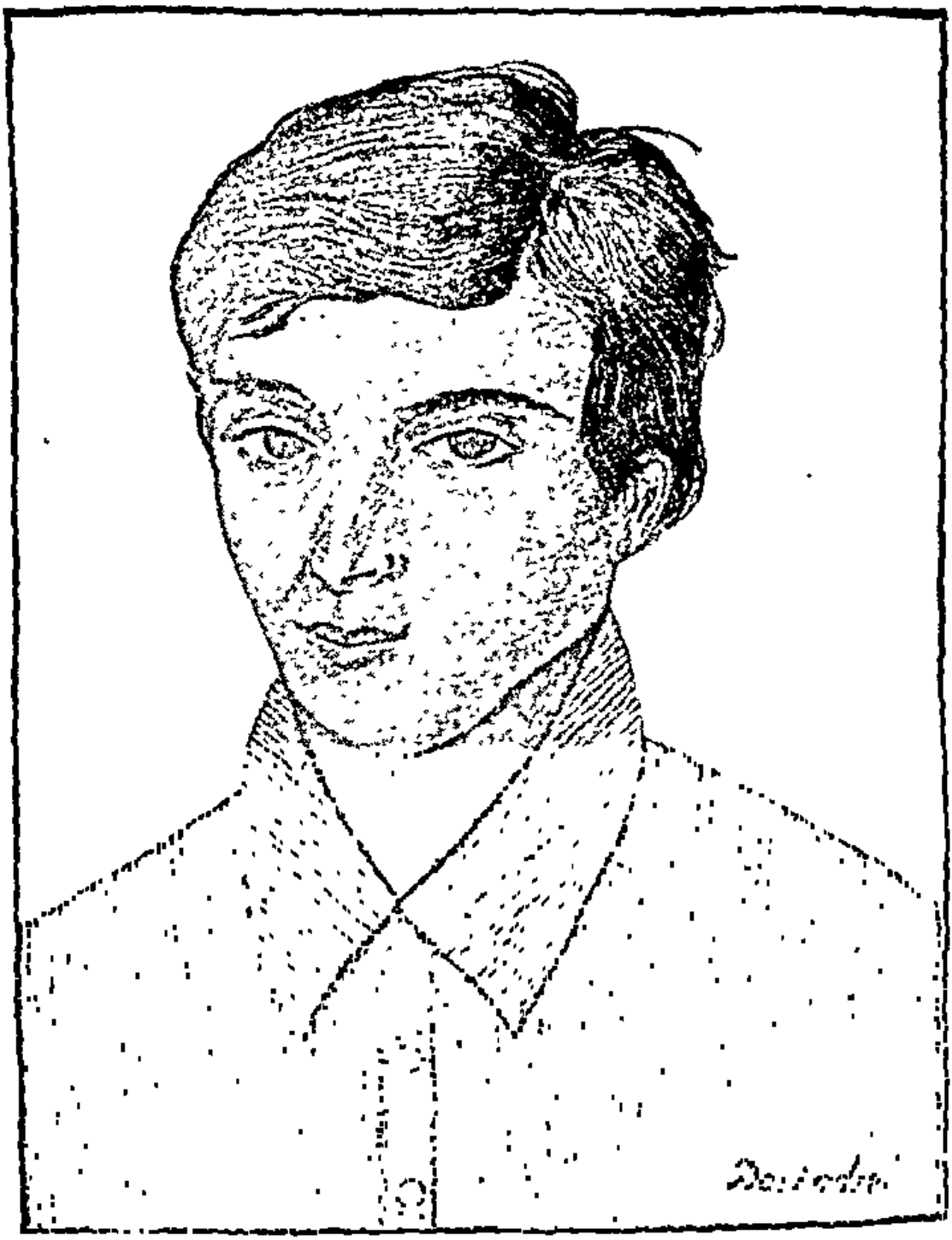


E. Galois. (1812—1832)

Evariste Galois was killed in a duel on the 30th of May, 1832 at the age of 20. On the eve of his death, he wrote a long letter to a friend mentioning a number of additional results to the first draft of his theory of Algebraic equations which had been already presented to the Paris Academy.

A TEXT BOOK
OF
MODERN ABSTRACT ALGEBRA

By
SHANTI NARAYAN,
Principal,
Hans Raj College, Delhi.
(Delhi University)

1965
S. CHAND & CO.,
DELHI—NEW DELHI—JULLUNDUR
LUCKNOW—BOMBAY

Books by the Same Author

A Course of Mathematical Analysis	...	Rs. 15·00
Theory of Functions of a Complex Variable	...	Rs. 12·50
A Text Book of Matrices	...	Rs. 7·50
A Text Book of Vector Algebra	...	Rs. 6·50
A Text Book of Vector Calculus	...	Rs. 7·50
A Text Book of Cartesian Tensors	..	Rs. 6·50
Differential Calculus	...	Rs. 7·00
Integral Calculus	...	Rs. 6·25
Analytical Solid Geometry	...	Rs. 6·00
Modern Pure Geometry	...	Rs. 5·00

A Text Book of General Topology (*Under preparation*)

S. CHAND & CO.,

Ram Nagar	—	New Delhi
Fountain	—	Delhi
Mai Hiran Gate	—	Jullundur
Hazratganj	—	Lucknow
Lamington Road	—	Bombay

First Edition	*1958*
Second Edition	*1961*
Reprint	*1965*

Price : **Rs. 14·00**

Published by S. Chand & Co., Ram Nagar, New Delhi and offset by Eurasia Offset Printers, Ram Nagar, New Delhi-1.

PREFACE TO THE SECOND EDITION

It has been considered desirable to effect a change in th notation for a function and for a function value inasmuch as th notation $f(x)$ has been employed in place of $x\sigma$ or xf. This has bee done with a view to linking the subject with classical Mathematics a also with mordern topological and topological algebraic studies. More over, it was felt that a beginner would feel more at home with thi notation and a possible mysterious significance underlying $x\sigma$ woul be avoided. Also two slips which had been brought to my notic have been removed.

November, 1961 THE AUTHOR

PREFACE

The inherent appeal of Modern Abstract Algebra and the importance of its impact on other branches of Mathematics are being increasingly realised and the appearance of this book is motivated by a feeling that the presentation of this subject in a text book form will greatly help the popularisation of this fundamental branch of Pure Mathematics. It is this feeling again which has determined the form of presentation adopted in the book in the light of the author's experience of teaching the subject to the students of the University of Delhi. In this context it is believed that a systematic use of the symbols $\Longrightarrow$, $\Longleftrightarrow$ for one-way and two-way implications respectively which have been adopted here will greatly help the reader in his grasp of the chain of arguments. Further the main purpose of the author is to treat the fundamentals of Galois theory and it is this purpose which has, in the main, determined the content and scope of the book. Thus the subject proceeds along a road leading to the portals of Galois Theory with occasional short pauses at places to steal glances at the sides.

Chapter I introduces some basic Set-Theoretic concepts of mappings, Binary compositions in a set, Equivalence and order relations.

Chapters II and III have been devoted to Group Theory with no exclusive emphasis on Finite order groups only. Permutation groups have not been given any separate place but different aspects of the same have been taken up at appropriate places for providing illustrations in respect of the Theory of Abstract groups.

Chapter IV deals with Ring Theory in relation to Sub-rings and Ideals and Chapter V with Polynomial rings. In the latter chapter, Unique Factorisation Domains (U.F.D.) have been defined and it has been shown that a Principal Ideal Domain (P.I.D.) is such a domain. It is also shown that a Euclidean domain is a P.I.D. and hence also a U.F.D.

Chapter VI deals with Vector Spaces, Linear Transformations of Vector Spaces and with co-ordinatisation of the same relatively to some given base or bases.

Chapter VII is concerned with Vector Spaces of Linear Transformations and thus paves the way for the introduction of the

concepts of Linear Associative Algebras over a field. Several illustrations of Linear Algebras have been given. The concept of the Dual of a vector space has also been introduced and the reflexivity of Finite Dimensional Spaces established. The portals are now reached and Galois Theory is introduced in Chapter VIII in the setting of the Theory of Finite field extensions. The last chapter is devoted to developing Criteria for 'Solvability by Radicals' and 'Constructibility by Ruler and Compass' thus vindicating the rise of Galois Theory.

It is very much hoped that, as a result of a careful study of the book, the reader would acquire an appreciation and fascination for Abstract Algebra and thus be led on to deeper studies of special branches of the subject.

The author takes this opportunity to thank his old student and present colleague Shri Mohanlal Abrol who very kindly went through a considerable part of the manuscript and made useful suggestions which helped him to remove a number of slips and obscurities.

Suggestions for improvements and notices of errors would be gratefully acknowledged.

September, 1958 THE AUTHOR

CONTENTS

CHAPTER I

Set-Theoretic Prelminaries

Sections			*Pages*
1.	Introduction. Two-way and one-way implications	...	1
2.	Some Set-theoretic Concepts	...	2
3.	Mappings or Functions	...	5
4.	Transformations of a set	...	12
5.	Composition in a set	...	17
6.	Composition tables for finite sets	...	18
7.	Algebraic Structures	...	20
8.	Some types of Compositions	...	21
9.	Binary relations in a set	...	23
10.	Quotient Set	...	26
11.	Lattices	...	26

CHAPTER II

Groups and their Sub-groups

12.	Introduction	...	28
13.	Groups. Illustrations of groups.	...	28
14.	Some general properties of groups	...	35
15.	Orders of elements of a group	...	40
16.	Commutativity of elements of a group	...	41
17.	An alternative set of postulates for a group	...	42
18.	Isomorphism of groups. Notion of an abstract group	...	43
	Cayley's Theorem	...	51
19.	Complexes and sub-groups of a group	...	52
20.	Algebra of complexes of a group	...	54
21.	Criteria for a sub-group	...	56
22.	Algebra of the set of sub-groups of a group	...	58
23.	Systems of generators of a group	...	60

Sections			*Pages*
24.	Multiplication of two sub-groups	...	63
25.	Right and left cosets of a sub-group. Coset decompositions of a group. Congruence modulo a sub-group	...	65
26.	Lagrange's Theorem	...	69
27.	Cyclic groups	...	70
28.	Groups of coincidence rotations of regular bodies	...	75

CHAPTER III

Groups and their Normal Sub-groups

29.	Introduction	...	82
30.	Conjugate elements. Equivalence relation of conjugacy in a group	...	82
31.	Classes of conjugate elements of the Symmetric group of degree n	...	84
32.	Structure of classes of conjugate elements. Normaliser of an element	...	86
33.	Conjugate Complexes. Classes of conjugate sub-groups	...	88
34.	Self-conjugate sub-groups. Simple groups	...	90
35.	Algebra of Normal sub-groups of a group	...	92
36.	Quotient Group	...	94
37.	Commutator Sub-group of a group	...	97
38.	Homomorphism	...	98
39.	Concerning the totality of homomorphic images of a group	...	102
40.	Two laws of Isomorphism	...	103
41.	Binary relations compatible with group structure	...	106
42.	Jordan Holder theorem for finite groups	...	107
43.	Automorphisms of a group	...	110
44.	External Direct products	...	116
45.	Internal Direct products	...	118
46.	Structure of Cyclic groups	...	123
47.	Survey of abstract groups with order not exceeding 8	...	124

CHAPTER IV

Rings : Their sub-rings and ideals

Sections			*Pages*
48.	Introduction of Rings	...	138
49.	Some general properties of rings	...	140
50.	Types of rings	...	142
51.	Integral domains. Fields. Division Rings	...	144
52.	Isomorphism of two rings.	...	146
53.	The Quotient field of an integral domain	...	148
54.	Sub-rings	...	152
55-56	Algebra of the set of sub-rings	...	153-54
57.	Quotient rings or residue class rings. Ideals in a ring	...	155
58.	Ring homomorphisms	...	159
59.	*A fundamental theorem*	...	162
60.	Relations compatible with ring structure	...	165
61.	Algebra of Ideals	...	166
62.	Principal ideals and principal ideal rings	...	168
63.	Direct product of rings	...	168
64.	The ring of endomorphisms of an Abelian group	...	171
65.	Sub-Fields	...	175
66.	Homomorphism of fields	...	176
67.	Maximal Ideals	...	177
68.	Characteristic of a field	...	178
69.	Prime fields. Structure of prime fields	...	179

CHAPTER V

Polynomial Rings

Factorisation in Integral Domains

70.	Introduction	186
71.	Polynomial Rings. Division algorithm for Polynomials over a field	186
72.	Factorisation in Integral domains	194
73.	Greatest Common divisor	199

Sections			Pages
74.	Lowest Common mutliple	...	201
75.	Prime and Composite elements of an integral domain.	...	201
76	Unique Factorisation domains and some of their properties	...	202
77.	Principal ideal domain as a unique factorisation domain	...	204
78.	Euclidean Domains	...	207
79.	Polynomial rings over unique factorisation domains	...	209
80.	Irreducibility criterion due to Eisenstein	...	214

CHAPTER VI

Vector Spaces and Linear Transformations

81	Introduction		216
82.	Vector Spaces	...	217
83.	Some general properties of vector spaces	...	218
84.	Vector Sub spaces	...	219
85.	Algebra of Sub-spaces	...	220
86.	Quotient Space	...	223
87.	Vector Space homomorphisms. Linear Transformations	...	225
88.	Isomorphisms of vector spaces	...	227
89.	Direct Sum of spaces	...	227
90.	Vector Space as a direct sum of sub-spaces	...	228
91.	Basis of a vector space	...	229
92.	Finitely generated spaces and their bases	...	230
93.	Some properties of finite dimensional spaces	...	233
94.	Dimension of a quotient space	...	236
95.	Dimension of a direct sum	...	237
96.	Isomorphism of finite dimensional vector spaces	...	239
97.	Co-ordinatisation of an abstract space	...	241
98.	Rank and Nullity of a linear transformation	...	242
99.	Linear equations	...	242

CHAPTER VII

Vector Space of Linear Transformations

Linear Algebras

Sections			*Pages*
100.	Introduction	...	245
101.	Vector Space of linear transformations	...	245
102.	Dual space of a vector space	...	247
103.	Annihilator of a sub-space	...	252
104.	Co-ordinatisation of a linear transformation	...	254
105.	Product of linear transformations represented as product of corresponding matrices	...	255
106.	Linear Algebra over a field	...	257

CHAPTER VIII

Finite Field Extensions

Galois Theory

107.	Introduction	...	266
108.	Field extensions	...	266
109.	Roots of a polynomial	...	266
110.	Polynomial equations and field extensions	...	267
111.	Finite field extensions	...	268
112.	Algebraic field extensions	...	270
113.	Simple field extensions	...	271
114.	Existence of simple field extensions	...	277
115.	Solution of algebraic equations	...	277
116.	Decomposition field of a polynomial	...	280
117.	Solution of algebraic equations	...	284
118.	Normal extension fields	...	284
119.	Separable polynomials. Separable elements and separable field extensions	...	286
120.	Simplicity of finite separable extensions. Theorem of the primitive element	...	292
121.	Galois Theory	...	294
122.	Fundamental Theorem of Galois Theory	...	297

Sections			Pages
123.	Conjugate elements. Conjugate sub-fields and conjugate sub-groups	...	299
124.	Galois group of a separable polynomial	...	301
125.	Finite Fields	...	305
126.	Some preliminaries	...	306
127.	Existence and Uniqueness	...	307
128.	Structure of the multiplicative group of a finite field	...	308
129.	Construction of Galois fields	...	309
130.	*Subfields of a Galois field*	...	310

CHAPTER IX

Solvability by Radicals

Ruler and Compass Constructions

131.	Introduction	...	314
132.	Cyclotomic equations and fields	...	316
133.	Galois groups of cyclotmic fields	...	319
134.	Galois groups of pure equations	...	321
135.	Solvability by radicals of cyclotomic fields	...	323
136.	Fundamental theorem on Solvability by radicals	...	324
137.	Galois group of a generic equation	...	327
138.	Abels' Theorem	...	329
139.	Ruler and Compass Constructions	...	331
140.	Determination of conditions for constructibility	...	332
141.	Illustrations. Duplicating a cube. Trisecting an angle. Squaring a circle. Constructibility of a regular polygon.	...	336
	Bibliography	..	340
	Index	...	342

CHAPTER 1

SET-THEORETIC PRELIMINARIES

1. Introduction. Modern Pure Mathematics can be described as a study of *Sets equipped with assigned structures*—also known as *mathematical systems.* The present book is concerned with the study of *Algebraic systems* which are sets equipped with Algebraic structures in terms of the meaning of the same given in § 7, page 20.

The various algebraic systems to be considered in this book are

Group, Rings, Fields, Vector Spaces, Linear Algebras.

Classical Mathematics abounds with particular types of these algebraic systems as will be made clear by means of the several illustrations which we would be giving. The approach, in this book, however, would be distinguished from that of classical Mathematics by means of its *Abstract and Axiomatic* nature. Also it would be seen that each abstract concept actually arises as a result of an analysis of concrete situations and in fact each abstract concept seeks to synthesise a number of concrete situations by taking note of some of their common features.

Since the subject matter of the book is to consist of a systematic deduction of conclusions from given premises, we shall see that it will be of great help in stating our arguments and chains of reasoning in a compact form if we adopt the following notations for

two-way and one-way implications.

If P and Q denote two statemets such that the truth of P implies that of Q, we shall write

$$P \Longrightarrow Q \qquad \textit{(One-way implication)}$$

Also we shall write

$$P \Longleftrightarrow Q \qquad \textit{(Two-way implication)}$$

if

$$P \Longrightarrow Q \text{ and } Q \Longrightarrow P.$$

Thus we write $P \Longleftrightarrow Q$ if the truth of P implies that of Q as well as vice-versa, *i.e.*, when P is true if and only if Q is true.

In view of the basic importance of the notion of a pure set without reference to any structure for the study of every algebraic system, we shall in this chapter introduce some fundamental *Set-theoretic* concepts.

2. Some Set-theoretic Concepts. Any collection of objects is called a set or an aggregate and is said to be defined if there is given a rule or rules such that it is possible, in terms of the same, to say whether any given object is or is not an object belonging to the set.

A set is often described as follows :

$S=\{x : P\}$ and we say that S is a set consisting of elements x such that x has the property P.

Two sets S and T, are said to be equal, in symbols, $S=T$, if they consist essentially of the same objects so that each object belonging to one also belongs to the other and vice-versa.

If, a, is any object belonging to a set S, we write in symbols,

$$a \in S$$

and say that, a is a *member* of S or that it is an *element* of S.

Illustrations. The following are some examples of sets :

(i) The set **Z** of all natural numbers.

(ii) The set **J** of all integers.

(iii) The set **Q** of all rational numbers.

(iv) The set **R** of all real numbers.

(v) The set **C** of all complex numbers.

(vi) The set of all real valued functions defined in a closed interval [0, 1].

(vii) The set of all real valued continuous (differentiable or integrable) functions in [0, 1].

(viii) The set of all infinitely differentiable real valued functions defined in [0, 1].

(ix) The set of all real valued functions capable of representation by means of Maclaurin's series in [0. 1].

(x) The set of all triangles (circles or conics) in a plane.

(xi) The set of all rotations of a given rigid body about a given straight line

(xii) The set of all movements of a rigid body.

(xiii) A set containing no object.

Throughout this book, the sets of

(i) Natural Numbers, *(ii)* Integers, *(iii)* rational numbers, *(iv)* real numbers, *(v)* complex numbers, will be denoted by the symbols

$$\mathbf{Z}, \mathbf{J}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$$

respectively.

Ex. Give some examples of sets.

2·1. Null set. It is found useful to conceive of a set containing no element, known as a null set, void set or empty set. A null

set will always be denoted by the symbol φ. A set which is not a null set may be referred to as a *non-empty* or a non-void set.

2·2. Finite and infinite sets. A set containing only a finite number of elements is known as a finite set and one which is not finite is known as an infinite set.

A set consisting of a single element, a, will be denoted by the symbol $\{a\}$. Further a finite set consisting of n elements

$$a_1, a_2, \ldots\ldots, a_n$$

will be denoted by the symbol

$$\{a_1, a_2, \ldots\ldots, a_n\}.$$

A set consisting of n elements may be described as an n-elementic set.

2·3. Inclusion relation. If S, T, are two sets such that each member of S is as well a member of T, we shall write

$$S \subseteq T.$$

and say that S is *contained* or *included* in T or that S is a *sub-set* of T.

Also we write

$$S \subset T$$

if

$$S \subseteq T \text{ and } S \neq T.$$

In this case, we say that S is *proper* sub-set of T.

It is very important to notice that if

$$S \subseteq T \quad T \subseteq S$$

then

$$S = T$$

and conversely. In other words, have

$$S \subseteq T, T \subseteq S \longleftrightarrow S = T.$$

This fact will be seen to constitute an important technique for proving equality of sets.

2·4. Intersection and Union of Sets.

Intersection. If S, T are two given sets, then a set D will be called the intersection of S and T, if it is defined by the rule that any given object is a member of D if and only if it is a member of S as well as of T. In symbols, we exhibit this relationship as

$$D = S \cap T$$

and read the same as, *D is the intersection of S and T.*

Thus

$$x \in S \cap T \longleftrightarrow x \in S \text{ and } x \in T.$$

We may also write

$$S \cap T = D = \{x;\ x \in S \text{ and } x \in T\}.$$

The set D will be void if S and T have no member in common. Two such sets S and T are called *disjoint*. Thus for two disjoint sets S and T, we have

$$\varphi = S \cap T.$$

A meaning may similarly be given to the intersection set of any arbitrary family of sets as a set consisting of elements common to all the members of the family.

Union. A set U is called the union of two given sets S and T, if it is defined by the rule that any given object is a member of U if and only if it is member of S **or** of T or of both. In this case we write, in symbols,

$$U = S \cup T,$$

and say that U is the union of S and T.

Thus we have

$$x \in S \cup T \Longleftrightarrow x \in S \text{ or } x \in T.$$

Also, we may write

$$S \cup T = U = \{x\ ;\ x \in S \text{ or } x \in T\}.$$

We may also give a meaning to the union of any arbitrary family of sets.

Ex. Prove that

(*i*) $(S_1 \cup S_2) \cup S_3 = S_1 \cup (S_2 \cup S_3)$.

(*ii*) $(S_1 \cap S_2) \cap S_3 = S_1 \cap (S_2 \cap S_3)$.

(*iii*) $S_1 \cup (S_2 \cap S_3) = (S_1 \cup S_2) \cap (S_1 \cup S_3)$.

(*iv*) $S_1 \cap (S_2 \cup S_3) = (S_1 \cap S_2) \cup (S_1 \cap S_3)$.

2·5. Product of sets. If S, T be two given sets, then the set consisting of ordered pairs

$$(a, b), \qquad a \in S, b \in T$$

is called the Product set of S and T and is denoted by

$$S \times T.$$

Illustration. If

$$S = \{a, b\},\ T = \{l, m, n\},$$

then

$$S \times T = \{(a, l), (a, m), (a, n), (b, l), (b, m), (b, n)\}$$

Generalising we may say that if

$$S_1, S_2, \ldots\ldots, S_n,$$

be any n given sets, then the set of n-tuples

$$(a_1, a_2, \ldots\ldots, a_n)$$

where

$$a_1 \in S_1, a_2 \in S_2, \ldots\ldots, a_n \in S_n$$

is called the product set denoted by

$$S_1 \times S_2 \times \ldots \times S_n.$$

3. Mappings or Functions. The notion of Mappings whose character is as fundamental as that of sets will be introduced now.

Let S and T be two given sets and let there exist a correspondence, denoted by f, which associates to each member of S a *unique* member of T. We then say that f is a mapping of S into T or that f is a function on S to T. Also the element of T which the mapping, f, associates to any element x of S will be denoted by the symbol

$$f(x)$$

and called the f-image of x or the value of the function for x. Also the element, x, may be referred to as a pre-image of $f(x)$.

The fact that, f, is a mapping of S into T will often be symbolised as

$$f : S \longrightarrow T,$$

S is called the *Domain* and T the *Range* of the mapping f.

Also the set of all f-images of the elements of S will be denoted by the symbol $f(S)$. We may thus write

$$f(S) = \{f(x) : x \in S\}.$$

Obviously

$$f(S) \subseteq T.$$

3·1. Equality of Mappings. Two mappings f and g of S into T are said to be equal, in symbols $f = g$, if and only if

$$f(x) = g(x), \text{ for every } x \in S.$$

Thus for two unequal mappings of S into T, there must exist at least one element of S which is mapped differently by the two mappings.

3·2. Mappings into and Mappings onto. If the mapping f is such that each element of T is the f-image of atleast one elen ent of S, we say that f is a mapping of S *onto* T instead of into T. Thus if f is a mapping of S onto T and y is any element of T, there necessarily exists an element x of S such that

$$f(x)=y.$$

In the case of f being an onto mapping, we have

$$f(S)=T.$$

3·3. Many-one mappings. One-one mappings. It is important to notice that, in terms of our definition, if f is a mapping of S into (or onto) T, then it is quite possible that two *different* elements of S have the same f-image, *i.e.*, we may have

$$f(a)=f(b) \text{ even if } a\neq b.$$

This means that a given element of T may have more than one pre-image.

It should, however, be remembered that no element of S can have more than one f-image.

Thus for any arbitrary mapping f of S into (onto) T,

$$a=b \Longrightarrow f(a)=f(b)$$

but *not* conversely.

Now a mapping f of S into T is called **one-one**, if two different members of S necessarily correspond to two different images of T, *i.e.*, if

$$f(a)=f(b) \Longrightarrow a=b$$

or alternatively

$$a\neq b \Longrightarrow f(a)\neq f(b)$$

A mapping which is not one-one may be referred to as many-one in as much as in this case many, *i.e.*, more than one element of S may correspond to the same element of T.

Finally, we may have a one-one mapping of one set onto the other.

3·4. Identity Mapping. A very simple but important case of a mapping arises when each element of a set is mapped on itself. Such a mapping is known as the *Identity mapping* and will be usually denoted by the symbol e or ϵ. Thus if e denotes the identity mapping of a set S, we have

$$e(x)=x \text{ for every } x \in S.$$

Note. The notion of mapping which is the *same thing* as a function is met with quite early in our studies in Calculus as well as in classical Algebra. By an abuse of language, however, it is $f(x)$ rather than f which is referred to as a function in these studies. It may be noticed that in point of fact f is the function and $f(x)$ is the element of the range which the function f associates to the element x of the domain.

Illustrations.

(*i*) $y=x^2$ determines a mapping of the set $\mathbf{R}$ of real numbers *into* itself so that denoting the same by f, we have, in terms of our present notation,

$$f : \mathbf{R} \longrightarrow \mathbf{R}$$

defined by

$$f(x)=x^2 ; x \in \mathbf{R}.$$

This mapping is neither onto nor one-one.

(*ii*) $y=x^2$ determines a mapping of the set $\mathbf{R}$ of real numbers *onto* the set of all non-negative real numbers.

(*iii*) The mapping f defined by

$$f(x)=\sin x$$

is a one-one mapping of the set of real numbers x, $-\frac{1}{2}\pi \leqslant x \leqslant \frac{1}{2}\pi$, *onto* the set of real numbers y, $-1 \leqslant y \leqslant 1$.

(*iv*) $w=|z|$ determines a mapping of the set $\mathbf{C}$ of complex numbers, $z \in \mathbf{C}$, into the set $\mathbf{R}$ of real numbers, $w \in \mathbf{R}$.

This mapping is neither one-one nor onto.

(*v*) The mapping $f : Z \to Z$ defined by

$$f(n)=2n$$

is a one-one into (not onto) mapping.

The image set, as may be easily seen, is a proper sub-set of the set $\mathbf{Z}$ even though the mapping is one-one.

(*vi*) Let T denote the finite set of numbers $0, 1, 2$ so that $T=\{0, 1, 2\}$ and let $f(x)$ denote the least non-negative remainder obtained on dividing $x \in \mathbf{Z}$ by 3. Then f is a many-one mapping of $\mathbf{Z}$ onto T.

(*vii*) The mapping, f, defined by

$$f(x)=x^{-1},$$

is a one-one mapping of the set of all non-zero real numbers onto itself.

(*viii*) Let S denote the set of all triangles and T the set of positive real numbers. Then the mapping f which maps each member of S on its area is a many-one mapping of S onto T.

(*ix*) Each movement of a body is essentially a mapping of the set S of points occupied by the particles of the body in any initial position onto the set T of points occupied in the final position such that each point $P \in S$ is mapped on $Q \in T$ to which the particle at P has moved.

Ex. 1. Describe the mappings defined as follows as *into* or *onto* and as *one one* or *many-one*, stating carefully the *Domain* and the *Range sets* :

(*i*) $y=\log x$ (*ii*) $y=\sqrt{x}$ (*iii*) $y=\tan x$,
x denoting a real number.

Ex. 2. Give some examples of mappings which are

(*i*) into and many-one, (*ii*) onto and many-one,
(*iii*) into and one-one, (*iv*) onto and one one.

Ex. 3. What is the total number of distinct mappings of an n-elementic finite set into itself. How many of these are

(*i*) one-one. (*ii*) onto.

3·5. Inverses of one-one onto mappings. Let f be a *one-one mapping of a set S onto a set T.* Also let b be any member of T.

Then f being a mapping of S onto T, there exists *atleast one* member a of S such that

$$b = f(a),\ b \in T,\ a \in S.$$

Since f is also one-one, there exists *only* one such member a of S.

Thus we define a mapping of T onto S which associates to each $b \in T$, the element $a \in S$ (uniqueness and existence of, a, having been already seen) such that

$$f(a)=b.$$

We denote this mapping of T onto S by f^{-1} and call the same as the **Inverse** of f.

Thus we have

$$f^{-1}(b)=a \longleftrightarrow f(a)=b\ ;\ b \in T,\ a \in S.$$

We now show that

$$f^{-1} \text{ is also one-one.}$$

Suppose now that b_1 and b_2 are two different elements of T Also let

$$f^{-1}(b_1)=a_1,\ f^{-1}(b_2)=a_2; a_1 \in S, a_2 \in S.$$

Now

$$f^{-1}(b_1)=a_1 \Longrightarrow f(a_1)=b_1,\ f^{-1}(b_2)=a_2 \Longrightarrow f(a_2)=b_2.$$

Also, f being one-one, we have

$$f(a_1)\neq f(a_2) \Longrightarrow a_1\neq a_2.$$

Thus f^{-1} is also one-one.

Note 1. It should be noted that only one-one onto mappings possess inverses which again are one-one onto. The one-one onto mappings are also known as *Inversible*, *Invertible*, *Non-singular* or *Biuniform*.

Note 2. Irrespective of the fact that a mapping f of S onto T is one-one or not, we shall agree to denote by the symbol

$$f^{-1}(b),\ b \in T,$$

the set consisting of all those elements of S which are mapped on the same element b of T *i e.*, the set of all the f pre-images of b. Also, if T_1 be any sub-set of T,

$$f^{-1}(T_1)$$

will denote the sub-set S_1 of S consisting of all those elements of S which are mapped on a member of T_1. Thus

$$f^{-1}(T_1)=\{x\,;\ x \in S_1, f(x) \in T_1\}.$$

$f^{-1}(T_1)$ is also often described as the set of all the *Total Originals* of the members of T_1.

It should, however, be remembered that f^{-1} can be described as a mapping of T into S only if and only if f is a one-one onto mapping.

Ex. 1. If f is a mapping of the set $\mathbf{R}$ of real numbers into itself defined by

$$f(x)=x^2\,;\ x \in \mathbf{R},$$

describe explicitly the sets

$$f^{-1}(2), f^{-1}(\mathbf{Z}).$$

Ex. 2. Show that the mapping f of $\mathbf{Z}$ into itself defined by

$$f(n)=2n+3,\ n \in \mathbf{Z}$$

is inversible. Describe explicity the inverse mapping f^{-1}.

3·6. Products of mappings. We shall now introduce the notion of *Product of mappings* also known as *Resultant* or the *Composite of mappings*. This notion corresponds to what is known in Calculus as the notion of *Function of a Function*.

Suppose that S, T, U are three sets and f is a mapping of S nto T and g that of T into U.

Then the mapping of S into U which maps each element $x \in S$ into the g-image of the f-image of x is denoted by the symbol

$$gof$$

or simply, gf, if no confusion be possible and called the product or the resultant of f and g taken in this order.

Thus, by def.,

$$(gf)(x)=g(f(x)),\ x \in S.$$

Here

$$x \in S, f(x) \in T, g(f(x)) \in U.$$

Note 1. If f, g are both mappings of a set S into itself, then gf is as well a mapping of S into itself.

Note 2. If f is a one-one mapping of S onto itself so that it is inversible *i.e.*, f^{-1} exists, then we have

$$ff^{-1}=e=f^{-1}f,$$

where e is the identity mapping of S

Let, a be any arbitrary element of S and let $f(a)=b$.

We have

$$f(a)=b \Longleftrightarrow f^{-1}(b)=a,$$

so that as a (b) ranges over $S(S)$, then b (a) ranges over $S(S)$.

We have then

$$(f^{-1}f)(a)=f^{-1}(f(a))=f^{-1}(b)=a$$
$$(ff^{-1})(b)=f(f^{-1}(b))=f(a)=b$$

Thus each of

$$ff^{-1} \text{ and } f^{-1}f$$

is the identity mapping of S.

Illustrations. If f is a mapping of **R** into itself defined by

$$f(x)=\sin x,$$

and g is a mapping of **R** into itself defined by

$$g(x)=x^2,$$

then, gf, is the mapping of **R** into itself given by

$$(gf)\ (x)=\sin^2 x.$$

Note. The following two sub sections are devoted to proving two important properties of Products of mappings.

3·61. Associativity of Products of mappings.

Let

$$S, T, U, V$$

be four sets and let

$$f, g, h$$

be mappings of

$$S \text{ into } T, T \text{ into } U, U \text{ into } V$$

respectively.

It may then be seen that each of

$$(hg)f,\ h(gf)$$

is a mapping of S into V.

We shall show that they are both equal, *i.e.*, they map each element x of S alike.

We have, by def. of products of mappings,

$$\begin{aligned}[(hg)f](x) &= (hg)[f(x)] \\ &= h\{g[f(x)]\} \\ &= h[(gf)(x)] \\ &= [h(gf)](x)\end{aligned}$$

so that

$$(hg)f = h(gf).$$

3·62. Inversibility of the product of inversible mappings.

If f is a one-one mapping of S onto T and g is a one-one mapping of T onto U so that f and g are both inversible, then gf is also inversible and

$$(gf)^{-1} = f^{-1}g^{-1}.$$

We shall show that

(*i*) gf is one-one, (*ii*) gf is onto, (*iii*) $(gf)^{-1} = f^{-1}g^{-1}$.

(*i*) We have, $a \in S$, $b \in S$,

$$\begin{aligned}(gf)(a) = (gf)(b) &\Longrightarrow g[f(a)] = g[f(b)] \\ &\Longrightarrow f(a) = f(b)\ ;\ g \text{ being one-one} \\ &\Longrightarrow a = b\ ;\ f \text{ being one-one.}\end{aligned}$$

Thus gf is one-one.

(*ii*) Let c be any element of U.

As g is an onto-mapping of T onto U, there exists $d \in T$, such that

$$g(d) = c.$$

Again f being an onto mapping of S onto T, there exists $e \in S$ such that

$$f(e) = d.$$

There exists, therefore $e \in S$ such that

$$\begin{aligned}(gf)(e) &= g[f(e)] \\ &= g(d) = c.\end{aligned}$$

Thus gf is a mapping of S onto U.

As gf is one-one onto, $(gf)^{-1}$ exists.

(*iii*) We have

$$g(d)=c \Longrightarrow d=g^{-1}(c),$$
$$f(e)=d \Longrightarrow e=f^{-1}(d),$$
$$(gf)(e)=c \Longrightarrow e=(gf)^{-1}(c)$$

Now

$$(f^{-1}g^{-1})(c)=f^{-1}[g^{-1}(c)]$$
$$=f^{-1}(d)=e=(gf)^{-1}(c)$$

$$\therefore \quad (gf)^{-1}=f^{-1}g^{-1}.$$

Ex. Show that

$$f(S_1 \cup S_2)=f(S_1) \cup f(S_2)$$
$$f(S_1 \cap S_2) \subseteq f(S_1) \cap f(S_2)$$
$$f^{-1}(T_1 \cup T_2)=f^{-1}(T_1) \cup f^{-1}(T_2)$$
$$f^{-1}(T_1 \cap T_2)=f^{-1}(T_1) \cap f^{-1}(T_2),$$

where, f, is a mapping of a set S into a set T, S_1, S_2 are sub-sets of S and T_1, T_2 are sub-sets of T.

4. Transformations of a set. In the following, we shall be referring to the mappings of a set into (onto) itself as transformations of the set. An important transformation of a set is the Identity transformation which maps each element of the set on itself.

4·1. Permutations. Special types of transformations.

Def. *A one one mapping of a finite set onto itself is called a permutation.*

Thus the one-one onto (inversible) transformations of a finite set will be referred to as Permutations. The number of elements in the finite set is known as the **Degree** of the permutation.

The set of **all** permutations of a set containing, n, elements will be denoted by $\mathbf{P}_n$ and known as the symmetric set of degree n. It may be easily seen that the number of members in the set $\mathbf{P}_n$ is $n!$

4·2. Symbol for a permutation. It will be found convenient to adopt a symbol of the form

$$\begin{pmatrix} a_1 \ldots\ldots a_i \ldots\ldots a_n \\ b_1 \ldots\ldots b_i \ldots\ldots b_n \end{pmatrix} \qquad (1)$$

to denote a permutation. This symbol with two rows is such that the upper row consists of the n elements

$$a_1 \ldots\ldots, a_i, \ldots\ldots a_n$$

of the set permuted and each element in the lower row is the image of the one immediately above the same. Here, of course, each b is some, a, and no, a, occurs more than once as a b. Thus the symbol (1) denotes a permutation σ defined by

$$\sigma(a_1)=b_1, \ldots, \quad \sigma(a_i)=b_i, \ldots, \quad \sigma(a_n)=b_n.$$

It is clear that any given permutation can be written in several ways in as much as we may write the elements of the permuted set in the upper row (lower row) in any manner we like, provided only that we write below (above) each element in the same the corresponding image (pre-image).

Thus, as an example,

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 1 & 5 & 4\end{pmatrix}=\begin{pmatrix}3 & 1 & 2 & 5 & 4\\ 1 & 2 & 3 & 4 & 5\end{pmatrix}=\begin{pmatrix}2 & 4 & 5 & 1 & 3\\ 3 & 5 & 4 & 2 & 1\end{pmatrix}$$

In fact the columns in (1) may be interchanged in any manner we like without any change in the permutation.

Ex. 1. Put down all the transformations of a set containing

(*i*) two, (*ii*) three

elements. Which of these are permutations ?

Ex. 2. What is the total number of transformations of a set containing n elements.

How many of these are permutations.

Ex. 3. Given

(*i*) $\sigma=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 1 & 5 & 4\end{pmatrix}$, $\eta=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 5 & 4 & 3 & 2\end{pmatrix}$;

(*ii*) $\sigma=\begin{pmatrix}2 & 3 & 4 & 5 & 1 & 6\\ 1 & 2 & 5 & 4 & 6 & 3\end{pmatrix}$, $\eta=\begin{pmatrix}4 & 1 & 5 & 6 & 3 & 2\\ 2 & 3 & 6 & 1 & 5 & 4\end{pmatrix}$;

compute the permutations.

$$\sigma\eta,\ \eta\sigma,\ \sigma^{-1},\ \eta^{-1},\ \sigma^{-1}\eta^{-1},\ \eta^{-1}\sigma^{-1},\ (\sigma\eta)^{-1},\ (\eta\sigma)^{-1}.$$

4·3. Cyclic permutations. A permutation σ is called *cyclic* or simply a *cycle* if it is possible to arrange the objects of the set permuted in a row in such a way that the σ-image of each element in the row is the element following the same and that of the last element is the first. For example

$$\sigma=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 1 & 3\end{pmatrix}$$

is a cyclic permutation in as much as we can write the objects permuted in a line, *viz.*,

$$1 \quad 2 \quad 4 \quad 3$$

such that

$$\sigma(1)=2,\ \sigma(2)=4,\ \sigma(4)=3,\ \sigma(3)=1.$$

The permutation

$$\begin{pmatrix} 1 & 2 & 4 & 3 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

is, however, not cyclic.

