  and  $(-n)\chi = -n\chi$ , where  $\theta$  is the neutral element, in the case where the monoid is a group. In the case of an associative monoid, it will follow that for all positive integers  $m$  and  $n$ , and, in the case of a group, for all integers  $m$  and  $n$ , that  $(m+n)\chi = m\chi + n\chi$ .

In the case of a ring  $(X, +, \cdot)$ , the above relation obviously holds; furthermore, we have, for all integers  $m, n$ , and any pair of elements  $x, y \in X$ ,  $(m\chi).(ny) = mn(\chi y)$ .

Now consider the set  $\mathcal{K}$  of all pairs  $(m, \chi)$  with  $m$  an integer and  $\chi \in X$ . Define the operations  $+$  and  $\cdot$  on  $\mathcal{K}$  according to

$$(m, \chi) + (n, y) = (m+n, \chi + y)$$

$$(m, \chi) \cdot (n, y) = (mn, my + n\chi + \chi y)$$

It is easily verified that  $(\mathcal{K}, +, \cdot)$  is a ring, and that

the mapping  $x \rightarrow (0, x)$  is an isomorphism between  $X$  and the subring of  $\mathcal{X}$  consisting of all elements  $(0, x)$  with  $x \in X$ . Further,  $(1, \theta)$  plays the role of a unit in  $\mathcal{X}$ , where  $\theta$  is the neutral element of  $X$ . Thus we have embedded  $(X, +, \cdot)$  into a ring with unit. The latter ring, as we know, is isomorphic to a ring of endomorphisms of its own (Abelian) additive group. Hence the given ring is isomorphic to a sub-ring of this ring of endomorphisms.

The homomorphic image of a ring: As in the case of monoids and groups, it is true that the image of a diploid under a morphism is a diploid, and, of a ring, a ring. We now examine a question similar to what we have answered for groups, namely, the characterization of all homomorphic images of a ring.

Let  $(X', +, \cdot)$  be the homomorphic image under of the ring  $(X, +, \cdot)$ . Let  $K$  be the subset of  $X$  consisting of all elements  $x \in X$  such that  $\phi(x) = \theta'$ , the neutral element of  $X'$  (incidentally, we note that  $\phi(\theta) = \theta'$ ): we call  $K$  the Kernel of the homomorphism. We have:

$K$  is a two-sided ideal of  $X$ .

By a two-sided ideal  $\gamma$  of  $X$ , we mean a subset of  $X$  such that (i)  $(\gamma, +)$  is an Abelian group; and (ii) if  $x \in X$ ,  $y \in \gamma$ , we have  $xy \in \gamma$ ,  $yx \in \gamma$ .

Proof: If  $x \in K$ ,  $y \in K$ , then  $x - y \in K$ , since  $\phi(x - y) = \phi(x) - \phi(y) = \theta' - \theta' = \theta'$ ; hence  $(K, +)$  is a sub-group of  $(X, +)$ .

Also, if  $x \in X$ ,  $y \in K$ , then  $\phi(xy) = \phi(x) \cdot \phi(y) = \phi(x) \cdot \theta' = \theta'$ . Similarly,  $\phi(yx) = \theta'$  also. Hence

$xy$  and  $y^x$  both belong to  $K$ .

Now, let us define  $x \equiv y$  iff  $\phi(x) = \phi(y)$ , i.e., iff  $x - y \in K$ . Then this is an equivalence relation, and if we denote the equivalence class containing  $x$  by  $[x]$ , as usual, we find that we can unambiguously define operations  $+$  and  $\cdot$  over the set of  $[x]$ 's according to

$$[x] + [y] = [x + y]$$

$$[x] \cdot [y] = [xy]$$

For,  $x \equiv x', y \equiv y' \Rightarrow (x' + y') - (x + y) = (x' - x) + (y' - y) \in K$ , since  $(x' - x) \in K, (y' - y) \in K$ , and  $(K, +)$  is a group, so that  $x' + y' \equiv x + y$ . And,  $x \equiv x', y \equiv y' \Rightarrow xy - x'y' = x(y - y') + (x - x')y \in K$  since  $K$  is a two-sided ideal and  $y - y' \in K, x - x' \in K$ , so that  $xy \equiv x'y'$ .

Thus the mapping  $\phi(x) \rightarrow [x]$  gives us an isomorphism of  $[X', +, \cdot]$  onto the above ring of equivalence classes, showing that every homomorphic image of a ring is isomorphic to a certain ring of equivalence classes which is the difference-ring relative to a two-sided ideal of the ring, namely, the kernel of the homomorphism. (We have also incidentally proved the converse, namely, that on a difference-ring relative to any two-sided ideal, addition and multiplication can be defined suitably and unambiguously to make it a homomorphic image of the given ring.)