A cyclic permutation can be conveniently denoted by a one row symbol consisting of the objects of the set permuted placed in such an order that the image of each is the one following it and that of the last is the first. Thus we may write

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}=(1 \quad 2 \quad 4 \quad 3).$$

We can of course have more than one one-row symbol to denote a given cyclic permutation in as much as any of the objects permuted can be put in the first position. Thus, as an example,

$$(1 \quad 2 \quad 4 \quad 3)=(2 \quad 4 \quad 3 \quad 1)=(4 \quad 3 \quad 1 \quad 2)=(3 \quad 1 \quad 2 \quad 4).$$

The number of objects permuted by a cycle is called its *length.*

4·4. Transpositions. A cycle of length *two* is called a transposition. Thus a transposition is a transformation which maps each object on itself excepting two, each of which is mapped on the other.

A cycle of length one implies that the object involved is mapped on itself, *i.e.*, is invariant.

4·5. Permutation expressed as a product of disjoint cycles. Theorem. *Every permutation can be expressed as a product of disjoint cycles.*

The cycles are said to be disjoint if they have no object in common.

Let σ be a given permutation of the set

$$\{a_1, a_2, \ldots\ldots, a_n\}$$

Firstly, we put down cycles of length one each determined by objects, if any, which remain invariant.

Then we start with a non-invariant object and construct a row starting with the same and putting after each element the σ-image of the same. The number of objects being finite, we shall, after a finite number of steps arrive at an element whose σ-image is the one

we started with. This row gives a cycle. In case all the objects have not been included in the cycles so far obtained, we shall start again with one such object and obtain another cycle.

In this manner, after a finite number of steps, we must arrive at a stage such that each object has been included in one or the other cycle. Hence the theorem.

Note. From above it is clear that the manner of decomposing a permutation as a product of disjoint cycles is unique. The order, however, of the cycles can be changed at will, for they are disjoint.

Example.

$$\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&3&4&6&5&1&8&9&7\end{pmatrix}=(5,(1\ 2\ 3\ 4\ 6)(7\ 8\ 9).$$

Ex. Express the following as a product of disjoint cycles.

(*i*) $\begin{pmatrix}1&2&3&4&5&6\\2&4&3&6&1&5\end{pmatrix}$ (*ii*) $\begin{pmatrix}1&3&4&5&6&7&2\\2&1&3&5&7&6&4\end{pmatrix}$.

4·6. Decomposition as a product of transpositions. Theorem. Every permutation can be expressed as a product of transpositions.

Firstly we may see that every cycle can be expressed as a product of transpositions. In fact, we have, as may be easily verified

$$(a_1\ a_2\ a_3.....a_i.....a_k)=(a_1a_k).....(a_1a_i).....(a_1a_2).$$

The result now follows from the facts that every permutation can be expressed as a product of cycles and each cycle can be expressed as a product of transpositions.

We should remember that we are not free to change the order of the transpositions, for they may not be disjoint.

Note. It should be clearly understood that the expression of a permutation as a product of transpositions is not unique. In fact any transposition can again be written as a product of transpositions, *e.g.*,

$$(ab)=(ac)(cb)(ca).$$

There is however one aspect of all these decompositions which remains invariant. This is examined in the following sub section.

Ex. Exhibit the permutations given in the exercises after § 4·2, page 13 as products of transpositions.

4·61. Even and odd permutations. Theorem. *For any manner of expressing a given permutation as a product of transpositions, the number of transpositions is either necessarily odd or even.*

Let σ be any given permutation and let

$$\sigma=(a_1a_2\ldots a_r)(b_1b_2\ldots b_s)(c_1c_2\ldots c_t)\ldots\ldots$$

be the expression of the same as a product of disjoint cycles, r, s, t etc., being the lengths of the cycles. We associate a natural number $N(\sigma)$ with σ defined as follows :

$$N(\sigma)=(r-1)+(s-1)+(t-1)+\ldots$$

so that $N(\sigma)$ is *fixed* for a given σ and denotes the number of transpositions in one manner of expressing σ as a product of transpositions

Let

$$\sigma=(ab)(cd)\ldots\ldots(uv), \tag{1}$$

be any expression of σ as a product of transpositions. We have, then,

$$\sigma(uv)\ldots\ldots(ab)=\varepsilon. \tag{2}$$

where ε denotes the Identity permutation.

We have a **lemma.**

We have, as may be easily verified,

(i) $(u\ p_1\ p_2\ldots p_k v\ q_1\ q_2\ldots q_l)(uv)=(v\ p_1\ldots p_k)(u\ q_1\ldots q_l)$,

(ii) $(u\ v\ p_1\ p_2\ldots p_k)(u\ v)\quad\quad=(v)(u\ p_1\ldots p_k)$,

(iii) $(u\ p_1\ p_2\ \ p_k)(v\ q_1\ q_2\ldots q_l)(u\ v)=(v\ p_1\ p_2\ldots p_k\ u\ q_1\ldots q_l)$,

so that

(1) u and v occur in the same cycle and are not consecutive in (i),

(2) u and v occur in the same cycle and are consecutive in (ii),

(3) u and v occur in different cycles in (iii).

Denoting by η the permutation to the left of the transposition (uv) in each of three cases above, we may see that

$N[\eta(uv)]=k+l=(k+l+1)-1=N(\eta)-1$; in (i),

$N[\eta(uv)]=k=(k+1)-1=N(\eta)-1$, in (ii),

$N[\eta(uv)]=k+l+1=(k+l)+1=N(\eta)+1$, in (iii).

Thus we see that in either case

$$N[\eta(uv)]=N(\eta)\pm1.$$

Applying the result of the lemma successively to (2), we obtain

$$0=N(\varepsilon)=N(\sigma\overbrace{\pm1\pm1\pm1\quad\quad\pm1}^{m\text{ times}}), \tag{3}$$

m denoting the number of transpositions in (1) From (3), we see that

$$N(\sigma)-m$$

is necessarily even so that $N(\sigma)$ and m are either both odd or both even.

Hence the theorem.

Def. *A permutation is said to be odd (even) if, when expressed as a product of transpositions, the number of the same is odd (even).*

Ex. 1. Describe the permutations given at the end of § 4 2, as odd or even.

Ex. 2. Split up the permutations of P_3 and P_4 as products of disjoint cycles and describe each as odd or even.

Ex 3. Show that the product of two permutations both even (odd) is even and the product of an odd with an even permutation is odd.

Ex. 4. Show that the total number of odd permutations in P_n is $\frac{1}{2}(n\ !)$.

The set of all even permutations of degree n will be referred to as the **Alternating set** and denoted by the symbol A_n.

5. Compositions in a set. *We shall now introduce the* very important notion of Binary composition in a set.

Def. *For any given set S, a mapping of the product set $S \times S$ into S is called a binary composition in S.*

In the following, we shall omit the word binary, since every composition which we shall consider will necessarily be binary.

By the def. above, we see that a composition in a set S is a mapping which associates to each ordered pair of members of S a member of S.

Illustrations.

1. The mapping

$$(a, b) \longrightarrow a+b,\ a \in \mathbf{Q},\ b \in \mathbf{Q}$$

which associates to each ordered pair a, b of rational numbers, the rational number $a+b$ is a composition in the set $\mathbf{Q}$ of rational numbers, known as *addition* composition.

2. The mapping

$$(a, b) \longrightarrow ab,\ a \in \mathbf{Q},\ b \in \mathbf{Q}$$

is a composition in the set $\mathbf{Q}$ of rational numbers, known as *multiplication* composition.

3. The mapping which associates to every pair of natural numbers their L.C.M. (G.C.M.) is a composition in $\mathbf{Z}$.

4. If $\mathbf{D}$ denote the set of all vectors (Directed line segments) in space, then

$$(a, b) \longrightarrow a \times b,\ a \in \mathbf{D},\ b \in \mathbf{D}$$

is a composition in $\mathbf{D}$, known as vector multiplication.

5. If Σ denote the set of all sub-sets of a given set S, then

$$(S_1, S_2) \longrightarrow S_1 \cup S_2;\ S_1 \in \Sigma,\ S_2 \in \Sigma$$
$$(S_1, S_2) \longrightarrow S_1 \cap S_2$$

are compositions in Σ known as *Union* and *intersection* compositions respectively.

6. If $\mathbf{P}_n$ denote the set of all permutations of degree n, then

$$(\sigma, \eta) \longrightarrow \sigma\eta,\ \sigma \in \mathbf{P}_n,\ \eta \in \mathbf{P}_n$$

is a composition in $\mathbf{P}_n$, known as Product or Resultant composition.

7. If Σ denote the set of all transformations of a set S, finite or infinite, then

$$(\sigma, \eta) \longrightarrow \sigma\eta,\ \sigma \in \Sigma,\ \eta \in \Sigma$$

is a composition in Σ, known as Product or Resultant composition in Σ.

6. Composition tables for finite sets. A composition in a finite set can be often described by means of what may be called a *composition table*, as we proceed to explain.

We write the elements

$$a_1, a_2, \ldots\ldots, a_r, \ldots\ldots a_n$$

of the set in a horizontal row as well as in a vertical column and put down at the intersection of the row headed by a_s and the column headed by a_r, the element associated to the ordered pair (a_s, a_r).

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_5	σ_6	σ_3	σ_4
σ_3	σ_3	σ_6	σ_1	σ_5	σ_4	σ_2
σ_4	σ_4	σ_5	σ_6	σ_1	σ_2	σ_3
σ_5	σ_5	σ_4	σ_2	σ_3	σ_6	σ_1
σ_6	σ_6	σ_3	σ_4	σ_2	σ_1	σ_5

As an illustration, we consider the set $\mathbf{P}_3$ consisting of all the permutations of degree three. Taking the objects permuted as a, b, c, we may see that the members of $\mathbf{P}_3$ can be written as,

$$\sigma_1 = \varepsilon,\ \sigma_2 = (ab),\ \sigma_3 = (bc),\ \sigma_4 = (ca),$$

$$\sigma_5 = (abc),\ \sigma_6 = (acb).$$

By actual composition, we may see that we have the composition table for the product composition in $\mathbf{P}_3$ as given on the preceding page.

As another illustration, we consider the set consisting of the five elements

$$0, 1, 2, 3, 4 \tag{1}$$

where *composition is the ordinary addition reduced modulo 5.* This means that to any two elements of the set (1), we associate the least non-negative remainder obtained on dividing the ordinary sum by 5. Denoting this composition additively, we have

$$4+3=2,\ 3+3=1.$$

The following is the composition table in question.

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(Addition modulo 5)

We may similarly consider multiplication modulo 5 for which the composition table is given below.

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(*Multiplication Modulo 5*)

Ex. 1. How many different compositions are possible in a set containing (*i*) two elements, (*ii*) three elements, and (*iii*) n elements.

Ex. 2. Consider the set Σ of all sub-sets of a set containing three elements a, b, c and draw up composition tables for the intersection and union compositions in Σ.

Ex. 3. Construct tables for addition and multiplication reduced modulo 6 for the set of elements

0, 1, 2, 3, 4, 5.

Ex. 4. Put down the composition table for the resultant composition in the set of all transformations of a set with two elements.

Ex. 5. Express as products of disjoint cycles all the even permutations of degree 4 on the symbols a, b, c, d and display the composition table for the resultant composition in the same.

7. Algebraic Structures. A set with one or more compositions is known as an **Algebraic system** and we say that the compositions have equipped the set with an **Algebraic structure.**

Notations for Compositions. It has become customary to adopt certain accepted notations for compositions in concrete systems. We shall here mention two notations—*Additive* and *Multiplicative*.

In terms of additive notation, the element of S associated to the element (a, b) of $S \times S$ is denoted by $a+b$ and in terms of multiplicative notation, the element of S associated to (a, b) is ab.

For the resultant composition in a set of transformations, we have already adopted the multiplicative notation.

For the union and intersection composition in the set of all subsets of a set, we have adopted the cup-$\cup$-and cap-$\cap$-notation.

8. Some types of Compositions. We shall now distinguish between some types of compositions.

These types are suggested by the various concrete mathematical systems which arise in applications. We shall describe these types by adopting multiplicative notation for composition.

8·1. Commutative Compositions. *A composition in a set S is called commutative or Abelian if*

$$ab=ba$$

for every $a \in S$, $b \in S$.

Here, as stated above, we have adopted multiplicative notation for the composition.

Illustrations.

1. The addition and multiplication compositions in $\mathbf{Z}$, ($\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$) are commutative.

2. The intersection and union compositions in the set of all sub-sets of a set are both commutative.

3. The resultant composition in the set of all transformations of a set is not commutative.

4. The vector multiplication composition in the set $\mathbf{D}$ of all vectors in space is not commutative.

5. The multiplication composition in the set $\mathbf{M}_n$ ($\mathbf{Q}$) of all $n \times n$ matrices over the set of rational numbers is not commutative.

Ex. Put down tables for all possible compositions in set containing two elements. Which of these compositions are Abelian ?

8·2. Associative Composition. *A composition in a set S is called associative if*

$$(ab)c=a(bc),$$

for every $a \in S$, $b \in S$, $c \in S$.

Illustrations. 1. The addition and multiplication compositions in $\mathbf{Z}$ ($\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$) are associative.

2. The intersection and union compositions in the set of all sub-sets of a set are both associative.

3. The resulant composition in the set of all transformations of a set is associative [Refer § 3·61, page 10].

4. The vector multiplication composition in the set **D** of all vectors in space is *not* associative.

Ex. Put down tables for some possible compositions is a set with three elements, both associative and otherwise.

8·3. Identity for a composition. *An element $e \in S$ is said to be an identity for a composition in S, if*

$$ae=a=ea,$$

for every $a \in S$.

Of course for any given composition in a set, identity may or may not exist so that we may have compositions with or without any identity. In case, however, identity exists, it must be unique. In fact if e, e' be two identities, we have

$ee'=e$ for e' is an identity,

$ee'=e'$ for e is an identity,

so that

$$e=e'$$

Identity element for a composition is also known as *Neutral* element.

8·4. Inversible elements for a composition with identity. An element a of a set S is said to be inversible for a composition with identity, denoted multiplicatively, if there exists $b \in S$ such that

$$ab=e=ba.$$

Also then b is said to be an inverse of a.

It can be shown that for an associative composition with identity, an inversible element possesses *unique* inverse Thus if b, c be two inverses of a, we have

$$(ba)c=ec=c,$$
$$b(ac)=be=b,$$

and

$$(ba)c=b(ac),$$

so that

$$b=c.$$

Illustrations. 1. For the addition composition in **Z**, we have no identity and accordingly no inversible element.

2. For the multiplication composition in **Z**, 1 is the identity and no inversible element other than 1.

3. For the composition in **Z** which associates to every pair of members their L.C.M., 1 is the identity but no element other than 1 is inversible.

4. For the addition composition in **Q**, (**R**, **C**). *0 is the identity* and every element is inversible.

5. For the multiplication composition in Q, (R, C), 1 is the identity and every element other than 0 is inversible.

6. For the vector multiplication composition in the set **D** of all vectors, we have no identity and accordingly the question of inversible elements does not arise.

7. For the intersection composition in the set Σ of all sub-sets of a set S, the members S of Σ is the identity and no element other than S of Σ is inversible.

8. For the union composition in the set Σ of all sub-sets of a set S, the null set $\varphi \in \Sigma$ is the identity and no element other than φ of Σ is inversible.

9. For the resultant composition in the set of all transformations of a set, the identity transformation is the identity and the one-one onto transformations are the only inversible transformations.

10. For the set of elements 0, 1, 2, 3, 4 with composition addition modulo 5 whose table is given on page 19, 0 is the identity and each element is inversible, 0, 4, 3, 2, 1 being the inverses of 0, 1, 2, 3, 4 respectively.

9. Binary relations in a set. We say that a binary relation R is defined in a set S, if for any ordered pair of elements a, b of S, it is meaningful to say whether a has or has not the relation R to b.

We write

$$a\,R\,b$$

if a has the relation R to b.

Note 1. It is important to remember that for a binary relation R defined in a set S, we may, for a given pair of elements a, b to S have

neither $a\,R\,b$ nor $b\,R\,a$.

Two such elements a; b may be said to be *incomaprable* relatively to the relation R and otherwise comparable.

Note 2. Since binary relations are the only relations we shall be concerned with in the course of this book, we shall often omit the word 'Binary' to describe our relations.

Note 3. It may be seen that every relation R in a set S gives rise to a sub-set A of the product set $S \times S$ defined as follows:

$$A = \{(a, b) : a\,R\,b\}.$$

relatio

(i) **reflexive** if $a\,R\,a$ for each $a \in S$,

(ii) **symmetric** if $a\,R\,b \Rightarrow b\,R\,a$ where $a \in S$, $b \in S$

(iii) **anti-symmetric** if $a\ R\ b, b\ R\ a \Longrightarrow a=b$,

(iv) **transitive** if $a\ R\ b, b\ R\ c \Longrightarrow a\ R\ c$,

Ex. Show that a relation defined in a set with two or more elements cannot be simultaneously symmetric and antisymmetric.

Illustrations.

1. The relation $a \geqslant b$ in $\mathbf{Z}$ is reflexive, antisymmetric and transitive. Further any two elements are comparable.

2. It is usual to write

$$a \mid b \text{ where } a \in \mathbf{Z},\ b \in \mathbf{Z}$$

to denote that a is a divisor of b.

This relation $a \mid b$ is reflexive, anti-symmetric and transitive. All pairs of elements are *not* comparable for this divisibility relation.

3. The relation $S_1 \subseteq S_2$ in the set Σ of of sub-sets of a set is reflexive, antisymmetric and transitive. All pairs of elements of Σ are not comparable for this inclusion relation.

4. The relation $a \parallel b$ of parallelism in the set of all straight lines is symmetric as well as transitive. (What about reflexivity ?)

5. The relation $a \perp b$ of perpendicularity in the set of all straight lines is symmetric but neither reflexive nor transitive.

6. The relation 'a loves b' in the set of all human beings is devoid of reflexivity, symmetry as well as transitivity. It is not even anti-symmetric.

9·2. Equivalence relations and Partial order relations.

The two types of relations to be now defined often arise in applications.

Def. 1. *A relation in a set is said to be an equivalence relation. if it is*

(i) *reflexive*, (ii) *symmetric and* (iii) *transitive.*

Def. 2. *A relation in a set is said to be a partial order relation if it is*

(i) *reflexive*, (ii) *anti-symmetric, and* (iii) *transitive.*

Ex. Point out which of the relations occurring in the illustrations to the preceding sub-section are equivalence or partial order relations.

9·21. Equivalence classes induced by an equivalence relation. The importance of equivalence relations depends upon the following theorem

Theorm. *Corresponding to an equivalence relation R defined in a set S, there exists a partition of S in a set of mutually disjoint classes such that*

(i) for any two members a and b of the same class, a has the relation R to b.

(ii) for any two members, a, b of different classes, a does not have the relation R to b.

Consider any member a of S and the class $\mathbf{C}_a$ consisting of members of S in the relation R to a so that we have

$$\mathbf{C}_a = \{ x : x \, R \, a \}$$

The relation R being reflexive, we have

$$a \, R \, a \text{ so that } a \in \mathbf{C}_a.$$

Let b, c be any two members of $\mathbf{C}_a$ so that we have

$$b \, R \, a, \; c \, R \, a.$$

Then we have

$$c \, R \, a \Longrightarrow a \, R \, c \qquad \text{[By symmetry of } R\text{]}$$

$$b \, R \, a, \; a \, R \, c \Longrightarrow b \, R \, c. \qquad \text{[By transitivity of } R\text{]}$$

Thus each member of $\mathbf{C}_a$ is in relation R to each member of the same.

Now either $\mathbf{C}_a = S$ or there exists an element say, p of S not belonging to $\mathbf{C}_a$. Thus in case $\mathbf{C}_a \neq S$, we have a class $\mathbf{C}_p$ constructed *as above and consisting of elements in relation R to p.*

Then, we have

$$\mathbf{C}_a \cap \mathbf{C}_p = \varphi. \qquad (1)$$

To prove this, suppose, that

$$h \in \mathbf{C}_a \cap \mathbf{C}_p.$$

Now

$$h \in \mathbf{C}_a \Longrightarrow h \, R \, a$$

$$h \in \mathbf{C}_p \Longrightarrow h \, R \, p \Longrightarrow p \, R \, h$$

and

$$p \, R \, h, \; h \, R \, a \Longrightarrow p \, R \, a \Longrightarrow p \in \mathbf{C}_a.$$

Thus we arrive at a contradiction and we have accordingly (1).

Hence we obtain the partition as required. The partition of S obtained here is said to correspond to or induced by the equivalence relation R and the classes themselves are known as **equivalence classes** for the relation R.

It should be remembered that each equivalence class can be *thought of as determined by any one member thereof.* In the course

of the book, we shall often denote the equivalence class determined by any element a by the symbol $\bar{a}$.

Note. As a converse to the above we have the following result :

Any partition of a set S into a set of mu ually disjoint classes gives rise to an equivalence relation, the corresponding partition of S for which coincides with the given partition.

In fact the relation R defined as

$$a \, R \, b,$$

if and only if a and b belong to the same class, is the relation in question.

10. Quotient Set. *The set of mutually disjoint equivalence classes in which a set S is partitioned relatively to an equivalence relation R, is said to be the Quotient set of S for the equivalence relation R and is denoted by S/R.*

Ex. 1. The ordinary equality of numbers in **C** is an equivalence relations in **C** what are the corresponding equivalence classes.

Ex. 2. Give examples of Equivalence and Partial order Relations met with in classical Algebra and Analysis.

Canonical set for an equivalence relation. A sub set S_1 of a set S is said to be a canonical set for an equivalence relation R in S if each member of S is in the relation R to one and only one member of S_1. Also each member of S_1 is said to be a representative of the equivalence class to which the same belongs. Thus *a canonical set is a sub-set consisting of the single representatives of the equivalence classes.*

Illustration. Let S denote the set of all straight lines in a plane and R denote the relation of parallelism.

Then a canonical set consists of all lines through a given point.

Natural Mapping of S onto S/R. The mapping of S onto S/R which associates to each element a, of S the equivalence class $\bar{a}$ which is a member of S/R is known as the *Natural mapping* of S onto S/R. The natural mapping is, in general, many-one in as much as any member $\bar{a}$ of S/R is the image of all those elements of S which are in relation R to a.

11. Lattices. Let S be any partially ordered set for a relation which we would denote by $\geqq$.

Upper bound. Least upper bound. If a, b be two given members of S, then $c \in S$ is said to be an upper bound of a, b if

$$c \geqslant a, \; c \geqslant b.$$

Further c is said to be the least upper bound (l. u. b.), if c is an upper bound and further d being any upper bound, we also have

$$d \geqslant c.$$

In case there exists a *l. u. b.* of a, b then it must necessarily be unique. Thus if c and d are two least upper bounds, we have

$$c \geqslant d \text{ as well as } d \geqslant c$$

so that, by virtue of the anti-symmetry of the relation $\geqslant$, we obtain

$$c = d.$$

Lower bound. Greatest lower bound. An element c is said to be a lower bound of a and b if

$$a \geqslant c,\ b \geqslant c$$

and is said to be a greatest lower bound (*g. l. b.*) if in addition to being a lower bound it is such that d being any lower bound, we have

$$c \geqslant d.$$

It can be shown that if *g. l. b.* exists, it is unique.

Lattice. Def. *A partially ordered set is said to be a lattice relative to the partial ordered relation in question, if any two elements of the set have a l. u. b. as well as g. l. b.*

Illustrations. 1. The set Z is a lattice for the divisibility relation $a \mid b$; greatest common divisor being the *l. u. b* and lowest common multiple being the *g. l. b.*

2. The set of all sub-sets of a set is a lattice for the inclusion relation

$$S_1 \supseteq S_2 ;$$

union $S_1 \cup S_2$ being the *l. u. b.* and the intersection $S_1 \cap S_2$ being the *g. l. b.*

CHAPTER II

GROUPS AND THEIR SUB-GROUPS

12. Introduction. Historically the notion of a group arose in connection with linear transformations in Geometry and in the Galois theory of Algebraic equations where we are concerned with groups of permutations of the roots. Moreover, the theory of groups is, at present, one of the richest and most fundamental branches of Abstract Algebra and has played an important part in unifying various apparently unrelated parts of mathematics.

This chapter will also deal with some of the general properties of the sub-groups of a group.

13. Group. Def. *A set G with a composition is called a group (adopting multiplicative notation for the composition) the composition satisfies the following postulates :*

I. *The composition is associative, i.e.,*

$$(ab)c=a(bc)$$

for every triad of elements a, b, c of G.

II. *There exists an identity for the composition,* i.e., there exists an element e of G such that

$$ea=a=ae$$

for every $a \in G$.

III. *Every element is inversible,* i.e., to each $a \in G$, there corresponds an element $b \in G$ such that

$$ab=e=ba.$$

As in § 8·3, page 22 it can be shown that the identity e of a group is unique and that every element a possesses a unique inverse b. Since, we have adopted multiplicative notation for the composition, we would write

$$b=a^{-1}.$$

13·1. Abelian groups. *A group whose composition is commutative is called Abelian or commutative.* Thus for an Abelian group, we have

$$ab=ba,$$

for every $a \in G$, $b \in G$.

13·2. Finite and infinite groups. Order of a finite group. A group whose set is finite is called a finite group and otherwise an infinite group. The number of elements in a finite group is called the *order* of the group. Also an infinite group is said to be of infinite order.

Note 1. It should be thoroughly understood, that associated with any group, we have

(*i*) an underlying set, and

(*ii*) an underlying composition in the underlying set,

such that the three postulates listed above in I, II, III are satisfied. It is not enough to say that a certain set is a group unless the composition is also mentioned. In fact it may be possible to equip any given set with different group structures by defining different compositions. In case, however, there is no ambiguity about the underlying composition in any given context, we may refer to a given set itself as a group.

Note 2. The importance and richness of the concept of a group arises from the fact that in different contexts, we come across groups such that the natures of the elements of the underlying sets and of the underlying compositions are widely different.

Note 3. The element ab^{-1} also denoted by $a \div b$ is called the *right quotient* of a by b. Then $b^{-1}a$ may be referred to as the *left quotient* of a by b.

Note 4. If instead of the multiplicative notation, we adopt the additive one, we shall write

$$a+b \text{ in place of } ab,$$

$$0 \text{ in place of } e \text{ or } 1,$$

$$-a \text{ in place of } a^{-1},$$

$$a-b=a+(-b) \text{ in place of } a \div b = ab^{-1}.$$

It is usual, however, to adopt additive notation for Abelian groups.

The identity is referred to as zero and the inverse of a as the negative of a for groups with additively denoted compositions. Also instead of the word 'quotient' we use the word 'difference' for groups with additively denoted compositions.

Illustrations. We shall now consider some illustrations of groups—finite and infinite, Abelian and non-Abelian—drawn from different contexts.

I. Groups of Numbers.

(*i*) The set **J** of all integers (**Q** of all rational numbers, **R** of all real numbers, **C** of all complex numbers) with addition composition is an infinite Abelian group. The zero is the identity and, $-a$, is the inverse of a.

(*ii*) The set of all non-zero rational (real, complex) numbers with multiplication composition is an infinite Abelian group ; 1 is the identity and $1/a$ the inverse of a.

(*iii*) The set of all positive rational (real) numbers with multiplication composition is an infinite Abelian group.

(*iv*) The set of all n n-th roots of unity with multiplication composition is a finite Abelian group of order n ; n being any given natural number. This group consists of the n numbers

$$e^{2i\pi k/n},\ 0 \leqslant k \leqslant (n-1);$$

1 is the identity and the inverse of $e^{2i\pi k/n}$ is the number $e^{2i\pi(n-k)/n}$

(*v*) The set of all n-th roots of unity where n ranges over the set **Z** of all natural numbers is an infinite Abelian group with multiplication composition.

(*vi*) The set of all unimodular complex numbers is an infinite Abelian group with multiplication composition.

II. Groups-of-Vectors.

(*i*) The set **D** of all vectors with vector addition as the composition is an infinite Abelian group.

(*ii*) The set of all coplanar vectors with vector addition as the composition is an infinite Abelian group.

It may be noted that the set **D** of vectors is not a group for the vector product composition. In fact none of the three postulates for the composition in a group are satisfied for this vector-product composition.

III. Groups of Matrices.

(*i*) The set of all $m \times n$ matrices having their elements as integers (rational, real or complex numbers) is an infinite Abelian group with matrix addition as composition.

(ii) The set of all $n \times n$ non singular matrices having their elements as rational (real or complex) numbers is an infinite non-Abelian group with matrix multiplication as composition.

The set of $n \times n$ non singular matrices having elements as integers is *not* a group for matrix multiplication, for not all such matrices are inversible.

For example, the matrix

$$\begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix}$$

whose determinant is -4 is non-singular but non-invertible in as much there exists no 2×2 matrix with elements as integers whose product with the given matrix is the identity matrix.

An inverse, however, exists with elements as non-integral rational numbers, *viz.*,

$$\begin{bmatrix} -\frac{1}{2} & \frac{1}{2} \\ \frac{3}{4} & -\frac{1}{4} \end{bmatrix}$$

IV. **Groups of transformations.** In this set of illustrations, the composition will always be understood as the *Resultant composition.* Also we may note that the Associativity of this resultant composition has already been proved in § 3·61, page 10 so that all we have to verify is that the resultant of two members of the set is again a member of the set, identity is a member of the set and that every element of the set is inversible.

Symmetric group P_n of degree n.

(i) The set P_n of all permutations of degree n is a finite non-Abelian group of order $n\,!$

This group is known as the **Symmetric group** of degree n.

Taking $n = 1, 2, 3, 4$, we may see that the elements of P_1, P_2, P_3, P_4 are

$$P_1 : \varepsilon,$$

$$P_2 : \varepsilon, (ab)$$

$$P_3 : \varepsilon, (ab), (bc), (ca), (abc), (acb).$$

$$P_4 : \begin{cases} \varepsilon, (ab), (ac), (ad), (bc), (bd), (cd), \\ (abc), (acb), (abd), (adb), (acd), (adc), (bcd), (bdc), (ab)(cd), \\ (bc)(ad), (ca)(bd), \\ (abcd), (abdc), (acbd), (acdb), (adbc), (adcb). \end{cases}$$

(ii) **Alternating group A_n of degree n.**

The set A_n of all even permutations of degree n is a finite non-abelian group, known as Alternating group of order $\frac{1}{2}\,n\,!$

Let

$$\sigma_1, \ldots\ldots, \sigma_k \tag{1}$$

be the members of $\mathbf{A}_n$ so that they are all even permutations. Let $\rho = (ab)$ be any transposition,

Then

$$\sigma_1\rho, \ldots\ldots, \sigma_k\rho \tag{2}$$

are all odd and different. In fact

$$\sigma_i\rho = \sigma_j\rho \longrightarrow (\sigma_i\rho)\rho = (\sigma_j\rho)\rho \longrightarrow \sigma_i(\rho\rho) = \sigma_j(\rho\rho)$$
$$\longrightarrow \sigma_i = \sigma_j.$$

Also any odd permutation say σ can be written as the product of an even permutation with ρ in fact

$$\sigma = \sigma(\rho\rho) = (\sigma\rho)\rho \ ; \ \sigma\rho \text{ being even.}$$

Thus the two sets (1) and (2) exhaust all the permutations of $\mathbf{P}_n$ and accordingly $k = \frac{1}{2}\, n\,!$

The alternating group $\mathbf{A}_3$ consists of the 3 permutations

$$1, (abc), (acb)$$

and $\mathbf{A}_4$ consists of the 12 permutations

$$I, (abc), (acb), (abd), (adb), (acd), (adc), (bcd), (bdc)$$
$$(ab)(cd), (bc)(ad), (ca)(bd).$$

(iii) The set of all bilinear transformations of the infinite complex plane is an infinite non-Abelian group.

Let z denote any complex number. Then a bilinear transformation is given by

$$z \longrightarrow \frac{az+b}{cz+d},$$

where a, b, c, d are arbitrary complex numbers with $ad-bc \neq 0$. It may be shown that this is a one-one mapping of the infinite complex plane onto itself.

Let now ρ, σ be two bilinear transformations defined by

$$\rho : z \longrightarrow \rho(z) = \frac{az+b}{cz+d}. \quad ad-bc \neq 0$$

$$\sigma : z \longrightarrow \sigma(z) = \frac{\alpha z+\beta}{\gamma z+\delta} \quad \alpha\delta-\beta\gamma \neq 0.$$

$$(\sigma\rho)(z) = \sigma[\rho(z)]$$

$$= \sigma\left(\frac{az+b}{cz+d}\right) = \frac{\alpha[(az+b)/(cz+d)]+\beta}{\gamma[(az+b)/(cz+d)]+\delta}$$

$$= \frac{(a\alpha+c\beta)z+(b\alpha+a\beta)}{(a\gamma+c\delta)z+(b\gamma+d\delta)}.$$

Here

$$(a\alpha+c\beta)(b\gamma+d\delta)-(b\alpha+d\beta)(a\gamma+c\delta)$$
$$= (ad-bc)(\alpha\delta-\beta\gamma) \neq 0.$$

Thus $\sigma\rho$ is also a bilinear transformation.

Again

$$z \longrightarrow z = \frac{1z+0}{0z+1},$$

is the identity transformation which is bilinear.

Finally, we may show that

$$z \longrightarrow (b-dz)/(cz-a)$$

is the inverse of ρ. In fact, denoting it by τ, we have

$$(\tau\rho)(z) = \tau[\rho(z)] = \tau\left(\frac{az+b}{cz+d}\right)$$

$$= \frac{b-d[(az+b)/(cz+d)]}{c[(az+b)/(cz+d)]-a} = z = \varepsilon(z)$$

so that $\tau\rho = \varepsilon$.

Similarly $\rho\tau = \varepsilon$.

(iv) The *set of six special bilinear mappings*

$$\rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6$$

defined by

$$\rho_1(z) = z,\ \rho_2(z) = \frac{1}{z},\ \rho_3(z) = 1-z,\ \rho_4(z) = \frac{z}{z-1},\ \rho_5(z) = \frac{1}{1-z},\ \rho_6(z) = \frac{z-1}{z}$$

of the infinite complex plane onto itself is a finite non-abelian group of order 6.

We may carry out the computations and show that following is the composition table for the set in question .

	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
ρ_1	ρ_1	ρ_2	ρ_3	ρ_4	ρ_5	ρ_6
ρ_2	ρ_2	ρ_1	ρ_5	ρ_6	ρ_3	ρ_4
ρ_3	ρ_3	ρ_6	ρ_1	ρ_5	ρ_4	ρ_2
ρ_4	ρ_4	ρ_5	ρ_6	ρ_1	ρ_2	ρ_3
ρ_5	ρ_5	ρ_4	ρ_2	ρ_3	ρ_6	ρ_1
ρ_6	ρ_6	ρ_3	ρ_4	ρ_2	ρ_1	ρ_5

This table shows that ρ_1 is the identity and the elements are all inversible, in fact the inverses of

$$\rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6$$

are

$$\rho_1, \rho_2, \rho_3, \rho_4, \rho_6, \rho_5$$

respectively.

The composition is non-abelian, *e.g.*,

$$\rho_2\rho_3 = \rho_5 \neq \rho_6 = \rho_3\rho_2.$$

(*v*) The set of four special bilinear transformations

$$\sigma_1, \sigma_2, \sigma_3, \sigma_4$$

defined by

$$\sigma_1(z) = z, \sigma_2(z) = -z, \sigma_3(z) = \frac{1}{z}, \sigma_4(z) = -\frac{1}{z}$$

of the infinite complex plane onto itself is an abelian group of order 4 The following is the composition table for this group

	σ_1	σ_2	σ_3	σ_4
σ_1	σ_1	σ_2	σ_3	σ_4
σ_2	σ_2	σ_1	σ_4	σ_3
σ_3	σ_3	σ_4	σ_1	σ_2
σ_4	σ_4	σ_3	σ_2	σ_1

(*vi*) The set of mappings

$$x \longrightarrow ax+b, \qquad a \neq 0$$

of a line onto itself is an infinite non-abelian group, x denoting the abscissa of any point on the line and a, b any real numbers.

(*vii*) The set of all rotations of an equilateral triangle given in position such that the position remains invariant is a finite non-abelian group of order 6.

V. Additive group of integers modulo m. J_m. Conside

the set of m integers

$$0, 1, 2, \ldots \ldots, m-1.$$

We define a composition in this set to be called **addition modulo m** and to be denoted additively such that if a, b are any two members of the set, then $a+b=r$; where r denotes the least positive remainder, $0 \leqslant r < m$, obtained on dividing the *ordinary* sum of a and b by m.

This composition is associative in as much as $(a+b)+c$ as well as $a+(b+c)$ denotes the least positive remainder obtained on dividing the ordinary sum of a, b, c by m.

Also, 0, is the identity and $m-r$ is the inverse of r. Thus the set in question is a finite abelian group of order m.

VI. Multiplicative group of integers modulo a prime p. Consider the set of $(p-1)$ integers

$$1, 2, \ldots\ldots, p-1$$

p being any given prime.

We define a composition in this set to be called **Multiplication modulo p** and denoted multiplicatively such that if a, b, are two arbitrary members of the set, ab, denotes the least positive remainder obtained on dividing the ordinary product of a and b by p. This composition is associative in as much as $(ab)c$ as well as $a(bc)$ denotes the least positive remainder obtained on dividing the ordinary product of a, b, c by p.

Also, 1, is the identity for this composition.

Finally let a, be any member of the set.

Consider the following products

$$1a, 2a, 3a, \ldots\ldots, (p-1)\,a.$$

No two of these can be equal so that one of these must equal 1. Thus if $a'a=1$ we see that a' is the inverse of a.

Thus the set in question with the composition as defined is an Abelian group of order $p-1$.

It should be seen that the condition regarding p to be prime has played an important part here. As against this m could be any *arbitrary* integer when we are considering Additive group of integers modulo m.

14. Some general properties of groups.

I. *For any group* G.

$$ba=ca \Longrightarrow b=c, \quad \textit{(Right cancellation law)}$$

$$ab=ac \Longrightarrow b=c, \quad \textit{(Left cancellation law)}$$

where $a \in G$, $b \in G$, $c \in G$.

We have

$$ba=ca \Rightarrow \begin{cases} (ba)\,a^{-1}=(ca)\,a^{-1} \\ b\,(aa^{-1})=c\,(aa^{-1}) \\ be=ce \\ b=c. \end{cases}$$

We may similarly establish the left cancellation law.

II. Theorem. *For any given pair of elements a, b of a group G, there exist unique elements x, y of G such that*

$$ax=b,\ ya=b.$$

The proof is immediate. It may be shown that

$$x=a^{-1}b,\ y=ba^{-1}.$$

III. General Associative law. For a group, we have

$$(ab)\,c=a\,(bc). \tag{1}$$

We shall now state and prove a generalisation of this Associative law for any arbitrary set of n elements.

Consider first an ordered set

$$a_1, a_2, a_3, a_4$$

of four elements. We can, without changing the order of the elements, consider a number of different associations giving rise to the corresponding product. Thus we may have

$$[(a_1a_2)a_3]a_4,\ (a_1a_2)(a_3a_4),\ [a_1(a_2a_3)]a_4,\ \{a_1[(a_2a_3)a_4]\},\ \text{etc.}$$

The fact now is that as a consequence of the associative law (1) holding for three elements, all these products are equal. In fact this result holds for any arbitrary number of elements.

The reader is advised to put down different forms of products of five elements by adopting different ways of parenthesising.

Theorem. *All the possible products of an ordered arbitrary set of elements of a group arrived at by different manners of parenthesising are equal.*

Consider an ordered set of elements

$$a_1, a_2, \ldots\ldots, a_n.$$

We denote by

$$\prod_{i=1}^{n} a_i$$

the product corresponding to a *special* manner of parenthesising, *viz.* the one defined as follows :

$$\left.\begin{aligned}\prod_{i=1}^{1} a_i &= a_1 \\ \prod_{i=1}^{r} a_i &= \left(\prod_{i=1}^{r-1} a_i\right) a_r\end{aligned}\right\}$$

[Thus for example

$$\prod_{i=1}^{4} a_i = [\{(a_1 a_2) a_3\} a_4]$$

Firstly we shall show that

$$\left(\prod_{i=1}^{r} a_i\right)\left(\prod_{j=1}^{s} a_{r+j}\right) = \prod_{k=1}^{r+s} a_k.$$

By definition of the symbol employed, the equality is true for $s=1$.

Suppose now that the result is true for $s=m$, *i.e.*,

$$\left(\prod_{i=1}^{r} a_i\right)\left(\prod_{j=1}^{m} a_{r+j}\right) = \left(\prod_{k=1}^{r+m} a_k\right).$$

Then

$$\left(\prod_{i=1}^{r} a_i\right)\left(\prod_{j=1}^{m+1} a_{r+j}\right) = \left(\prod_{i=1}^{r} a_i\right)\left[\left(\prod_{j=1}^{m} a_{r+j}\right) a_{r+m+1}\right], \text{ by def.}$$

$$= \left[\left(\prod_{i=1}^{r} a_i\right)\left(\prod_{j=1}^{m} a_{r+j}\right)\right] a_{r+m+1}$$

By the associative law.

$$= \left(\prod_{k=1}^{r+m} a_k\right) a_{r+m+1} \qquad \text{By the supposition.}$$

$$= \prod_{k=1}^{r+m+1} a_k \qquad \text{By def. of the symbol.}$$

The result now follows by the principle of induction.

Consider now the product given by any manner of parenthesising

$$a_1, a_2, \ldots\ldots, a_n.$$

This then is the product of the form

$$bc,$$

where, b, is the product given by some manner of parenthesising

$$a_1, a_2, \ldots, a_t \qquad 1<t<n$$

and, c, is the product given by some manner of parenthesising

$$a_{t+1}, \ldots, a_n.$$

Again, we suppose that the general associative law required to be proved, is true for every number $<n$. Thus

$$b = \prod_{i=1}^{t} a_i, \quad c = \prod_{j=t+1}^{n} a_j.$$

$$\therefore \quad bc = \left(\prod_{i=1}^{t} a_i \right) \left(\prod_{j=t+1}^{n} a_j \right) = \prod_{k=1}^{n} a_k.$$

Thus all products associated with the ordered set of n elements $a_1, \ldots, a_n$ are equal and in fact this product is the same as

$$\prod_{i=1}^{n} a_i$$

defined as above.

Cor. I. Inverse of the product of an arbitrary number of elements.

If a, b be any two elements of a group G, we have

$$(ab)^{-1} = b^{-1}a^{-1}.$$

In fact, by using the general associative law,

$$(ab)(b^{-1}a^{-1}) = [a(bb^{-1})]a^{-1}$$
$$= (ae)a^{-1} = aa^{-1} = e,$$

and also

$$(b^{-1}a^{-1})(ab) = e.$$

By the principle of induction, and the use of the general associative law, we may show that

$$\left(\prod_{i=1}^{n} a_i \right)^{-1} = \prod_{i=1}^{n} \left(a_{n+1-i} \right)^{-1}.$$

This means that *the inverse of the product of any number of elements is equal to the product of the inverses taken in the reverse order.*

Cor. II. General integral powers of elements. Consider the product of n elements each equal to a.

By the general associative law, this product is independent of the manner of parenthesising and there is a unique value of the product. We shall denote this product by the symbol

$$a^n \qquad ; n \text{ being a positive integer.}$$

Now suppose n is a negative integer, say $-m$, so that m is a positive integer. We shall then write by def.,

$$a^n = a^{-m} = (a^m)^{-1}.$$

By Cor. I, we have

$$\underbrace{(a.a\ldots\ldots a)}_{m \text{ times}}{}^{-1} = \underbrace{a^{-1}a^{-1}\ldots\ldots a^{-1}}_{-m \text{ times}}$$

so that

$$(a^m)^{-1} = (a^{-1})^m.$$

Thus we also have

$$a^n = (a^{-1})^m,$$

where $n = -m$,

Also, by def., we shall write

$$a^0 = e.$$

Thus we have given a meaning to the symbol

$$a^n,$$

for every integral value of n, positive negative or zero.

Laws of indices. It may now be easily shown that

$$a^{m+n} = a^m a^n,$$
$$(a^m)^n = a^{mn},$$

for every $a \in G$ and integers m and n.

Additive notation. Adopting additive instead of multiplicative notation, we shall write

$$\underbrace{a+a+\ldots.+a}_{n \text{ times}} \text{ instead of } \underbrace{a\ a\ \ldots.a}_{n \text{ times}}$$

and denote the same by na.

Also if n be a negative integer, we have

$$na = -[(-n)a].$$

Finally

$$0\ a = 0.$$

Here, 0, on the left is the integer zero and, 0, on the right is the identity of the group.

Laws of indices to be now known as laws of multiples, take the form

$$(m+n)a = ma + na$$
$$n(ma) = (nm)a.$$

15. Orders of elements of a group, Def. *The smallest positive integer m, if it exists, such that*

$$a^m = e$$

where a is any element of a group G with identity e, is called the order of a. In the contrary case, we say that the order of a is infinite.

We shall now show that

The order of every element of a finite order group is finite. Consider the positive integral powers

$$a, a^2, a^3, a^4, \ldots$$

of a They are all members of G. Since, however, the order of G is finite, these elements cannot be all different. Suppose that

$$a^k = a^l, \qquad k > l.$$

This gives

$$a^{k-l} = a^k a^{-l} = a^l a^{-l} = a^{l-l} = a^0 = e.$$

There exists, therefore, a positive integer m such that $a^m = e$. Every set of positive integers necessarily having a least member, we find that the set of all those positive integers m such that $a^m = e$ has a least member, called the order of a.

Hence the result.

In the case of infinite groups, some or all elements may have finite order. The identity of a group is always an element of order one It may also be shown that the only element of order one in a group is the identity.

The group formed of all n—th roots of unity ; n ranging over all natural numbers, is such that even though the group is infinite, every element thereof is of finite order.

The elements 1 and -1 are the only two elements of finite order in the infinite multiplicative group of the non-zero rational numbers ; -1 being of order 2.

The following results are capable of easy proofs.

(*i*) *The order of an element a is the same as that of its inverse a^{-1}*

(*ii*) The orders of elements

$$a, x^{-1}ax$$

are the same ; a, x being arbitrary elements of G. This follows from the fact that

$$a^k = (x^{-1}ax)^k = x^{-1}a^k x :$$

for every positive integer k.

(*iii*) The orders of ab, ba are the same; a, b being arbitrary elements of G.

This follows from the equality

$$ab=b^{-1}(ba)b,$$

and the result (*ii*) above.

Ex. 1. Find the orders, of the elements of the groups $\mathbf{P}_3$ and $\mathbf{P}_4$.

Ex. 2. Show that the order of a cyclic permutation of degree n is n.

[If $\sigma=(a_1\, a_2 \ldots a_n)$, then n is the smallest positive integer such that $\sigma^n=\varepsilon$].

16. Commutativity of elements of a group. We shall now establish the general law of commutativity of the elements of a group. We shall prove that *if*

$$a_1, a_2, \ldots\ldots, a_n$$

is any system of n elements, **commutative in pairs** *and*

$$\begin{pmatrix} 1 & 2 & \ldots\ldots & n \\ i_1 & i_2 & \ldots, & i_n \end{pmatrix}$$

is any permutation of the set of n objects

$$1, 2, \ldots\ldots, n,$$

then

$$a_1 a_2 \ldots\ldots a_n = a_{i_1}\ a_{i_2}\ \ldots\ .\ a_{i_n}.$$

The result will be proved by induction.

Suppose that the result is true for products of $n-1$ or less elements.

Two cases arise.

Case I. Let $i_n=n$. We have then

$$a_1 a_2 \ldots a_n = (a_1\, a_2 \ldots a_{n-1})\, a_n,$$

(General Associative law)

$$= \left(a_{i_1}\ a_{i_2}\ \ldots\ldots a_{i_{n-1}} \right) a_{i_n}$$

(By supposition)

$$= a_{i_1}\ a_{i_2}\ \ldots\ldots a_{i_{n-1}}\ a_{i_n}$$

(General Associative law)

Case II. Let $n \neq i_n$, $k=i_n$. Then

$$a_1 a_2 \ldots a_{k-1}\, a_k\, a_{k+1} \ldots a_n$$

$$= (a_1 a_2 \ldots a_{k-1})(a_k a_{k+1} \ldots a_n)$$

(General Associative law)

$$= (a_1\, a_2 \ldots a_{k-1})(a_{k+1} \ldots a_n\, a_k)$$

(By supposition)

$$=(a_1\, a_2 \ldots a_{k-1})[(a_{k+1} \ldots a_n)\, a_k]$$
$$=[(a_1\, a_2\, .\, a_{k-1})\, a_{k+1} \ldots a_n)]\, a_k$$
$$=(a_1\, a_2 \quad a_{k-1}\, a_{k+1}\, ..a.)\, a_k$$
$$=\left(\begin{matrix} a_{i_1} & a_{i_2} & \ldots\ldots & a_{i_{n-1}} \end{matrix}\right) a_{i_n}.$$
$$= a_{i_1}\ a_{i_2} \ldots a_{i_n}$$

Hence the result.

Cor. If a, b are any two elements of a group such th

$$ab=ba,$$

then

$$(ab)^m=a^m b^m,$$

m being any integer.

17. An alternative set of postulates for a group. We shall now show that alternatively a group can be defined as follows:

A set G with a composition is a group if the composition is associative and is such that

(*i*) *for every pair of elements a, b, of G, there exist elements x, y of G such that*

$$ax=b,\ ya=b.$$

To establish the equivalence of the two sets or postulates for a group, we have only to show that the postulates II and III in § 13, page 28 are equivalent to (*i*) above.

It has been already seen in § 14 that II and III imply (*i*).

Suppose now that (*i*) is true for a set G.

Consider an element a of G.

By (*i*), there exist elements, say e_a and f_a such that

$$ae_a=a,\ f_a a=a.$$

Let now b be *any arbitrary* element of G. There exist elements x and y such that

$$ax=b,\ ya=b.$$

We have then

$$be_a=(ya)\ e_a=y\ (ae_a)=ya=b.$$
$$f_a b=f_a\ (ax)=(f_a a)\ x=ax=b.$$

Thus e_a and f_a are two elements such that for *every element* b of G,

$$be_a=b,\ f_a\, b=b.$$

Also, in particular taking b as f_a and e_a, we have

$$f_a e_a=f_a,\ f_a e_a=e_a.$$

$\therefore \qquad f_a = e_a.$

We denote this element by e and see that

$$be=b, \ eb=b$$

for every element b of G. This establishes the postulate II of § 13.

Again, there exist elements z, t of G such that

$$az=e, \ ta=e.$$

$\therefore \ t(az)=te \longrightarrow (ta)z=t \longrightarrow ez=t \longrightarrow z=t.$

Thus for each element a of G, there exists an element z of G such that

$$az=e, \ za=e,$$

so that III of § 13 is a consequence of (*i*).

Ex. Show that a finite set G with a composition is a group if the composition is associative and the right and left cancellation laws hold in G, *i.e.*,

$$ax=bx \longrightarrow a=b, \quad xa=xb \longrightarrow a=b.$$

Show further that the validity of the cancellation laws does not characterise infinite groups and characterises finite groups only.

18. Isomorphism of groups. Notion of an abstract group. We now introduce the very important notion of isomorphic groups.

Let G, G' be two given groups. We suppose that the two underlying compositions in the two groups are both denoted multiplicatively.

Then we say that *G is isomorphic to G' and in symbols*

$$G \cong G',$$

if there exists a one-one mapping f of G onto G' such that

$$f(ab)=f(a)\,f(b) \qquad \ldots (1)$$

for every $a \in G$, $b \in G$; i.e., the image of the product is the product of the images.

Also then, f, is said to be an isomorphic mapping or simply an isomorphism of G onto G'.

Briefly, we may say that f is an isomorphic mapping of G onto G' if it is *one-one onto and* **preserves** *the compositions* in G and G' *i.e.*, is composition preserving.

It may be remarked that if G is isomorphic to G', then there may exist more than one isomorphic mapping of G onto G'.

The condition (1) states that if

$$ab=c, \qquad a \in G, \ b \in G, \ c \in G,$$

then we also have

$$a'b'=c'$$

where

$$a'=f(a),\ b'=f(b),\ c'=f(c)$$

so that each relation between the elements of G is carried over to a corresponding relation between the corresponding elements of G'.

Note. The following points about isomorphic mappings are important. We shall suppose that f is an isomorphic mapping of G onto G'.

(i) *The image of the identity of G is the identity of G', i.e., $f(e)$* is the identity of G'.

Let a' be any element of G' so that there exists $a \in G$ such that

$$f(a)=a'.$$

Now

$$ae=a \Longrightarrow f(a)\,f(e)=f(a) \Longrightarrow a'\,f(e)=f(a)=a',$$
$$ea=a \Longrightarrow f(e)\,f(a)=f(a) \Longrightarrow f(e)\,a'\quad f\,a)=a'.$$

Hence $f(e)$ is the identity in G'.

(ii) *The image of the inverse of any element a is the inverse of the image of a, i.e.,*

$$f(a^{-1})=[f(a)]^{-1}.$$

We have

$$aa^{-1}=e \Longrightarrow f(a)\,f(a^{-1})=f(e),$$
$$a^{-1}a=e \Longrightarrow f(a^{-1})\,f(a)=f(e)$$
$$\therefore \qquad [f\,a)]^{-1}=f(a^{-1}).$$

(iii) *The order of the image of any element is the order of the element, i.e., the order of an element is invariant for isomorphic mappings.*

Suppose that a is an element of G of finite order m so that

$$a^m=e.$$
$$\therefore \qquad [f(a)]^m=f(e),$$

$\therefore$ the order of $f(a)$ is $\leqslant m$. If now the order of $f(a)$ is $k<m$ so that

$$[f(a)]^k=f(e),$$

it follows that

$$f(a^k)=f(e) \Longrightarrow a^k=e$$

so that we arrive at a contradiction.

It can also be shown that if the order of a is infinite, then that of $f(a)$ cannot be finite.

Illustrations. (*i*) The additive group G consisting of all integers

$$\ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\ldots$$

is isomorphic to the additive group G' consisting of all the integral multiples

$$\ldots\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\ldots$$

for any given integer m.

It may be verified that

$$a \longrightarrow ma,\ a \in G,\ ma \in G'$$

is an isomorphic mappings of G onto G'.

(*ii*) Let G denote the additive group of all integers

$$\ldots\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\ldots$$

and G' the multiplicative group of all positive and negative powers of an integer, say, 2, *viz*,

$$\ldots\ldots, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \ldots\ldots$$

Then

$$m \longrightarrow 2^m$$

is an isomorphic mapping of G onto G' The mapping, clearly, is one one and onto and we have also

$$m+n \longrightarrow 2^{m+n} = 2^m . 2^n$$

so that the sum of any two members of G corresponds to the product of the corresponding members of G'.

Here the elements of both the groups are numbers but the composition in G is addition whereas that in G' is multiplication.

(*iii*) The additive group G of all real numbers is isomorphic to the multiplicative group G' of all positive real numbers ;

$$x \longrightarrow e^x,$$

being an isomorphic mapping of G onto G'.

(*iv*) The multiplicative group G consisting of the four fourth roots of unity, *viz.*,

$$1, -1, i, -i$$

is isomorphic to the group G' formed of the four permutations

$$I, (abcd), (ac)(bd), (adcb)$$

each of degree four.

We denote the four permutations by A_1, A_2, A_3, A_4 respectively.

The following are the composition tables for the two groups.

	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

	A_1	A_2	A_3	A_4
A_1	A_1	A_2	A_3	A_4
A_2	A_2	A_1	A_4	A_3
A_3	A_3	A_4	A_1	A_2
A_4	A_4	A_3	A_2	A_1

These show that if we replace

$$f_1,\ f_2,\ f_3,\ f_4$$

by

$$A_1,\ A_2,\ A_3,\ A_4$$

respectively, the composition table for G becomes that for G'.

Thus the mapping g defined by

$$g(f_1)=A_1,\ g(f_2)=A_2,\ g(f_3)=A_3,\ g(f_4)=A_4,$$

is an isomorphic mapping of G onto G'.

Hence the result.

Note. The reader may verify that the following mappings of G onto G' are also isomorphisms :

(i) $f_1\to A_1,\quad f_2\to A_3,\quad f_3\to A_4,\quad f_4\to A_2$

(ii) $f_1\to A_1,\quad f_2\to A_3,\quad f_3\to A_2,\quad f_4\to A_4$

(iii) $f_1\to A_1,\quad f_2\to A_4,\quad f_3\to A_2,\quad f_4\to A_3$

(iv) $f_1\to A_1,\quad f_2\to A_4,\quad f_3\to A_3,\quad f_4\to A_2$

(v) $f_1\to A_1,\quad f_2\to A_2,\quad f_3\to A_4,\quad f_4\to A_3$

(vi) The group G formed by the six bilinear transformations

$$P_1,\ P_2,\ P_3,\ P_4,\ P_5,\ P_6$$

as defined on page 33 and the group P_3 formed of the six permutations

We write

$$A_1=1,\quad A_2=i,\qquad A_3=-1,\qquad A_4=-i$$
$$B_1=I,\quad B_2=(abcd),\quad B_3=(ac)(bd),\quad B_4=(adbc)$$

and set up the composition tables. They are as follows :—

	A_1	A_2	A_3	A_4
A_1	A_1	A_2	A_3	A_4
A_2	A_2	A_3	A_4	A_1
A_3	A_3	A_4	A_1	A_2
A_4	A_4	A_1	A_2	A_3

	B_1	B_2	B_3	B_4
B_1	B_1	B_2	B_3	B_4
B_2	B_2	B_3	B_4	B_1
B_3	B_3	B_4	B_1	B_2
B_4	B_4	B_1	B_2	B_3

It is obvious that if we replace

$$A_1, A_2, A_3, A_4$$

by

$$B_1, B_2, B_3, B_4$$

in the composition table for G, we reproduce the complete composition table in G'.

This shows that the mapping f of G onto G' defined by

$$f(A_1)=B_1,\ f(A_2)=B_2,\ f(A_3)=B_3,\ f(A_4)=B_4$$

is an isomorphism.

Note. The reader may verify that the mapping g of G onto G' defined by

$$g(A_1)=B_1,\ g(A_2)=B_4,\ g(A_3)=B_3,\ g(A_4)=B_2$$

is also an isomorphism.

(v) The group G formed of the four bilinear transformations f_1, f_2, f_3, f_4, defined by

$$f_1(z)=z,\ f_2(z)=-z,\ f_3(z)=\frac{1}{z},\ f_4(z)=-\frac{1}{z}$$

is isomorphic to the permutation group of degree four formed by the four permutations

$$I,\ (ab),\ (cd),\ (ab)(cd).$$

We denote the four permutations by A_1, A_2, A_3, A_4 respectively.

The following are the composition tables for the two groups.

	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

	A_1	A_2	A_3	A_4
A_1	A_1	A_2	A_3	A_4
A_2	A_2	A_1	A_4	A_3
A_3	A_3	A_4	A_1	A_2
A_4	A_4	A_3	A_2	A_1

These show that if we replace

$$f_1,\ f_2,\ f_3,\ f_4$$

by

$$A_1,\ A_2,\ A_3,\ A_4$$

respectively, the composition table for G becomes that for G'.

Thus the mapping g defined by

$$g(f_1)=A_1,\ g(f_2)=A_2,\ g(f_3)=A_3,\ g(f_4)=A_4,$$

is an isomorphic mapping of G onto G'.

Hence the result.

Note. The reader may verify that the following mappings of G onto G' are also isomorphisms :

(*i*) $f_1\to A_1,\quad f_2\to A_3,\quad f_3\to A_4,\quad f_4\to A_2$

(*ii*) $f_1\to A_1,\quad f_2\to A_3,\quad f_3\to A_2,\quad f_4\to A_4$

(*iii*) $f_1\to A_1,\quad f_2\to A_4,\quad f_3\to A_2,\quad f_4\to A_3$

(*iv*) $f_1\to A_1,\quad f_2\to A_4,\quad f_3\to A_3,\quad f_4\to A_2$

(*v*) $f_1\to A_1,\quad f_2\to A_2,\quad f_3\to A_4,\quad f_4\to A_3$

(*vi*) The group G formed by the six bilinear transformations

$$\rho_1,\ \rho_2,\ \rho_3,\ \rho_4,\ \rho_5,\ \rho_6$$

as defined on page 33 and the group P_3 formed of the six permutations

$$I,\ (ab),\ (bc)\ \ (ca),\ (abc),\ (acb)$$

are isomorphic.

We denote the permutations by $A_1, A_2, A_3, A_4, A_5, A_6$ respectively.

On comparing the table given on pages 33 and that for $\mathbf{P}_3$, we may see that the mapping which maps

$$\rho_1, \rho_2, \rho_3, \rho_4, \rho_5\ \rho_6$$

on

$$A_1, A_2, A_3, A_4, A_5, A_6,$$

respectively is an isomorphism.

Note. We may suggest other possible isomorphic mappings of G onto G', also. While doing this we may bear in mind the fact that only elements of equal orders can be mapped on each other through an isomorphic mapping.

Note. It is important to remember that if G, G' be two finite groups, such that f is an isomorphic mapping of G onto G', then, *if we replace each element in the composition table for G by its f-image*, then we obtain the corresponding composition table for G'.

The composition tables of two isomorphic groups are thus the same except for the notations for the elements of the groups.

18·1. Relation of isomorphism in the set of all groups. Theorem. *The relation of isomorphism in the set of all groups is an equivalence relation.*

Reflexivity. We have

$$G \cong G$$

for the identity mapping of G onto itself is an isomorphism.

Symmetry. Let

$$G \cong G',$$

and let f be an isomorphic mapping of G onto G'. As f is a one one onto mapping, f^{-1} exists and is also one onto. We shall show that f^{-1} is an isomorphic mapping of G' onto G.

Let a', b' be any elements of G'. Let

$$f^{-1}(a') = a \in G, f^{-1}(b') = b \in G,$$

so that

$$a' = f(a),\ b' = f(b).$$

We have

$$\begin{aligned} f^{-1}(a'\ b') &= f^{-1}[f(a)\ f(b)] \\ &= f^{-1}[f(ab)] \end{aligned}$$

for f is an isomorphism,

$$\therefore \quad f^{-1}(a'b') = f^{-1}[f(ab)]$$
$$= (ab) = [f^{-1}(a')][(f^{-1}(b')].$$
$$\therefore \quad G' \cong G.$$

Transitivity. Let

$$G \cong G',\ G' \cong G'',$$

and let f, g be the respective isomorphic mappings.

As f, g are one-one onto, $\therefore$ gf is also one-one onto. Further

$$(gf)(ab) = [g(f(ab))],\ a \in G,\ b \in G$$
$$= g[f(a)f(b)]$$
$$= g[f(a)]\ g[f(b)]$$
$$= [(gf)(a)]\ [(gf)(b)].$$

$\therefore$ gf is an isomorphic mapping of G onto G'', so that

$$G \cong G''.$$

Ex. Supply explicit reasons for each of the steps in the above proof.

Note 1. This theorem shows that there exists a partition of all the groups in mutually disjoint classes such that any two groups belonging to the same class are isomorphic and no two groups belonging to two different classes are isomorphic. Any member of a class characterises the entire class so far as the group properties are concerned. Abstract study of groups consists in the determination of properties which relate to an entire class of isomorphic groups and which as such take no account of the particular natures of the elements and of the compositions of the groups in the same class. Accordingly two isomorphic groups are also said to be *Abstractly identical.*

Note 2. The theory of groups had first been developed as a theory of permutation groups in the context of the use of the same in the Galois theory of Algebraic equations. However, it soon came to be noticed that for a major part of the problems, the actual nature of the elements, *viz.*, permutations were not of any special significance and that the only thing of importance is the fact of existence of a composition defined in a set such that certain postulates are satisfied. In this context, the theorem, due to Cayley, to be proved in § 18, page 51 acquires special signifinance. This theorem states that there exists a permutation group isomorphic to every finite group. In other words it means that in every equivalence class of finite order isomorphic groups, there is present a certain permutation group.

Note 3. It may help the reader to recall that the notion of natural numbers has also been arrived at through a process of

abstraction, in as much as each natural number is representative of an equivalence class of finite equivalent sets which are defined such that there exists a one-one mapping of the one onto the other.

Ex. Show that the total number of abstractly different groups of any given finite order is finite. State some upper bound of the total number of abstractly different groups of order n.

17·2. Transference of group structures. Theorem. *If G is a group and G' is a set with a composition (supposed denoted multiplicatively) and there exists a one-one mapping f of G onto G' such that*

$$f(ab) = f(a)\, f(b),\ a \in G,\ b \in G,$$

then G' is also a group isomorphic to G for the composition in question.

It has here to be shown that the composition in G' satisfies the three group postulates.

Associativity. Let a', b', c' be three arbitrary elements of G'. There then exists three elements a, b, c of G such that

$$f(a) = a',\ f(b) = b',\ f(c) = c'.$$

We have

$$\begin{aligned}(a'b')\,c' &= [f(a)\,f(b)]\,f(c)\\ &= [f(ab)]\,f(c)\\ &= f[(ab)c]\\ &= f[a\ (bc)]\\ &= f(a)[f\ (bc)]\\ &= f(a)\ \{[f(b)]\ [f(c)]\} = a'(b'c')\end{aligned}$$

Existence of Identity. If e denote the identity for the group G, we have

$$\begin{aligned}[f(e)]\,a' &= [f\ (e)][f(a)]\\ &= f(ea) = f(a) = a'.\end{aligned}$$

Similarly

$$a'[f(e)] = a'.$$

Thus $f(e)$ which is the image of the identity e in G is the identity in G'.

Inversibility. We have

$$aa^{-1} = e.$$

$$\therefore \quad f(a)\, f(a^{-1}) = f(e),$$

i.e.,

$$a'\, f(a^{-1}) = f(e)$$

Similarly

$$f(a^{-1})\, a' = f(e)$$

Thus $f(a^{-1})$ is the inverse of a' in G', i.e.,

$$(f(a))^{-1} = (a')^{-1} = f(a^{-1})$$

Hence the theorem.

Note. It is important to remember that the image of the identity in G is the identity in G' and also the image of the inverse is the inverse of the image.

The reader may seek a verification of these facts by an examination of the isomorphisms considered in the illustrations (*iv*), *v*), (*vi*) on pages 45-48

18. Cayley's Theorem. Every finite group G is isomorphic to a permutation group.

Suppose that G is a finite group of order n and that its n elements, *in some order*, are

$$a_1, a_2, \ldots\ldots, a_i, \ldots\ldots, a_n. \qquad (1)$$

Let b be any element of G so that it is one of the elements in the set (1).

Then

$$ba_1, ba_2, \ldots\ldots, ba_i, \ldots\ldots, ba_n$$

are all different elements of G and accordingly they are the elements of G written in a possibly different order. In fact

$$ba_i = ba_j \Longrightarrow b^{-1}(ba_i) = b^{-1}(ba_j) \Longrightarrow (b^{-1}b)a_i = (b^{-1}b)a_j$$
$$\Longrightarrow a_i = a_j.$$

Thus

$$a_i \longrightarrow ba_i,$$

is a one-one mapping of the set (1) onto itself so that

$$\begin{pmatrix} a_1 \ldots\ldots\ldots a_i \ldots\ldots\ldots a_n \\ ba_1 \ldots\ldots\ldots ba_i \ldots\ldots\ldots ba_n \end{pmatrix}$$

is a permutation of degree n. We shall denote it briefly by

$$\begin{pmatrix} a_i \\ ba_i \end{pmatrix} \text{ or by } \Pi_b.$$

Thus we see that we have a permutation of degree n, *viz.*, Π_b corresponding to each $b \in G$.

Let G' denote the set of all the permutations Π_b corresponding to the elements of the set (1).

Consider the mapping

$$f : b \longrightarrow \begin{pmatrix} a_i \\ ba_i \end{pmatrix} = \Pi_b$$

of G onto G'.

Firstly, this mapping of G onto G' is one-one for

$$b \neq c \longrightarrow ba_i \neq ca_i \longrightarrow \Pi_b \neq \Pi_c.$$

Again

$$bc \longrightarrow \Pi_{bc} = \begin{pmatrix} a_i \\ bca_i \end{pmatrix} = \begin{pmatrix} ca_i \\ bca_i \end{pmatrix}\begin{pmatrix} a_i \\ ca_i \end{pmatrix}$$

$$= \begin{pmatrix} a_i \\ ba_i \end{pmatrix}\begin{pmatrix} a_i \\ ca_i \end{pmatrix} = \Pi_b \Pi_c.$$

Thus we see that we have a one-one mapping f of the group G onto a set G' of permutations such that

$$f(bc) = \Pi_{bc} = \Pi_b \Pi_c = f(b)\, f(c)$$

Thus G' is a group isomorphic to the group G.

Hence the theorem.

Ex. Proceeding as in the theorem, find the permutation group isomorphic to

(*i*) the multiplicative group of the fourth roots 1, -1, i, $-i$, of unity.

(*ii*) the group of bilinear transformations of order 4 given in Ex. (*v*), page 34,

(*iii*) the group of bilinear transformations of order 6 given in Ex. (*iv*), page 33.

Ex. Show that for an any group G, not necessarily of a finite order,

$$\Pi_a : x \longrightarrow ax \; ; \; x \in G, \; a \in G,$$

is a one-one mapping of G onto itself. Hence prove the generalisation of Cayley's theorem *viz., that every group is isomorphic to a transformation group.*

19. Complexes and Subgroups of a group. The important notion of subgroup of a group will be introduced now. In doing this, we shall continue to adopt the multiplication notation for the group composition.

Let G be any group. Then G also denotes, according to our convention, the set of elements of the group. Let, now, H be any sub set of G. To each ordered pair a, b of H, regarded as members of G, corresponds a member ab of G which may or may not belong to H. If, however, H is such that

$$a \in H, \; b \in H \longrightarrow ab \in H,$$

we say that H is *stable* for the composition in G and that the com-

position in G has *induced* a composition in H and finally the composition in H given by

$$(a, b) \longrightarrow ab,\ a \in H,\ b \in H,$$

is called the **Induced Composition.** Further it may be possible, that H is itself a group for this induced composition and if it be so we say that H is a subgroup of G.

Def. *A non void sub-set H of a group G is called a sub group of G if it is stable for the composition in G and is a group for the induced composition.*

The sub-set consisting of the identity alone and the entire set G constitute two sub-groups of the group G. A sub-group other than these two sub-groups is often known as a *proper* sub-group.

In general, any sub-set H of a group, whether a sub-group or not is known as a *complex.*

Illustrations.

(*i*) The additive group of integers is a sub-group of the additive group of rational numbers.

(*ii*) The multiplicative group of positive rational numbers is a sub-group of the multiplicative group of non-zero real numbers.

(*iii*) The additive group of a system of coplanar vectors is a sub-group of the additive group of all vectors.

(*iv*) The group formed of the six bilinear transformations of the complex plane given is Ex. (*iv*), page 33 is a sub-group of the totality of bilinear transformations of the plane.

(*v*) The set of all n n-th roots of unity is a sub-group of the $2n$ $2n$-th roots of unity ; group composition being the multiplication of numbers.

It may be shown that

(*i*) the identity of a sub-group is the same as that of the group.

(*ii*) the inverse of any element of a sub-group is the same as the inverse of the same regarded as an element of the group.

Ex. Show that the order of any element of a sub-group is the same as that of the element regarded as a member of the group.

Ex. Show that the following sub-sets of elements of $\mathbf{P}_3$ constitute sub-groups of $\mathbf{P}_3$:

(*i*) I, (ab). (*ii*) I, (ca). (*iii*) I, (ab). (*iv*) I, (abc), (acb).

Ex. Show that the following sub-sets of elements of $\mathbf{P}_4$ constitute sub-groups of the same :

(i) I, $(ab)(cd)$, $(ac)(bd)$, $(ad)(bc)$.
(ii) I, (ab), (cd), $(ab)(cd)$.
(iii) I, (ac), (bd), $(ac)(bd)$.
(iv) I, $(abcd)$, $(ac)(bd)$, $(adcb)$, $(ab)(cd)$, $(ad)(cb)$, (ac), (bd).

20. Algebra of complexes of a group. Let Σ denote the set of all complexes of a group G. We shall now seek to introduce some useful binary compositions in Σ and also obtain relations between the same.

Two of the compositions are purely *set theoretic*, i. e., they take no account of the group composition. These are the intersection and the union compositions. Thus if K, L are two members of Σ, we can associate to K and L, the two members of Σ, *viz.*,

$$K \cap L \text{ and } K \cup L.$$

A third binary composition which takes account of the group composition is the one which associates to K, L the complex

$$KL$$

consisting of the elements of G obtained on multiplying each member of K with each member of L. This complex way be referred to as product of K with L.

The following relations can now be established

(i) $$(KL)M = K(LM).$$

(Associativity of multiplication)

(ii) $$K(L \cup M) = KL \cup KM,$$

so that multiplication is distributive with union.

(iii) $$K(L \cap M) \subseteq KL \cap KM.$$

(i) Let x, y, z be any arbitrary elements of K, L, M respectively so that

$$(xy)z \in (KL)M.$$

But

$$(xy)z = x(yz) \in K(LM).$$

$$\therefore \quad (KL)M \subseteq K(LM).$$

Similarly

$$K(LM) \subseteq (KL)M.$$

Thus

$$K(LM) = (KL)M.$$

(ii) Each member of $K(L \cup M)$ is of form xy where

$$x \in K, \; y \in L, \text{ or } y \in M.$$

Now

$$x \in K, y \in L \implies xy \in KL,$$
$$x \in K, y \in M \implies xy \in KM,$$

Thus

$$xy \in KL \cup KM,$$

so that

$$K(L \cup M) \subseteq KL \cup KM. \qquad (1)$$

Also every member of $KL \cup KM$ is of the form xy where

$$xy \in KL \text{ or } xy \in KM$$

so that every member of $KL \cup KM$ is of the form xy where

$$x \in K,\ y \in L \text{ or } M,\ i.e.,\ y \in L \cup M.$$

Thus

$$KL \cup KM \subseteq K(L \cup M). \qquad (2)$$

From (1) and (2), we have

$$K(L \cup M) = KL \cup KM.$$

(iii) Every member of $K(L \cap M)$ is of the form xy where

$$x \in K \text{ and } y \in L \text{ as well as } y \in M$$

so that

$$xy \in KL \text{ as well as } xy \in KM$$

and accordingly $xy \in KL \cap KM$.

Thus

$$K(L \cap M) \subseteq KL \cap KM.$$

In general, however, we do *not* have

$$K(L \cap M) = KL \cap KM$$

This may be seen on considering the complexes K, L, M of $\mathbf{P}_3$, where

$$K \equiv (bc),\ (ab)\ ;\ L \equiv (ab),\ M \equiv (ac).$$

The basic reason for this is that a common member of KL and KM, may arise for different members of K.

Note. It may sometimes happen that two complexes K, L are such that $KL = LK$. In this case say that the two complexes are commutative. It should, however, be remembered that this equality does *not* mean that each element of K is commutative with each element of L. All that this equality means is that if a, b be any arbitrary elements of K and L respectively, then there exist $c \in L$ and $d \in K$ such that

$$ab = cd, \qquad ab \in KL,\ cd \in LK.$$

Note. It is also sometimes necessary to consider a *Unary* composition in Σ which associates to each complex K another complex denoted by K^{-1} and consisting of the inverses of the elements of K.

21. Criterion for a complex to be a sub-group

Theorem. *A necessary and sufficient condition for a complex H of group G to be a sub-group is that*

$$a \in H,\ b \in H \Longrightarrow ab^{-1} \in H.$$

The condition is necessary. Let H be a sub group and let

$$a \in H,\ b \in H.$$

Then we have, H being a sub-group,

$$b \in H \Longrightarrow b^{-1} \in H,$$

$$a \in H,\ b^{-1} \in H \Longrightarrow ab^{-1} \in H.$$

The condition is sufficient. Let $a \in H$.

Then, by virtue of the condition, we have

$$a \in H,\ a \in H \Longrightarrow aa^{-1} = e \in H.$$

Again

$$e \in H,\ a \in H \Longrightarrow ea^{-1} = a^{-1} \in H.$$

Let now b be any member of H, so that as already shown $b^{-1} \in H$.

We have

$$a \in H,\ b^{-1} \in H \Longrightarrow a(b^{-1})^{-1} = ab \in H.$$

Thus H is stable for the composition in G, possesses the identity and the inverse of every element. Hence H is a sub-group of G.

Another form. The condition obtained above may be reformulated as follows :

A necessary and sufficient condition for a complex H to be a sub-group is that

$$HH^{-1} \subseteq H.$$

This result can also be stated in a little sharper form as follow :

A necessary and sufficient condition for a complex H to be a sub group is that

$$H\,H^{-1} = H.$$

All that we have to do is to show that

$$H\,H^{-1} \subseteq H \Longleftrightarrow H\,H^{-1} = H.$$

if H is a sub-group.

21·1. Criteria in the case of finite groups. We shall now prove a form of condition valid for finite groups only.

Theorem. *A necessary and sufficient condition for a complex H of a finite group G to be a subgroup is that*

$$a \in H,\ b \in H \Longrightarrow ab \in H.$$

The necessity for the condition is immediate.

Let $a \in H$. The group G being finite, the order of a is finite, say n. Then

$$a^n = e.$$

$\therefore$ by successive applications of the given criterion, we have

$$a \in H \Longrightarrow a^n = e \in H,\ a^{n-1} = a^{-1} \in H.$$

Thus the condition is also sufficient

Another form. *A necessary and sufficient condition for a complex H of a finite group to be a subgroup thereof is that*

$$HH = H.$$

The proof is left to the reader.

Ex. Show, by means of an example, that the criterion obtained above in § 21·1 is not valid for infinite groups.

[The sub-set of all positive integers of the additive group of integers satisfies the criterion in question without being a subgroup].

21·2. Subgroups of the additive group J of integers. It may be easily verified that the set of all multiples of integers by a given integer m is a sub-group of J. We shall now prove the converse.

Let H be any sub-group of J. If H does not consist of the identity alone, then for any member l of H, $-l$ is also a member of H so that H does contain positive members also. Let m be the smallest of the positive members of H.

Let, now, n be any member of H. There then exist two integers q, r such that

$$n = mq + r,\ 0 \leqslant r < m.$$

As $n \in H$, $mq \in H$,

$\therefore$ $$r = n - mq \in H.$$

$\therefore$ $$r = 0,$$

and $$n = mq.$$

Thus every member of H is a multiple of m.

Also since $m \in H$, $\therefore$ every multiple of $m \in H$.

Hence the result.

Note. It is also sometimes necessary to consider a *Unary* composition in Σ which associates to each complex K another complex denoted by K^{-1} and consisting of the inverses of the elements of K.

21. Criterion for a complex to be a sub-group

Theorem. *A necessary and sufficient condition for a complex H of group G to be a sub-group is that*

$$a \in H,\ b \in H \Longrightarrow ab^{-1} \in H.$$

The condition is necessary. Let H be a sub group and let

$$a \in H,\ b \in H.$$

Then we have, H being a sub-group,

$$b \in H \Longrightarrow b^{-1} \in H,$$

$$a \in H,\ b^{-1} \in H \Longrightarrow ab^{-1} \in H.$$

The condition is sufficient. Let $a \in H$.

Then, by virtue of the condition, we have

$$a \in H,\ a \in H \Longrightarrow aa^{-1} = e \in H.$$

Again

$$e \in H,\ a \in H \Longrightarrow ea^{-1} = a^{-1} \in H.$$

Let now b be any member of H, so that as already shown $b^{-1} \in H$.

We have

$$a \in H,\ b^{-1} \in H \Longrightarrow a(b^{-1})^{-1} = ab \in H.$$

Thus H is stable for the composition in G, possesses the identity and the inverse of every element. Hence H is a sub-group of G.

Another form. The condition obtained above may be reformulated as follows :

A necessary and sufficient condition for a complex H to be a sub-group is that

$$HH^{-1} \subseteq H.$$

This result can also be stated in a little sharper form as follow :

A necessary and sufficient condition for a complex H to be a sub group is that

$$H\,H^{-1} = H.$$

All that we have to do is to show that

$$H\,H^{-1} \subseteq H \Longleftrightarrow H\,H^{-1} = H.$$

if H is a sub-group.

21·1. Criteria in the case of finite groups. We shall now prove a form of condition valid for finite groups only.

Theorem. *A necessary and sufficient condition for a complex H of a finite group G to be a subgroup is that*

$$a \in H,\ b \in H \Longrightarrow ab \in H.$$

The necessity for the condition is immediate.