Chapter 6:

MODULES AND VECTOR-SYSTEMS

The most satisfactory way of defining a module is to consider it as comprising an Abelian group  $(X, +)$  written additively, together with a distinguished sub-ring  $R_0$  of its ring of endomorphisms  $R$ , so that, for any  $x \in X$ ,  $r_0 \in R_0$ , we have  $r_0 x \in X$ . ( $R$  itself may be trivial and consist, for instance, merely of 'multiples' of the identity mapping.)

In the case where  $R_0$  is a division-ring (i.e., a ring in which the non-neutral elements form a group under multiplication), we obtain a vector-system (over  $R_0$ ); in particular, if  $R_0$  is a field, i.e., a commutative division-ring.

If a sub-group  $Y$  of  $X$  is left invariant by (all the members of)  $R_0$ , then  $(Y, R_0)$  is called a sub-module of  $(X, R_0)$ . A sub-module  $(Y, R_0)$  defines an equivalence relation on  $(X, R_0)$  according to

$$x \equiv y \iff x - y \in Y.$$

which has the further property that  $x \equiv y \implies r_0 x \equiv r_0 y$  for all  $r_0 \in R_0$ . For,  $x \equiv y \implies x - y \in Y \implies r_0(x - y) \in Y \implies r_0 x - r_0 y \in Y \implies r_0 x \equiv r_0 y$ . The equivalence classes therefore form a module, with  $r_0[x]$  being defined as  $[r_0 x]$ : this module is called the difference-module of  $X$  relative to the sub-module  $Y$ .

Suppose  $(X, R_0)$  and  $(X', R'_0)$  are two modules, where  $R_0$  is isomorphic to  $R'_0$  (in particular, they may be identical). Then a mapping  $\phi$  from the first into the second is called a

morphism if

$$(1) \quad \phi(x+y) = \phi(x) + \phi(y),$$

$$(2) \quad \phi(\gamma_0 x) = \gamma_0 \phi(x).$$

As before, the image of a module under a morphism is again a module. It is clear that the difference-module of a module relative to a sub-module is a homomorphic image of the given module.

Characterization of homomorphs of a module: Suppose  $(X, \mathcal{R}_0)$  is mapped homomorphically by  $\phi$  onto a module  $(X', \mathcal{R}'_0)$ . Consider the "Kernel"  $K = \{x : \phi(x) = e'\}$ . Then,  $x \in K \Rightarrow \phi(\gamma_0 x) = \gamma_0' \phi(x) = \gamma_0' e' = e'$ , so that  $\gamma_0 x \in K$  also, and consequently  $K$  is a sub-module of  $X$ . We can form the 'difference-module' of  $X$  relative to  $K$  consisting of the equivalence classes corresponding to the relation given by  $x \equiv y \Rightarrow x-y \in K$ , which is again a module over the same  $\mathcal{R}_0$ ,  $\gamma_0[x]$  being the equivalence class  $[\gamma_0' x]$ . Each homomorphic image of a module is then seen to be isomorphic to the difference-module of the given module with respect to a particular sub-module.

A more usual method of presenting modules and vector-spaces is by means of the theory of groups with operators. We start with a group  $X$  (written additively) and a set  $\Omega$  of 'operators'. We consider mappings of  $\Omega \times X$  into  $X$ . We denote the image of the pair  $(\alpha, x)$  by  $\alpha x$  and we link the mapping to the group-operation by the requirement.

$$\alpha (x + y) = \alpha x + \alpha y.$$

In other words, we require that, for fixed  $\alpha$ , the mapping  $\{\lambda_\alpha: X \rightarrow X\}$  be an endomorphism of the given group. The correspondence  $\alpha \rightarrow \lambda_\alpha$  will be one-one iff  $\alpha x = \beta x$  for all  $x \Rightarrow \alpha = \beta$ ; in other words, if  $\alpha \neq \beta$ , there must exist some  $x$  such that  $\alpha x \neq \beta x$ .