Let $a \in H$. The group G being finite, the order of a is finite, say n. Then

$$a^n = e.$$

$\therefore$ by successive applications of the given criterion, we have

$$a \in H \Longrightarrow a^n = e \in H,\ a^{n-1} = a^{-1} \in H.$$

Thus the condition is also sufficient

Another form. *A necessary and sufficient condition for a complex H of a finite group to be a subgroup thereof is that*

$$HH = H.$$

The proof is left to the reader.

Ex. Show, by means of an example, that the criterion obtained above in § 21·1 is not valid for infinite groups.

[The sub-set of all positive integers of the additive group of integers satisfies the criterion in question without being a subgroup].

21·2. Sub-groups of the additive group J of integers. It [illegible] f integers by a [illegible] now prove the converse.

Let H be any sub-group of J. If H does not consist of the identity alone, then for any member l of H, $-l$ is also a member of H so that H does contain positive members also. Let m be the smallest of the positive members of H.

Let, now, n be any member of H. There then exist two integers q, r such that

$$n = mq + r,\ 0 \leqslant r < m.$$

As $n \in H$, $mq \in H$,

$\therefore$ $$r = n - mq \in H.$$

$\therefore$ $$r = 0,$$

and $$n = mq.$$

Thus every member of H is a multiple of m.

Also since $m \in H$, $\therefore$ every multiple of $m \in H$.

Hence the result.

22. Algebra of the set of sub-groups of a group. We shall now examine what happens to the compositions of intersection, union and multiplication in the context of the set of all sub-groups of a group G.

22·1. Intersection. Largest subgroup contained in two subgroups. Theorem. *The intersection of any two subgroups of a group G is again a subgroup of G.*

The intersection of two sub-groups cannot be void, for identity is, at least, the element common to both.

Consider any two subgroups

$$H_i, \qquad i=1, 2,$$

Let

$$a \in H_1 \cap H_2,\ b \in H_1 \cap H_2.$$

Now

$$a \in H_1 \cap H_2 \Longrightarrow a \in H_1,\ a \in H_2,$$
$$b \in H_1 \cap H_2 \Longrightarrow b \in H_1,\ b \in H_2.$$

Again, H_1, H_2 being subgroups,

$$a \in H_1,\ b \in H_1 \Longrightarrow ab^{-1} \in H_1,$$
$$a \in H_2,\ b \in H_2 \Longrightarrow ab^{-1} \in H_2.$$

Thus

$$ab^{-1} \in H_1 \cap H_2.$$

Accordingly, we see that

$$a \in H_1 \cap H_2,\ b \in H_1 \cap H_2 \Longrightarrow ab^{-1} \in H_1 \cap H_2$$

Thus, by § 21, page 56, H_2 is a subgroup of G.

Important. $H_1 \cap H_2$ is the *largest* subgroup contained in H_1 as well as H_2 in the sense that it is contained in H_1 as well as H_2 and contains every subgroup contained in H_1 and H_2.

Generalisation. Proceeding, as above, we may also show that *the intersection of any arbitrary family of subgroups of a group is a subgroup.*

22·2. Union. Smallest subgroup containing two sub-groups. The set theoretic union of two subgroups may not be a sub-group. Consider, for example, the two subgroups

$$H_1 \equiv I,\ (ab)\ ;\ H_2 \equiv I,\ (bc)$$

of the symmetric group $\mathbf{P}_3$. Then the complex $H_1 \cap H_2$, consisting as it does of the elements,

$$I, (ab), (bc)$$

is not a subgroup of $\mathbf{P}_3$: This is so atleast because

$$(bc)(ab)=(acb)$$

is not a member of the union $H_1 \bigcup H_2$. We now pose the problem in another way corresponding to the idea of the *largest subgroup contained in H_1 and H_2*. Let us now be interested in the *smallest subgroup containing H_1 as well as H_2*.

We may, infact, view the problem from a little more general point of view and instead of considering the complex $H_1 \bigcup H_2$ consider any arbitrary complex.

22·3. Smallest subgroup containing a complex. Let M be any arbitrary complex of a group G. Then a subgroup H of G is called *the smallest subgroup of G containing M if*

$$H \supseteq M,$$

and any sub-group K containing M contains H.

It can be shown that *the smallest subgroup containing a complex exists and is unique.*

Assuming existence, we see that if H_1, H_2 be two smallest subgroups containing M, we have

$$H_1 \subseteq H_2 \text{ as well as } H_2 \subseteq H_1,$$

so that $H_1=H_2$ and accordingly we have established the uniqueness.

We shall now prove two theorems in this context.

Theorem I. *The intersection of the family of subgroups which contains the complex M is the smallest subgroup containing M.*

The family F, in question, is not void for atleast G is a member of the same.

Let H denote the intersection of the family F so that, as proved in § 22·1, H is a subgroup of G. Also obviously

$$H \supseteq M.$$

If K be any subgroup containing M so that K is a member of F, we have

$$K \supseteq H.$$

Hence the theorem.

Theorem II. *The set of elements of G expressible as products of positive and negative powers of finite numbers of elements of M is the smallest subgroup containing M.*

By § 21, page 56, this set is necessarily a subgroup. Also, clearly, it must be contained in every subgroup containing M.

Hence the theorem.

Def. *The smallest sub-group containing a complex M is said to be the subgroup generated by M and is denoted by $\{M\}$.*

Thus the smallest subgroup containing two subgroups H_1 and H_2 is the subgroup generated by the complex $H_1 \bigcup H_2$ and denoted by the symbol

$$\{H_1 \bigcup H_2\}.$$

This sub group is also known as the **Composite** of the two subgroups H_1 and H_2.

Note. If follows from the results proved above that the set of all the subgroups of a group is a Lattice for the partial order 'Contained in'. The least upper bound and the greatest lower bound of any two members, H_1, H_2 being

$$\{H_1 \bigcup H_2\} \text{ and } H_1 \bigcap H_2$$

respectively.

23. Systems of generators of a group. A sub-set M of a group G is said to be a generating system of G, if the subgroup generated by M coincides with G, *i.e.*,

$$\{M\} = G.$$

Also we say that M generates G.

Of course every arbitrary group possesses atleast one generating system, *viz.*, the group itself.

Also a generating system is said to be **irreducible** or **independent** if no **proper** sub-set of the same generates the group, *i.e.*, if no member of M belongs to the subgroup generated by the set of remaining member of the same. A group may not, however, possess an independent generating system.

It can be shown *that every* **finite** *group possesses an independent generating system.* In fact we can even establish a little more general result, *viz.*, that *every generating system of a finite group possesses an independent generating sub-system.*

Now if M be any generating set of a finite group G, then the set M' obtained on eliminating from M each such element as belongs to the subgroup generated by the remaining members of M is the required independent generating set. Clearly, we can arrive at M' after a finite number of steps.

It should be seen however that a finite group may possess several distinct independent generating systems containing different

numbers of elements. As an example, consider the group G formed by the *six 6th* roots of unity,

$$1, a, a^2, a^3, a^4, a^5,$$

where

$$a = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3}.$$

The orders of the elements a, a^2, a^3, a^3, a^5 respectively are

$$6, 3, 2, 3, 6.$$

We then have

$$G = \{a\},\ G = \{a^5\}.$$

Also

$$G = \{a^2, a^3\}.$$

Also the 2 elements a^2, a^3 form an independent generating system in as much as of these two elements no one lies in the subgroup generated by the other.

An infinite group may *not* possess an independent generating system.

23·1. Independent relations satisfied by the members of the independent generating system of a finite group.

It is clear that the system of all possible *formal* products of positive and negative powers of elements of an independent generating system M is infinite.

Since, however, G is finite, these products of powers cannot all be different and accordingly the members of M must necessarily be subjected to some relations of the form

$$a^{\alpha_1}\ b^{\beta_1}\ c^{\gamma_1}\ldots\ldots = a^{\alpha_2}\ b^{\beta_2}\ c^{\gamma_2}\ldots\ldots,$$

or of the form

$$a^{\alpha}\ b^{\beta}\ c^{\gamma}\ \ldots\ldots = e$$

where $a, b, c, \ldots\ldots$ are different members of G and $\alpha, \beta, \gamma\ldots\ldots$ are some positive or negative integers.

Of course some of these relations must necessarily be of the form

$$a^m = e,\ b^n = e, \text{ etc.},$$

m, n etc., being the orders of a, b, etc. respectively.

It should thus be seen that when we say that a certain generating system is independent, it does not mean that the elements of the system are not connected by relations. In fact, as shown above, such relations *must* exist. Of course, no one element of such a system can be expressed in terms of the others.

Illustrations.

1. *The set of permutations*

$$(12), (13), \ldots\ldots, (1n)$$

is an independent generating set for $\mathbf{P}_n$.

We already know that every member of $\mathbf{P}_n$ is a product of cycles and shall now show that every cycle is a product of members of the given set.

For a cycle containing the symbol 1, we have

$$(1\ a_1a_2\ldots\ldots a_k)=(1a_k)\ldots\ldots\ (1a_2)(1a_1).$$

For a cycle not containing the symbol 1, we have

$$(b_1b_2\ldots\ .\ b_l)=(1b_1)(1b_l)\ldots\ldots(1b_2)(1b_1).$$

Also since each member of the given set of permutations contains an element not contained in any of the others, we see that the given set is independent.

2. *The set of permutations*

$$(123), (124), \ldots\ldots, (12n)$$

is an independent generating set for $\mathbf{A}_n$.

We shall show that the product of every pair of transpositions is expressible as product of the permutations of the given set.

Each even permutation can be expressed as a product of pairs of permutations

$$(12), (13), \ldots, (1n).$$

We have

$$(1i)(12)=(12i),\ i\neq 1,\ i\neq 2$$

$$(1i)(1j)=(1ji)=(12i)\ (12i)\ (12j)\ (12i),$$
$$i\neq 1,\ i\neq 2\ ;\ j\neq 1,\ j\neq 2,\ j\neq i.$$

3. Consider $\mathbf{P}_3$ with elements

$$I,\ (ab),\ (bc),\ (ca),\ (abc),\ (acb).$$

We denote these elements by

$$I,\ A,\ B,\ C,\ D,\ E$$

respectively. As seen above in (1), the elements

$$A=(ab),\ B=(bc)$$

constitute an independent generating system of $\mathbf{P}_3$.

The following independent relations are satisfied by A, B:

$$A^2=I,\ B^2=I,\ (AB)^3=(acb)^3=I.$$

Ex. 1. Exhibit all the permutations of $\mathbf{P}_4$ as products of powers of the permutations

$$(12), (13), (14).$$

Ex. 2. Exhibit all the permutations of $\mathbf{A}_4$ as products of powers of the permutations

$$(123), (124).$$

Ex. 3. Show that the $(n-1)$ permutations

$$(1\ 2),\ (2\ 3),\ldots\ldots,\ (n-1\ n)$$

constitute a set of independent generators of $\mathbf{P}_n$.

We have

$$(23)(12)(23)=(13),\ (34)(13)(34)=(14),\ldots\ldots,$$

$$(n-1\ n)(1\ n-1)(n-1\ n)=(1\ n)$$

so that

$$(12),\ (13),\ldots\ldots,\ (1\ n)$$

belong to the group generated by the given permutations.

Ex. 4. Show that the two permutations

$$\sigma=(1\ 2\ 3\ 4\ldots\ldots n),\ \tau=(12)$$

constitute a set of independent generators of $\mathbf{P}_n$.

We have

$$\sigma^{-1}\tau\sigma=(23),\ \sigma^{-2}\tau\sigma^2=(34),\ \ldots\ldots,\ \sigma^{(n-1)}\tau\sigma^{(n-1)}=(n-1\ n).$$

Ex. 5. A system consisting of the integer 1 generates the additive group **J** of integers. Also a system consisting of any two mutually prime integers is an independent generating system of **J**.

Ex. 6. The system consisting of all prime integers is an independent generating system of the multiplicative group of positive rational numbers.

24. Multiplication of two sub-groups. Theorem. *The product H_1H_2 of two sub-groups of a group is a sub-group if and only if*

$$H_1H_2=H_2H_1.$$

Also then

$$H_1H_2=\{H_1\cup H_2\}.$$

Firstly suppose that

$$H_1H_2=H_2H_1.$$

In the following a_1, b_1, c_1 etc., will denote elements of H_1 and a_2, b_2, c_2 etc., those of H_2.

Now a_1a_2, b_1b_2 are arbitrary elements of the complex H_1H_2.

We have

$$(a_1a_2)(b_1b_2)^{-1}=a_1(a_2b_2^{-1})b_1^{-1}$$

$$=a_1c_2b_1^{-1},\ c_2\in H_2.$$

By virtue of the equality $H_1H_2=H_2H_1$, there exist members d_1, d_2 of H_1, H_2 such that

$$a_1c_2=d_2d_1.$$

$\therefore \quad (a_1a_2)(b_1b_2)^{-1}=d_2(d_1b_1^{-1})=d_2e_1 \in H_2H_1=H_1H_2$

$\therefore$ H_1H_2 is a sub-group. (§ 21)

Now suppose that H_1H_2 is a sub-group.

Let

$$a_1 \in H_1,\ a_2 \in H_2$$

so that

$$a_1=a_1e \in H_1H_2,\ a_2=ea_2 \in H_1H_2.$$

$\therefore \quad a_2a_1 \in H_1H_2.$

Thus

$$H_2H_1 \subseteq H_1H_2. \tag{1}$$

Again, we have

$$a_1a_2 \in H_1H_2.$$

$\therefore \quad (a_1a_2)^{-1}=a_2^{-1}a_1^{-1} \in H_1H_2$, for H_1H_2 is a sub-group.

Also $\quad a_2^{-1}a_1^{-1} \in H_2H_1.$

By virtue of (1), we see that there exist elements

$$b_1 \in H_1,\ b_2 \in H_2 \text{ such that}$$

$$a_2^{-1}a_1^{-1}=b_1b_2.$$

$\therefore \quad (a_1a_2)^{-1}=b_1b_2.$

$\therefore \quad a_1a_2=b_2^{-1}b_1^{-1} \in H_2H_1,$

so that

$$H_1H_2 \subseteq H_2H_1.$$

Hence we obtain

$$H_1H_2=H_2H_1$$

We have now to show that

$$H_1H_2=\{H_1 \cup H_2\}.$$

We have

$$H_1 \subseteq H_1H_2,\ H_2 \subseteq H_1H_2,$$

so that H_1H_2 contains H_1 as well as H_2.

Also it is obvious, that every subgroup which contains H_1 as well as H_2 must necessarily contain H_1H_2.

Thus H_1H_2 is the smallest subgroup containing H_1 and H_2 and hence the result

Note 1. This result shows that in case $H_1H_2=H_2H_1$, then the sub-group $\{H_1 \cup H_2\}$ has a rather simple structure in as much as every

element of the same can be expressed as product of an element of H_1 with an element of H_2.

Note 2. In the case of Abelian groups, the condition $H_1H_2=H_2H_1$ is automatically satisfied so that the complex H_1H_2 is in this case a group.

Adopting additive notation, as is customary for Abelian groups, we see that if H_1, H_2 are two sub-groups, then the set H_1+H_2 consisting of the sums obtained on adding every element of H_1 to every element of H_2 is a sub-group.

* **25. Right and left cosets of a sub-group. Coset decompositions of a group. Congruence modulo a subgroup.** We shall now introduce the very important concepts of right and left cosets of any subgroup. These are also referred to as* Residue classes modulo a subgroup. Cosets are only special types of complexes.

If H be any sub-group, then complexes of the form

$$Ha,\ aH, \qquad a \in G$$

are respectively known as *right and left cosets* of H.

It would thus appear that to each $a \in G$, there corresponds a right coset and a left coset of H. In this context, we prove the following result :

Theorem. *Any two right (left) cosets of a subgroup are either disjoint or identical.*

Also

$$Ha=Hb \Longleftrightarrow ab^{-1} \in H,$$

and

$$aH=bH \Longleftrightarrow b^{-1}a \in H.$$

Lemma. *If h be any element of the subgroup H, then*

$$Hh=H.$$

Let h' be *any* element of H. We have

$$h' \in H \Longrightarrow h'h \in H \Longrightarrow Hh \subseteq H.$$

Further

$$h'=(h'h^{-1})h \in Hh \Longrightarrow H \subseteq Hh.$$

Hence the lemma.

---

*For motivation of this terminology, reference may be made to Note 2 at the end of this section.

We may similarly show that $hH=H$.

Consider now two right cosets

$$Ha \text{ and } Hb$$

and suppose that they are not disjoint. There exist, therefore, elements $h_1 \in H$, $h_2 \in H$ such that

$$h_1 a = h_2 b,$$

or

$$b = h_2^{-1} h_1 a.$$

$$\therefore \quad Hb = H(h_2^{-1}h_1 a) = (Hh_2^{-1}h_1)\, a = Ha. \quad \text{(By the lemma)}$$

Thus we have proved that any two right cosets, if not disjoint, are equal, i.e.,

$$\text{either } Ha \cap Hb = \varphi \text{ or } Ha = Hb.$$

Now suppose that

$$Ha = Hb \text{ so that } a \in Hb.$$

We have

$$a \in Hb \longrightarrow ab^{-1} \in H$$

Conversely,

$$ab^{-1} \in H \longrightarrow Hab^{-1} = H \longrightarrow Ha = Hb.$$

We may similarly prove the corresponding results for left cosets.

25·1. Right coset decomposition. The set of all right cosets of a subgroup H constitutes a decomposition of G into mutually disjoint classes. Also each class i.e., a coset is such that for any two elements a, b of the same class, we have

$$ab^{-1} \in H.$$

The point to be specially noticed is *that the relation* $ab^{-1} \in H$ *is an equivalence relation in* G *such that the set of the corresponding equivalence classes coincides with the set of distinct cosets of* H *in* G.

Let us write

$$a \equiv b \pmod{H},$$

and say that a is congruent to b mod H if and only if

$$ab^{-1} \in H.$$

We shall show that this is an equivalence relation in G.

Reflexivity. We have

$$a \equiv a \pmod{H},$$

for

$$aa^{-1} = e \in H.$$

Symmetry. Let

$$a \equiv b \pmod{H}$$

so that

$$ab^{-1} \in H.$$

We now have

$$(ab^{-1})^{-1} = ba^{-1} \in H \Longrightarrow b \equiv a \pmod{H}.$$

Transitivity. Let

$$a \equiv b \pmod{H},\ b \equiv c \pmod{H}.$$

$$\therefore \quad ab^{-1} \in H,\ bc^{-1} \in H.$$

We now have

$$ac^{-1} = (ab^{-1})(bc^{-1}) \in H \Longrightarrow a \equiv c \pmod{H}.$$

Also, we may easily see that the class of elements congruent to $a \pmod{H}$ is just the coset Ha in as much as we may show that each element of Ha is congruent to, a, and every element congruent to, a, is a member of Ha.

We may similarly show that the relation

$$b^{-1}a \in H,$$

is also an equivalence relation in G such that the set of the corresponding equivalence classes coincides with the set of the left cosets of H in G.

To distinguish between the two equivalence relations giving rise to the right and left coset decompositions, we may refer to them as right and left congruence so that we say that *a is right congruent to b mod H or in symbols*

$$a \equiv_r b \ (mod\ H) \ if\ ab^{-1} \in H,$$

and

$$a \equiv_l b \pmod{H} \ if\ a^{-1}b \in H.$$

Note 1. For commutative groups, the right and left coset decompositions are the same.

Note 2. The reader may be already aware of the notion of congruence in the set of integers modulo a given integer which we come across in elementary number theory.

In that context we say that

$$a \equiv b \pmod{m} \qquad (1)$$

if $(a-b)$ is divisible by m *i.e.*, $a-b$ is of the form km where k is some integer.

Now the multiples of m form a subgroup H of the additive group J of integers. Thus (1) is the same as

$$a-b \in H.$$

This shows that the congruence considered in elementary number theory is only a special case of what we have done here. Also the residue classes modulo any integer m in Number Theory are the same as the cosets of the subgroup of H in the additive group J of integers.

Ex. 1. Show that two right cosets

$$Ha_1, Ha_2$$

are distinct if and only if the two left cosets

$$a_1^{-1}H, a_2^{-1}H$$

are distinct.

Ex. 2. Show that the totality of the inverses of the elements of a right coset is a left coset.

Ex. 3. Given that

$$G=H \cup Ha_2 \cup Ha_3 \ldots\ldots\ldots \cup Ha_k$$

is the right coset decomposition of G relative to H, prove that

$$G=H \cup a_2^{-1} H \cup a_3^{-1} H \ldots\ldots \cup a_k^{-1} H$$

is the left coset decomposition of G relative to H.

Illustrations.

1. If J denote the additive group of integers and H the subgroup of J formed of all the even integers, we have

$$\mathrm{J}=H \cup (H+1),$$

so that we have two cosets; the coset $H+1$ consisting of all the odd integers.

2. If J denote the additive group of integers and H the subgroup of J consisting of all the multiples of a given integer m, we have

$$\mathrm{J}=H \cup (H+1) \cup (H+2) \cup \ldots\ldots \cup H+(m-1).$$

Here the coset $H+a$, $1 \leqslant a \leqslant m-1$), consists of all the integers of the form

$$mq+a\,;\ q \text{ being any integer.}$$

3. If $H \equiv I, (ab)$, we have

$$\mathrm{P}_3=H \cup H(bc) \cup H(ca),$$

as may be easily verified.

26. Lagrange's Theorem. *The order of each subgroup of a finite group is a divisor of the order of the group.*

Let H be any subgroup of a finite group G. We shall consider the right coset decomposition of G relative to H.

We shall first show *that each coset, Ha, has as many members as is the order of the subgroup H.*

Let

$$h_1, h_2, \ldots\ldots, h_m$$

be the m members of H. Then

$$h_1a, h_2a, \ldots\ldots, h_ma$$

are the m members of Ha, all distinct.

In fact

$$h_ia = h_ja \Longrightarrow h_iaa^{-1} = h_jaa^{-1} \Longrightarrow h_i = h_j.$$

Now suppose that

$$G = H \cup Ha_2 \cup \ldots\ldots \cup Ha_k$$

so that the right coset decomposition of G relative to H contains k cosets. Since the cosets are all disjoint, we have

$$\text{order of } G = mk = (\text{order of } H)\ k.$$

Hence the theorem.

Index. *The number of distinct right (left) cosets of any subgroup of a finite group is called the index of the same.*

It follows from above that the *index of every subgroup of a finite group is a divisor of the order of the same.*

It may happen that the number of distinct right (left) cosets of a subgroup of an infinite group is finite. If this be the case, we may refer to this number also as the index of the subgroup.

Cor. *The order of every element of a finite group is a divisor of the order of the group.*

Let $a \in G$ be of order m so that m is the least positive integer such that

$$a^m = e.$$

Then, as is easy to show, the elements

$$a, a^2, a^3, \ldots\ldots, a^{m-1}, a^m = e$$

of G are all distinct and form a subgroup.

This subgroup being of order m, we see that m is a divisor of the order of the group.

Note. The reader may note that there may not exist a subgroup of a finite group whose order is any given divisor of that of the given group.

27. Cyclic groups. Def. *A group capable of being generated by a single element is called Cyclic or Monogenic.*

The each element of a cyclic group is some positive or negative power (multiple) of the generator; the composition being denoted multiplicatively (additively).

Adopting multiplicative notation for the group composition, we may see that the elements of the cyclic group $\{a\}$ are all of the form

$$\ldots, a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, \ldots$$

not necessarily all distinct. Also with additive notation, the elements of the cyclic group $\{a\}$ are all of the form

$$\ldots, (-3)a, (-2)a, (-1)a, 0a = 0, 1a, 2a, 3a, \ldots$$

not necessarily all distinct.

Of course, we can have finite as well as infinite cyclic groups.

Clearly a cyclic group is necessarily Abelian.

Illustrations.

1. The additive group J of integers is an infinite cyclic group; the integer, 1, being the generator.

2. The set of all n nth roots of unity is a finite cyclic group with multiplication composition;

$$\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

being a generator.

In the following, it will be shown that there *exists only one abstract infinite cyclic group and also only one abstract finite cyclic group of a given order n.*

Ex. 1. Show that the additive group of integers which are multiples of a given integer m is an infinite cyclic group isomorphic to the cyclic additive group of integers.

Ex. 2. Show that the four permutations

$$I, (abcd), (ac)(bd), (adcb)$$

form a cyclic group isomorphic to the multiplicative group necessarily cyclic formed by the four numbers $\pm 1, \pm\sqrt{-1}$.

Ex. 3. Show that every isomorphic image of a cyclic group is again cyclic.

Ex. 4. Show that every independent generating system of a non-cyclic finite group must contain atleast two elements.

27·1. Structure of Cyclic groups. Let

$$G=\{a\}$$

be any given cyclic group. Adopting multiplicative notation, the elements of G are of the form

$$a^m,$$

m being any integer ; positive, negative or zero.

Now two cases arise :

Case I. *No two different powers of, a, are the same.* In this case the cyclic group is necessarily infinite.

Consider the mapping

$$m \longrightarrow a^m$$

of the set of all integers onto G. This mapping is one-one for

$$a^m=a^n \Longrightarrow m=n, \text{ as is assumed.}$$

Also

$$m+n \longrightarrow a^{m+n}=a^m a^n,$$

so that the mapping, in question, is isomorphic also.

Thus in this case *the cyclic group is infinite and isomorphic to the additive group* **J** *of integers.*

Case II. *Some two powers of a are the same.*

Then as shown in § 15, page 40 where we have introduced the concept of the order of an element of a group, there exists a least non-negative integer n such that

$$a^n=e.$$

Then it can be shown that no two elements of the set

$$a, a^2, a^3, \ldots\ldots, a^{n-1}, a^n=e \qquad (1)$$

are the same and that each power of, a, is equal to some member of the set (1).

Now, if

$$1\leqslant i\leqslant n,\ 1\leqslant j\leqslant n,\ i>j, \text{ then}$$

$$a^i=a^j \Longrightarrow a^{i-j}=e, \qquad 0<i-j<n$$

so that we arrive at a contradiction.

Again suppose that, s, is any given integer. There, then exist two integers q and r such that

$$s=nq+r, \qquad 0\leqslant r<n.$$

$$a^s=a^{nq+r}=a^{nq}a^r=a^r.$$

Thus we see that in this case the cyclic group consists of the n elements given in (1).

Suppose now that G' denotes the multiplicative group formed of the n nth roots of unity. Then

$$a^m \longrightarrow e^{2\pi i m/n}$$

is, as may be easily seen, an isomorphic mapping of G onto G'.

Thus in this case *the cyclic group is finite of order n and is isomorphic to the multiplicative group of the n nth roots of unity.*

We have thus proved the following :

I. An infinite cyclic group is isomorphic to the additive group J of integers.

II. A finite cyclic group of order n is isomorphic to the multiplicative group of the n nth roots of unity.

27·2. Generators of Cyclic groups. Let $G=\{a\}$ be any given cyclic group.

If G is infinite, we know, that no two different powers of a represent the same element. This means that no element a^m, $m\neq 1$ can be a generator of G in this case, for no member a^{1m} of the cyclic group $\{a^m\}$ can be the same as a. Thus *there exists one and only one generator for a given infinite cyclic group.*

Now suppose that G is finite of order n. We shall show that a^m is a generator of G if and only if m is less than n and prime to n.

Let

$$H=\{a^m\} \qquad \text{where } 1\leqslant m\leqslant n.$$

Surely

$$H \subseteq G.$$

Suppose now that m is prime to n. There then exist two integers u, v such that

$$um+vn=1.$$

$$\therefore \quad a^{um}\ a^{vn}=a.$$

$$\therefore \quad (a^m)^v=a \text{ for } a^{vn}=e.$$

This shows that

$$G \subseteq H.$$

Thus $H=G$ and a^m is a generator of G.

Conversely suppose that a^m is a generator of G so that there exists an integer u, $1\leqslant u\leqslant n$ such that $a^{mu}=a$. Now

$$a^{mu}=a \Longrightarrow mu-nv=1 \text{ for some } v.$$

Thus m is prime to n.

27·3. Sub-groups of cyclic groups. We shall naturally be considering the cases of infinite and finite cyclic groups separately.

Case of infinite cyclic group. We shall prove that *every proper subgroup of an infinite cyclic group is itself an infinite cyclic group and accordingly isomorphic to the group itself.*

Each member of a proper subgroup H of a cyclic group

$$G=\{a\}$$

is some power of a.

Let m be the smallest non-negative integer such that

$$a^m \in H,$$

and let a^k be any arbitrary element of H.

There exist integers q and r such that

$$k=mq+r, \qquad 0\leqslant r<m.$$

$$\therefore \qquad a^k=a^r \in H.$$

Hence $r=0$ and we have

$$k=mq$$

so that k is a multiple of m

Also, conversely, if k is any multiple of m, we have

$$a^k \in H.$$

Thus

$$H=\{a^m\},$$

consisting, as it does, of the elements

$$\ldots\ldots, a^{-2m}, a^{-m}, a^{0m}=e, a^m, a^{2m}, a^{3m}\ldots\ldots$$

The equality of any two members of the set would imply that

$$a^m=e$$

which, however, is not the case. Thus H is an infinite cyclic group.

Note. It follows from § 21·1, page 57, that every subgroup of the additive group J of integers which is an infinite cyclic group can be written as $\{m\}$ where m is some integer; of course m is its generator.

Case of finite cyclic group. We shall prove that *every subgroup of a finite cyclic group is cyclic and to every divisor l of the order of the group, there corresponds one and only one subgroup of that order.*

Let

$$G=\{a\},$$

be a cyclic group of order n so that it consists of the n elements

$$a, a^2, \ldots\ldots, a^{n-1}, a^n=e.$$

As in the preceding case, we may show that if m be the smallest positive integer such that a^m belongs to a given subgroup H of G, then H consists of the powers of a^m so that

$$H=\{a^m\},$$

and is accordingly cyclic.

Let l be the order of H so that l is the least positive integer such that

$$a^{ml}=(a^m)^l=e,$$

and H consists of the l distinct elements

$$a^m, a^{2m}, \ldots\ldots, a^{lm}=e.$$

Of course, by Lagrange's theorem, l is a divisor of n.

Thus every subgroup is cyclic.

Suppose now that l is any divisor of n and let $n=lm$. Then

$$H=\{a^m\},$$

is a subgroup of G of order l.

It can be obtained on taking the mth power of each element of G.

We have now to show that this is the *only* subgroup of order l. This is a consequence of the fact that a subgroup of order l is obtained when we take the mth powers of the elements of G where $m=n/l$ so that its relationship to G is given in terms of the order l only.

Ex. $H=\{a^m\}$ is a subgroup of an infinite cyclic group $G=\{a\}$; show that

$$G=H \cup Ha \cup Ha^2 \cup \ldots\ldots \cup Ha^{m-1}.$$

Also prove that the index of every subgroup of an infinite cyclic group is finite and there corresponds to each positive integer m one and only one subgroup of index m.

274. **Theorem I.** *Every group of prime order is cyclic.* Assuming that the order is greater than one, let, a, be any element other than the identity. Then

$$H=\{a\}$$

is a cyclic subgroup of the given group. The order of H being a divisor of p, other than 1, is necessarily p and as such, we have

$$G=H.$$

Hence the result.

275. **Theorem II.** *Every finite group of composite order possesses proper subgroups.*

Let G be a finite group of order lm where neither l nor m is 1.

If G is cyclic and a is any generator thereof, then

$$H=\{a^l\}$$

is a proper sub-group of G ; being of order m.

Suppose now that G is non-cyclic. Then each independent generating system of G will contain atleast 2 elements. Then the cyclic group generated by any member of an independent generating system is a proper sub-group of the given group.

28. Groups of coincidence rotations of regular bodies.

By a coincidence rotation of a rigid body is meant a rotation such that as a result of the body being subjected to the same, the final position comes to coincide with the initial. Clearly a coincidence rotation of a rigid body is a special transformation of the aggregate of points of the body.

It may be known to the reader that a rotation of a rigid body about a point O can be specified by the symbol (l, α) where, l, denotes the axis of rotation and, α, the angle of rotation.

Also, we may note that in this case, there exists a unique well-defined rotation which maps two given points A, B onto two given points P, Q such that

$$\angle AOB=\angle POQ.$$

It may be seen that the set of all coincidence rotations of a regular body is a group for the resultant composition.

1. The resultant of two coincidence rotations is again a coincidence rotation.

2. The resultant composition of coincidence rotations is associative, the same being true for the composition of mappings in general.

3. Identical mapping is the identical coincidence rotation.

4. The rotation $(l,-\alpha)$ is the inverse of any given rotation (l, α).

We shall now consider the natures of the groups of coincidence rotations of some regular bodies.

28·1. Equilateral triangle.

The rotations to be denoted by

$$f_1, f_2, f_3$$

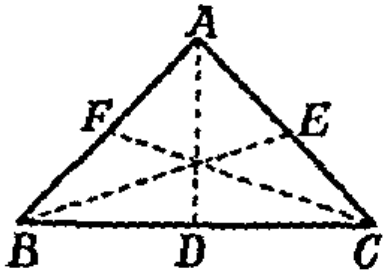
about the line through the centre perpendicular to the plane through angles

$$0,\ 2\pi/3,\ 4\pi/3$$

and the rotations to be denoted by

$$\rho_4,\ \rho_5,\ \rho_6$$

about the altitudes AD, BE, CE of the triangle each through π are clearly six coincidence rotations of the triangle.



Also we may see by the considerations outlined in the introduction that these six are the only possible coincidence rotations of the equilateral triangle.

We may also easily set up a group of permutations isomorphic to this group of coincidence rotations. Taking into consideration the manner in which the set of vertices A, B, C is mapped onto itself for any coincidence rotation, we have the following correspondence between the group of rotations and the symmetric group $\mathbf{P}_3$ whose elements permute the objects A, B, C

$$\rho_1 \longleftrightarrow I$$
$$\rho_2 \longleftrightarrow (ABC)$$
$$\rho_3 \longleftrightarrow (ACB)$$
$$\rho_4 \longleftrightarrow (BC)$$
$$\rho_5 \longleftrightarrow (CA)$$
$$\rho_6 \longleftrightarrow (AB).$$

Thus *the group of coincidence rotations of an equilateral triangle is isomorphic with* $\mathbf{P}_3$.

28·2. Square. The rotations

$$\rho_1,\ \rho_2,\ \rho_3,\ \rho_4$$

about the line through the centre, perpendicular to the plane through angles

$$0,\ \frac{\pi}{2},\ \pi,\ \frac{3\pi}{2}$$

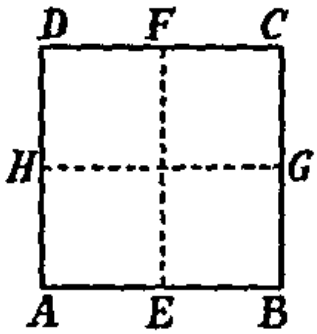
and the rotations

$$\rho_5,\ \rho_6,\ \rho_7,\ \rho_8$$

about the lines

$$EF, GH, AC, BD$$

each through π are the 8 coincidence rotations of the square.



The following correspondence exhibts an isomorphism between this group of 8 coincidence rotations and a certain sub-group of the symmetric group $\mathbf{P}_4$ of the four symbols A, B, C, D.

$$\rho_1 \longleftrightarrow I, \qquad \rho_2 \longleftrightarrow (ABCD)$$
$$\rho_3 \longleftrightarrow (AC)(BD), \quad \rho_4 \longleftrightarrow (ADCB)$$
$$\rho_5 \longleftrightarrow (AB)(CD), \quad \rho_6 \longleftrightarrow (BC)(AD)$$
$$\rho_7 \longleftrightarrow (BD), \qquad \rho_8 \longleftrightarrow (AC).$$

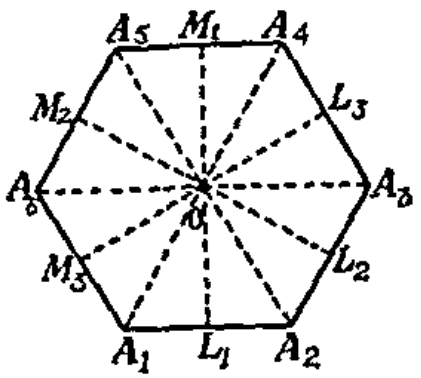
Thus the group of coincidence rotations of a square is isomorphic to the group of permutations

$$I, (ABCD), (AC)(BD), (ADCB)$$
$$(AB)(CD), (BC)(AD), (BD), (AC),$$

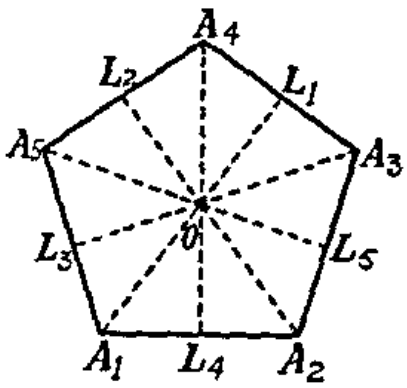
28·3. Regular polygon of n sides.

Rotations about the line through the centre perpendicular to the plane through angles

$$0, \frac{2\pi}{n}, \frac{4\pi}{n}, \ldots\ldots, \frac{2(n-1)\pi}{n}$$



$(n=6)$



$(n=5)$

are n of the coincidence rotations. We denote these by

$$\rho_1, \rho_2, \ldots\ldots, \rho_n.$$

If n is odd, we have n more coincidence rotations consisting in the rotations through the angle π about the n lines joining the centre to the n vertices.

On the other hand, if n is even, we have n coincidence rotations consisting in the rotations through angle π about the $\frac{1}{2}n$ lines through the centre perpendicular to pairs of parallel sides and the $\frac{1}{2}n$ lines through the centre joining pairs of vertices collinear with the same.

We denote these by

$$\sigma_1, \sigma_2, \ldots\ldots, \sigma_n.$$

Also we may verify that these $2n$ are the only coincidence rotations of a regular polygon of n sides so that *the group of coincidence rotations of a regular polygon of* n sides *is of order* $2n$. It is known as the **Dihedral group** of order $2n$ and will, in the following, be denoted by $\mathbf{D}_{2n}$.

For the sake of clarity, we exhibit the isomorphism of the groups $\mathbf{D}_{10}$ and $\mathbf{D}_{12}$ of coincidence rotations of regular polygons of 5 and 6 sides and certain permutation groups of 5 and 6 symbols.

Dihedral group of order 10

$\rho_1 \longleftrightarrow I,$

$\rho_2 \longleftrightarrow (ABCDE), \quad \rho_3 \longleftrightarrow (ACEBD),$

$\rho_4 \longleftrightarrow (ADBEC) \quad \rho_5 \longleftrightarrow (AEDCB)$

$\sigma_1 \longleftrightarrow (BE)(CD), \quad \sigma_2 \longleftrightarrow (AC)(DE)$

$\sigma_3 \longleftrightarrow (BD)(AE), \quad \sigma_4 \longleftrightarrow (CE)(AB)$

$\sigma_5 \longleftrightarrow (AD)(BC).$

Dihedral group of order 12

$\rho_1 \longleftrightarrow I \qquad \rho_2 \longleftrightarrow (ABCDEF)$

$\rho_3 \longleftrightarrow (ACE)(BDF), \quad \rho_4 \longleftrightarrow (AD)(BE)(CF)$

$\rho_5 \longleftrightarrow (AEC)(BFD), \quad \rho_6 \longleftrightarrow (AFEDCB)$

$\sigma_1 \longleftrightarrow (BF)(CE), \quad \sigma_2 \longleftrightarrow (AC)(DF),$

$\sigma_3 \longleftrightarrow (BD)(AE) \quad \sigma_4 \longleftrightarrow (AB)(DE)(CF),$

$\sigma_5 \longleftrightarrow (BC)(AD)(EF) \quad \sigma_6 \longleftrightarrow (CD)(BE)(AF).$

EXERCISES

1. Discuss the statement : 'There is one and only one abstract group of prime order p.'

2. A set of 2×2 matrices consists of all those which have either cube roots of 1 on the principal diagonal and zeros elsewhere or zeros on the principal diagonal and cube roots of 1 elsewhere. Show that the whole set forms a group G. Arrange the matrices in sub-sets putting all those of the same order in the same sub-set. Obtain as many Abelian subgroups of G of order 6 as you can. Are there any non-abelian subgroups of G of order 6 ?

3. Prove that the six matrices of the form

$$\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}, \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$

where $\theta=0,\ 2\pi/3,\ 4\pi/3$ determine a group isomorphic to the symmetric group $\mathbf{P}_3$ and interpret this fact geometrically.

4. If a finite group possesses an element of order 2, prove that it possesses an odd number of such elements.

5. Show that the positive integers modulo 13 form a cyclic group of order 12 under multiplication. Find subgroups of orders 2, 3, 4 and 6. Are these isomorphic with sets of positive integers modulo 3, 4, 5 and 7 under multiplication.

6. Show that the matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} w & 0 \\ 0 & w^2 \end{bmatrix}, \begin{bmatrix} w^2 & 0 \\ 0 & w \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & w^2 \\ w & 0 \end{bmatrix}, \begin{bmatrix} 0 & w \\ w^2 & 0 \end{bmatrix}$$

where $w^3=1,\ w\neq 1$ form a group of order six with respect to matrix multiplication.

Prove also that this group is isomorphic with $\mathbf{P}_3$ the symmetric group of degree 3.

7. A group G has the property that for each element a of G.

$$a^2=e\ ;\ e \text{ being the identity.}$$

Prove that G is abelian.

8. A group G has independent generators a, b which are subject to

$$a^2=b^2=(ab)^2=I.$$

Show that G is of order 4 and write down its multiplication table.

A group H has independent generators A, B which are subject to

$$A^3=B^3=(AB)^2=I.$$

Show that

$$AB,\ BA,\ A^2BA^2$$

(which you may assume to be distinct) are all of order 2 and that together with I they constitute a subgroup K isomorphic to G. Show also that

$$GA=AG.$$

9. Prove that the set of all rotations of a rigid body which leave a point O fixed form a group.

OX, OY are mutually perpendicular axes fixed in space. A is a rotation of 90° about OX and B a rotation of 180° about OY. Prove that $AB=BA^3$ and find the order of the group generated by A and B.

[Simple geometrical considerations will show that

$$(x, y, z)\ A=(x, -z, y),$$
$$(x, y, z)\ B=(-x, y, -z)\ ;$$

where (x, y, z) denote a point with rectangular cartesian coordinates x, y, z.]

10. Show that the operations of reflections in a line and reflection in a point on the line are commutative.

[Taking the given line as $x-$axis and the fixed point as the origin, we have

$$(x, y, z)\ A=(x, -y, -z), (x, y, z)\ B=(-x, -y, -z)$$

where A denotes reflection in $x-$axis and B denotes reflection in the origin O.]

11. Prove that those elements of a group G which commute with the square of a given element b of G form a sub-group N and those which commute with b itself form a sub-group of N.

12. G is a finite group ; S is the complex formed of elements of G of order exactly p, where p is prime. Prove that the relation "y is a power of x" is an equivalence relation in S. Deduce that the number of elements in S is divisible by $p-1$.

If G is a group of order 35, prove that G contains elements of order 5 and elements of order 7.

CHAPTER III

GROUPS AND THEIR NORMAL SUBGROUPS

29. Introduction. This chapter will be devoted to the developments of the important notion of a distinguished type of subgroups known as **Normal.** This notion was first introduced by Galois in connection with his work on the Algebraic theory of equations.

The notion of the homomorphic images of a group which has an important bearing on that of Normal sub-groups will also form the subject matter of discussion in this chapter.

Finally, the notion of the automorphism of a group and that of Direct Product which has an important role to play in the Structure theory of groups will be taken up.

30. Conjugate elements. Equivalence relation of conjugacy in a group. Let G be any group.

Def. *An element $a \in G$ is said to be conjugate to $b \in G$ if there exists some element $x \in G$ such that*

$$a = x^{-1}bx.$$

In symbols we denote this as

$$a \overset{c}{=} b.$$

Also if $a = x^{-1}bx$, we may say that a is the **transform** of b by x.

It will now be shown that this relation of conjugacy is an equivalence relation.

Reflexivity. We have

$$a \overset{c}{=} a \text{ for } a = e^{-1}ae.$$

Symmetry. Let

$$a \overset{c}{=} b,$$

so that there exists $x \in G$ such that

$$a = x^{-1}bx.$$

Rewriting this as

$$b = xax^{-1} = (x^{-1})^{-1}a(x^{-1}),\ x^{-1} \in G,$$

we have

$$b \overset{c}{=} a,$$

Transitivity. Let

$$a \overset{c}{=} b, \quad b \overset{c}{=} c.$$

There exist, therefore, two elements x, y of G such that

$$a = x^{-1}bx, \quad b = y^{-1}cy,$$

These give

$$a = x^{-1}y^{-1}\, c\, yx = (yx)^{-1}\, c\, (yx)\ ;\ yx \in G,$$

so that

$$a \overset{c}{=} c.$$

30·1. Classes of conjugate elements. The relation of conjugacy in G being an equivalence relation, we obtain the corresponding division of G into mutually disjoint equivalence classes known as *classes of conjugate elements* such that

(*i*) any two members of the same class are conjugate,

(*ii*) no two members of different classes are conjugate.

We shall use the symbol $\bar{a}$ to denote the class of elements conjugate to a. Of course the class $\bar{a}$ can be determined by any member of the same.

We may see that

$$\bar{a} = \bar{b} \Longleftrightarrow a \overset{c}{=} b$$

30·2. Self-conjugate elements. Def. *An element $a \in G$ is said to be self-conjugate, if a is the only member of the class $\bar{a}$ of elements conjugate to a.* Thus, a, is self-conjugate if and only if

$$a = x^{-1}ax \text{ for every } x \in G,$$

i.e.,

$$xa = ax \text{ for every } x \in G.$$

Thus a *self-conjugate element of a group may be characterised as one which commutes with every element of the group.*

A self-conjugate element is also sometimes known as an **Invariant** element.

Central of a group. Theorem. *The set Z of all self-conjugate elements of a group G is a sub-group of the group.*

Let

$$a \in Z, \ b \in Z$$

so that

$$xa = ax \tag{1}$$

$$bx = xb \tag{2}$$

CHAPTER III

GROUPS AND THEIR NORMAL SUBGROUPS

29. Introduction. This chapter will be devoted to the developments of the important notion of a distinguished type of subgroups known as **Normal.** This notion was first introduced by Galois in connection with his work on the Algebraic theory of equations.

The notion of the homomorphic images of a group which has an important bearing on that of Normal sub-groups will also form the subject matter of discussion in this chapter.

Finally, the notion of the automorphism of a group and that of Direct Product which has an important role to play in the Structure theory of groups will be taken up.

30. Conjugate elements. Equivalence relation of conjugacy in a group. Let G be any group.

Def. *An element $a \in G$ is said to be conjugate to $b \in G$, if there exists some element $x \in G$ such that*

$$a = x^{-1}bx.$$

In symbols we denote this as

$$a \overset{c}{=} b.$$

Also if $a = x^{-1}bx$, we may say that a is the **transform** of b by x.

It will now be shown that this relation of conjugacy is an equivalence relation.

Reflexivity. We have

$$a \overset{c}{=} a \text{ for } a = e^{-1}ae.$$

Symmetry. *Let*

$$a \overset{c}{=} b,$$

so that there exists $x \in G$ such that

$$a = x^{-1}bx.$$

Rewriting this as

$$b = xax^{-1} = (x^{-1})^{-1}a(x^{-1}),\ x^{-1} \in G.$$

we have

$$b \overset{c}{=} a.$$

Transitivity. Let

$$a \overset{c}{=} b, \quad b \overset{c}{=} c.$$

There exist, therefore, two elements x, y of G such that

$$a = x^{-1}bx, \quad b = y^{-1}cy,$$

These give

$$a = x^{-1}y^{-1}\, c\, yx = (yx)^{-1}\, c\, (yx)\ ;\ yx \in G,$$

so that

$$a \overset{c}{=} c.$$

30·1. Classes of conjugate elements. The relation of conjugacy in G being an equivalence relation, we obtain the corresponding division of G into mutually disjoint equivalence classes known as *classes of conjugate elements* such that

(*i*) any two members of the same class are conjugate,

(*ii*) no two members of different classes are conjugate.

We shall use the symbol $\bar{a}$ to denote the class of elements conjugate to a. Of course the class $\bar{a}$ can be determined by any member of the same.

We may see that

$$\bar{a} = \bar{b} \Longleftrightarrow a \overset{c}{=} b$$

30·2. Self-conjugate elements. Def. *An element $a \in G$ is said to be self-conjugate, if a is the only member of the class $\bar{a}$ of elements conjugate to a.* Thus, a, is self-conjugate if and only if

$$a = x^{-1}ax \text{ for every } x \in G,$$

i.e.,

$$xa = ax \text{ for every } x \in G.$$

Thus a *self-conjugate element of a group may be characterised as one which commutes with every element of the group.*

A self-conjugate element is also sometimes known as an **Invariant** element.

Central of a group. Theorem. *The set Z of all self-conjugate elements of a group G is a sub-group of the group.*

Let

$$a \in Z, \ b \in Z$$

so that

$$xa = ax \tag{1}$$

$$bx = xb \tag{2}$$

for every $x \in G$.

From (2), we have

$$b^{-1}bxb^{-1}=b^{-1}xbb^{-1}$$

i.e.,

$$xb^{-1}=b^{-1}x. \tag{3}$$

From (1) and (3),

$$\begin{aligned} x(ab^{-1}) &= (xa)b^{-1} \\ &= (ax)b^{-1} \\ &= a(xb^{-1}) = a\,(b^{-1}x) = (ab^{-1})x \end{aligned}$$

so that

$$a \in Z,\ b \in Z \Longrightarrow ab^{-1} \in Z.$$

Hence Z is a sub-group of G. This sub-group is known as the **central** of G.

The central of a group may also be described as the set of elements commutative with every element of the group.

Ex. Show that identity is a self conjugate element for every group. Also show that each element of an Abelian group is self-conjugate.

31. Illustration. Classes of conjugate elements of $\mathbf{P}_n$. We shall first obtain a condition for two elements of $\mathbf{P}_n$ to be conjugate as a preliminary to the determination of the classes of conjugate elements in $\mathbf{P}_n$.

Let

$$\rho=\begin{pmatrix} a_i \\ b_i \end{pmatrix},\quad \sigma=\begin{pmatrix} c_i \\ a_i \end{pmatrix}$$

be two arbitrary members of $\mathbf{P}_n$. We take σ^{-1} in the form

$$\sigma^{-1}=\begin{pmatrix} b_i \\ d_i \end{pmatrix}$$

Here the lower row of σ is the upper one of ρ and the upper row of σ^{-1} is the lower one of ρ and the others are suitably adjusted.

We then have

$$\begin{aligned} \sigma^{-1}\rho\sigma &= \begin{pmatrix} b_i \\ d_i \end{pmatrix}\begin{pmatrix} a_i \\ b_i \end{pmatrix}\begin{pmatrix} c_i \\ a_i \end{pmatrix} \\ &= \begin{pmatrix} c_i \\ d_i \end{pmatrix} = \begin{pmatrix} \sigma^{-1}(a_i) \\ \sigma^{-1}(b_i) \end{pmatrix} \end{aligned}$$

Thus the transform $\sigma^{-1}\rho\sigma$ of

$$\rho=\begin{pmatrix} a_i \\ b_i \end{pmatrix}$$

by σ is given by

$$\begin{pmatrix} \sigma^{-1}(a_i) \\ \sigma^{-1}(b_i) \end{pmatrix}$$

so that the *transform is obtained on replacing each object in the two-row representation of* ρ *by the corresponding* σ^{-1}*-image.*

This rule also holds if we represent ρ as product of disjoint cycles. Thus let

$$\rho=(a_1a_2\ldots\ldots ah)(b_1b_2\ldots\ldots b_l)(c_1c_2\ldots\ldots c_m)\ldots\ldots$$

Then we can represent ρ by the two-row symbol as follows :

$$\rho=\begin{pmatrix} a_1\ a_2\ldots\ldots a_k & b_1\ b_2\ldots\ldots b_l & c_1\ c_2\ldots\ldots c_m \\ a_2\ a_3\ldots\ldots a_1 & b_2\ b_3\ldots\ldots b_1 & c_2\ c_3\ldots\ldots c_1 \end{pmatrix}\ldots\ldots$$

$$\therefore\ \sigma^{-1}\rho\sigma=\begin{pmatrix} \sigma^{-1}(a_1)\ldots\ldots\sigma^{-1}(a_k)\ \sigma^{-1}(b_1)\ \ldots\ldots\sigma^{-1}(b_l) \\ \sigma^{-1}(a_2)\ldots\ldots\sigma^{-1}(a_1)\ \sigma^{-1}(b_2)\ \ldots\ldots\sigma^{-1}(b_1)\ldots\ldots \end{pmatrix}$$

$$=(\sigma^{-1}(a_1)\ \sigma^{-1}(a_2)\ldots\ldots\sigma^{-1}(a_k)\ \sigma^{-1}(b_1)\ \sigma^{-1}(b_2)\ldots\ldots\sigma^{-1}(b_l)$$

so that $\sigma^{-1}\rho\sigma$ is obtained on replacing each element by its σ-image in the expression for ρ as a product of disjoint cycles.

Ex. 1. If

$$\rho=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&5&4&3&8&7&6&1\end{pmatrix},\ \sigma=\begin{pmatrix}1&2&3&4&5&6&7&8\\7&6&5&1&8&3&2&4\end{pmatrix}$$

then

$$\sigma^{-1}\rho\sigma=\begin{pmatrix}4&7&6&8&3&2&1&5\\7&3&8&6&5&1&2&4\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&1&5&7&4&8&3&6\end{pmatrix}.$$

The result may also be directly verified.

Ex. 2. If

$$\rho=(134)(56)(2789),\ \sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\7&8&9&6&4&5&2&3&1\end{pmatrix}$$

then

$$\sigma^{-1}\rho\sigma=(985)(64)(7123).$$

We now introduce a definition.

Similar permutations. Two permutations are said to be similar, if each can be expressed as a product of the same number of disjoint cycles and the two sets of cycles can be put in one-one correspondence such that the corresponding cycles have the same length.

The reader my see that in Ex. 1 and Ex. 2, above ρ and $\sigma^{-1}\rho\sigma$ are similar permutations.

We shall now prove that *two permutations of* $\mathbf{P}_n$ *are conjugate if and only if they are similar.*

From the manner of finding the transform of a permutation, we see that two conjugate permutations of $\mathbf{P}_n$ are similar so that only converse remains to be established.

Consider now two similar permutations

$$\rho=(a_1.....a_k)\quad(b_1.....b_l)(c_1.....c_m).....$$
$$\tau=(a'_1.....a'_k)(b'_1.....b'_l)(c'_1.....c'_m).....$$

Then

$$\sigma^{-1}=\begin{pmatrix} a_1.....a_k & b_1 .... b_l & c_1.... c_m..... \\ a'_1.....a'_k & b'_1.....b'_l & c'_1.....c'_m..... \end{pmatrix}$$

is such that

$$\tau^{-1}\rho\sigma=\tau,$$

Hence the result.

(i) The classes of conjugate elements of $\mathbf{P}_3$ are

$$I$$
$$(ab),\ (bc),\ (ca)$$
$$(abc),\ (acb)$$

so that we have three classes of conjugate elements.

(ii) The classes of conjugate elements of $\mathbf{P}_4$ are

$$I$$
$$(ab),\ (ac),\ (ad),\ (bc),\ (bd),\ (cd)$$
$$(abc),\ (acb),\ (abd),\ (adb),\ (acd),\ (adc),\ (bcd),\ (bdc)$$
$$(ab)(cd),\ (bc)(ad),\ (ca)(bd),$$
$$(abcd),\ (abdc),\ (acbd),\ (acdb),\ (adbc),\ (adcb)$$

so that we have 5 classes of conjugate elements.

Ex. 1. How many classes of conjugate elements of $\mathbf{P}_5$ do we have ?

Ex. 2. Show that identity is the only self-conjugate element of the symmetric group $\mathbf{P}_n$.

32. Structure of classes of conjugate elements. Normaliser of an element. Let a be any member of a group G. Then the class $\bar{a}$ of conjugate elements determined by a is the totality of elements

$$x^{-1}ax$$

when x runs through G. The elements $x^{-1}ax$ arising for different elements, x, may not necessarily be different so that we may have

$$x^{-1}ax=y^{-1}ay \text{ even though } x\neq y.$$

Naturally our first interest lies in those elements x of G for which we have

$$x^{-1}ax=a,$$

i.e.,

$$ax=xa.$$

Thus an element $x \in G$ transforms, a, to itself if and only if x is commutative with a.

We shall now show that *all such elements, x, as are commutative with a given element, a, form a sub-group of G.*

Let us denote by N the complex formed by all those elements of G which commute with, a, and let

$$x \in N, y \in N,$$

so that

$$xa=xa, ya=ay.$$

We have

$$ay=ya \longrightarrow y^{-1}a=ay^{-1},$$

$$\therefore \quad a(xy^{-1})=(ax)y^{-1}$$
$$=(xa)y^{-1}=x(ay^{-1})=x(y^{-1}a)=(xy^{-1})a.$$

Thus we see that

$$x \in N, y \in N \longrightarrow xy^{-1} \in N.$$

Accordingly N is a sub-group of G. This sub-group is known as the **Normaliser** of, a, in the group G.

Now suppose that two elements x, y of G are such that they transform, a, alike, *i.e.*,

$$x^{-1}ax=y^{-1}ay.$$

This implies

$$yx^{-1}a=ayx^{-1}$$

i.e., that

$$yx^{-1} \in N.$$

From this it follows that we have the equality

$$Nx=Ny$$

of the two right cosets Nx and Ny.

Again if $z \in N$ so that $zx \in Nx$, we have

$$(zx)^{-1}a(zx)=x^{-1}(z^{-1}az)x=x^{-1}ax$$

so that each element of the coset Nx transforms a just as x does.

Thus we see that *two elements x, y of G transform, a, alike if and only if they belong to the same right coset of the Normaliser N of a.*

To each right coset of the Normaliser of a, corresponds a single element conjugate to a, in as much as each element of the same right coset transforms a alike and two elements of different right cosets transform a differently.

Thus there exists a one-one mapping of the set of all right cosets of the Normaliser of a, onto the class $\bar{a}$ of elements conjugate to a.

From this it follows that for *a finite group G, the number of elements in the class $\bar{a}$ of elements conjugate to a is equal to the index of the Normaliser of a in G.* In particular, we see that the order of a class of conjugate elements of a finite group divides the order of the group.

Ex. 1. Show that the normaliser of a self-conjugate element of a group is the group itself.

Ex. 2. Show that $N \supseteq \{a\}$, N being the normaliser of a.

Ex. 3. Find the number of elements conjugate in $\mathbf{P}_n$ to a cyclic permutation of length n and show that the only permutations in $\mathbf{P}_n$ commutative with a cyclic permutation of length n are the powers of the cycle.

Ex. 4. Show that the only self-conjugate element of $\mathbf{P}_n$ is the identity.

Ex. 5. *Show that a finite group whose order is some power of a prime number necessary possesses self-conjugate elements other than the identity.* In other words, show that the central of a group of prime power order is distinct from the identity subgroup.

Let G be a group of order p^m ; p being some prime integer. Let

$$n_1, n_2, \ldots\ldots, n_k$$

denote the numbers of elements in the different classes of conjugate elements of G. We have then

$$p^m = n_1 + n_2 + \ldots\ldots + n_k. \qquad (1)$$

Now each particular n_i, being a divisor of p^m, is either 1 or a multiple of p. Also atleast one n_i is 1, being the number of elements in the class of elements conjugate to the identity.

Thus atleast p of the summands on the right of (1) must be equal to 1 each so that there are atleast p self-conjugate elements.

33. Conjugate Complexes. Equivalence relation of conjugacy in the set Σ of all complexes of a group.

Extending the ideas of the preceding section, we say that a complex K is conjugate to a complex L, if there exists an element $x \in G$, such that

$$K = x^{-1} Lx.$$

It may be shown that this relation of conjugacy in the set Σ of all complexes of a group G is an equivalence relation. Accordingly, we have a partition of Σ into mutually disjoint classes of conjugate complexes.

As in the preceding section, we may prove the following two results :

I. *The set of all those elements of G which commute with a given complex K is a subgroup of G.*

This subgroup is called the **Normaliser** of K in G.

II. There exists a one-one mapping of the set of right cosets of the normaliser N of K and the class of complexes conjugate to K such that two members of the same right coset transform K alike and any two members of different cosets transform K differently.

Ex. 1. Show that any two conjugate complexes of a finite group contain the same number of elements.

Ex. 2. Show that each member of the class H of complexes conjugate to a sub-group H is a sub-group, *i e.*, each complex conjugate to a sub-group is a sub-group.

33·1. Classes of conjugate sub-groups. Naturally it is of importance to attend to the class of complexes conjugate to a sub-group. We shall show that *each complex conjugate to a sub-group is a sub-group.*

Let H be any sub-group and, x, any element of G. We shall show that the complex

$$x^{-1}Hx \tag{1}$$

conjugate to H is actually a sub-group.

Let

$$x^{-1}h_1x,\ x^{-1}h_2x\ ; \qquad h_1 \in H,\ h_2 \in H$$

be any two members of the complex (1).

Then we have

$$(x^{-1}h_1x)(x^{-1}h_2x)^{-1} = x^{-1}(h_1h_2^{-1})x \in x^{-1}Hx,$$

so that

$$x^{-1}Hx$$

is a sub-group.

This result may also be stated as follows : Each member of the class H of complexes conjugate to a sub-group H is a sub-group.

Illustrations. I. The three sub-groups :

$$H_1 \equiv \{I, (bc)\} \; ; \; H_2 \equiv \{I, (ca)\} \; ; \; H_3 \equiv \{I, (ab)\}$$

constitute a class of conjugate sub-groups of $\mathbf{P}_3$.

The sub-group

$$\mathbf{A}_3 \equiv \{I, (abc), (acb)\}$$

is the only member of the class of conjugate sub-groups of $\mathbf{P}_3$ determined by $\mathbf{A}_3$.

II. (*i*) The sub-groups

$$\{I, (ab)\} \; ; \; \{I, (ac)\} \; ; \; \{I, (ad)\} \; ; \; \{I, (bc)\} \; ; \; \{I, (bd)\} \; ; \; \{I, (cd)\}$$

constitute a class of conjugate sub-groups of $\mathbf{P}_4$.

(*ii*) The class of conjugate sub-groups of $\mathbf{P}_4$ obtained by the sub-group

$$\{I, (abc), (acb)\}$$

consists of the sub-groups

$$\{I, (abc), (acb)\} \; ; \; \{I, (abd), (adb)\} \; ;$$
$$\{I, (acd), (adc)\} \; ; \; \{I, (bcd), (bdc)\}.$$

(*iii*) The normaliser of the sub-group with elements I, (ab) of the group $\mathbf{P}_4$ is the sub-group with elements

$$I, (ab), (cd), (ab)(cd).$$

The normaliser being of order 4, the class of conjugate sub-groups must, therefore, consist of 6 sub-groups.

The normaliser of the sub-group with elements

$$I, (abc), (acb)$$

is the sub-group with elements

$$I, (abc), (acb), (ab), (bc), (ca).$$

The normaliser of the sub-group consisting of the eight elements

$$I, (abcd), (ac)(bd), (adcb), (ab)(cd), (ad)(bc), (ac), (bd)$$

coincides with itself and hence the corresponding class of conjugate sub-groups consists of three sub-groups, *viz.*, the given one and two more.

We are now led to the important notion of **Self-conjugate** sub-groups analogous to that of self-conjugate elements.

34. Self-conjugate sub-groups. Def. *A sub-group H of G is said to be self-conjugate, if H is the only member of the class H of sub-groups conjugate to H.*

A self-conjugate sub-group is also often referred to as **Normal** or **Invariant.** We shall generally be using the word 'Normal'.

34·1. Different Characterisations of Normal sub-groups. It is possible to have a number of different useful characterisations of a Normal sub-group. Here below, we give the same.

I. A normal sub-group of a group is commutative with every element of the group. Thus

H is a normal sub-group if and only if

$$x^{-1}Hx = H \text{ for every } x \in G,$$

i.e.,

$$Hx = xH \text{ for every } x \in G.$$

II. The right and left coset decompositions of a group relative to a normal sub-group are the same.

III. Every element conjugate to an element of a normal sub-group is an element of the same, i.e. if H is a normal sub-group, we have

$$a \in H \Longrightarrow \bar{a} \subset H.$$

Now H is normal sub-group if and only if

$$x^{-1}Hx = H \text{ for every } x \in G$$

so that

$$x^{-1}ax \in H$$

for every $a \in H$ and every $x \in G$.

IV. A normal sub-group is a union of complete classes of conjugate elements.

Follows from III.

Ex. 1. Show that a normal sub-group is commutative with every complex. Also show that if M is a normal and N is any sub-group of a group G, then MN is also a normal sub-group of G.

Ex. 2. H is a normal sub-group of G and K is a sub-group such that

$$H \subset K \subset G.$$

Show that H is also a normal subgroup of K.

Ex. 3. Show that every sub-group of an Abelian group is normal.

34·2. Simple groups. Every group G possesses at least two normal sub-groups *viz.*, G and the identity. There exist groups for which these are the only normal sub-groups. Such groups are known as simple.

Def. *A group having no proper normal sub-group is called a simple group.*

Illustrations.

1. Every group of prime order is simple. In fact such a group has no proper sub-groups.

2. No cyclic group of composite order is simple, for such a group necessarily possesses a proper sub-group which again is necessarily normal.

3. No Abelian group of composite order is simple.

4. There exist simple non-abelian groups of composite orders. It will later on be shown that *the alternating group* $\mathbf{A}_5$ *of degree 5 whose order is 60 is simple.*

Ex. 1. Show that $\mathbf{A}_3$ is the only proper normal subgroup of $\mathbf{P}_3$.

Ex. 2. Show that $\mathbf{A}_4$ and the sub-group consisting of the permutations

$$I,\ (ab)(cd),\ (ac)(bd),\ (ad)(bc)$$

are the only two proper normal subgroups of $\mathbf{P}_4$.

35. Algebra of Normal subgroups of a group. We shall now examine the nature of the compositions of

Intersection, union and multiplication

in the context of the set of all Normal subgroups of a group.

Theorem. *The intersection of any two normal subgroups of a group is a normal subgroup.*

Let

$$H_i, \quad i=1, 2$$

be two normal subgroups of G.

Let

$$a \in H_1 \cap H_2,$$

so that

$$a \in H_1, a \in H_2.$$

As H_1, H_2 are normal sub-groups, we have

$$x^{-1}ax \in H_1,\ x^{-1}ax \in H_2 \text{ for every } x \in G.$$

Thus we see that

$$a \in H_1 \cap H_2 \Longrightarrow x^{-1}ax \in H_1 \cap H_2$$

for every $x \in G$.

Hence $H_1 \cap H_2$ is a normal subgroup.

Largest normal subgroup contained in the normal sub groups H_1 and H_2. It is clear that $H_1 \cap H_2$ is the largest normal subgroup contained in H_1 as well as H_2.

Generalisation. Proceeding exactly as above, we may show that the intersection of any arbitrary family of normal subgroups of a group is a normal subgroup thereof.

Smallest normal subgroup containing a complex. Let M denote any complex of G. Then a subgroup H of G is called a smallest normal subgroup of G containing M if H is a normal subgroup which contains M and which is contained in every normal subgroup containing M.

Assuming existence, we may easily show that the smallest normal subgroup containing a complex is unique.

Concerning existence, we prove the following two theorems.

Theorem I. *The intersection of the family of normal subgroups which contain a complex M is the smallest normal subgroup containing M.*

The proof is similar to that of the corresponding theorem for arbitrary subgroups. (§ 22·3, page 59).

Theorem II. *The subgroup generated by the union of M and the complexes conjugate to M is the smallest normal subgroup containing M.*

Firstly, we show that the subgroup H generated by the union of the complexes

$$x^{-1}Mx, \qquad x \in G$$

is normal.

Every element a of H is expressible as

$$a = b_1 b_2 \ldots\ldots b_t$$

where each, b, is either a member of a complex of the form $x^{-1}Mx$ for some x or the inverse of some element of the same type.

We now have

$$y^{-1}ay = (y^{-1} b_1 y)(y^{-1} b_2 y)\ldots(y^{-1} b_t y)$$

so that we see that

$$y^{-1} ay \in H.$$

Thus

$$a \in H \Longrightarrow y^{-1} ay \in H \text{ for every } y \in H.$$

Hence H is normal.

Also every normal subgroup containing the complex M must necessarily contain every complex $x^{-1} Mx$ conjugate to M.

Hence the theorem

Ex. 1. Show that the subgroup generated by the union of any set of self-conjugate complexes is normal.

Ex. 2. Show that the subgroup generated by any complete class K of conjugate complexes is normal.

36. Quotient Group. We shall now introduce the very important concept of **Quotient Groups.**

Let H be any normal subgroup of a group G. Consider the coset decomposition of G relative to H. The subgroup H being normal, each right coset of H is as well a left coset and vice versa so that we do not have to distinguish between the right and the left coset decompositions.

Now, it is interesting to see that it is possible to assign this set of cosets itself the structure of a group. This possibility is due to the fact that the set of all cosets of any normal subgroup H of a group G, as a sub-set of the set of all complexes of G, is *stable* for the composition of the multiplication of complexes as considered in § 22, page 58, Ch. II. This means that the product of two cosets, as two complexes, is again a coset. As a result of this, there is defined in the set of all cosets a composition. Thus if Ha_i, Ha_j be two cosets of a normal subgroup H, we have, making use of the Associativity of the multiplication of complexes,

$$(Ha_i)(Ha_j) = (Ha_iH)a_j = (HH)a_ia_j = Ha_ia_j,$$

so that the product of two cosets, as two complexes, is again in this case a coset.

Theorem. *The set of all cosets of a normal subgroup is a group with multiplication of complexes as the composition.*

Let G' denote the set of all cosets of a normal subgroup H of a group G.

I. Since

$$(Ha_i)(Ha_j) = H(a_ia_j),$$

the multiplication of complexes is a composition in G' in as much as the same assigns to each ordered pair of members of G' another member of G'.

II. *The composition is associative.* This follows from the fact that the multiplication of arbitrary complexes *is associative.* Even otherwise, we have

$$\begin{aligned}[(Ha_i)(Ha_j)]\, Ha_k &= [H(a_ia_j)]\, Ha_k \\ &= H[a_ia_j)a_k] \\ &= H[a_i(a_ja_k)] = Ha_i[(Ha_j)(Ha_k)].\end{aligned}$$

III. **Existence of identity.** The member H of G' is the identity, in as much as

$$H(Ha_i)=Ha_i=(Ha_i)H,$$

for every member Ha_i of G'.

IV. **Inversibility of each element.** Each member Ha_i of G' is inversible with inverse Ha_i^{-1}.

In fact, we have

$$(Ha_i)(Ha_i^{-1})=H(a_ia_i^{-1})$$
$$=He=H=(Ha_i^{-1})(Ha_i).$$

Hence the theorem.

Def. Quotient Group. The group formed by the set of all cosets of a normal subgroup H of a group G with multiplication of complexes as composition is called the Quotient group of G relative to H and is denoted by the symbol G/H.

A quotient group is also known as a **factor group.** It is also known as the **Group of residue classes mod H of** G.

Illustrations. 1. Let G denote the symmetric group of degree three so that it consists of the six elements.

$$I,\ (ab),\ (bc),\ (ca),\ (abc),\ (acb).$$

The sub-group H consisting of the elements

$$I,\ (acb),\ (abc)$$

is a normal sub-group of G.

Then G/H is a group of order two having as its members the two cosets

$$H,\ H(ab).$$

Of course it is a cyclic group.

It may be noted that instead of $H(ab)$, we could as well write $H(bc)$ or $H(ca)$.

Note. The reader may note that the set K consisting of two elements I, (ab) is a sub-group which is not normal. The cosets of K in G are

$$K,\ K(bc),\ K(ca).$$

These cosets do *not* form a group for the multiplication of complexes as the composition. In fact the product of two cosets may not be a coset. Thus in this case, we have

$$K\equiv I,\ (ab);\ K(bc)\equiv(bc),\ (abc);\ K(ca)\equiv(ca),\ (acb)$$

so that

$$[K(bc)]\,[K(ca)] = (abc),\ (ab),\ (bc),\ I$$

and we do not get a coset as the product.

2. Let G denote the symmetric group of degree four. Then the set consisting of the four permutations

$$I,\ (ab)(cd),\ (ac)(bd),\ (ad)(cb)$$

is a normal sub-group H of G.

The quotient group G/H is of order six.

The elements of G/H, viz., the cosets of H in G are

$$H : I,\ (ab)(cd),\ (ac)(bd),\ (ad)(cb)$$
$$H\ (abcd) : (abcd),\ (ac),\ (adcb),\ (bd)$$
$$H\ (acbd) : (acbd),\ (adbc),\ (ab),\ (cd),$$
$$H\ (abdc) : (abdc),\ (ad),\ (bc),\ (acdb)$$
$$H\ (abc) : (abc),\ (acd),\ (bdc),\ (adb)$$
$$H\ (bcd) : (bcd),\ (acb),\ (adc),\ (abd).$$

The quotient group G/H is isomorphic to the symmetric group $\mathbf{P}_3$ of degree three. The reader may prove this without much difficulty.

3. **Quotient groups of the additive group J of integers.** We know that every sub-group H of J consists of all multiples of integers by some integer m so that

$$H = \{m\}.$$

Also J being a commutative group, H is a normal sub-group of J.

The cosets of H in J are

$$H,\ H+1,\ H+2,\ \ldots\ldots,\ H+(m-1)$$

so that the quotient group $\mathbf{J}/H$ is of order m.

The composition is given by

$$(H+i)+(H+j) = H+(i+j).$$

As special case, we consider the quotient group which arises when $m=6$. Also for the sake of brevity, we shall denote $H+i$ by $\overline{i}$. Here we have $H=\{6\}$.

Thus the members of $\mathbf{J}/H$ are

$$\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}.$$

The composition table for J/H is the following:

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

It should of course be remembered that a coset is capable of more than one representation.

Thus for example

$$\{6\}+2=\{6\}+8=\{6\}+14.$$

Ex. Show that every Quotient group of an Abelian (cyclic) group is Abelian (cyclic).

37. Commutator subgroup of a group. Conditions for a quotient group to be Abelian. Every quotient group of an Abelian group is necessarily Abelian but the converse is not necessarily true. We now proceed to discuss conditions under which G/H is Abelian. This depends upon the notion of the commutator of a pair of elements.

Def. *The element $a^{-1}b^{-1}ab$ is called the commutator of two elements a, b taken in this order.* It may be seen that the commutator of a, b is the inverse of that of b, a. Also the commutator of two elements is the identity, e, if and only if the two elements commute.

Consider now the complex formed of the commutators of all the pairs of elements of G. As the product of two commutators is not necessarily a commutator, this complex may not be a sub-group. This complex, like any other, *generates* a sub-group all right. The *subgroup generated by the complex consisting of the commutators of all the ordered pairs of elements of the group is called the commutator sub-group of the group.*

It may be shown that the commutator subgroup of a group is a normal subgroup. It is because every element conjugate to a commutator is a commutator.

Theorem. *A quotient group G/H is Abelian if and only if H contains the commutator subgroup of G.*

Let a, b be two arbitrary elements of G so that Ha, Hb are two elements of G/H. Now

$Ha\ Hb = HbHa \longleftrightarrow Hab = Hba \longleftrightarrow ab(ba)^{-1} = aba^{-1}b^{-1} \in H.$

Suppose that G/H is Abelian. Then we see that for every pair of elements a, b of G,

$$ab\ a^{-1}b^{-1} \in H.$$

This shows that every commutator of G and accordingly the commutator subgroup of G is contained in H.

Conversely also it appears from the above line of reasoning that G/H is Abelian if H contains the commutator subgroup of G.

Ex. Show that the commutator subgroup of $\mathbf{P}_3$ is $\mathbf{A}_3$.

Illustration. 1. *The commutator group of $\mathbf{P}_n$ is $\mathbf{A}_n$.*

We have

(12) (13) (12) (13) = (132) (132) = (123) is a commutator.

Thus each of the generators,

(123), (124),..... (12n) of $\mathbf{A}_n$ is a commutator of $\mathbf{P}_n$.

38. Homomorphism. We shall now introduce the notion of the homomorphic images of a group and the corresponding notion of homomorphic mappings. This notion is a generalisation of that of isomorphic mappings and has a very fundamental relation with that of quotient groups.

Let G, G' be two groups. We shall suppose that the compositions in both the groups are denoted multiplicatively.

Then we say that *G is homomorphic to G' or that G' is a homomorphic image of G if there exists a mapping f of G onto G' such that*

$$f(ab) = f(a)f(b),\ a \in G,\ b \in G.$$

Also then f is said to be a homomorphic mapping or simply a homomorphism of G onto G'.

Further we express this relation of homomorphism by writing

$$G \simeq G'.$$

Of course, if G is homomorphic to G', then there may exist more than one homomorphism of G onto G'.

We may note that a homomorphic mapping is distinguished from an isomorphic mapping in as much as the former may be many-one whereas the latter is necessarily one-one.

Thus the relation of homomorphism is not symmetric in that if G is homomorphic to G', then G' may not be homomorphic to G.

Illustration. 1. Let G' denote the multiplicative group of numbers $+1, -1$. Then the mapping f of $\mathbf{P}_n$ onto G' such that each even permutation is mapped on 1 and each odd permutation is mapped on -1 is a homomorphism of $\mathbf{P}_n$ onto G'.

This follows from the fact that the product of two permutations, both odd or both even, is even and the product of one odd and one even is odd.

2. Let G denote the multiplicative group of all $n \times n$ non-singular matrices with elements as real numbers and let G' denote the multiplicative group of non-zero real numbers.

Then the mapping which maps each matrix member of G onto its determinant which is a member of G', is a homomorphism of G onto G' in as much that

$$|AB| = |A| \; |B| ;$$

A, B being two $n \times n$ matrices.

Note : 1. Transference of group Structure. As in § 17·2, page 50 it can be shown that if G is a group and G' is a set with a composition such that there exists a mapping f of G onto G' such that

$$f(ab) = f(a)\, f(b) ; \qquad a \in G, b \in G,$$

the two compositions having been denoted multiplicatively, then G' is a group such that G is homomorphic to G'.

We shall utilise this result to give a shorter proof of the theorem of § 36, page 94 regarding the existence of Quotient Groups.

Let H be a normal subgroup of a group G.

Let G' denote the *set* of all cosets of H in G.

Then the composition

$$(Ha)(Hb) = H(ab) \qquad \ldots (1)$$

is well defined in G'.

Consider now the mapping

$$a \longrightarrow Ha,$$

of G onto G'. We have

$$ab \longrightarrow Hab = (Ha)(Hb).$$

Thus by the result stated here in this note, it follows, that the set G' is a group for the composition defined in (1). This proof

eliminates the necessity of the steps II, III, IV in the proof of the theorem on the existence quotient groups given in § 36, page 94.

Note : 2. Homomorphism into. If f is mapping of a group G, *into* a group G', such that

$$f(ab)=f(a)\,f(b)\,; \qquad a \in G, b \in G$$

then we say that f is a homomorphism of G into G'

Also we may easily see that the set $f(G)$ is a subgroup of G' and is a homomorphic image of G.

Note : 3. The following points about homomorphic mappings may be easily proved. The proof consists in almost a reproduction of those of the corresponding results for isomorphic mappings.

1. The homomorphic image of the identity of G is the identity of G'.

2. The homomorphic image of the inverse of any element, a, is the inverse of the image of a.

3. The order of the homomorphic image of any element, a, is a *divisor* of the order of a.

Ex. 1. Show that every homomorphic image of an Abelian (cyclic) group is Abelian (cyclic).

Further show that the converse is not true.

Ex. 2. Show that every homomorphic image of a group of finite order is finite but that the converse is not true.

38·1. Kernel of a homomorphism. Theorem. *If f is a homomorphism of G onto G', then the set H of all those elements of G which are mapped on the identity e' of G' i.e., the subset $f^{-1}(e')$ of G is a normal subgroup of the same.* [Refer § 3·5, note 2, page 9].

Let $a \in H$, $b \in H$ so that

$$f(a)=e',\ f(b)=e'\ ;$$

e' being the identity of G'.

We then have

$$\begin{aligned} f(ab^{-1}) &= f(a)\,f(b^{-1}) \\ &= f(a)[f(b)]^{-1} \\ &= e'e'^{-1}=e'. \end{aligned}$$

Thus

$$a \in H, b \in H \Longrightarrow ab^{-1} \in H,$$

and hence H is a subgroup of G, (§ 21, page 56)

Again if x be any member of G, we have

$$f(x^{-1}ax) = f(x^{-1})f(a)f(x)$$
$$= [f(x)]^{-1} e'[f(x)]$$
$$= [f(x)]^{-1} f(x) = e',$$

so that

$$a \in H, x \in G \Longrightarrow x^{-1}ax \in H.$$

Hence H is a normal sub-group of G.