Now, two natural compositions for the operators are given by:

$$+ : (\alpha + \beta)x = \alpha x + \beta x,$$

$$\times : (\alpha \times \beta)x = \alpha(\beta x).$$

If the original group be Abelian, then the set  $\Omega$  of operators can be enlarged into a ring by adjoining to it a null operator  $\textcircled{H}$  and the operators  $\{-\alpha \mid \alpha \in \Omega\}$ , where, for all  $x \in X$ ,  $\textcircled{H}x = \theta$  and  $(-\alpha)x = -\alpha x$ . The correspondence  $\alpha \rightarrow \lambda_\alpha$  will be one-one, for  $\alpha x = \beta x$  for all  $x \iff (\alpha - \beta)x = 0$  for all  $x \iff \alpha - \beta = \textcircled{H}$ . Further, it is a homomorphism since  $\lambda_{\alpha + \beta} = \lambda_\alpha + \lambda_\beta$  and  $\lambda_{\alpha \times \beta} = \lambda_\alpha \times \lambda_\beta$  and so is an isomorphism. Thus, the set of operators  $\Omega$  of an Abelian group with operators can always be enlarged to a ring of operators which is isomorphic to a ring of endomorphisms of the basic group. This fact provides the connection between groups-with-operators and modules.

Vector-systems: In this case, the distinguished subring  $\mathcal{R}_0$  has an identity which we shall denote by  $e$  (i.e.,  $e\alpha_0 = \alpha_0 e = \alpha_0$  for  $\alpha_0 \in \mathcal{R}_0$ ). It does not, however, follow that  $e x = x$  for all  $x \in X$ . If we consider the set  $Y$

of elements  $y$  satisfying the relation  $ey = y$ , we get a sub-module  $(Y, \mathcal{R}_0)$  such that  $e$  acts as the identity on  $Y$ .

[If  $y \in Y$ , then  $ey = y \Rightarrow e(e_0 y) = (ee_0)y = e_0 y$ ; and, by definition,  $e$  acts as the identity mapping on  $Y$ .] Now, any element  $x$  of  $X$  can be represented as

$$x = ex + (x - ex).$$

The elements  $\{ex \mid x \in X\}$  form the above module; if  $N = \{x - ex \mid x \in X\}$ , then it is clear that  $N = \{z \in X \mid ez = 0\}$ , so that  $N$  is obviously a module and  $e$  acts as an annihilator on  $N$ . Hence  $X$  is the 'direct sum' of two modules,  $Y$  and  $N$ .

If we now replace  $X$  by the difference-module  $\bar{X} = X \ominus N$ , which will be isomorphic to  $Y$ , the identity element of  $\mathcal{R}_0$  coincides with the identity mapping on  $\bar{X}$  and the usual properties of vector-systems follow ( $x, y \in \bar{X}$ ):

$$\alpha(x + y) = \alpha x + \alpha y$$

$$(\alpha + \beta)x = \alpha x + \beta x$$

$$\alpha(\beta x) = (\alpha\beta)x$$

$$ex = x.$$

These properties are enough to make the correspondence  $\alpha \rightarrow \lambda_\alpha$  (where  $\lambda_\alpha$  is the mapping  $x \rightarrow \alpha x$ ) an isomorphism. For,  $\alpha x = 0$  either  $\alpha = \mathbb{0}$ , the null-mapping, or  $\alpha \neq \mathbb{0}$ , in which case  $\alpha^{-1}$  exists and we have  $x = ex = (\alpha^{-1}\alpha)x = \alpha^{-1}(\alpha x) = \mathbb{0}$ . Hence, a 'vector-system (over a division ring)' is indeed an Abelian group together with a certain division-ring of endomorphisms thereof.



Remark: We mention in passing that the modules we have considered above are the so-called 'left modules'; modules comprising an Abelian group  $(X, +)$  together with a distinguished sub-ring  $R_0$  of its ring of endomorphisms  $R$  such that for any  $x \in X, \gamma_0 \in R_0$ , we have  $x\gamma_0 \in X$  are called 'right-modules'. It suffices to consider only one kind since the properties of the other will be merely duals of those of this kind. Sometimes it is useful to deal with 'bi-modules', i.e., modules with one ring of left-multiplications and another ring of right-multiplications.

Commutant of subsets of  $R$  in a module  $(X, R_0)$ : Let  $X$  be an Abelian group and  $R$  the ring of its endomorphisms. Let  $R_0$  be a distinguished sub-ring of  $R$ .  $(X, R_0)$  is then a module, by definition.

For any subset  $A$  of  $R$ , we define the commutant  $A'$  of  $A$  according to

$$A' = \{ \alpha \in R \mid \alpha\beta = \beta\alpha \text{ for all } \beta \in A \cup R_0 \}.$$

It follows that  $R'_0$  is precisely the set of all endomorphisms of the module  $(X, R_0)$ , remembering that  $\alpha$  is an endomorphism iff (1)  $\alpha(x+y) = \alpha x + \alpha y$  for all  $x, y \in X$ , and (2)  $\alpha(\gamma_0 x) = \gamma_0(\alpha x)$  for all  $x \in X, \gamma_0 \in R_0$ . These endomorphisms, are called linear operators or linear transformations, especially in connection with vector-systems.