Def. *If f is a homomorphism of G onto G', then the sub-set H consisting of all those elements of G which are mapped on the identity of G' is a normal sub-group of G, called the Kernel of the homomorphism.*

Illustration. 1. The Kernel of the homomorphic mapping of $\mathbf{P}_n$ onto the multiplicative group formed by the numbers 1, -1 is the alternating sub-group $\mathbf{A}_n$ of $\mathbf{P}_n$.

2. The Kernel of the homomorphic mapping of the multiplicative group of all $n \times n$ non-singular matrices with real numbers as elements onto the multiplicative group of non-zero real numbers is the set of matrices with determinant equal to 1.

Ex. Show that f defined by

$$f(x+iy) = x$$

is a homomorphic mapping of the additive group of complex numbers onto the additive group of real numbers. What is the kernel of f?

Ex. Show that

$$z \longrightarrow |z|$$

is a homomorphic mapping of the multiplicative group of non-zero complex numbers onto the multiplicative group of non-zero real members, the kernel of the homomorphism being the multiplicative group of unimodular complex numbers.

Ex. Show that

$$z \longrightarrow E(z)$$

is a homomorphic mapping of the additive group of complex numbers onto the multiplicative group of non-zero complex numbers, the kernel of the homomorphism being the additive group of complex numbers $2ik\pi$; k being any integer.

Ex. If H be the kernel of a homomorphism f of G onto G', then the set of all those elements of G which have the same image as a given element $a \in G$, is the coset Ha of G.

In other words prove that

$$f^{-1}(f(a))$$

is the coset Ha of G.

Ex. If f is a homomorphism of G onto G' and g a homomorphism of G' onto G'', show that gf is an homomorphism of G onto G'' : the kernel being a sub-group K of G such that $(fg)(K)$ is the identity of G''. Also show that the kernel of f is a sub-group of that of gf.

39. Concerning the totality of homomorphic images of a group. We shall now state and prove a theorem which will throw light on the structures of all the possible homomorphic images of a group.

Theorem on Homomorphism. *Every homomorphic image of a group G is isomorphic with some quotient group thereof, in fact this is so for the quotient group relative to the kernel of the homomorphism. Also, conversely every quotient group of a group is a homomorphic image of the group.*

This theorem amounts to showing, that from an abstract point of view, the set of all quotient groups of a group constitutes the complete set of homomorphic images of the group.

Suppose that G' is a homomorphic image of G and f denotes the corresponding homomorphic mapping. Let H denote the kernel of this homomorphism. We shall show that

$$G/H \cong G',$$

the corresponding isomorphism being defined by

$$Ha \longrightarrow f(a) \tag{1}$$

$Ha \in G/H$ and $f(a) \in G'$.

We have first to see that this mapping (1) is well defined. The necessity for this is due to the fact that the image of a coset member Ha of G/H has been made to depend on the f-image of a member of the coset.

We must therefore show that the f-image of each member of Ha is the same so that with each coset member Ha of G/H we associate that member of G' which is the f-image of any member of Ha.

In fact if h_i be any member of H, we have

$$f(h_i a) = f(h_i)\, f(a) = e' f(a) = f(a)$$

so that the mapping is well-defined.

We now show that it is one-one.

Let

$$f(a) = f(b).$$

We then have

$$f(ab^{-1}) = f(a)\,[f(b)]^{-1} = e'$$

so that

$$ab^{-1} \in H.$$

As we have

$$ab^{-1} \in H \Longrightarrow Ha = Hb.$$

Thus

$$f(a) = f(b) \Longrightarrow Ha = Hb,$$

Finally, we have

$$(Ha)(Hb) = H(ab) \longrightarrow f(ab) = f(a)\,f(b)$$

so that

$$(Ha)(Hb) \longrightarrow f(a)\,f(b).$$

Thus we have the first part.

To prove that

$$G \simeq G/H,$$

consider the mapping

$$a \longrightarrow Ha \tag{1}$$

of G onto G/H. We have

$$ab \longrightarrow H(ab) = (Ha)(Hb)$$

so that (1) is a homomorphism of G onto G/H. Hence the theorem.

The mapping (1) is known as a **Natural Mapping** of G onto G/H. The kernel of this natural homomorphic mapping of G onto G/H is the subgroup H of G.

Cor. If H is the kernel of a homomorphism f of a group G onto a group G', then

$$G/H \cong G',$$

the corresponding isomorphism being given by

$$Ha \longrightarrow f(a)$$

Ex. 1. Show that the order of every homomorphic image of a finite order group is a divisor of the order of the group.

Ex. 2. Show that

$$G/G \cong \{e\},\ G/\{e\} \cong G.$$

Ex. 3. Show that each homomorphic image of the additive group J of integers is isomorphic to the additive group modulo m for some integer m.

4. A Fundamental theorem. Two laws of isomorphism.

Let H be any normal subgroup of a group G.

Let Σ denote the set of all those subgroups of G which contain H as a subgroup and let Σ' denote the set of all the subgroups of the quotient group G/H which we denote by G'. Then

$$K \longrightarrow K/H = K',\ K \in \Sigma,\ K' \in \Sigma',$$

is a one-one mapping of Σ onto Σ'.

Also if K is a normal subgroup of G, then K' is a normal subgroup of G' and

$$G/K \cong G'/K'.$$

Let K be any member of Σ so that it is a subgroup of G containing H, *i.e*,

$$H \subseteq K \subseteq G.$$

As H is a normal subgroup of G, it is also a normal subgroup of K and accordingly the symbol K/H is meaningful.

Firstly we prove that the mapping

$$K \longrightarrow K/H = K'$$

is a mapping of Σ *onto* Σ'

Let K' be any member of Σ', *i.e.*, any subgroup of G/H so that it is a certain set of cosets of H.

Let K denote the sub-set of G which arises as the union of these coset members of K' as complexes of G. In fact if f denotes the natural mapping of G onto G/H, then $K = f^{-1}(K')$.

Then if $a_1 \in K$, $a_2 \in K$ so that $Ha_1 \in K'$, $Ha_2 \in K'$, we have

$$[(Ha_1)(Ha_2)^{-1}] \in K',$$

i.e.,

$$H(a_1 a_2^{-1}) \in K'$$

so that

$$a_1 a_2^{-1} \in K.$$

Thus K is a subgroup of G containing H and accordingly a member of Σ.

Also K' can be written as K/H, *i.e.*, each member of Σ' can be written as K/H for some subgroup K of G containing H.

Now to show that the mapping is one-one. Each member of Σ' can be written as K/H where K is a subgroup of G containing H.

Let K_1/H, K_2/H be two members of Σ'. We shall, then prove that $K_1 = K_2$ if $K_1/H = K_2/H$.

Let $k_1 \in K_1$ so that $Hk_1 \in K_1/H = K_2/H$.

There exists, $\therefore$, a member k_2 of K_2 such that

$$Hk_1 = Hk_2.$$

$\therefore$ $$k_1 \in Hk_2.$$

$\therefore$ $$k_1 \in K_2.$$

Hence

$$K_1 \subseteq K_2.$$

Similarly

$$K_2 \subseteq K_1$$

$$\therefore \quad K_1 = K_2$$

Suppose now that K is a normal subgroup of G containing H. We shall prove that K/H is a normal subgroup of G/H. Let Ha be any member of K/H so that a is a member of K and let Hx be any member of G/H.

We have

$$(Hx)^{-1}\,(Ha)\,(Hx) = H\,(x^{-1}ax).$$

Now K being normal in G,

$a \in K \Longrightarrow x^{-1}ax \in K \Longrightarrow H(x^{-1}ax) \in K/H.$

$\therefore$ K/H is a normal subgroup of G/H.

We may also easily show that if K/H is a normal subgroup of G/H, then K is a normal subgroup of G.

Consider the natural homomorphisms (By the Homomorphisn Theorem].

$$G \simeq G/H = G' \tag{1}$$

$$G' \simeq G'/K' \tag{2}$$

The resultant of these gives us a homomorphism of G onto G'/K' so that we have

$$G \simeq G'/K' \tag{3}$$

We now require the kernel of this homomorphism.

The kernel of the homomorphism (2) is the subgroup K' of G'. We have

$$K' = K/H.$$

Again, as a result of the homomorphism (1), the sub-group K of G is mapped on the subgroup K' of G'. Thus K is the kernel of (3).

Hence, by the theorem on homomorphisms,

$$G/K \simeq G'/K'.$$

Note. The result $G/K \simeq G'/K'$ proved above is known as the **first law of isomorphism.**

Cor. Let f be a homomorphic mapping with kernel H of a group G onto a group G'. Corresponding to any sub-group K of G, K' is defined to be the set of images under f of the elements in K. Then

$$K \longrightarrow K'$$

is a one-one mapping of the subgroups K of G containing H onto the subgroups of G' with the following properties :

(*i*) K is a normal subgroup of G if and only if K' is a normal subgroup of G',

(*ii*) $G/K \cong G'/K'$.

40·1. Second law of isomorphism. *If L is any sub-group of G and H any normal sub-group of G, then*

$$LH/H \cong L/(L \cap H).$$

Since H is a normal sub-group of G, we have

$$HL = LH$$

and accordingly, $L H$ is a sub-group. Also we have

$$H \subseteq LH \subseteq G,$$

and accordingly H is a normal subgroup of LH so that the symbol LH/H is meaningful.

In the natural homomorphism

$$f : G \to G' = G/H,$$

each $a \in G$ is mapped on $Ha \in G'$.

Clearly then

$$f(L) = LH/H.$$

$$\therefore \qquad L \simeq LH/H.$$

The kernel of this homomorphism is the sub-group $L \cap H$. Accordingly, by the law of homomorphism,

$$L/(L \cap H) \simeq LH/H.$$

This is known as the second law of Isomorphism.

41. Relations compatible with group structure.

We say that a binary relation R defined in a group G is compatible with the group structure of G, if

$$aRb, cRd \Longrightarrow ac\ RbRd.$$

Illustrations. 1. The relation $a \leqslant b$ in the additive group of integers is compatible with the group structure in as much as we have

$$a \leqslant b, c \leqslant d \Longrightarrow a + c \leqslant b + d.$$

2. The relation $a \leqslant b$ in the multiplicative group of positive rational numbers is compatible with the group structure, for

$$a \leqslant b, c \leqslant d \Longrightarrow ac \leqslant bd.$$

3. The relation $a \mid b$ of divisibility in the additive group of

integers is *not* compatible with group structure for

$$a \mid b,\ c \mid d$$

does not necessarily imply

$$(a+c) \mid (b+d).$$

4. The relation of conjugacy of elements in a group is not in general compatible with group structure.

41·1. Equivalence relations compatible with group structure. The study of *equivalence relations in a group compatible with group structure* throws very interesting light on the notion of Quotient groups and that of homomorphic images of a group.

The following results may be easily established .

(1) If R is an equivalence relation in a group G compatible with group structure, then the equivalence class $\bar{e}$ determined by the identity e of G is a normal sub-group H of G. Also the equivalence class $\bar{a}$ determined by any element a of G is the coset Ha of H in G. Finally the set of all equivalence classes is the same as the set of cosets of H in G.

(2) If G' is a homomorphic image of a group G, f being the corresponding homomorphism, then the relation R defined in G by

$$aRb \Longleftrightarrow f(a) = f(b)$$

is an equivalence relation compatible with group structure. Further the set of *corresponding equivalence classes in* G *is such that*

(*i*) any two elements of the same equivalence class have the same σ-image,

(*ii*) no two elements of different equivalence classes have the same σ-image.

The proofs which are easy are left to the reader.

42. Jordan Holder theorem for finite groups. By a **maximal** normal sub-group of a group G is meant a normal sub-group H such that the only normal sub-group of G, containing H and other than H, coincides with G, itself, *i.e.*, if H is a maximal normal sub group and K is a normal sub-group such that

$$H \subset K \subseteq G,$$

then we must have $K=G$.

Theorem. *A normal sub-group H of a group G is maximal, if and only if the quotient group G/H is simple.*

We have seen that to each normal sub-group K of G containing H, there corresponds a normal sub-group K/H of G/H and this correspondence is one-one. The result now follows from the fact that to a normal sub-group K, properly contained between H and G

identical, apart from order. Thus the two series (1) and (2) are also abstractly identical.

Case II. Let $H_2 \neq L_2$. Now H_2L_2 is a normal subgroup of G containing H_2 (also L_2) and H_2 being maximal, we have

$$H_2L_2 = G.$$

By the second theorem of isomorphism,

$$G/H_2 = H_2L_2/H_2 = L_2/(H_2 \cap L_2) \tag{5}$$

Also

$$H_2L_2/L_2 = H_2/(H_2 \cap L_2). \tag{6}$$

As G, H_2 is simple, $L_2/(H_2 \cap L_2)$ is simple and accordingly $H_2 \cap L_2$ is a maximal normal subgroup of L_2. Also $H_2 \cap L_2$ is a maximal normal subgroup of H_2.

Suppose now

$$H_2 \cap L_2, M_2, M_3 \ldots\ldots, M_t\ (=e)$$

is a composition series of $H_2 \cap L_2$.

Consider now the following two composition series of $G = H_2L_2$,

$$G = H_2L_2, H_2, H_2 \cap L_2, M_2, M_3, \ldots\ldots, M_t = (e), \tag{7}$$

$$G = H_2L_2, L_2, H_2 \cap L_2, M_2, M_3, \ldots\ldots, M_t = (e). \tag{8}$$

Making use of (5) and (6), we see that the two series of composition factor groups arising from the composition series (7) and (8) are abstractly identical.

Consider also the two composition series

$$G, H_2, H_3, \ldots\ldots, H_k = (e) \tag{9}$$

$$G, L_2, L_3, \ldots\ldots, L_l = (e). \tag{10}$$

The theorem being assumed for H_2 and L_2, we see that the series of composition factor groups arising from (9) is abstractly identical with that arising from (7) and the one arising from (10) is abstractly identical with that arising from (8).

Thus it follows that the series of composition factor groups arising from (9) and (10) are abstractly identical.

Hence the theorem.

er.

ra

2.

42·2. Composition factor groups and Composition factors.

If

$$G, H_2, H_3, \ldots\ldots, H_l = \{e\} \qquad (i)$$

is any composition series for a group G, then the quotient groups

$$G/H_2, H_2/H_3, \ldots\ldots, H_{l-1}/H_l$$

which are necessarily simple are called *Composition factor groups* and their orders are called *composition factors* corresponding to the given composition series (1).

We shall now prove an important theorem known as **Jordan Holder theorem.**

42·3. Theorem. *Let G be any given finite group and let*

$$G, H_2, H_3, \ldots\ldots, H_k = \{e\}$$
$$G, L_2, L_3, \ldots\ldots, L_t = \{e\}$$

be two composition series of G so that

$$G/H_2, H_2/H_3, \ldots\ldots, H_{k-1}/H_k \qquad (1)$$
$$G/L_2, L_2/L_3, \ldots\ldots, L_{t-1}/L_t \qquad (2)$$

are the corresponding series of Composition factor groups. Then there exists a one-one mapping of either series of composition factor groups on to the other such that the corresponding factor groups are isomorphic.

Briefly, we may say that the two series of composition factor groups are *abstractly* the same apart from order.

We shall now use the principle of mathematical induction in terms of the order of a group for the proof of the theorem.

Clearly the theorem is true for a group of order one. We *suppose* that it is true for every group whose order is less than that of G.

Case I. Let $H_2 = L_2$ so that $G/H_2 = G/L_2$.

Then

$$H_2, H_3, \ldots\ldots, H_k = \{e\}$$
$$H_2, L_3, \ldots\ldots, L_t = \{e\}$$

are two composition series for H_2 with corresponding series of composition factors groups

$$H_2/H_3, \ldots\ldots, H_{k-1}/H_k \qquad (3)$$
$$L_2/L_3 = H_2/L_3, \ldots\ldots, L_{t-1}/L_t. \qquad (4)$$

The theorem being assumed true for H_2 whose order is less than that of G, we see that the two series (3) and (4) are abstractly

will correspond a normal sub-group K of G/H different from the identity sub-group H/H and the entire group G/H.

Hence the result.

42·1. Composition Series of a group. *By a composition series of a group G is meant a finite series of groups*

$$G,\ H_2,\ H_3,\ \ldots,\ H_l=\{e\}$$

such that each member is a maximal normal sub-group of its predecessor on the left.

For every finite group G, there always exists atleast one composition series, in view of the fact the set of all normal sub-groups of a group is finite and accordingly some one of them must be maximal.

An infinite group, however, may *not* possess a composition series. The additive group of integers, for example, does not possess a composition series. In fact, in this case, there always exists a *proper* sub-group contained in every given sub-group and every sub-group is normal.

Illustrations.

1. Let

$$G\equiv\mathbf{P}_3\equiv[I,\ (ab),\ (bc),\ (ca),\ (abc),\ (acb)].$$
$$H_2\equiv[I,\ (abc),(acb)].$$

Then

$$G,\ H_2,\ \{e\},$$

is a composition series for G.

2. Let G be a cyclic group $\{a\}$ of order 12

Then

$$\{a\},\ \{a^2\},\ \{a^4\},\ \{e\}$$
$$\{a\},\ \{a^3\},\ \{a^6\},\ \{e\}$$

are two composition series of G.

3. Let G be a cyclic group $\{a\}$ of order 24.

Then

$$\{a\},\ \{a^2\},\ \{a^4\},\ \{a^8\},\ \{e\}$$
$$\{a\},\ \{a^2\},\ \{a^4\},\ \{a^{12}\},\ \{e\}$$
$$\{a\},\ \{a^3\},\ \{a^6\},\ \{a^{12}\},\ \{e\}$$
$$\{a\},\ \{a^4\},\ \{a^8\},\ \{a^{12}\},\ \{e\}$$

are four different composition series for G.

42·2. Composition factor groups and Composition factors.

If

$$G, H_2, H_3, \ldots\ldots, H_t = \{e\} \qquad (i)$$

is any composition series for a group G, then the quotient groups

$$G/H_2, H_2/H_3, \ldots\ldots, H_{t-1}/H_t$$

which are necessarily simple are called *Composition factor groups* and their orders are called *composition factors* corresponding to the given composition series (1).

We shall now prove an important theorem known as **Jordan Holder** theorem.

42·3. Theorem. *Let G be any given finite group and let*

$$G, H_2, H_3, \ldots\ldots, H_k = \{e\}$$

$$G, L_2, L_3, \ldots\ldots, L_s = \{e\}$$

be two composition series of G so that

$$G/H_2, H_2/H_3, \ldots\ldots, H_{k-1}/H_k \qquad (1)$$

$$G/L_2, L_2/L_3, \ldots\ldots, L_{s-1}/L_s \qquad (2)$$

are the corresponding series of Composition factor groups. Then there exists a one-one mapping of either series of composition factor groups on to the other such that the corresponding factor groups are isomorphic.

Briefly, we may say that the two series of composition factor groups are *abstractly* the same apart from order.

We shall now use the principle of mathematical induction in terms of the order of a group for the proof of the theorem.

Clearly the theorem is true for a group of order one. We *suppose* that it is true for every group whose order is less than that of G.

Case I. Let $H_2 = L_2$ so that $G/H_2 = G/L_2$.

Then

$$H_2, H_3, \ldots\ldots, H_k = \{e\}$$

$$H_2, L_3, \ldots\ldots, L_t = \{e\}$$

are two composition series for H_2 with corresponding series of composition factors groups

$$H_2/H_3, \ldots\ldots, H_{k-1}/H_k \qquad (3)$$

$$L_2/L_3 = H_2/L_3, \ldots\ldots, L_{t-1}/L_t. \qquad (4)$$

The theorem being assumed true for H_2 whose order is less than that of G, we see that the two series (3) and (4) are abstractly

Ex. If m is any given positive integer, show that $z \to z^m$ is an endomorphism of the multiplicative group of non-zero complex numbers; what is its kernel?

43·1. Group of automorphisms of a group. Theorem. *The set of all automorphisms of a group with resultant composition is a group.*

I. *The product of two automorphism is an automorphism.*

Let f, g be two automorphisms. As f, g are one-one mappings of G onto itself, fg is also a one-one mapping of G onto itself.

Again, a, b being arbitrary members of G

$$\begin{aligned}(fg)(ab) &= f[g(ab)] \\ &= f[g(a)g(b)] \\ &= \{f[g(a)]\}\{f[g(b)]\} \\ &= [(fg)(a)]\,[(fg)(b)]\end{aligned}$$

[Supply reason for each step].

Thus fg is also an automorphism.

II. *The multiplication of automorphisms is associative.* In fact it has already been proved, that the multiplication of arbitrary mappings is associative.

III. *The identity mapping is an automorphism.*

IV. *Each automorphism is inversible.* In fact; as may be easily proved, the inverse mapping f^{-1} of any automorphism f is itself an automorphism. (Prove it).

Hence the theorem.

Ex. 1. Show that the group of automorphisms of the four-group is isomorphic to the symmetric group $\mathbf{P}_3$ of degree three.

Ex. 2. Show that the group of automorphisms of a cyclic group of degree four is of order two.

Ex. 3. Show that the order of the group of automorphism of a finite group of order n is a divisor of $n!$

Ex. 4. Show that the group of automorphisms of $\mathbf{P}_3$ is isomorphic to itself.

Ex. 5. If a is any given non-zero complex number; show that $z \longrightarrow az$ is an automorphism of the additive group of complex numbers.

Show further that the totality of these automorphisms arising for all non-zero complex numbers a is an abelian group for the resultant composition isomorphic to the multiplicative group of all non-zero complex numbers.

43·2. Inner automorphisms of a group. We shall now study a special type of automorphisms known as Inner automorphisms.

It can be shown that the mapping

$$\sigma_a = \begin{pmatrix} x \\ a^{-1}xa \end{pmatrix},$$

where x ranges over G and a is a fixed element of G, is an automorphism of G.

As

$$a^{-1}xa = a^{-1}ya \Longrightarrow x = y,$$

we see that σ_a is one-one.

Again, if y be any element of G, we have

$$a^{-1}xa = y \Longleftrightarrow x = aya^{-1},$$

so that

$$\sigma_a(x) = a^{-1}(aya^{-1})a = y,$$

and accordingly σ_a is onto.

Finally

$$\begin{aligned} \sigma_a(xy) &= a^{-1}xya \\ &= (a^{-1}xa)(a^{-1}ya) = \sigma_a(x)\sigma_a(y). \end{aligned}$$

Thus σ_a is an automorphism.

Automorphisms of the type

$$\begin{pmatrix} x \\ a^{-1}xa \end{pmatrix}$$

are called **Inner** automorphisms. Also an outomorphism which is not inner is called **Outer.**

Identity is the only inner automorphism of an Abelian group.

43·3. Group of inner automorphisms. Theorem. *The set of all inner automorphisms of a group G is a sub-group of the group of all automorphisms and is isomorphic to the quotient group G/Z of G relative to the central Z.*

Let

$$\sigma_a = \begin{pmatrix} x \\ a^{-1}xa \end{pmatrix}, \quad \sigma_b = \begin{pmatrix} x \\ b^{-1}xb \end{pmatrix}$$

be two inner automorphisms of G.

We have

$$\sigma_a(\sigma_b)^{-1} = \begin{pmatrix} x \\ a^{-1}xa \end{pmatrix}\begin{pmatrix} b^{-1}xb \\ x \end{pmatrix} = \begin{pmatrix} b^{-1}xb \\ a^{-1}xa \end{pmatrix}$$

We write $y = b^{-1}xb$ so that $x = byb^{-1}$.

$\therefore \quad a^{-1}xa = a^{-1}byb^{-1}a = (b^{-1}a)^{-1}y\,(b^{-1}a) = c^{-1}yc$

where we write $c = b^{-1}a$.

Thus

$$\sigma_a\,\sigma_b^{-1} = \begin{pmatrix} y \\ c^{-1}yc \end{pmatrix} = \sigma_c$$

Hence the set of inner automorphisms is a sub-group of the group of automorphisms.

Consider now the mapping

$$a \longrightarrow \sigma_{a^{-1}} \tag{1}$$

of G onto the set of inner automorphisms.

We have

$$ab \longrightarrow \sigma_{(ab)^{-1}} = \begin{pmatrix} x \\ (ab)\,x(ab)^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} bxb^{-1} \\ abxb^{-1}a^{-1} \end{pmatrix}\begin{pmatrix} x \\ bxb^{-1} \end{pmatrix} = \sigma_{a^{-1}}\,\sigma_{b^{-1}}$$

$\therefore$ the mapping defined by (1) is a homomorphism of G onto the group of inner automorphisms. Now we find the kernel of this homomorphism. We have

$$\sigma a^{-1} = \begin{pmatrix} x \\ a\;\; xa^{-1} \end{pmatrix} = I,$$

if and only if

$$a\,xa^{-1} = x, \text{ i.e., } xa = ax,$$

for every $x \in G$. Thus

$$\sigma_{a^{-1}} = I \Longleftrightarrow a \in Z.$$

Thus Z is the kernel of the homomorphism.

Accordingly, by the *Homomorphism theorem*, the group of inner automorphisms is isomorphic to the quotient group G/Z.

Hence the theorem

Ex. Prove that the group of inner automorphisms of the symmetric group $\mathbf{P}_n$ of degree n is isomorphic to $\mathbf{P}_n$ if $n \neq 2$.

43·4. Group of automorphisms of a cyclic group. Let

$$G = (a)$$

be any cyclic group. Any automorphism σ of G is defined by a relation of the form

$$\sigma(a) = a^m, \tag{1}$$

where m is some suitable positive integer.

Now (1) gives

$$\sigma(a^k)=(\sigma(a))^k=a^{km}\ ; \qquad (2)$$

k being any integer. The mapping σ being an automorphism, we deduce from (2), that a^m must be a generator of the cyclic group.

Now if G is infinite, the only generators are a and a^{-1} so that the only automorphisms are the identity mapping I wherefor

$$I(a)=a \Longrightarrow I(a^k)=a^k \qquad \text{for } k \in \mathbf{J}.$$

and the mapping f defined by

$$f(a)=a^{-1}.$$

Thus the group of automorphism of an infinite cyclic group is of order two.

Now suppose that G is of finite order n. We then know that a^m is a generator of G if and only if m is prime to n and less than n.

We shall now show that for every such choice of m, the mapping σ defined by (1) is an automorphism.

The mapping σ is one-one. Now

$$a^{k_1 m} = a^{k_2 m} \Longrightarrow a^{(k_1-k_2)m}=e \Longrightarrow n \mid (k_1-k_2)m.$$

If we suppose that $1 \leqslant k_2 < k_1 \leqslant n$, as is quite legitimate, we see that n is not a divisor of $(k_1-k_2)m$; n being prime to m and

$$1 \leqslant k_1-k_2 < n.$$

Thus the mapping σ is one-one.

The mapping is onto. We have to show that for some integer k such that $1 \leqslant k \leqslant n$, a^{km} is the same as any given element of G. This follows from the fact that

$$a^m, a^{2m}, a^{3m}, \ldots\ldots, a^{nm}$$

are all the n *different* elements of G ; σ being one-one.

Finally we see that

$$\begin{aligned}\sigma(a^{k_1}\ a^{k_2}) &= \sigma(a^{k_1+k_2}) \\ &= (\sigma(a))^{k_1+k_2} \\ &= a^{m(k_1+k_2)} \\ &= a^{mk_1}\ a^{mk_2} = \sigma(a^{k_1})\,\sigma(a^{k_2}).\end{aligned}$$

Thus the mapping (1) is an automorphism for each positive integer m less then n and prime to n. This shows that the group of automorphisms of a cyclic group of order n is of order $\varphi(n)$ where $\varphi(n)$ denotes the number of integers less than n and prime to n.

We shall now see that this group of automorphisms is Abelian Let $\sigma_{m_1}, \sigma_{m_2}$ be 2 automorphisms defined by

$$\sigma_{m_1}(a) = a^{m_1},\ \sigma m_2(a) = a^{m_2}.$$

Then

$$(\sigma_{m_1}\ \sigma_{m_2})(a) = \sigma_{m_1}\left(\sigma_{m_2}\right)(a) = \sigma_{m_1}\left(a^{m_2}\right) = a^{m_1 m_2}.$$

Similarly

$$(\sigma_{m_2}\ \sigma_{m_1})\ (a) = a^{m_1 m_2}.$$

Thus

$$\sigma_{m_1}\ \ \sigma_{m_2} = \sigma_{m_2}\ \sigma_{m_1}$$

so that the group of automorphisms is Abelian.

44. External direct products. Let G_1, G_2 be two arbitrary given groups. We shall now define a new group starting from these two groups.

In fact, we shall see how, with the help of the two group compositions in G_1, G_2, we can define a composition in the product set $G_1 \times G_2$ relative to which it acquires a group structure.

Let

$$(a_1, a_2) \in G_1 \times G_2,\ (b_1, b_2) \in G_1 \times G_2,$$

so that

$$a_1 \in G_1\ \ b_1 \in G_1\ ;\ a_2 \in G_2\ \ b_2 \in G_2.$$

A composition in $G_1 \times G_2$ denoted multiplicatively is now defined as follows :

$$(a_1, a_2\ (b_1, b_2) = {}'a_1 b_1\ \ a_2 b_2). \tag{1}$$

We may now easily verify that the product set $G_1 \times G_2$ is a group for the composition defined in (1). It is known as the **External direct product group** of $G_1\ G_2$ denoted by $G_1 \times G_2$.

The identity for this group is

$$(e_1, e_2)$$

where e_1, e_2 are the identities of G_1 and G_2 respectively.

Also

$$(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1}).$$

The following facts about the group $G_1 \times G_2$ may now be easily established :

I. The sub-set of $G_1 \times G_2$ consisting of elements

$$(a_1, e_2) :$$

a_1 being an arbitrary element of G_1, is a sub-group of $G_1 \times G_2$, isomorphic to the group G_1 ; an isomorphism being given by

$$(a_1, e_2) \longrightarrow a_1.$$

This sub-group of $G_1 \times G_2$ isomorphic to G_1 will, in the following, be denoted by G_1',

Similarly

$$(e_1, a_2) \longrightarrow a_2$$

is an isomorphic mapping of a sub-group G_2' consisting of the elements (e_1, a_2) on the group G_2.

Also G_1', G_2' are normal subgroups of $G_1 \times G_2$.

II. Each element of G_1' is commutative with each element of G_2'. In fact, we have

$$\begin{aligned}(a_1, e_2)(e_1, a_2) &= (a_1 e_1, e_2 a_2) \\ &= (e_1 a_1, a_2 e_2) = (e_1, a_2)(a_1, e_2).\end{aligned}$$

III. Each element of $G_1 \times G_2$ is uniquely expressible as product of an element of G_1' and an element of G_2'.

We have

$$(a_1, a_2) = (a_1, e_2)(e_1, a_2).$$

Also

$$(a_1, a_2) = (b_1, e_2)(e_1, b_2)$$

implies

$$(a_1, a_2) = (b_1 e_1, e_2 b_2) = (b_1, b_2)$$

so that

$$a_1 = b_1, \quad a_2 = b_2.$$

From this it follows that

$$G_1 \times G_2 = G_1' G_2'.$$

IV. The sub-groups G_1', G_2' of $G_1 \times G_2$ have no element other than the identity (e_1, e_2) in common.

V. The group $G_1 \times G_2$ is isomorphic to the group $G_2 \times G_1$; an isomorphism being given by

$$(a_1, a_2) \longrightarrow (a_2, a_1).$$

Generalisation. In a manner analogous to the above process, we may easily define the external direct product

$$G_1 \times G_2 \times \ldots \times G_n$$

of any finite number n of groups

$$G_1, G_2, \ldots\ldots, G_n$$

and also define sub-groups,

$$G_1', G_2', \ldots\ldots G_n'$$

of the same such that

(*i*) any two elements belonging to two different subgroups are commutative,

(*ii*) no two subgroups have an element other than the identity in common, and

(*iii*) each element of $G_1 \times G_2 \times \ldots \times G_n$ is uniquely expressible as product of elements of $G_1', \ldots\ldots, G_n'$.

Ex. 1. Show that $G_1 \times G_2$ is Abelian if and only if G_1 and G_2 are both Abelian.

Ex. 2. Show that

$$G_1 \cong H_1, G_2 \cong H_2 \Longrightarrow G_1 \times G_2 \cong H_1 \times H_2.$$

45. Internal direct product. We shall now introduce the very important notion of a **group as a direct product of its sub-groups.** To distinguish this concept from that introduced in the preceding sub-section, we shall refer to this notion as that of **Internal** direct product to emphasise the fact that the 'factors' are in this case the subgroups of the direct product.

Def. *A group G is said to be a direct product of its two sub-groups H_1 and H_2, if*

(1) *each element of H_1 is commutative with each element of H_2,*

(2) *each element of G is uniquely expressible as product of an element of H_1 and an element of H_2.*

Also we then write

$$G = H_1 \times H_2.$$

Note. If additive notation is used for the composition in a group, then we refer to G as the Direct sum of its sub-groups H_1 and H_2 and write in symbols

$$G = H_1 + H_2.$$

The reader would do well to give a direct formulation of the *notion of a group as a direct sum of its subgroups.*

Ex. 1. The Four group consisting of the four permutations

$$I, (ab), (cd), (ab)(cd)$$

is the direct product of its two sub groups H_1 and H_2 where we have

$$H_1 \equiv [I, (ab)], H_2 \equiv [I, (cd)].$$

Ex. 2. The symmetric group P_3 consisting of the permutations

$$I, (cb), (bc), (ca), (abc), (acb)$$

is *not* the direct product of its two sub-groups H_1, H_2 where

$$H_1 \equiv [I, (ab)], H_2 \equiv [I, (abc), (acb)]$$

even though we have

$$P_3 = H_1 H_2.$$

Ex 3. Show that $G = H_1 \times H_2 \Longrightarrow G = H_1 H_2$ but the converse is not true.

Ex. 4. Show that

$$G = G \times (e).$$

Ex. 5. Show that the additive group of all complex numbers is the direct sum of the subgroups of all the real and of all the purely imaginary numbers.

Theorem. *If $G = H_1 \times H_2$ where H_1, H_2 are two subgroups of G, then H_1, H_2 are normal subgroups of G and*

$$G/H_1 \cong H_2,\ G/H_2 \cong H_1.$$

We define a mapping σ of G onto H_1 as follows.

Let x be any element of G. Then

$$\sigma(x)$$

denotes the uniquely determined element $x_1 \in H_1$ such that

$$x = x_1 x_2,\ x_1 \in H_1,\ x_2 \in H_2.$$

Thus

$$\sigma(x) = x_1.$$

Again, if y be any element of G and

$$y = y_1 y_2,\ y_1 \in H_1,\ y_2 \in H_2,$$

then

$$\sigma(y) = y_1.$$

We have

$$xy = x_1 x_2 y_1 y_2$$

$$= (x_1 y_1)(x_2 y_2) : x_1 y_1 \in H_1,\ x_2 y_2 \in H_2.$$

$$\therefore \quad \sigma(xy) = x_1 y_1 = \sigma(x)\ \sigma(y).$$

Thus σ is a hormomorphism of G onto H_1. Also the kernel of σ *consists of all those elements of G which are mapped on the identity of G, i.e.,* which are of the form

$$e x_2 = x_2, \qquad x_2 \in H_2.$$

Thus H_2 is the kernel of σ. By the Homomorphism theorem, we see that H_2 is a normal sub-group of G and

$$G/H_2 \cong H_1.$$

The theorem can now be easily completed.

The result can also follow by the use of the Second Isomorphism Theorem.

We have

$$G/H_1 = H_1H_2/H_1 \cong H_2/(H_2 \cap H_1) = H_2/\{e\} \cong H_2.$$

Similarly

$$G/H_2 \cong H_1.$$

Ex. Show directly without the use of the Homomorphism theorem that $G = H_1 \times H_2$ implies that H_1. H_2 are normal sub-groups of G.

Ex Show that

$$G = H_1 \times H_2 \longrightarrow G = H_2 \times H_1.$$

45·1. Theorem. *Necessary and sufficient conditions that a group G is the direct product of its two sub-groups H_1 and H_2 are*

(1) *H_1 and H_2 are normal sub-groups of G,*

(2) *Identity is the only element common to H_1 and H_2, i.e.,*

$$H_1 \cap H_2 = \{e\}$$

(3) $$G = H_1H_2.$$

The conditions are necessary. Let

$$G = H_1 \times H_2,$$

The condition (1) has already been established in the preceding theorem. We shall, however, give another direct proof also.

Let a be any element of H_1 and x any element of G.

We have

$$x = x_1x_2, \qquad x_1 \in H_1, x_2 \in H_2.$$

$$\therefore \quad x^{-1}ax = x_2^{-1}(x_1^{-1}ax_1)x_2$$

$$= x_1^{-1}(x_2^{-1}ax_2)x_1, \qquad \text{(By (1) def. § 45)}$$

$$= x_1^{-1}(x_2^{-1}x_2a)x_1 = x_1^{-1}ax_1 \in H_1.$$

Thus

$$a \in H_1, x \in G \longrightarrow x^{-1}ax \in H_1.$$

Hence H_1 is a normal sub-group of G. Similarly H_2 is a normal sub-group of G.

Let, if possible, $d \neq e$ be an element common to H_1 and H_2. We have then

$$d = de = ed,$$

and accordingly, there exist atleast *two* ways of expressing an element of G as product of an element of H_1 with an element of H_2 and (2) of the def. of § 45 would be violated.

Thus

$$H_1 \cap H_2 = \{e\}.$$

Finally by (2) of the def,

$$G = H_1 \times H_2 \longrightarrow G = H_1 H_2.$$

The conditions are sufficient. Suppose that H_1, H_2, are two normal sub-groups of G having only the identity in common.

Let x_1, x_2 be the arbitrary elements of H_1, H_2 respectively. Consider the element

$$x_1^{-1} x_2^{-1} x_1 x_2.$$

We have

$x_1^{-1}x_2^{-1}x_1x_2 = x_1^{-1}(x_2^{-1}x_1x_2) \in H_1$; H_1 being normal,

$x_1^{-1}x_2^{-1}x_1x_2 = (x_1^{-1}x_2^{-1}x_1)x_2 \in H_2$; H_2 being normal,

$\therefore$ $x_1^{-1}x_2^{-1}x_1x_2 \in H_1 \cap H_2$.

Thus $x_1^{-1}x_2^{-1}x_1x_2 = e$.

Also $x_1^{-1}x_2^{-1}x_1x_2 = e \longrightarrow x_1x_2 = x_2x_1$.

Thus each element of H_1 is commutative with each element of H_2.

Again since $G = H_1H_2$, each element of G is expressible as product of an element of H_1 and an element of H_2. The uniqueness of this expression has now to be shown.

Let, if possible

$$x_1x_2 = y_1y_2 \; ; \; x_1 \in H_1, \; y_1 \in H_1 \; ; \; x_2 \in H_2, \; y_2 \in H_2.$$

$\therefore$ $y_1^{-1}x_1 = y_2x_2^{-1} \in H_1 \cap H_2$.

Thus $y_1^{-1}x_1 = e = y_2x_2^{-1}$

Also $y_1^{-1}x_1 = e = y_2x_2^{-1} \longrightarrow y_1 = x_1, \; y_2 = x_2$.

Thus the conditions are also sufficient.

45·2. Generalisation. Def. *A group G is said to be a direct product of its sub-groups*

$$H_1, \ldots\ldots, H_n$$

if

(1) *each element of H_k is commutative with each element of H_l ; $k \neq l$,*

(2) *each element of G is uniquely expressible as a product*

$$x_1x_2 \ldots x_k \ldots x_n \text{ where } x_k \in H_k \; ; \; 1 \leqslant k \leqslant n.$$

Also we then write

$$G = H_1 \times H_2 \times H_3 \ldots\ldots \times H_k \times \ldots\ldots \times H_n.$$

Theorem. *Necessary and sufficient conditions for a group G to be the direct product of its sub-groups*

$$H_1, \ldots\ldots, H_k, \ldots\ldots, H_n$$

are that

(i) *each* H_k, $1 \leqslant k \leqslant n$, *is a normal sub-group of* G,

(ii) $H_k \bigcap H_1 H_2 \ldots\ldots H_{k-1} H_{k+1} \ldots\ldots H_n = \{e\}$; $1 \leqslant k \leqslant n$

(iii) $G = H_1 H_2 \ldots\ldots H_k \ldots\ldots H_n$.