It follows at once from the definition that (1)  $A' \subset R'_0$  and (2)  $A \subset B \Rightarrow A' \supset B'$ . Hence, every member of  $A'$  is an endomorphism of the module; furthermore, as is easily verified,  $A'$  is indeed a ring of endomorphisms of the module. In particular,

$R'_0$  is the ring of endomorphisms of the module, and  $A'$ , consequently, is a sub-ring of this ring. We further have

$$(3) \quad A \cap R'_0 \subset A''$$

Proof:  $A'' = \{ \alpha \in R \mid \alpha\beta = \beta\alpha \text{ for all } \beta \in A' \cup R'_0 \}$ .

If  $\alpha \in A \cap R'_0$  and  $\beta \in A' \cup R'_0$ , it is clear that  $\alpha\beta = \beta\alpha$ ; so that the assertion follows.

In particular, (4) if  $A \subset R'_0$ , then  $A \subset A''$ . By (1) above,  $A' \subset R'_0$  and so, applying (1) to  $A'$ , we have  $A' \subset (A')''$ . Again,  $A \subset A'' \Rightarrow (A') \supset (A'')'$ , by (?). Now, it is almost at once obvious that  $(A')'' = (A'')'$ ; denoting this set by  $A'''$ , we have: (5) for all sets  $A \subset R'_0$ ,  $A' = A'''$ .

In particular, again, if  $A \subset A'$ , so that  $A$  is commutative (in fact, for  $A \subset R'_0$  to be commutative, it is both necessary and sufficient that  $A \subset A'$ , as is easily verified), we have  $R'_0 \supset A' \supset A$  by (1), so that  $A \subset A''$  and  $A' = A'''$ , by (4) and (5) respectively.

Abelian sets: Sets  $A$  with the above property:  $A \subset A'$  are called Abelian sets. (According to what we have seen above,  $R''_0$  is an Abelian set.)

An Abelian set  $A$  is maximal Abelian if  $B \subset B'$ ,  $B \supset A \Rightarrow B = A$ . Abelian sets are obviously commutative; their most important properties include the following two:

(1) For an Abelian set  $A$  to be maximal Abelian, it is necessary and sufficient that  $A' = A$

Proof: If  $A = A'$ , then suppose  $B \subset B'$ ,  $B \supset A$ . Then  $A \subset B \subset B' \subset A'$ , so that  $A = A' \Rightarrow B = A$ .

If  $A \neq A'$ , then  $A$  being contained in  $A'$ , there exists an element  $\alpha$  belonging to  $A'$  but not to  $A$ . We assert that  $B = A \cup \{\alpha\}$  is an Abelian set. For, if  $\beta \in B$  and  $\gamma \in B \cup \mathcal{R}_0$ , we must have either (i)  $\beta \in B \subseteq A'$ , and  $\gamma \in A \cup \mathcal{R}_0$  or (ii)  $\beta \in A$  and  $\gamma = \alpha \in A'$ , or (iii)  $\beta = \gamma = \alpha$ , and in all these cases  $\beta\gamma = \gamma\beta$  so that  $B \subset B'$ . Since  $B$  includes  $A$  in the strict sense,  $A$  is not maximal Abelian.

(2) If  $A$  is Abelian, then there exists a maximal Abelian set containing  $A$ .

If  $A = A'$ , by (1), the assertion is trivially true. Hence we need only consider the case  $A \neq A'$ . Let  $\mathcal{B}$  be the class of all sets  $B$  such that  $A \subset B \subset B' \subset A'$ :  $\mathcal{B}$  is not empty, since  $A$  belongs to it. We introduce a partial ordering on  $\mathcal{B}$  namely, the ordering by inclusion. If  $\{B_\lambda, \lambda \in \Delta\}$  be a chain (linearly ordered subset of  $\mathcal{B}$ ) then it has an (in fact, a least) upper bound, namely,  $\cup \{B_\lambda : \lambda \in \Delta\}$ . For denoting this set by  $B$ , we have to show that  $B \subset B'$ , i.e., if  $\beta \in B$  and  $\gamma \in B \cup \mathcal{R}_0$ , then  $\beta\gamma = \gamma\beta$ . But  $\beta \in B_\mu$  and  $\gamma \in B_\nu \cup \mathcal{R}_0$  for some  $\mu, \nu \in \Delta$ , so that  $\beta \in B_\lambda$  and  $\gamma \in B_\lambda \cup \mathcal{R}_0$ , where  $B_\lambda$  is the larger of the two sets  $B_\mu$  and  $B_\nu$  (remembering that they are members of a chain). But, since  $B_\lambda$  is an Abelian set,  $\beta\gamma = \gamma\beta$ , and so  $B \subset B'$ . Hence, by Zorn's axiom,  $\mathcal{B}$  has a maximal element, i.e., there exists a set  $B_0$  such that

$A \subset B_0 \subset B'_0 \subset A'$  and if  $B$  be any set with the same property and such that  $B \supset B_0$ , then  $B = B_0$ . This implies that  $B_0 = B'_0$ , since, otherwise, our construction in the proof of Property (1) applies, and we can find a set  $B_0 \cup \{\alpha\}$  which is also Abelian. Hence  $A$  is contained in a maximal Abelian set.

This result has important applications in the theory of operators. For instance, following Von Neumann, we may call a set  $A$  a factor if  $A = A'$  and  $A \cap A' = \mathcal{R}_0''$ . (If  $A$  is a factor, obviously so is  $A'$ .) There exists a theory of decomposition of rings into 'factors'.

Remark: By definition,  $\mathcal{R}_0'' = \mathcal{R}_0' \cap \{\alpha \mid \alpha\beta = \beta\alpha \text{ for all } \beta \in \mathcal{R}_0'\}$  the set of all linear operators which commute with every linear operator: this, by definition, is the center of the ring  $\mathcal{R}_0'$ .

Semi-metrics and metrics on groups: right-invariance:

Suppose we have a group which is at the same time a (semi-) metric space. Mathematical systems of interest are those in which the group operation and the distance function are suitably connected. We may, for instance, require that the group product be continuous and/or that the inverse be continuous. Or we may replace a given distance function by another, topologically equivalent to it, but more closely connected in some manner to the group operation.

In all the discussions that follow, we assume  $d$  to be a right-invariant semi-metric, i.e., for all  $x, y, z \in X$ ,  $d(x, y) = d(xz, yz)$ . Whatever be  $z \in X$ ,  $d(xz, yz)$  can be made arbitrarily small by making  $d(x, y)$  small enough:

in other words, left multiplication in the group is uniformly continuous. (We are not in a position to say anything about the continuity of right-multiplication.)

Theorem 1 If  $d$  is a right-invariant metric, then  $xy$  is jointly continuous in  $x$  and  $y$  iff it is continuous for each  $x$  at  $y = e$ .

Proof: The 'only if' part is immediate, since  $xy$  jointly continuous in  $x$  and  $y \Rightarrow$  for each fixed  $x$ ,  $d(xy, xe)$  is small if  $d(y, e)$  is small. Here we do not need the right-invariance of  $d$ .

If  $xy$  is continuous at  $y = e$  for each fixed  $x$ :

$$d(x'y', xy) = d(x'y'y^{-1}, x) = d(x \cdot x^{-1}x'y'y^{-1}, x)$$

By our hypothesis, this is small if  $d(x^{-1}x'y'y^{-1}, e)$  is small. But the last expression  $= d(x^{-1}x', y(y')^{-1})$  by right-invariance,

$$\leq d(x^{-1}x', e) + d(y(y')^{-1}, e)$$

$$= d(x^{-1}x'x^{-1}, x^{-1}) + d(y, y') \text{ by right-invariance.}$$

Again, by our hypothesis, the first member of the last expression is small if  $d(x'x^{-1}, e)$  is small, i.e., if  $d(x', x)$  is small (by right-invariance). Hence it follows that  $d(x'y', xy)$  is small if  $d(x, x')$  and  $d(y, y')$  are small, i.e.,  $xy$  is jointly continuous in  $x$  and  $y$ .

Theorem 2: If  $d$  is right-invariant and  $xy$  is jointly continuous in  $x$  and  $y$ , then the inverse is continuous:

Proof:  $d(x^{-1}, y^{-1}) = d(x^{-1}y, e) [= d(e, y^{-1}x)]$  by right invariance.  $d(x^{-1}y, e) = d(x^{-1}y, x^{-1}x)$  ; is small, by joint-continuity of  $xy$ , if  $d(y, x)$  is small.

The converse is also true, namely,

Theorem 3: If  $d$  is right-invariant and the inverse is continuous, then  $xy$  is jointly continuous in  $x$  and  $y$ .