The conditions are necessary. Let

$$G = H_1 \times H_2 \times \ldots\ldots \times H_n.$$

Let a_k be any element of H_k and x any element of G. We have, by the def.,

$$x = x_1 x_2 \ldots\ldots x_k \ldots\ldots x_n \; , \; x_k \in H_k.$$

$$\therefore \quad x^{-1} a_k x = x_k^{-1} a_k x_k \in H_k. \qquad \text{by (i)}$$

$\therefore$ H_k is a normal sub-group of G.

Let, if possible, $d_k \neq e$ be a common member of

$$H_k \text{ and } H_1 H_2 \ldots\ldots H_{k-1} H_{k+1} \ldots\ldots H_n.$$

There then exist members

$$y_1, \ldots\ldots, y_{k-1}, y_{k+1}, \ldots\ldots, y_n$$

of

$$H_1, \ldots\ldots, H_{k-1}, H_{k+1}, \ldots\ldots, H_n$$

respectively such that

$$d_k = y_1 \ldots\ldots y_{k-1} \, y_{k+1}, \ldots\ldots, y_n.$$

We now have two different expressions of d_k as product of elements of

$$H_1, \ldots\ldots, \ldots\ldots, H_n,$$

viz.,

$$d_k = e \ldots\ldots e d_k e \ldots\ldots e$$

$$d_k = y_1 \ldots\ldots y_{k-1} e y_k \ldots\ldots y_n$$

so that we arrive at a contradiction. Thus follows (ii).

Finally (iii) immediately follows from (2) of the def. in § 45·2.

The conditions are sufficient.

By (ii), we see that

$$H_k \bigcap H_l = \{e\} \text{ if } k \neq l.$$

Let, now, $x_k \in H_k$ and $x_l \in H_l$; $k \neq l$.

so that each element of G is expressible as product of elements of

$$H_1 \ldots\ldots, H_k \ldots\ldots, H_n.$$

Let, now, L_k be a subgroup of G of order

$$N/p_k^{m_k}.$$

Then the order of the sub group

$$L_k \cap H_k$$

being a common divisor of $p_k^{m_k}$ and $N/p_k m_k$ is necessarily 1 so that

$$L_k \cap H_k = (e). \tag{1}$$

Since the order of each of

$$H_1, \ \ldots, H_{k-1}, H_{k+1}, \ldots\ldots H_n$$

is a divisor of the order of L_k, we see that each of them is a subgroup of L_k so that

$$L_k \supseteq H_1 \ldots\ldots H_{k-1} \ H_{k+1} \ldots\ldots H_n \tag{2}$$

From (1) and (2), it follows that

$$H_k \cap H_1 \ldots\ldots H_{k-1} H_{k+1} \ldots \ H_n = (e)$$

The conditions of the Theorem of § 45·2 being all satisfied, we see that

$$G = H_1 \ldots \ldots H_{k-1} H_k \ H_{k+1} \ldots\ldots H_n$$

Hence the theorem.

47. Survey of abstract groups with order not exceeding 8.

It is easy to see that there exist only a *finite* number of different abstract groups of any given finite order. In fact the number of different abstract groups of order n cannot exceed $(n\,!)^n$. This, however, is only the upper bound and the number is, in general, much smaller. The problem of the determination of the actual number of different abstract groups of a given finite order has not, as yet, been solved in the general case. The theory developed so far may help us, however, to arrive at the number in any given case. For the sake of interest, we proceed here to solve this problem for

$$n \leqslant 8.$$

It has been seen that there exists one and only one abstract cyclic group of any given order and that a group with a prime order is necessarily cyclic. From this it follows that there exists one and only one abstract group whose order is

1, 2, 3, 5 or 7

and each of these is cyclic.

We now proceed to the consideration of groups of orders

4,6,8.

Firstly we need to prove a simple lemma.

LEMMA. *A group G each of whose elements other than the identity is of order 2 is necessarily Abelian and if it be finite it is expressible as a direct product of cyclic subgroups of order 2 and th order of the group is some power of 2.*

Let a, b be arbitrary elements of G so that

$$a^2=e,\ b^2=e,\ (ab)^2=e.$$

We have

$$a\,b\,a\,b=e \longrightarrow a\,a\,b\,a\,b\,b=a\,e\,b \longrightarrow b\,a=a\,b,$$

so that the group is Abelian.

Now suppose that a_1 is any element of G so that

$$H_1=\{e,\ a_1\}$$

is a subgroup of G order 2.

If $G=H_1$, we have finished. In the alternative case, suppose that a_2 is a member of G not belonging to H_1. Then

$$H_2=\{e,\ a_2\}$$

is a subgroup of G of order 2. By the theorem of § 45 1, we see that

$$H_1H_2=H_1\times H_2$$

so that the subgroup H_1H_2 of G is of order 4.

If $G=H_1H_2$, we have again finished. In the alternative case, suppose that a_3 is a member of G not belonging to H_1H_2. Again, by the theorem, of § 45·3, we may see that

$$H_1H_2H_3=H_1\times H_2\times H_3$$

so that $H_1H_2H_3$ is a subgroup of G of order 8.

Proceeding in this manner, we shall arrive at the required result in a *finite* number of steps.

Groups of order 4. We have already come across the following two groups of order 4 which are not isomorphic :

(*i*) The multiplicative group formed of the four numbers :

$$1,\ -1,\ i,\ -i \text{ where } i=\sqrt{-1},$$

which are the four fourth roots of unity.

This group is cyclic.

(*ii*) The group formed of the four permutations :

$$I,\ (ab),\ (cd),\ (ab)(cd).$$

This group is Abelian but non-cyclic.

It may be easily seen that this group is the direct product of its two sub-groups

$$\{I, (ab)\}; \{I, (cd)\}$$

both of order 2.

We shall now see that there are only *two* abstract groups of order 4 respectively isomorphic to the two above groups.

Let G be any group of order 4. Each non-identity element of G is either of order 2 or 4. If G has an element of order 4, it is necessarily cyclic. In the alternative case, each non-identity element is of order 2 and accordingly, by the lemma, it is Abelian and a direct product of its two sub-groups of order 2 each. Thus we have proved the required result in as much as we have *a cyclic group of order* 4 and *an Abelian non-cyclic group of order* 4. This latter group is such that each non-identity element is of order 2 and it is accordingly known as the quadratic group. This is also known as *the Four group* or *The Klien group*. The three non-identity elements of this group are such that the product of any two equals the third.

Groups of order 6. We have already come across the following two groups of order 6

(*i*) The multiplicative group formed of the six sixth roots of unity, *viz.*

$$\pm 1, \cos\frac{\pi}{3} \pm i \sin\frac{\pi}{3}, \cos\frac{2\pi}{3} \pm i \sin\frac{2\pi}{3}.$$

This group is cyclic.

(*ii*) The symmetric group $\mathbf{P}_3$ of degree 3.

It will now be shown that there are only two abstract groups of order 6 respectively isomorphic to the two groups above.

An element, other than the identity of a group of order 6 is necessarily of order 2, 3 or 6. Further a group of order 6 with an element of order 6 is necessarily the cyclic group of order 6.

For the following we suppose that the group G has no element of order 6, *i.e.*, we consider only non-cyclic groups G of order 6.

Now, not each element, other than the identity, can be of order 2, for the order of such a group would necessarily be some power of 2. Thus G must have at least one element of order 3. Let, a, denote an element of G of order 3. Then the set of elements

$$e, a, a^2 \qquad (1)$$

is a sub-group, say, H of G ; e denoting the identity.

Let b denote an element of G which, however, does not belong to the sub-group H.

Then the set of elements

$$b,\ ab,\ a^2b \tag{2}$$

is the coset Hb of the sub-group H. Accordingly these are three different elements of G and also different from each of the 3 elements in (1). Thus

$$e,\ a,\ a^2,\ b,\ ab,\ a^2b \tag{3}$$

are the 6 different elements of G.

Now ba, being a member of G, must be equal to some one of the six elements in (3)

Since

$$ba=e \longrightarrow b=a^2,\ ba=a \longrightarrow b=e,$$
$$ba=a^2 \longrightarrow b=a,\ ba=b \longrightarrow a=e.$$

we see that ba must be different from each one of e, a, a^2, b. Thus we have only the two possibilities

$$ba=ab,\ ba=a^2b.$$

Again b^2, being a member of G, must be equal to some one of the elements in (3).

Since

$$b^2=b \longrightarrow b=e,\ b^2=ab \longrightarrow b=a,\ b^2=a^2b \longrightarrow b=a^2,$$

we see that b^2 must be different from each one of b, ab, a^2b.

Again if $b^3=a$, we have

$$b^3=ab\neq e,\ b^4=a^2\neq e,\ b^5=a^2b\neq e,$$

so that b is an element of order 6 and we have already excluded the consideration of this case.

We may similarly show that if $b^2=a^2$, then b is an element of order 6.

Accordingly, b^2 must equal e.

Thus we have the following two possibilities :

$$ba=ab,\ b^2=e\ ;\ ba=a^2b,\ b^2=e.$$

Considering the first possibility, we have

$$(ba)^2=a^2,\ (ba)^3=b,\ (ba)^4=a,\ (ba)^5=ba^2,\ (ba)^6=e$$

so that ba is an element of order six, and we are not considering this possibility.

Thus, only, one possibility remains, *viz.*,

$$ba=a^2b,\ b^2=e.$$

It may be easily seen that this group is the direct product of its two sub-groups

$$\{I, (ab)\}; \{I, (cd)\}$$

both of order 2.

We shall now see that there are only *two* abstract groups of order 4 respectively isomorphic to the two above groups.

Let G be any group of order 4. Each non-identity element of G is either of order 2 or 4. If G has an element of order 4, it is necessarily cyclic. In the alternative case, each non-identity element is of order 2 and accordingly, by the lemma, it is Abelian and a direct product of its two sub-groups of order 2 each. Thus we have proved the required result in as much as we have *a cyclic group of order* 4 and *an Abelian non-cyclic group of order* 4. This latter group is such that each non-identity element is of order 2 and it is accordingly known as the quadratic group. This is also known as *the Four group* or *The Klien group*. The three non-identity elements of this group are such that the product of any two equals the third.

Groups of order 6. We have already come across the following two groups of order 6.

(*i*) The multiplicative group formed of the six sixth roots of unity, *viz.*

$$\pm 1, \cos\frac{\pi}{3} \pm i \sin\frac{\pi}{3}, \cos\frac{2\pi}{3} \pm i \sin\frac{2\pi}{3}.$$

This group is cyclic.

(*ii*) The symmetric group $\mathbf{P}_3$ of degree 3.

It will now be shown that there are only two abstract groups of order 6 respectively isomorphic to the two groups above.

An element, other than the identity of a group of order 6 is necessarily of order 2, 3 or 6. Further a group of order 6 with an element of order 6 is necessarily the cyclic group of order 6.

For the following we suppose that the group G has no element of order 6, *i.e.*, we consider only non-cyclic groups G of order 6.

Now, not each element, other than the identity, can be of order 2, for the order of such a group would necessarily be a power of 2. Thus G must have at least one element of order 3. Let, a, denote an element of G of order 3. Then the set of elements

$$e, a, a^2$$

is a sub-group, say, H of G, e denoting the identity.

Let b denote an element of G which, however, does not belong to the sub-group H.

Then the set of elements

$$b,\ ab,\ a^2b \tag{2}$$

is the coset Hb of the sub-group H. Accordingly these are three different elements of G and also different from each of the 3 elements in (1). Thus

$$e,\ a,\ a^2,\ b,\ ab,\ a^2b \tag{3}$$

are the 6 different elements of G.

Now ba, being a member of G, must be equal to some one of the six elements in (3)

Since

$$ba=e \longrightarrow b=a^2,\ ba=a \longrightarrow b=e,$$
$$ba=a^2 \longrightarrow b=a,\ ba=b \longrightarrow a=e.$$

we see that ba must be different from each one of e, a, a^2, b. Thus we have only the two possibilities

$$ba=ab,\ ba=a^2b.$$

Again b^2, being a member of G, must be equal to some one of the elements in (3).

Since

$$b^2=b \longrightarrow b=e,\ b^2=ab \longrightarrow b=a,\ b^2=a^2b \longrightarrow b=a^2,$$

we see that b^2 must be different from each one of b, ab, a^2b.

Again if $b^2=a$, we have

$$b^3=ab\neq e,\ b^4=a^2\neq e,\ b^5=a^2b\neq e,$$

so that b is an element of order 6 and we have already excluded the consideration of this case.

We may similarly show that if $b^2=a^2$, then b is an element of order 6.

Accordingly, b^2 must equal e.

Thus we have the following two possibilities :

$$ba=ab,\ b^2=e\ ;\ ba=a^2b,\ b^2=e.$$

Considering the first possibility, we have

$$(ba)^2=a^2,\ (ba)^3=b,\ (ba)^4=a,\ (ba)^5=ba^2,\ (ba)^6=e$$

so that ba is an element of order six, and we are not considering this possibility.

Thus, only, one possibility remains, *viz.*,

$$ba=a^2b,\ b^2=e.$$

We have also the relation

$$a^3 = e.$$

With the help of these 3 relations and on the assumption of the composition being associative, we may complete the multiplication table for the six elements.

To see that the six elements do constitute a group, we have yet to verify the fact of associativity. The direct verification is, however, very laborious. Anyhow, we see from above that there exists, at the most, one non-cyclic group of order six.

Since, we already know that there exists a non cyclic group of order six, *viz.*, the symmetric group $\mathbf{P}_3$ of degree 3, we see in view of the preceding discussion, *that there exists one and only one non-cyclic group of order six.*

From this we may also conclude the associativity of the composition and the fact that there is *an abstract group of order six generated by two elements a, b which are subjected to the defining relations*

$$a^3 = e,\ b^2 = e,\ ba = a^2b.$$

Finally this latter group is isomorphic to $\mathbf{P}_3$. To exhibit an somorphism, we proceed as follows :

Supposing that the objects permuted are 1, 2, 3, the elements of $\mathbf{P}_3$ are

$$(1)(2)(3),\ (123),\ (132),\ (12),\ (23),\ (31).$$

In any isomorphism of the group $G \equiv \{a, b\}$, generated by a, b, with $\mathbf{P}_3$, the element a, can correspond only to (123) or (132) and b only to (12), (23) or (31) for corresponding elements are of the same order in every isomorphism. We write

$$\rho = (123),\ \sigma = (12).$$

Then the permutations

$$I,\ \rho,\ \rho^2,\ \sigma,\ \rho\sigma,\ \rho^2\sigma$$

are

$$I,\ (123),\ (132),\ (12),\ (13),\ (23)$$

respectively.

Consider now the mapping

$$\begin{aligned} e &\longrightarrow I, & b &\longrightarrow \sigma = (12) \\ a &\longrightarrow \rho = (123), & ab &\longrightarrow \rho\sigma = (13) \\ a^2 &\longrightarrow \rho^2 = (132), & a^2b &\longrightarrow \rho^2\sigma = (23) \end{aligned}$$

of G onto $\mathbf{P}_3$

Comparing the multiplication table of $\mathbf{P}_3$ with that of G, we may see that the mapping in question is certainly an isomorphism.

Groups of order 8. The following four groups each of order 8 such that no two are isomorphic are already known to us.

(*i*) The multiplicative group formed of the eight eighths roots of unity.

This is the cyclic group of order 8.

(*ii*) The sub-group of $\mathbf{P}_6$ which is the direct product of its three sub-groups

$$\{I, (ab)\}, \{I, (cd)\}, \{I, (ef)\}$$

each of which is cyclic of order 2.

(*iii*) The sub-group of $\mathbf{P}_6$ which is the direct product of its two sub-groups

$$\{I, (abcd), (ac)(bd), (adcb)\},$$

$$\{I, (ef)\}$$

which are cyclic of orders 4 and 2 respectively.

Three groups above are all Abelian ; one cyclic and the other two non-cyclic.

(*iv*) The Dihedral group $\mathbf{D}_8$ and the corresponding sub-group of $\mathbf{P}_6$ isomorphic to it.

We shall now consider the survey of all possible groups of order 8.

Let G be any group of order 8. Each non-identity element of G is of order 2, 4 or 8.

If G has an element of order 8, then it is necessarily cyclic and isomorphic to the group considered in (*i*) above.

If each non-identity element of G is of order 2, then it is *Abelian and direct product of three sub-groups each of order 2 so* that the group is ismorphic to the one considered in (*ii*) above.

Now suppose that G has an element a of order 4 so that the four elements

$$a, a^2, a^3, a^4 = e$$

form a subgroup, say H, of G.

Suppose that b is an element of G not belonging to H. The the elements

$$ab, a^2b, a^3b, b$$

form the coset Hb of H in G. We have

$$G = H \cup Hb.$$

We have, now,

$ba = a \longrightarrow b = e$, $\quad ba = a^2 \longrightarrow b = a$

$ba = a^3 \longrightarrow b = a^2$, $\quad ba = a^4 \longrightarrow b = a^3$

$ba = a^2b \longrightarrow bab^{-1} = a^2 \longrightarrow ba^2b^{-1} = e \longrightarrow a^2 = e$

$ba = b \longrightarrow a = e.$

Thus we are left with only two possibilities, *viz.*,

$$ba = ab,\ ba = a^3b.$$

We may similarly show that in respect of b^2, we have only the two following possibilities :

$$b^2 = a^2,\ b^2 = e.$$

Thus we have the following *four* alternatives in respect of ba and b^2 :

$$ba = ab,\ b^2 = a^2\ ; \qquad ba = ab,\ b^2 = e$$

$$ba = a^3b,\ b^2 = a^2\ ; \qquad ba = a^3b,\ b^2 = e$$

In each case, we have further

$$a^4 = e.$$

In the case

$$ba = ab,\ b^2 = e,\ a^4 = e,$$

we have, as may be easily seen,

$$G = \{e, a, a^2, a^3\} \times \{e, b\},$$

so that it is the direct product of two cyclic groups of orders 4 and 2 respectively and hence isomorphic to the group considered in (*iii*).

In the case

$$ba = ab,\ b^2 = a^2,\ a^4 = e,$$

we have

$$(ba)^2 = baba = bbaa = b^2a^2 = a^2a^2 = e,$$

so that ba is an element of G of order 2.

It may be seen that, in this case,

$$G = \{e, a, a^2, a^3\} \times \{e, ab\}$$

and we have again the case of (*iii*).

We are now left with only 2 possibilities.

We may now set up the multiplication table for the 8 elements

$$e, a, a^2, a^3, b, ab, a^2b, a^3b, \qquad (1)$$

where a, b are subject to the relations

$$ba=a^3b,\ b^2=e,\ a^4=e. \tag{2}$$

It may now be seen that in this case, we actually have a group isomorphic to the dihedral group D_8. In fact, it may be seen that the mapping

$$(1234) \longrightarrow a$$
$$(13) \longrightarrow b$$

determines an isomorphic mapping of the Dihedral group consisting of the permutations

$$I,\ (1234),\ (13)(24),\ (1432),\ (13),\ (12)(34),\ (24).(14)(23)$$

on the set of elements (1) in respect of the composition defined by (2)

Finally, we set up the multiplication table for the 8 elements

$$e,\ a,\ a^2,\ a^3,\ b,\ ab,\ a^2b,\ a^3b \tag{3}$$

where a, b are subject to the relations

$$ba = a^3b,\ b^2=a^2,\ a^4=e. \tag{4}$$

Again, we may see that the elements (3) subject to the relations (4) do constitute a group. To show this, we may first establish that the 8 matrices

$$\pm I,\ \pm i,\ \pm j,\ \pm k$$

where

$$I=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad i=\begin{bmatrix}\sqrt{-1} & 0\\ 0 & \sqrt{-1}\end{bmatrix}$$

$$j=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},\ k=\begin{bmatrix}0 & \sqrt{-1}\\ \sqrt{-1} & 0\end{bmatrix}$$

form a group and the mapping

$$i \longrightarrow a,\ j \longrightarrow b$$

determines an isomorphic mapping of this group of matrices on the set of elements (3) in respect of the composition defined by (4).

It may be seen that, we have in this case,

$$i^2=-I,\quad j^2=-I,\quad k^2=-I,$$
$$ij=k,\quad jk=i,\quad ki=j,$$
$$ji=-k,\quad kj=-i,\quad ik=-j.$$

The group is, in this case, known as the **Quaternion group.**

Thus we have 5 groups of order 8, three of which are Abelian and two non-abelian.

The two non-abelian groups are known as the

Octic or the Dihedral group and the Quaternion group.

Exercises

1. Show that the number prime to 15, under multiplication and remaindering modulo 15, form a group isomorphic with the direct product $C_4 \times C_2$ of cyclic groups C_4 and C_2 of orders 4 and 2 respectively.

2. In the symmetric group $\mathbf{P}_6$ of permutations on six symbols, determine all the elements that commute with the permutation (123) (456) and hence (or otherwise) obtain the number of elements of $\mathbf{P}_6$ conjugate to (123) (456).

3. G is an Abelian group written additively and Γ is a group of automorphisms of the same written multiplicatively. In the set F of all pairs (α, a) with $\alpha \in \Gamma$ and $a \in G$, a binary composition $\times$ is defined by the equality

$$(\alpha, a) \times (\beta, b) = (\alpha\beta, b\alpha + a\beta),$$

where $b\alpha$ denotes the image of $b \in G$ by $\alpha \in \Gamma$.

Show that F is a group under $\times$ if and only if Γ is Abelian and that if F is a group, it is an Abelian group.

Assuming, that F is a group, find sub-groups G' and Γ' isomorphic to G and Γ respectively and determine the order of (α, a) in F in terms of the orders of α in Γ and a in G.

4. The central of a group G is of finite index $f > 1$. Show that every element of G has fewer than f conjugates.

5. Denote by $\mathbf{P}_4$ the symmetric group of degree 4 and by $\mathbf{V}$ the four-group.

(*a*) Show that $\mathbf{V}$ is a normal sub-group of $\mathbf{P}_4$.

(*b*) Find a group of permutations which is isomorphic with the quotient group $\mathbf{P}_4/\mathbf{V}$.

(*c*) Show that

$$G = \mathbf{V} \cup (12)\mathbf{V}$$

is a sub-group but not a normal sub-group in $\mathbf{P}_4$.

(*d*) What is the normaliser of G in $\mathbf{P}_4$?

6. Give examples to show that for a group all automorphisms may be inner or all (excepting of course the identity) may be outer. Also prove that every group of order greater than 2 has automorphisms different from the identical one.

7. Show that the roots of the equation $x^{14} = 1$ form a cyclic group G under multiplication and determine all its generators. Hence, or otherwise, find all the automorphisms of G and distinguish between inner and outer automorphisms.

8. Show that every self-conjugate sub-group of a group G is the kernel of some homomorphic mapping of G.

9. Show that the dihedral group $\mathbf{D}_{12}$ has a central Z of order 2. Decompose $\mathbf{D}_{12}$ into cosets of Z and show that the quotient group $\mathbf{D}_{12}/Z$ is isomorphic to the symmetric group $\mathbf{P}_3$.

[The member $t_3 \equiv (AD)(BE)(CF)$ of $\mathbf{D}_{12}$ is commutative with each member of $\mathbf{D}_{12}$. Verify by direct computation.]

10. If a group G of order 8 contains an element a of order 4 and an element b such that $ab \neq ba$, show that $ba = a^3b$ and that b^2 is equal either to the identity or to a^2.

11. Show that the group with two generators a, b and defining relations

$$a^{-1}ba=b^{-1},\ b^{-1}ab=a^{-1}$$

is of order 8 and isomorphic to the quaternion group.

12. Prove that the rotations that leave a regular tetrahedron T invariant in space form a group G of order 12 and represent G as a permutation group on the vertices of T.

Prove that the order of a class of conjugate elements of a finite group divides the order of the group. Decompose G into classes of conjugate elements.

13. Define a composition series of a group.

Prove the Jordan Holder theorem of two different composition series of the same finite group.

Find all composition series of the groups of all permutations on 3, 4 and 5 objects.

14. Find all the composition series of all the groups of order 8.

15. An element C of a finite group G is of order mn where m and n are relatively prime numbers. Prove that C can be expressed in one, and only one, way as the product of two commuting elements, A and B, which are of orders m and n respectively.

16. If G is the symmetric group of all permutations on n elements of a set, prove that any element g of G is of the form

$$C_{\alpha_1} \cdots\cdots C_{\alpha_k}$$

where C_α is a cyclic permutation on α of the elements, and the $\sum_1^k \alpha_i$ elements permuted by $C_{\alpha_1}, \ldots\ldots, C_{\alpha_k}$ is a derangement of the set E. If

$$g=C_{\alpha_1}\cdots\cdots C_{\alpha_r},\ h=C_{\beta_1}\cdots\cdots C_{\beta_s},$$

show that there exists an element t of G such that

$$g=t^{-1}ht,$$

if and only if the set $\alpha_1, \ldots\ldots, \alpha_r$ is a derangement of $\beta_1, \ldots\ldots, \beta_s$.

17. Define the normaliser of an element in a group and show that the intersection of all normalisers of elements of a group is the centre of the group.

The centre of the group G has finite index $c>1$ in G. Show that no class of conjugate elements of G contains more than, $c-1$, different elements. Hence or otherwise prove that c is not a prime number.

18. Show that the non-abelian group of order 6 can not be the commutator group of any group.

19. Show that the centre of a group cannot itself be the normaliser of an element unless the group is abelian.

If C_a is the normaliser of the element a in the group G, show that the index $(G : C_a)$ equals the number of conjugates of a in G.

20. A group G of order ab has a subgroup A of order a and subgroup B of order b such that $G=AB$. Show that

(i) A and B have only the unit element in common.

(ii) $G=BA$.

(iii) If A' is conjugate to A and B' conjugate to B then $G=A'B'$ and A', B' have only the unit element in common.

If G is the alternating group of degree 6 and A a cyclic sub-group of order 6, find a sub-group B of order 60 such that $G=AB$.

21. Find how many permutations of a, b, c, d, e, f leave

$$(a+b)(c+d)(e+f)$$

invariant and do the same for

$$(a+b)(c+d+e+f).$$

How many permutations are in the set common to these two groups. Write out explicity the even permutation of the latter set and say, giving the reason for your statement, what type of group these constitute.

22. Show that the group $\mathbf{D}_8$ of coincidence rotations of a square has as its homomorphic image a certain group of permutations of its

(*i*) diagonals, (*ii*) axes, (*iii*) faces

and obtain the three corresponding normal sub-groups of $\mathbf{D}_8$. Also prove that $\mathbf{D}_8$ has apart from the whole group and the identity, one and only one normal sub group besides these three.

23. Show that a group of order p^2 is necessarily Abelian ; p being prime.

24. G is the set of all elements of the form

$$(x, y, z)$$

where x, y z are integers. Two elements (x, y, z) and (x', y', z') are considered to be identical if and only if

$$x\equiv x',\ y\equiv y',\ z\equiv z' \pmod p,$$

where p is a given prime number. Multiplication in G is defined by

$$x, y, z)(x', y', z')=(x+x', y+y', xy'+z+z').$$

Prove that G is a group of order p^3. Show that G is not Abelian and the set H of all elements (x, x, z) is an Abelian sub-group of G of order p^2.

Prove also that when $p=2$, H is cyclic and that when $p>2$, every element of H, other than the identity, is of order p.

25. Prove that in a permutation group of order n, number of even permutations is either n or $\frac{1}{2}n$. If

$$a=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, b=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

show that ab and ba generate a group of order 4, and deduce that the group G generated by a and b is of order 12.

Show that a and b are conjugates in the symmetric group of all the permutations on 1, 2, 3, 4.

26. Show that the dihedral group $\mathbf{D}_{12}$ has a central Z of order 2. Arrange the 12 elements of $\mathbf{D}_{12}$ as cosets of Z and show that

$$\mathbf{D}_{12}/Z \cong \mathbf{P}_2.$$

Put down all the normal sub-groups of $\mathbf{D}_{12}$.

27. A group G_1 has independent generators a, b which are subject to

$$a^2=b^2=(ab)^2=e.$$

Show that G_1 is of order 4 and write out its multiplication table.

A group G_2 has independent generators a, b which are subject to

$$a^2=b^3=(ab)^2=e.$$

Show that

$$ab,\ ba,\ a^2ba^2$$

which may be assumed to be all distinct, are all of order 2 and that together with e they constitute a sub-group H isomorphic with G_1.

Show that $Ha=aH$ and that H is an invariant sub group of G_2.

28. Discuss the group D of rotations which send a regular dodecahedron on (with fixed centre) into itself. Show that D is isomorphic with the alternating group on five letters. Determine the classes of conjugates of D.

29. Define the group of rotations of a regular solid. Describe the group of rotations of regular octahedron,

(*i*) when rotations only are allowed,

(*ii*) when reflections in a plane of symmetry also are allowed

30. A group G is generated by elements a, b, c where

$$ac=ca,\ bc=cb$$

and the orders of a, b, c and ab are 4, 2, 2 and 2 respectively. Show that G is of order 16 Find also the normaliser of the sub-group generated by b and c.

A group G is generated by elements a, b with the defining relations

$$a^6=e,\ b^2=a^3=(ab)^2.$$

Show that G is of order 12.

Find also the order of every element of G and find all the sub-groups of G.

31. Give an example of a group G whose commutator subgroup C is neither G nor the identity and which has a subgroup other than C and G whose quotient group is Abelian.

32. It is given that s and t are two elements of a group G which satisfy the equations

$$s^3=t^2=(st)^2=e,$$

where e is the identity of G. Show that

$$st=ts^2$$

and prove that the subgroup generated by s and t contains atleast six elements. If G is the group of permutations on 1, 2, 3, show that

$$s=(123),\ t=(12)$$

satisfy the above equations and that s, t generate G.

33. Split up P_5 into classes of conjugate elements and show that there are two permutations of each type whose product is a 3 cycle. Hence prove that any self conjugate subgroup of P_5 which contains a non-identity permutation contains all even permutations.

34. Show that the commutator group of a direct product is the direct product of the commutator groups of the factors.

35. Show that the group G generated by the elements x, y, z subject to the relations

$$x^3=y^3=z^3x=yx=e,$$

is isomorphic with the group of motions of a plane generated by the rotations through $2\pi/3$ about the vertices of an equilateral triangle lying in the plane.

36. Show that if two elements of a group are conjugate, then so are their inverses.

Show that in the Alternating group of degree four, no permutation of order 3 can be conjugate to its inverse.

37. Prove that those elements of a group G which commute with the square of a given element a of G form a subgroup N and those which commute with a itself form a subgroup of N.

38. Let E be a set and let S denote the set of all subsets of E. Let X, Y be elements of S and let XY be defined to be the member of S consisting of those elements of E which belong to one but not both of X and Y.

Show that with this definition of product, the set S becomes a group.

If E is spilt up into disjoint sets E_1 and E_2 and if S_1 and S_2 denote the sets of all sub-sets of E_1 and E_2 respectively, show that S_1 and S_2 are subgroups of S and that S is their direct product.

39. A group G has the property that for each element of G,

$$g^2 = e.$$

Prove that G is abelian.

If a is an element of G and H is the subgroup generated by a, show that H is self-conjugate and prove that the factor group G/H has the property that the square of each element is the identity element.

If G is finite, what are the possible orders of G.

40. The cross ratio $\lambda = (x_1, x_2, x_3, x_4)$ of four complex numbers x_1, x_2, x_3, x_4 is defined by

$$\lambda = \frac{(x_1 - x_4)(x_3 - x_2)}{(x_1 - x_2)(x_3 - x_4)}.$$

Prove that those permutations of the four symbols x_1, x_2, x_3, x_4 which leave λ invariant form a non cyclic Abelian group V of order 4 and show that V is a normal subgroup of the group of all permutations of the four symbols.

41. A group G is generated by a and b with the defining relations

$$a^3 = e, \quad b^{-1}ab = a^2.$$

Find all conjugates of b.

42. Show that each of the subgroups of the Quaternion group is normal.

Describe a non-abelian group of order 27 the elements of which are all of order 3.

43. Show that the direct product of the Quaternion group and the cyclic group of order 4 contains a sub-group which is not normal.

44. How many automorphisms has a cyclic group of order p where p is prime.

Find all automorphisms of the symmetric groups $\mathbf{P}_3$ and $\mathbf{P}_4$ and show that they are all inner automorphisms.

45. Calculate the orders of all the classes of conjugate elements of the symmetric group $\mathbf{P}_7$.

46. Find the commutator subgroups of

$$\mathbf{P}_3, \mathbf{P}_4 \text{ and } \mathbf{P}_5.$$

47. Express in terms of cycles all elements of the group generated by the permutations

$$(a\ b\ c\ d\ e),\ (b\ c\ e\ d).$$

48. Let G be a finite *regular* permutation group (*i.e.*, the order of G is equal to its degree). Show that every permutation of G is the product of mutually exclusive cycles of the same length.

49. List all abstract groups of orders 9, 10, 11 and 12.

CHAPTER IV

RINGS: THEIR SUB-RINGS AND IDEALS

48. Introduction. A ring is a set with *two* compositions satisfying certain postulates as against a group which is a set with a single suitably restricted composition. Like every abstract concept, the concept of a ring takes its stand upon situations which show concern with different types of entities but which have an underlying common abstract structure. The illustrations which follow the definition will give an idea of the richness of the concept of the ring and of the various contexts in which we meet systems which are rings. The reader would do well also to compare the developments here with those in the study of groups. It would be seen that keeping company with the corresponding developments in the case of groups so far as basic ideas are concerned, the treatment then parts to take note of problems peculiar to the situations where rings arise.

Rings. Def. *A set R with two compositions, to be denoted additively and multiplicatively, is called a ring, if the following postulates are satisfied:*

I. *The set R is an Abelian group for the addition composition.*

II. *Multiplication is associative, i.e.,*

$$(ab)c = a(bc),$$

for every $a \in R$, $b \in R$, $c \in R$.

III. *Multiplication is right as well as left distributive with respect to addition, i.e.,*

$$a(b+c) = ab + ac \text{ ; (Right distributive law)}$$
$$(b+c)a = ba + ca \text{ ; (Left distributive law)}$$

of every $a \in R$, $b \in R$, $c \in R$.

These two distributive laws give relations between the two compositions.

The symbol '0' will denote the identity and, $-a$, the inverse of, a, for the addition composition.

In the event of there being no doubt as to the underlying [illegible] we may also refer to the set R itself as a ring.

The set R with addition composition will be referred to as the **Additive group** of the ring.

Illustrations :

I. Rings of Numbers. The following are some of the examples of rings of numbers : the two compositions being the ordinary addition and multiplication of numbers.

(*i*) Tne ring of all integers.

(*ii*) The ring of all even integers.

(*iii*) The ring of all those integers which are multiples of some given integer m.

(*iv*) The ring of all rational (real or complex) numbers.

(*v*) The ring of all numbers, $a+ib$; a, b being any integers whatsoever.

(*vi*) The ring of all integers $a+\sqrt{2}\,b$; a, b being any rational numbers whatsoever.

The reader would do well to verify in detail the correctness of the statements made.

It may be noted that the set of natural numbers is *not* a ring.

While talking of the rings of numbers, it will be always understood that ring compositions are necessarily the usual addition and multiplication of numbers.

II. Rings of Polynomials. The set of all polynomials

$$a_0+a_1x+\ldots\ldots+a_nx^n$$

with ordinary addition and multiplication of polynomials as the two compositions is a ring when the coefficients $a_0,\ldots, a_n$ are numbers which are members of any ring of numbers such as those given in I above.

III. Rings of Matrices. The set of all $n\times n$ matrices with the addition and multiplication of matrices as the two ring compositions is a ring when the elements are numbers which are members of any ring of numbers such as those given in I above.

IV. Rings of functions. Let R denote the set of all real valued continuous functions defined in an interval [0, 1]. If then f, g denote any two such functions and we define $f+g$. fg as follows

$$(f+g)(x)=f(x)+g(x),\ (fg)(x)=f(x)g(x)$$

so that $f+g$, (fg) is the function which maps each x of [0, 1] on the sum (product) of the images of x by f and g, then R is a ring.

In brief we may say that $f+g$ and fg are defined with reference to pointwise addition and pointwise multiplication.

We may recall to ourselves that f, g being continuous, $f+g$ and fg are also continuous.

The additive identity of this ring is the function which maps each real number x on the number 0. Denoting this also by the symbol '0', we have

$$0(x)=0, \text{ for every } x \in [0, 1]$$

the symbol '0' on the two sides denoting different things. The additive inverse of a function f, denote by $-f$ is such that

$$(-f)x=-[f(x)].$$

We may also have rings of all

(*i*) derivable functions [0, 1],

(*ii*) integrable functions in [0, 1],

(*iii*) analytic functions of a complex variable in any domain,

(*iv*) integral functions of a single complex variable ;

the two compositions being similar to those defined above for continuous functions.

Note. The product of two functions referred to above and denoted by fg should be carefully distinguished from the notion of composite of functions denoted by fog and also by fg.

Ex. Give a detailed proof the fact that the set R with two compositions as defined is a ring in each of the preceding Illustrations.

49. Some general properties of rings.

49·1. Properties of zero and the additive inverses in relation to multiplication.

(*i*) $a0=0$, $0a=0$ *for every* $a \in R$,

(*ii*) $a(-b)=-(ab)$, $(-a)\,b=-(ab)$, $(-a)(-b)=ab$,

for every $a \in R$, $b \in R$,

(*iii*) $a(b-c)=ab-ac$, $(b-c)a=ba-ca$,

for every $a \in R$, $b \in R$, $c \in R$.

Proof. (*i*) We have

$$a0=a\,(0+0)=a0+a0.$$

$$\therefore \quad -(a0)+a0=-(a0)+\,[a0+a0]$$

$$=[-(a0)+a0]+a0=0+a0=a0.$$

$$\therefore \quad 0=a0.$$

Employing left distributive law instead of right, we may similarly show that

$$0a=0 \text{ for every } a \in R.$$

(*ii*) We have

$$0=a0=a\,(-b+b)=a(-b)+(ab).$$

$$\therefore \quad 0+[-(ab)]=[a(-b)+ab]+[-(ab)]$$
$$=a(-b)+\{ab+[-(ab)]\}$$
$$=a(-b)+0$$
$$\therefore \quad -(ab)=a(-b).$$

Employing left distributive law instead of right, we may show that

$$(-a)b=-(ab).$$

Again, using the two results established,

$$(-a)(-b)=-[(-a)b]=-[-(ab)]=ab.$$

(*iii*) We have

$$a(b-c)=a[b+(-c)]$$
$$=ab+a(-c)=ab+[-(ac)]=ab-ac.$$

Using left distributive law, we have

$$(b-c)a=ba-ca.$$

49·2. General associativity of addition and multiplication. It has been shown in § 14, page 35 that the general associative law, as stated there, holds for every associative composition. Thus we see that general associative law holds for the addition and multiplication compositions in any arbitrary ring R.

Thus as defined in Cor. II, page 38, the symbols

$$a^m,\ ma$$

respectively known as *Power* and *Multiple* of a are meaningful when a is any element of a ring R and m is any

(*i*) natural number in the case of a^m,

(*ii*) integer in the case of $m\ a$.

This distinction is there because of the fact that R is a group for addition so that additive identity 0 and additive inverse, $-a$, of *every* a exist but R may not have multiplicative identity and multiplicative inverse a^{-1} of a.

Also as a consequence of the general associative law, we have the following laws of powers and multiples :

$$a^{m+n}=a^m\,a^n,\ (a^m)^n=a^{mn}=(a^n)^m\ ;$$

m, n being arbitrary natural numbers ;

$$(m+n)a=ma+na,\ m(na)=(mn)a=n(ma)$$

m, n being arbitrary integers.

49·3. General Commutative law for addition. As shown in § 16, page 41, the general commutative law holds for every commutative composition. Accordingly the general commutative law holds for addition in every arbitrary ring.

As a consequence of this and the general associative law, we have

$$m(a+b)=ma+mb, \tag{1}$$

where $a \in R$, $b \in R$ and m is any integer.

Note. It may be carefully noticed that m being not a member of R, the equality (1) is *not* a consequence of the laws of distributivity of multiplication with respect to addition in a ring.

50. Types of rings.

50·1. Commutative rings. A ring R is said to be commutative, if the multiplication composition in R is commutative.