By theorem 1, it suffices to show that for each fixed  $x$ ,  $xy$  is continuous at  $y = e$ , i.e., that  $d(xy, x)$  is small if  $d(y, e)$  is. But, by continuity of inverse,  $d(xy, x)$  is small if  $d(y^{-1}x^{-1}, x^{-1})$  is small, i.e., (by right-invariance) if  $d(e, y)$  is small, since  $d(y^{-1}x^{-1}, x^{-1}) = d(y^{-1}x^{-1}xy, x^{-1}xy)$ .

Theorem 4: If  $xy$ , for every fixed  $y$ , and  $x^{-1}$  are continuous in  $x$ , then  $yx$ , for every fixed  $y$ , is also continuous in  $x$ .

Proof: For fixed  $y$ ,  $yx = (x^{-1}y^{-1})^{-1}$  is continuous in  $x^{-1}y^{-1}$  (by continuity of inverse), which is continuous in  $x^{-1}$ , which again is continuous in  $x$ .

We can also prove Theorem 3 with the help of Theorem 4. In the presence of a right-invariant  $d$ ,  $xy$  is continuous in  $x$  for each fixed  $y$  (in fact, uniformly for all  $y$ ) since  $d(xy, x'y) = d(x, x')$ . Then the assumptions of Theorem 3 imply (by Theorem 4) that, for fixed  $y$ ,  $yx$  is continuous in  $x$ , or, what is the same,  $xy$  is continuous in  $y$  for fixed  $x$ . Since  $d(xy, x'y') \leq d(x'y', xy') + d(xy', xy) = d(x', x) + d(xy', xy)$  it follows that it is small if  $d(x, x')$  and  $d(y, y')$  are small, as desired to prove.

Thus, under right-invariance of  $d$ , joint continuity of  $xy$  in  $x$  and  $y$  is equivalent to continuity of  $x^{-1}$  in  $x$ .

Semi-norms and norms corresponding to right-invariant distance functions: Let  $d$  be a right-invariant semi-metric on

a group  $X$ . We can make some special constructions using the fact that  $d(x, y) = d(xy^{-1}, e)$  and consequently the function of two variables,  $d$ , can be replaced by a function of a single variable as follows: define  $N(z) = d(z, e)$ . Then  $d(x, y) = N(xy^{-1}) = N(yx^{-1})$ .  $N$  has the following properties derived from corresponding properties of  $d$ :

- (1)  $N(x) \geq 0$ , and  $N(e) = 0$
- (2)  $N(x^{-1}) = N(x)$
- (3)  $N(xy) \leq N(x) + N(y)$ .

If  $d$  is a metric, then we have further,

- (4)  $N(x) = 0 \Rightarrow x = e$ .

A real-valued function  $N$  defined on a group and having properties (1) - (3) above is called a semi-norm; if it satisfies (4) also, then it is a norm. Thus every right-invariant (semi-) metric induces a (semi-) norm.

Conversely, given a (semi-) norm on a group, we can introduce a distance  $d$  according to  $d(x, y) = N(xy^{-1})$ ;  $d$  is also right-invariant, as an immediate consequence of the definition.

Thus, a (semi-) norm is equivalent to a right-invariant (semi-) metric.

Let us assume that  $N$  is a semi-norm on a group  $X$ . The set  $Y = \{x \mid N(x) = 0\}$  is a subgroup; for, if  $N(x) = N(y) = 0$ , then  $0 \leq N(xy^{-1}) \leq N(x) + N(y^{-1}) = N(x) + N(y) = 0$ , showing that if  $x, y \in Y$ , then so does  $xy^{-1}$ . The relation  $\equiv$  on  $X$  defined by  $x \equiv y$  iff  $xy^{-1} \in Y$  is then an equivalence relation such that, if  $x \equiv y$ , then  $xz \equiv yz$  for all  $z$ . Consider

the set of equivalence classes  $\bar{X} = \{ [x] \mid x \in X \}$ . For each  $z \in X$ , the mapping  $\rho_z : [x] \rightarrow [xz]$  is a one-one mapping of  $\bar{X}$  onto itself. We may now define  $\bar{d}$  on  $\bar{X} \times \bar{X}$  according to  $\bar{d}([x], [y]) = d(x, y)$  -- this definition being unambiguous -- and  $\bar{N}$  according to  $\bar{N}([x]) = N(x)$ .  $\bar{d}$  has the property  $\bar{d}([xz], [yz]) = \bar{d}([x], [y])$ . In general,  $\bar{X}$  is not a group, but  $(\bar{X}, \bar{d})$  is a metric space.

In the case where  $Y$  is an invariant subgroup of  $X$  (in particular, if  $X$  is Abelian), we know that  $\bar{X}$  is a group and that the above construction defines a right-invariant metric  $\bar{d}$  and an equivalent norm  $\bar{N}$  on this group.

Let now  $H$  be an invariant sub-group of a group  $G$  with a right-invariant semi-metric  $d$  and the equivalent semi-norm  $N$ . Let

$$\bar{N}(x) = \inf_{z \in H} N(xz) \quad \left[ = \inf_{z \in H} N(xz^{-1}) \text{ obviously} \right]$$

$\bar{N}$  is a semi-norm. For,

$$(i) \quad \bar{N}(e) = 0 \quad (\text{take } z = e \text{ to get } 0 \leq \bar{N}(e) \leq 0).$$

$$(ii) \quad \bar{N}(x^{-1}) = \inf_{z \in H} N(x^{-1}z) = \inf_{z \in H} N(z^{-1}x) = \\ \inf_{z \in H} N(x \cdot x^{-1}z^{-1}x) = \bar{N}(x),$$

since  $\{x^{-1}z^{-1}x \mid x \in G \text{ fixed, } z \in H\} = H$ ,  $H$  being an invariant sub-group.

$$(iii) \quad \bar{N}(xy) = \inf_{z \in H} N(xy z) = \inf_{z, w \in H} N(xw \cdot w^{-1}yz) \\ \leq N(xw) + N(w^{-1}yz) \\ = N(xw) + N(y \cdot yw^{-1}yz).$$



By the invariance of  $H$ ,  $y^{-1}w^{-1}y \in H$  and, therefore, so does  $y^{-1}w^{-1}yz$ : call it  $u$ . Note that since  $w$  and  $z$  are 'independent' variables, so are  $w$  and  $u$ . Given  $\epsilon > 0$  there exist  $w, u \in H$  such that  $N(xw) \leq \bar{N}(x) + \epsilon/2$  and  $N(yu) \leq \bar{N}(y) + \epsilon/2$ ; since  $\epsilon > 0$  is arbitrary, it then follows that  $\bar{N}(xy) \leq \bar{N}(x) + \bar{N}(y)$ . Hence our assertion.

Consider the set  $\{x : \bar{N}(x) = 0\}$ . This is a subgroup (as we have already noted for the case of an arbitrary semi-norm).  $x$  belongs to this set  $\iff \inf_{z \in H} N(xz^{-1}) = 0$   
 $\iff \inf_{z \in H} d(x, z) = 0 \iff x \in \bar{H}$ , the closure of  $H$ .  
 (under the metric topology induced by  $N$ ). Hence it follows that  $\bar{H}$  is a sub-group, but we do not know whether it is invariant or not. If, however, the group product is jointly continuous (equivalently, if the inverse is continuous), then,  $z \in \bar{H}$  can be approached by a sequence  $z_n \in H$ ,  $xz_n x^{-1} \in H \subset \bar{H}$  for every  $n$ , and, by the continuity of the product and the fact that  $\bar{H}$  is closed, we have  $xz x^{-1} \in \bar{H}$  for arbitrary  $x \in G$ , showing that  $\bar{H}$  is invariant in this case.

Since  $\bar{H} = \{x \mid \bar{N}(x) = 0\}$ , we can carry out the construction of the metric space of equivalence classes, exhibited above. Denoting it by  $G/\bar{H}$  (as usual) and the semi-norm induced by  $\bar{N}$  on this space by  $\bar{\bar{N}}$ , we have the

Theorem: If  $(G, d)$  is a complete metric space, so is  $(G/\bar{H}, \bar{\bar{N}})$ .

Proof: We have to show that if  $\bar{N}(x_m x_n^{-1}) \rightarrow 0$  as  $m, n \rightarrow \infty$ , then there exists  $x$  such that  $\bar{N}(x_n x^{-1}) \rightarrow 0$

as  $n \rightarrow \infty$  provided that  $N$  has the same property. We can find a sequence  $\{x_{n_p}\}$  such that  $\bar{N}(x_{n_{p+1}} x_{n_p}^{-1}) < 2^{-p-1}$  for all  $p$ . Denoting  $x_{n_p}$  by  $y_p$ , we have  $\bar{N}(y_{p+1} y_p^{-1}) < 2^{-p-1}$ . By the definition of  $\bar{N}$ , there exists  $u_p \in H$  such that  $N(y_{p+1} y_p^{-1} u_p) < \bar{N}(y_{p+1} y_p^{-1}) + 2^{-p-1} < 2^{-p}$ . Let

$$z_{p+1} = (y_{p+1} y_p^{-1} u_p) \cdot (y_p y_{p-1}^{-1} u_{p-1}) \cdot \dots \cdot (y_2 y_1^{-1} u_1).$$

Then, for  $q \geq p$ , we have

$$z_{q+1} z_{p+1}^{-1} = (y_{q+1} y_q^{-1} u_q) \cdot (\dots) \cdot (y_{p+2} y_{p+1}^{-1} u_{p+1}).$$

and

$$N(z_{q+1} z_{p+1}^{-1}) \leq \sum_{k=p+1}^q N(y_{k+1} y_k^{-1} u_k) \leq \sum_{k=p+1}^q 2^{-k} < 2^{-p}.$$

Hence,  $(X, N)$  being a complete metric space,  $z_{q+1}$  converges to some element  $z$  of  $X$ . Let  $y$  be such that  $z = y y_1^{-1}$ .

Then  $N(y y_1^{-1} z_{p+1}^{-1}) \leq 2^{-p}$ , as seen by letting  $q \rightarrow \infty$  in the last relation above. Now,

$$\begin{aligned} y y_1^{-1} z_{p+1}^{-1} &= y y_1^{-1} (u_1^{-1} y_1 y_2^{-1}) (u_2^{-1} y_2 y_3^{-1}) \dots (u_p^{-1} y_p y_{p+1}^{-1}) \\ &= y y_{p+1}^{-1} \cdot y_{p+1} [(y_1^{-1} u_1^{-1} y_1) (y_2^{-1} u_2^{-1} y_2) \dots (y_p^{-1} u_p^{-1} y_p)] y_{p+1}^{-1} \\ &= y y_{p+1}^{-1} w_p, \end{aligned}$$

where, by the invariance of  $H$ ,  $w_p \in H$ . Hence,

$$\begin{aligned} \bar{N}(y y_{p+1}^{-1}) &\leq N(y y_{p+1}^{-1} w_p) && \text{by definition of } \bar{N} \\ &= N(y y_1^{-1} z_{p+1}^{-1}) \leq 2^{-p} && \text{as } p \rightarrow \infty. \end{aligned}$$

Hence  $\{y_{p+1}\}$  converges to  $\gamma$  (relative to  $\bar{N}$ ). It follows that so does the original sequence  $\{x_n\}$ .

Semi-norms on vector-systems: Suppose we have a vector-system over the real or complex field, or over the division-ring of quaternions; in all these cases, we can define an "absolute value" or "modulus" for the elements of the field or division-ring, i.e., for the "scalars". Suppose further that a real-valued function  $N$  is defined on the vector-system having the properties ( $\alpha$  denoting a scalar and  $x$  a vector):

$$N(x) \geq 0, \quad N(0) = 0, \quad N(-x) = N(x), \quad N(\alpha x) = |\alpha| N(x),$$

$$\text{and } N(x+y) \leq N(x) + N(y).$$

Then  $N$  is called a semi-norm; if, further,  $N(x) = 0 \Rightarrow x = 0$ , then  $N$  is a norm.

Suppose  $N$  is a semi-norm on a vector-system of one of the above kinds.  $H = \{x \mid N(x) = 0\}$  is a vector-subsystem ("sub-space") of the given system. In particular, as a subset of the additive group, it is a sub-group of an Abelian group and so invariant. Hence the construction described above, of  $\bar{N}$  from  $N$ , applies and  $\bar{H} = \{x \mid \bar{N}(x) = 0\}$ .  $\bar{N}$  has the further property that  $\bar{N}(\alpha x) = |\alpha| \bar{N}(x)$ , and the difference system of  $G$  relative to  $\bar{H}$  is itself a vector-system (with the same scalars) and is a normed one with norm  $\bar{N}$  given by  $\bar{N}([x]) = \bar{N}(x)$ . If the original system

is complete, so is  $G / \bar{H}$ , according to what we have said earlier.

Norms in terms of suitable subsets of the vector-systems:

Consider the set  $\{x : N(x) \leq 1\}$ . Geometrically, this is a symmetric and convex set: for,  $N(x) \leq 1$  implies that  $N(-x) \leq 1$ ; and  $N(x) \leq 1, N(y) \leq 1, 0 \leq \alpha \leq 1, \alpha + \beta = 1$  implies that  $N(\alpha x + \beta y) \leq \alpha N(x) + \beta N(y) \leq \alpha + \beta = 1$ .

Conversely, if a symmetric and convex subset  $K$  of a vector-system is given, then a norm  $N$  can be so defined on the system that  $\{x | N(x) < 1\} \subset K \subset \{x | N(x) \leq 1\}$ . In fact, it is even possible to omit the symmetry requirement and merely require that  $K$  include the origin and be convex.