Thus the rings of numbers, polynomials and functions considered in I, II and IV of § 48 are all commutative whereas those of Matrices considered in III and V of § 48 are all non-commutative.

50·2. Rings with unity. Inversible elements in a ring with unity. We say that R is a ring with unity if there exists multiplicative identity in R. We shall, in our study of rings, denote the multiplicative identity of a ring with unity by 1 and call the same unity. This symbol must of course not be confused with the integer one also denoted by 1 just as the additive identity denoted by '0' of a ring must not be confused with the integer zero also denoted by the same symbol.

As an illustration, the ring of all integers is one with unity but that of all even integers is one without unity.

The ring of all $n \times n$ matrices with elements as rational numbers is one with unity ; the diagonal matrix with each diagonal element equal to the number 1 is the unity of the ring.

If R is a ring with unity, then an element $a \in R$ is called inversible, if there exists $b \in R$ such that

$$ab=1=ba.$$

Also, then, we write $b=a^{-1}$.

As illustrations, we may see that

(i) 1 and -1 are the only two inversible elements of the ring of all integers, and

(ii) $n \times n$ matrices with real numbers as elements and with non-zero determinants only are inversible.

50·3. Rings with or without zero divisors. Rings with cancellation law. It has been seen that for any arbitrary ring R,

$$0a=0,\ a0=0,\quad \text{for every } a \in R,$$

so that a product of two elements, one of which is, 0, is necessarily 0. There do, however, exist rings wherefor product of some two elements, both non-zero, is zero *i.e.*, we may have $ab=0$ even though

$$a\neq 0,\ b\neq 0.$$

Of course this situation cannot arise for Number rings, since, the product of two non-zero numbers cannot be zero.

The product of two non-zero matrices can be zero ; as for example, we have

$$\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}\begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix}=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}.$$

Again the product of two non-zero functions of the ring of continuous functions considered in IV of § 48 may be the zero function. For example, consider the two functions f and g defined as follows :

$$f(x)=\begin{cases}\frac{1}{3}-x \text{ for } 0\leqslant x\leqslant\frac{1}{3},\\ 0 \text{ for } \frac{1}{3}\leqslant x\leqslant 1;\end{cases}$$

$$g(x)=\begin{cases}0 \text{ for } 0\leqslant x\leqslant\frac{1}{3},\\ x-\frac{1}{3} \text{ for } \frac{1}{3}\leqslant x\leqslant 1.\end{cases}$$

Here, as may be easily seen,

$$fg=0 \text{ but } f\neq 0,\ g\neq 0.$$

As another example, we may see that in the ring of integers with addition and multiplication modulo 6, we have

$$2\times 3=0$$

so that the product of two non-zero elements is 0.

We say that *a ring R is without zero divisors if the product of no two non-zero elements of the same is zero, i e.*, if

$$ab=0 \Longrightarrow a=0 \text{ or } b=0,$$

and in the alternative case we say that R is a ring with zero divisors.

50·31. Cancellation law in a ring. It is possible to express the condition of a ring R being with or without zero divisors in another useful way as we proceed to explain.

We say *that cancellation law holds in a ring R if*

$$a\neq 0,\ ab=ac \Longrightarrow b=c$$

$$\text{and } a\neq 0,\ ba=ca \Longrightarrow b=c,$$

where

$$a \in R,\ b \in R,\ c \in R.$$

Theorem. *A ring R is without zero divisors if and only if the cancellation law holds in R,* i.e.,

R is without zero divisors $\Longleftrightarrow$ cancellation law holds in R.

Suppose that R is without zero divisors.

Let a, b, c be three elements of R such that

$$a \neq 0,\ ab = ac.$$

Now

$$ab = ac \Longrightarrow a(b-c) = 0.$$

As R is without zero divisors and

$$a \neq 0,$$

we must have

$$b - c = 0,$$

i e.,

$$b = c.$$

We may similarly show that

$$a \neq 0,\ ba = ca \Longrightarrow b = c.$$

Thus, the cancellation law holds in R.

Suppose now that the cancellation law holds in R.

Let, if possible,

$$ab = 0, \qquad a \neq 0,\ b \neq 0.$$

We have

$$ab = a0.$$

By virtue of cancellation law, we have

$$b = 0,$$

so that we arrive at a contradiction.

Hence the result as stated.

51. Integral domains. Fields. Division Rings.

51.1. Def. Integral domain. *A ring is called an integral domain if it is*

(i) *commutative*, (ii) *has unity*, (iii) *without zero divisors.*

The most important motivating example of an Integral domain is that of integers. It is this integral domain of integers which has laid down the trend for the possible course of developments *in the* study of abstract integral domains. Thus the study of abstract integral domains consists in examining how far the various *ideas*, processes and results available for the domain of integers are available for the same. This of course will lead to specialisations of the general

concept of an integral domain by the imposition of further restricting postulates so as to bring the treatment in line with that of the ring of integers.

Illustrations.

1. The ring of numbers $a+bi$; a, b being integers is an integral domain.

2. The rings of numbers

$$a+b\sqrt{-3}\ ,\ a+b\sqrt{2},$$

a, b being integers ; are integral domains.

3. Every ring of numbers with unity is an integral domain, for the same is necessarily commutative and without zero divisors.

4. The ring of all polynomials with co efficients as rational (real or complex) numbers is an integral domain.

51·2. Field. Def. *A ring R is called a field if it has at least two elements and*

(i) is commutative, (ii) has unity, (iii) is such that every non-zero element is inversible.

Firstly we shall show that a field is without zero divisors, *i.e.*,

$$ab=0 \Longrightarrow a=0 \text{ or } b=0,$$

where $a \in R$, $b \in R$ and R is a field.

Let $a\neq 0$ so that a^{-1} exists. Then

$$ab=0 \Longrightarrow a^{-1}(ab)=a^{-1}\,0 \Longrightarrow b=0.$$

Similarly we may show that if $b\neq 0$, then a must be zero.

Thus *a field has no zero divisors.* It thus follows that every field is an integral domain but not conversely ; ring of integers being an example of an integral domain which is not a field.

It should also be seen that for a field, unity and zero are distinct elements, *i.e.*,

$$1\neq 0.$$

In fact if, a, be any non-zero element (such an element exists by the definition of a field), we have

$$1=aa^{-1}\neq 0.$$

An important property of a field lies in the fact that if a, b are any two members of a field, then the symbols

$$a+b,\ a-b,\ ab,\ a\div b=ab^{-1} \text{ if } b\neq 0$$

are meaningful and are again elements of the field so that a field is a closed set for the four so called rational operations.

Illustrations. The rings of rational numbers, real numbers and complex numbers are fields.

The ring of numbers $a+b\sqrt{2}$ where a, b are any rational numbers is a field.

The set of integers with addition and multiplication modulo p, p, being prime, is an example of a field with a finite number p of elements. A detailed study of such fields will be made in a later Chapter.

Additive and Multiplicative groups of a field.

It is important to bear in mind another important characterisation of a field as a set, containing at least two elements, and with two compositions, denoted additively and multiplicatively such that

(*i*) the set is an Abelian group for the addition composition,

(*ii*) the set of all non-zero elements is an Abelian group for the multiplication composition,

(*iii*) the multiplication is distributive with respect to addition.

The groups referred to in (*i*) and (*ii*) above are known as the *Additive* and *Multiplicative groups* respectively of the field.

Also it is usual to denote by R^* the set of all non-zero elements of a ring R.

51·3. Division Rings or skew fields. Def. *A ring with at least two elements is called a Skew field or a Division ring if it is a ring with unity and is such that every non-zero element is inversible.*

Thus a skew field distinguishes itself from a field in regard to the multiplication composition being non-commutative.

As in the case of a field, one may show that a skew field is without zero divisors.

The set of all non-zero elements of a skew field forms a multiplicative non-Abelian group.

Illustration. *Skew field.*

The student may easily show that the set of matrices

$$\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}$$

where a, b are complex numbers and $\bar{a}$, $\bar{b}$ denote the complex conjugates of a, b is a skew field for the compositions of Matrix addition and multiplication.

52. Isomorphism of two rings. Relation of isomorphism in the set of all rings. Suppose that R, R' are two rings. We say *that R is isomorphic to R' and in symbols,*

$$R \cong R',$$

if there exists a one-one mapping f of R onto R' such that

$$f(a+b)=f(a)+f(b),\ f(ab)=f(a)\,f(b) \qquad (1)$$

for every $a \in R$, $b \in R$.

Also then f is said to be an isomorphic mapping of R onto R'.

Briefly speaking f is an isomorphic mapping of R onto R', *if it is one-one onto and preserves sums as well as products.*

It may of course be remembered that if R is isomorphic to R', then there may exist more than one isomorphic mapping of R onto R'.

The relations (1) mean that any relation between elements of R expressed in terms of the compositions in R is carried over to a relation between the corresponding elements in R' expressed in terms of the corresponding compositions in R'. Thus

if

$$f(a)=a',\ f(b)=b',\ f(c)=c',\ f(d)=d'$$

we have

$$a+b=c \longrightarrow a'+b'=c',\ ab=d \longrightarrow a'b'=d'.$$

As in the case of groups, we show that the *relation of isomorphism in the set of all rings is an equivalence relation.* Any two isomorphic rings, *i.e.*, rings belonging to the same equivalence class of mutually isomorphic rings are said to be *abstractly identical.*

52·1. The following results may be easily established :

1. Every isomorphic image of an integral domain (field or skew field) is an integral domain (field or skew field).

2. In every isomorphic mapping f of a ring R onto a ring R',

(*i*) the image of the zero of R is the zero of R', *i.e.*,

$$f(0)=0.$$

(*ii*) the image of the negative of an element of R is the negative of the image of the element, *i.e.*,

$$f(-a)=-(f(a)) \text{ for } a \in R.$$

3. Every isomorphic image of

(*i*) a commutative ring is a commutative ring,

(*ii*) a ring with unity is again a ring with unity,

(*iii*) a ring without zero divisors is a ring without zero divisors.

52·2. Transference of ring structure. The following theorem for rings analogous to that of groups may be easily established.

If f is a one-one mapping of a ring R onto a set R' with two compositions denoted additively and multiplicatively such that

$$f(a+b)=f(a)+f(b),\ f(ab)=f(a)\,f(b)$$

then the set R' is a ring.

53. The Quotient field of an Integral domain. By the quotient field K of an integral domain D is meant the smallest field containing D. Thus a field K is a quotient field of an integral domain D, *if K contains D and is itself contained in every field containing D.*

Illustration. The field $\mathbf{Q}$ of rational numbers is the quotient field of the integral domain $\mathbf{J}$ of all integers.

Surely $\mathbf{Q}$ contains $\mathbf{J}$. Moreover, if,

$$a \in \mathbf{J}, b \in \mathbf{J}, b \neq 0,$$

then any field containing $\mathbf{J}$ must necessarily contain

$$ab^{-1} = a/b$$

and $\mathbf{Q}$ is known to consist of just all numbers of the form a/b.

domain admits of a

egral domain and if

$$a \in D,\ b \in D,\ b \neq 0$$

and K is a field containing D, then K being a field and containing as it does the elements, a and $b \neq 0$, it must also contain the element ab^{-1}. Here the symbol b^{-1} has a meaning by vertue of b being a non-zero element of a field. Also we may easily verify that

$$ab^{-1} = cd^{-1} \longrightarrow (ab^{-1})(bd) = (cd^{-1})(bd) \longrightarrow ad = bc,$$

$$(ab^{-1} + cd^{-1}) = (ad + bc)b^{-1}d^{-1} = (ad + bc)(bd)^{-1}$$

$$(ab^{-1})(cd^{-1}) = acb^{-1}d^{-1} = (ac)(bd)^{-1}.$$

Now we may write

$$ab^{-1} = a/b$$

as is usual and see that these results take the form

$$\frac{a}{b} = \frac{c}{d} \longrightarrow ad = bc,$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$

$$\frac{a}{b} \div \frac{c}{d} = \frac{ac}{bd}.$$

These considerations give us a clue for the construction of the quotient field of an integral domain as we proceed to do. The symbol (a, b) which we shall introduce in the following is essentially a replacement of ab^{-1} or a/b]

Construction of the quotient field. Let D be any given integral domain.

We set up the set S of all ordered pairs

$$(a, b), \qquad a \in D, b \in D, b \neq 0.$$

and define in the same a relation which will shortly be seen to be an equivalence relation,

We write

$$(a, b) \sim (c, d)$$

if and only if

$$ad = bc.$$

We now verify that this is an equivalence relation.

Reflexivity. We have

$$(a, b) \sim (a, b) \text{ for } ab = ba.$$

Symmetry. We have

$$(a, b) \sim (c, d) \Longrightarrow ad = bc \Longrightarrow cb = da \Longrightarrow (c, d) \sim (a, b).$$

Transitivity. Let

$$(a, b) \sim (c, d) \text{ and } (c, d) \sim (e, f),$$

so that

$$ad = bc,\ cf = de.$$

This gives

$$adcf = bcde.$$

We now have

$$\begin{aligned} adcf = bcde &\Longrightarrow cd(af - be) = 0 \\ &\Longrightarrow af - be = 0, \text{ if } cd \neq 0, \text{ i.e., } c \neq 0 \\ &\Longrightarrow af = be \Longrightarrow (a, b) \sim (e, f). \end{aligned}$$

The same conclusion may be easily drawn if $c = 0$.

The relation, in question, being an equivalence relation, sets up a partition of S into mutually exclusive classes. We denote by

$$\overline{(a, b)}$$

the equivalence class determined by (a, b).

Now we define addition and multiplication compositions in this set of equivalence classes as follows :

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc,\ bd)}$$

$$\overline{(a, b)}\ \ \overline{(c, d)} = \overline{(ac,\ bd)}.$$

We have firstly to show that these compositions are well defined. In the present context, it means that these compositions, defined as they are in terms of the representatives of the classes, are actually independent of the same. Thus we have to show that if

$$(a, b) \sim (a_1, b_1) \text{ and } (c, d) \sim (c_1, d_1)$$

then

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(a_1, b_1)} + \overline{(c_1, d_1)},$$

and

$$\overline{(a, b)}\ \ \overline{(c, d)} = \overline{(a_1, b_1)}\ \ \overline{(c_1, d_1)}.$$

This amounts to showing that

if

$$ab_1 = ba_1 \text{ and } cd_1 = dc_1$$

then

$$\begin{cases} (ad+bc, bd) \sim (a_1d_1+b_1c_1, b_1d_1), \\ (ac, bd) \sim (a_1c_1, b_1d_1) \end{cases}$$

i.e.,

and

$$\begin{cases} (ad+bc)b_1d_1 = bd(a_1d_1+b_1c_1), \\ acb_1d_1 = bda_1c_1, \end{cases}$$

and these can be easily verified.

We now show that the set of equivalence classes with the addition and multiplication compositions as defined above has a field structure.

(*i*) *Commutativity of addition.*

$$\begin{aligned} \overline{(a, b)} + \overline{(c, d)} &= \overline{(ad+bc, bd)} \\ &= \overline{(cb+da, db)} \\ &= \overline{(c, d)} + \overline{(a, b)}. \end{aligned}$$

(*ii*) *Associativity of addition.*

$$\begin{aligned} [\overline{(a, b)} + \overline{(c, d)}] + \overline{(e, f)} \\ &= \overline{(ad+bc, bd)} + \overline{(e, f)} \\ &= \overline{((ad+bc)f+bde, bdf)} \\ &= \overline{(adf+bcf+bde, bdf)} \\ &= \overline{(adf+b(cf+de), bdf)} \\ &= \overline{(a, b)} + \overline{(cf+de, df)} \\ &= \overline{(a, b)} + [\overline{(c, d)} + \overline{(e, f)}]. \end{aligned}$$

(*iii*) *Existence of Additive identity.*

$$\overline{(a, b)} + \overline{(0, 1)} = \overline{(a \cdot 1 + b \cdot 0, b \cdot 1)} = \overline{(a, b)}$$

so that $\overline{(0, 1)}$ is the Additive identity.

(*iv*) *Existence of Additive Inverse.*

$$\begin{aligned} \overline{(a, b)} + \overline{(-a, b)} &= \overline{(ab + b(-a), b^2)} \\ &= \overline{(0, b^2)} = \overline{(0, 1)}, \end{aligned}$$

so that

$$\overline{(-a, b)} = -\overline{(a, b)}.$$

(v) *Commutativity of multiplication.*

$$\overline{(a, b)}\ \overline{(c, d)} = \overline{(ac, bd)}$$
$$= \overline{(ca, db)} = \overline{(c, d)}\ \overline{(a, b)}.$$

(vi) *Associativity of multiplication.*

$$[\overline{(a, b)}\ \overline{(c, d)}]\ \overline{(e, f)} = \overline{(ac, bd)}\ \overline{(e, f)}$$
$$= \overline{((ac)e, (bd)f)}$$
$$= \overline{(a(ce), b(df))}$$
$$= \overline{(a, b)}\ [\overline{(c, d)}\ \overline{(e, f)}]$$

(vii) *Existence of Multiplicative identity.*

$$\overline{(a, b)}\ \overline{(1, 1)} = \overline{(a, b)},$$

so that $\overline{(1, 1)}$ is the multiplicative identity.

(viii) *Existence of the multiplicative inverse of non-zero elements.*

Let $a \neq 0$ so that $\overline{(a, b)} \neq \overline{(0, 1)}$.

We have

$$\overline{(a, b)}\ \overline{(b, a)} = \overline{(ab, ba)} = \overline{(1, 1)}$$

so that

$$\overline{(b, a)} = [\overline{(a, b)}]^{-1}.$$

(ix) *Distributivity of addition w.r. to multiplication.*

The verification of the law

$$\overline{(a, b)}\ [\overline{(c, d)} + \overline{(e, f)}] = \overline{(a, b)}\ \overline{(c, d)} + \overline{(a, b)}\ \overline{(e, f)}$$

is left to the reader.

Thus the set in question with the addition and multiplication compositions defined in the same is a field.

We shall now show that this field contains an integral domain isomorphic to the given integral domain D.

Consider the mapping ; $f : D \longrightarrow K$ defined by

$$a \longrightarrow \overline{(a, 1)},$$

It may be easily seen that this mapping is such that to two different elements of D correspond different elements of K. Also we have

$$a + b \longrightarrow \overline{(a+b, 1)} = \overline{(a, 1)} + \overline{(b, 1)}$$
$$ab \longrightarrow \overline{(ab, 1)} = \overline{(a, 1)}\ \overline{(b, 1)}$$

Thus we see that the image $f\ D) \subset K$ is isomorphic to D.

Identification of $f(D)$ with D. We now identify $\overline{(a, 1)}$ with a and see that K is actually a field containing the integral domain D.

We thus have

$$\overline{(a\ b)}=\overline{(a, 1)}\ \overline{(b, 1)}=\overline{(a, 1)}\ [\overline{(1, b)}]^{-1}=ab^{-1},$$

so that each element of K is expressible as ab^{-1} where $a \in D$, $b \in D$, $b \neq 0$, Thus K is a quotient field of D.

Also since each quotient field of D must necessarily consist of elements of the form ab^{-1} where $a \in D$, $0 \neq b \in D$, we have seen that any given integral domain has a unique quotient field.

54. Sub-rings. Let S be any sub-set of a ring R. We say that the sub-set S of R is **stable** for the two compositions in R, if

$$a \in S, b, \in S \Longrightarrow a+b \in S, ab \in S.$$

Thus if S is a sub-set of R stable for the two compositions in R, then the compositions in R determine two corresponding compositions in S which to any two elements a, b of S associate the elements $a+b$ and ab of S. These two compositions in S are called **Induced Compositions.**

Def. *A sub-set S of a ring R is called a sub-ring of R, if it is stable for the two compositions in R and is a ring for the induced compositions.*

Conditions for a sub-ring. Theorem. *Necessary and sufficient conditions for a sub-set S of a ring R to be a sub-ring thereof are that*

$$a \in S, b \in S \Longrightarrow a-b \in S, ab \in S.$$

The condition

$$a \in S, b \in S \Longrightarrow a - b \in S,$$

is necessary and sufficient for S to be a sub-group of the additive group of R (§ 21, page 56).

The condition

$$a \in S, b \in S \Longrightarrow ab \in S,$$

means that S is stable for the multiplication composition.

Finally, the induced multiplication composition is associative and is distributive w. r. to the induced addition; the same properties holding good for the compositions in R

Ex. *Show that a sub-set S of a ring R will be a sub-ring of R, if and only if*

$$S+(-S)=S,\ SS \subseteq S.$$

[Refer to the analogous result for groups obtained in § 21, page 56]

[Here, $-S$, denote the set of negatives of the members of S; $S+(-S)$ denote the set obtained on adding each member of S to each member of $-S$; SS denotes the set obtained on multiplying arbitrary pairs of members of S.]

Illustrations

1. The set of all those integers which are multiples of a given integer, say; m viz.,

$$\ldots\ldots, -2m, -m, 0, m, 2m, \ldots\ldots$$

is a sub-ring of the ring of all integers.

Since, as seen in § 21·2, page 57, each subgroup of the additive group of integers consists of the set of all multiples of integers by some given integer m, we see that these are the only sub-rings of the ring of integers.

2. The set of all rational (real) numbers is a sub-ring of the ring of all real (complex) numbers.

3. The set of all integers is a sub-ring of the ring of numbers $a+ib$; a, b being any integers and $i=\sqrt{-1}$.

4. The set of polynomials over the ring of rational (real) numbers is a sub-ring of the ring of polynomials over the ring of real (complex) numbers.

5. The set of all $n \times n$ matrices over the ring of rational (real) numbers is a sub-ring of the ring of $n \times n$ matrices over the ring of real (complex) numbers.

6. The set of all $n \times n$ diagonal matrices over the ring of real numbers is a sub-ring of the ring of all $n \times n$ matrices over the ring of real numbers.

7. The set of all real valued derivable functions in [0, 1] is a sub-ring of the ring of all real valued continuous functions in [0, 1] and this latter is again a sub-ring of the ring of all those functions which are Riemann integrable.

55. **Algebra of the set of sub-sets of a ring.** Let Σ denote the set of all sub-sets of a ring R. If then, S_1, S_2, be two members of Σ, then we can associate to the same, the members

$$S_1 \cup S_2,\ S_1 \cap S_2,\ S_1+S_2,\ S_1-S_2,\ S_1S_2$$

of Σ. The first two compositions in Σ are purely set-theoretic and the remaining three take note of the two ring compositions. Here S_1+S_2 denotes the sub-set of R obtained on adding each member of S_1 to each member of S_2 and similar meanings may be given to S_1-S_2 and S_1S_2.

The following are some of the relations in these compositions and the same may be easily proved :

(i) $\quad S_3(S_1 \cup S_2)=S_3S_1 \cup S_3S_2$.

(*ii*) $S_3+(S_1 \cup S_2)=(S_3+S_1) \cup (S_3+S_2)$

(*iii*) $S_3(S_1 \cap S_2) \subseteq S_3S_1 \cap S_3S_2$

(*iv*) $S_3+(S_1 \cap S_2) \subseteq (S_3+S_1) \cap (S_3+S_2)$

(*v*) $(S_3+S_2)+S_1=S_3+(S_2+S_1)$

(*vi*) $(S_3S_2)\, S_1=S_3(S_2S_1)$.

56. Algebra of the set of sub-rings of ring. Let Σ' denote the set of all sub-rings of a ring R.

We shall now examine various compositions in Σ'.

56·1. Largest sub-ring contained in each of two sub-rings. Intersection of two sub-rings.

Theorem. *The intersection of any two sub-rings is a sub-ring.*

More generally,

the intersection of any arbitrary family of sub-rings is a sub-ring.

These results follow exactly as in the corresponding case of sub-groups on making use of the criteria for a sub-ring obtained in § 54.

The intersection of two sub-rings is the largest sub-ring contained in both in as much it is contained in both and contains every sub-ring contained in both.

56·2. Smallest sub-ring containing a given sub-set of a ring. Theorem. *The intersection of the family of sub-rings which contain a given sub-set of a ring R is the smallest sub-ring containing the given sub-set.*

It may be easily shown by the preceding theorem that this intersection is a sub-ring and is such that it contains the given sub-set and is contained in every sub-ring containing the sub set. Thus it is the smallest sub-ring containing the given sub-set.

The smallest sub-ring containing a given sub-set is said to be *generated* by the sub-set and the same is also said to generate the sub-ring.

It may also be easily shown that tho *smallest sub-ring containing a given sub-set M of a ring R consists of all those elements of R which are expressible as finite sums of products of the form*

$$\pm a_1 a_2 \ldots\ldots a_k$$

where

$$a_1, a_2, \ldots, a_k \in M.$$

All that we have to do is to see that these elements of R do constitute a sub-ring and that these elements must necessarily be contained in every sub-ring which contains M. Clearly also each member of M is an element of this type.

56·21. Composite of two sub-rings. *The smallest sub-ring containing two given sub-rings is called the composite of the sub-rings.*

This is the sub-ring generated by the union of the sub-rings.

Note. It may be easily seen that the set of all sub-rings of a ring is a Lattice for the partial order 'Included in' such that the composite of two sub-rings is the *l. u. b.* and intersection *g. l. b.*

A notation. If S be any sub-ring and $a_1, a_2, \ldots\ldots, a_k$ be any elements of a ring R, then the symbol

$$S[a_1, \ldots\ldots, a_k]$$

with *square* brackets denotes the sub-ring of R generated by S and the elements $a_1, \ldots\ldots, a_k$.

Ex. Explicity describe $\mathbf{J}[\sqrt{-1}]$, $\mathbf{Q}[\sqrt{2}]$, $\mathbf{R}[\sqrt{-1}]$.

Note. If S_1, S_2 are two sub-rings of a ring R, then the subset S_1+S_2 is not, in general, a sub-ring of R. Of course, by § 24, page 63 this is a sub group of the additive group of R, but it may not be stable for the multiplication composition in R.

Later on when we consider special types of sub-rings, known as right ideals, left ideals or two sided ideals, it will be seen that their sum is also the same type of ideal and hence also a sub-ring.

The product set S_1S_2 will be, by § 24, page 63, stable for multiplication if $S_1 S_2 = S_2 S_1$ but this may not be the case for addition.

57. Quotient rings or Residue class rings. Ideals in a ring. We shall now develop ideas for rings corresponding to those for groups relevant to the notion of Quotient groups. We may recall that the notion of quotient groups is based on that of a distinguished type of sub-groups known as Normal Sub-groups. For the notion of quotient rings, we have also to introduce the notion of a distinguished type of sub-rings known as two sided ideals. To arrive at this notion, we proceed to consider some *preliminaries*

Let S be any sub-ring of a ring R.

We shall consider, to start with, the aspect of S as a sub-group of the additive group of R. The addition being commutative, in R, S is a normal sub-group of the additive group of R.

Consider now the set R' of all cosets of the sub-group S relative to the additive group of R. By § 25, page 65, we know that

$$\text{either } S+a=S+b \quad \text{or} \quad S+a \cap S+b=\varphi.$$

Also

$$S+a=S+b \iff a-b \in S.$$

Further, we have the result,

$$(S+a)+(S+b)=S+(a+b).$$

This addition composition in R' is *well defined*, in as much as the sum of two cosets is independent of the particular representatives of the same.

A natural question now arises as to what further conditions, if any, must be imposed on S so that the totality of product elements obtained on multiplying each member of one coset with each member of another again belongs to a coset.

Consider two cosets

$$S+a,\ S+b$$

and any two members

$$\alpha+a,\ \beta+b, \qquad \alpha \in S, \beta \in S$$

of the same respectively. We have

$$(\alpha+a)(\beta+b)=\alpha\beta+\alpha b+a\beta+ab.$$

Here α, β are arbitrary elements of S.

Taking $\alpha=0$, $\beta=0$, we see that ab is a member of the product set.

Again, taking $\alpha=0$ and $\beta=0$ separately, we see that

$$a\beta+ab,\ \alpha b+ab,$$

are elements of the product set to which ab also belongs, whatever members α, β of S may be.

These products would belong to the same coset, if and only if

$$a\beta=(a\beta+ab)-ab \in S,$$
$$\alpha b=(\alpha b+ab)-ab \in S.$$

Thus we arrive at the following additional conditions to be satisfied by the sub-ring S :

(i) $\quad \alpha \in S, b \in R \implies ab \in S.$

(ii) $\quad \beta \in S, a \in R \implies a\beta \in S.$

These considerations lead us to introduce the important concepts of

(i) *Right ideals*, (ii) *left ideals*, and (iii) *two sided ideals*.

Right and left ideals. Def. *A sub-ring S of a ring R is called a right ideal if*

$$\alpha \in S, a \in R \implies \alpha a \in S,$$

and a left ideal if

$$\alpha \in S, a \in R \implies a\alpha \in S.$$

We may note that for a sub-ring, S, we require that each product of a member of S with a member of S should again be a member of S. For a right (left) ideal, S, we, however require a stronger condition, viz., that each product of a member of S with a member of R on the right (left) should again be a member of S.

Two sided ideals. Def. *A sub-ring S is called a two sided ideal or simply an ideal of R if it is both a right as well as left ideal, i.e., if*

$$\alpha \in S,\ a \in R \Longrightarrow a\alpha \in S,\ \alpha a \in S.$$

For commutative rings, the three concepts all coincide.

Illustrations. 1. Each sub-ring is an ideal of the ring of integers. Since, each sub-ring of the ring of integers consists of the multiples of integers by some integer m, we see that these are the only ideals of the ring of integers.

2. The set of all rational numbers is only a sub-ring but not an ideal of the ring of real numbers.

3. Let $\mathbf{Q}[x]$ denote the ring of all polynomials over the ring of rational numbers and let $f_1(x)$, $f_2(x)$ be two given members of the same. Then the set of polynomials

$$\varphi(x) f_1(x) + \psi(x) f_2(x),$$

where $\varphi(x)$, $\psi(x)$ range over $\mathbf{Q}[x]$ is an ideal of $\mathbf{Q}[x]$.

4. The set of Gaussian integers of the form

$$2m+2ni,\ (2m+1)i+(2n+1)i$$

is an ideal of the ring of Gaussian integers. Here m, n are arbitrary integers.

[A number $a+ib$ where a, b are integers is called a Gaussian integer.]

5. The set of all those, $n \times n$ matrices over the ring of real numbers which have some one given column (row) entirely composed of zeros is a left (right) ideal of the set of $n \times n$ matrices over the ring of real numbers.

6. Every ring R possesses two improper ideals ; one R itself and the other consisting of 0 only. These are respectively known as the **unit ideal** and the **null ideal.**

Theorem. *If S is a two sided ideal of a ring R, then the set R' of all cosets $S+a$; a being any arbitrary member of R, is a ring for the two compositions in R' defined as follows :*

$$(S+a)+(S+b) = S+(a+b),$$
$$(S+a)(S+b) = S+(ab).$$

Firstly we have to show that the compositions as given are well defined. The apparent weakness of these definitions is that while we have proposed compositions in the set of all cosets so as to relate uniquely to two given cosets two other cosets to be known as sum and product, the definitions given show dependence upon

particular members of the cosets. We shall now show that in point of fact there is no actual dependence.

Let

$$a' \in S+a,\ b' \in S+b,$$

so that

$$S+a=S+a',\ S+b=S+b'$$

There exist therefore members α, β of S such that

$$a'=\alpha+a,\ b'=\beta+b.$$

$$\therefore \quad a'+b'=(\alpha+\beta)+(a+b)$$

or $$(a'+b')-(a+b)=\alpha+\beta \in S.$$

$$\therefore \quad S+(a'+b')=S+(a+b).$$

Thus

$$S+a=S+a',\ S+b=S+b' \longrightarrow S+(a+b)=S+(a'+b').$$

Again, we have

$$a'b'=(\alpha+a)(\beta+b)$$
$$=\alpha\beta+\alpha b+a\beta+ab.$$

$$\therefore \quad a'b'-ab=\alpha\beta+\alpha b+a\beta \in S\ ;$$

S being a two sided ideal.

$$\therefore \quad S+a'b'=S+ab.$$

Thus

$$S+a=S+a',\ S+b=S+b' \longrightarrow S+ab=S+a'b'.$$

Now to show that R' is a ring.

By § 36, page 94, it follows that the set R' of cosets is an Abelian group for the addition composition.

Again, since

$$[(S+a)(S+b)]\ (S+c)=(S+ab)(S+c)$$
$$=S+(ab)c$$
$$=S+a(bc)$$
$$=(S+a)(S+bc)$$
$$=(S+a)\ [(S+b)(S+c)],$$

the multiplication is associative.

Also $$[(S+a)+(S+b)]\ (S+c)=[S+(a+b)]\ (S+c)$$
$$=S+(a+b)c$$
$$=S+(ac+bc)$$
$$=(S+ac)+(S+bc)$$
$$=(S+a)(S+c)+(S+b)(S+c)$$

so that multiplication is left distributive with respect to addition.

Similarly, we may show that multiplication is also right distributive with respect to addition.

The ring consisting of all the cosets of an ideal of a ring, with the compositions as defined above is known as a **Quotient Ring** or **Difference Ring.** As the cosets of S are also known as residue classes mod, S, we may refer to this ring also as **Residue Class Ring** denoted by R/S.

Note 1. It should be remembered that while the coset $S+(a+b)$ coincides with the totality of elements obtained on adding elements of $S+a$ to those of $S+b$, this is not a fact that the coset $S+(ab)$ coincides with the totality of elements obtained on multiplying elements of $S+a$ with those of $S+b$. All that is true is that the totality of products obtained on multiplying members of $S+a$ with those of $S+b$ *is contained* in $S+ab$.

Yet, however, $S+ab$ is completely determined by the cosets

$$S+a,\ S+b.$$

Note 2. We shall find it convenient, in the following, to denote each coset $S+a$ by the symbol $[a]$ in case there is no possibility of confusion about the ideal in equation.

Thus we have

$$[a]+[b]=[a+b],\ [a][b]=[ab].$$

If, as in § 25 1, page 66, we write

$$a \equiv b \pmod{S}$$

and say that a is congruent to b mod S, to denote that

$$b-a \in S$$

then the coset $[a]$ consists of all those elements which are congruent to, a, mod S.

In fact, as may be easily shown,

$$a \equiv b \pmod{S,}$$

sets up an equivalence relation in R such that the cosets of S are the equivalence classes for the relation in question.

58. **Ring homomorphisms. Def.** *A mapping f of a ring R onto a ring R' is called homomorphism, if*

$$f(a+b)=f(a)+f(b)$$
$$f(ab)=f(a)\,f(b)$$

for every

$$a \in R,\ b \in R.$$

Also we then say that R is homomorphic to R' or that R' is a homomorphic image of R and write in symbols

$$R \simeq R'.$$

Note 1. Transference of ring structure. If R is a ring and R' is a *set* with two compositions denoted additively and multiplicatively and there exists a mapping f of R onto R' such that

$$f(a+b)=f(a)+f(b),\ f(ab)=f(a)\,f(b)$$

for every

$$a \in R,\ b \in R,$$

then the set R' is a ring. The proof is left to the reader.

Ex. Use this result to simplify the proof of the theorem on the existence of Residue Class rings.

Note 2. Homomorphism into. If f is a mapping of a ring R *into* a ring R' such that

$$f(a+b)=f(a)+f(b),\ f(ab)=f(a)\,f(b)$$

for every

$$a \in R,\ b \in R,$$

we say that f is a homomorphism of R into R'. It can be seen that $f(R)$ is a sub-ring of R' in this case.

Note 3. The following points about homomorphic mappings may be easily proved; f denoting a homomorphism of R onto (into R');

1. $$f(0)=0.$$

Here 0 on the left (right) denotes the additive identity of $R(R')$.

2. $$f(-a)=-[f(a)];\ a \in R,$$

i.e., the image of the negative of a is the negative of the image of a.

Ex. 1. Show that every homomorphic image of a commutative ring is commutative and that of a ring with unity is one with unity.

Ex. 2. Show that a homomorphic image of an integral domain may *not* be an integral domain.

58·1. Kernel of a ring homomorphism. *If f is a homomrophism of a ring R onto a ring R', then the set S of all those elements of R which are mapped on the additive identity 0 of R' is a two sided ideal of R, i.e., the sub-set, $f^{-1}(0)$, of R is a two sided ideal of the same.*

Let

$$a \in S, b \in S$$

so that

$$f(a)=0, f(b)=0.$$

Also let α be any element of R.

We then have

$$\begin{aligned} f(a-b) &= f[a+(-b)] \\ &= f(a)+f(-b) \\ &= f(a)-f(b)=0-0=0. \end{aligned}$$

$$f(\alpha a)=f(\alpha)f(a)=f(\alpha)0=0,$$

$$f(a\alpha)=f(a)f(\alpha)=0\,f(\alpha)=0.$$

Thus

$$a \in S, b \in S, \alpha \in R \longrightarrow (a-b) \in S, \alpha a \in S, a\alpha \in S.$$

Hence S is a two sided ideal of R.

This two sided ideal S of R is called the *Kernel* of the homomorphism.

58·2. Concerning the totality of homomorphic images of a ring. Theorem on homomorphism. *Every homomorphic image of a ring is isomorphic to some residue class ring thereof. Also, conversely, every residue class ring of a ring is a homomorphic image of the ring.*

Suppose that a ring R' is a homomorphic image of R and f denotes the corresponding homomorphism. Also let S denote the kernel of this homomorphism. We shall then show that

$$R/S \cong R' ;$$

the corresponding isomorphism being defined by

$$S+a \longrightarrow f(a) ; \qquad (1)$$

$S+a \in R/S, f(a) \in R'$.

In (1), $f(a)$ is the f-image of every member of $S+a$.

Firstly we have to see that the mapping (1) is well defined. If α is any member of S, then $\alpha+a$ is a member of $S+a$ and we have

$$f(\alpha+a)=f(\alpha)+f(a)=0+f(a)=f(a).$$

Thus the mapping (1) is well defined.

We now show that it is one-one.

Let

$$f(a)=f(b).$$

We then have

$$f(a-b)=f(a)-f(b)=0,$$

so that

$$(a-b) \in S.$$

Also

$$a-b \in S \Longrightarrow S+a=S+b.$$

Thus

$$f(a)=f(b) \Longrightarrow S+a=S+b.$$

Finally, we have

$$(S+a)+(S+b)=S+(a+b) \longrightarrow f(a+b)=f(a)+f(b),$$
$$(S+a)(S+b)=S+ab \longrightarrow f(ab)=f(a)f(b).$$

Thus we have completely proved tha first part.

We have now to prove that if S be any two sided ideal of R, then

$$R \simeq R/S\,;$$

the corresponding homomorphism being

$$a \longrightarrow S+a. \qquad (2)$$

We have

$$a+b \longrightarrow S+(a+b)=(S+a)+(S+b),$$
$$ab \longrightarrow S+ab \quad =(S+a)(S+b),$$

so that we have proved that the mapping given by (2) is a homomorphism of R onto R/S.

The mapping (2) is known as the **Natural mapping** of R onto R/S ; the kernel of this being the ideal S of R.

Cor. If S is the kernel of the homomorphism f of a ring R onto a ring R', then

$$R/S \cong R',$$

the corresponding isomorphic mapping being given by

$$S+a \longrightarrow f(a)$$

59. **A fundamental theorem.** *Let S be any ideal of a ring R. Let Σ denote the set of all those sub-rings of R which contain S as a sub-ring and let Σ' denote the set of all the sub-rings of the residue-class ring R/S which we denote by R'. Then*

$$T \longrightarrow T/S=T',$$

is a one one mapping of Σ onto Σ'.

Also if T is an ideal of R, then T' is an ideal of R' and

$$R/S \cong R'/T'.$$

This latter is known as the **first law of isomorphism** for rings.

Let T denote any member of Σ so that it is a sub-ring of R containing S, *i.e.*,

$$S \subseteq T \subseteq R.$$

As S is an ideal of R, it is also an ideal of T and accordingly T/S is a meaningful symbol.

Firstly we prove that the mapping

$$T \longrightarrow T/S = T'$$

is a mapping of Σ onto Σ'

Let T' be any member of Σ', *i.e.*, any sub-ring of R/S. Let

$$T = f^{-1}(T'),$$

where f is the natural mapping defined by

$$f(a) = S + a$$

of R onto R/S.

Then, we prove that T is a member of Σ.

Then if

$$a_1 \in T,\ a_2 \in T,$$

so that

$$S + a_1 \in T',\ S + a_2 \in T',$$

we have, T' being a sub-ring,

$$[(S + a_1) - (S + a_2)] \in T',\ (S + a_1)(S + a_2) \in T',$$

i.e.,

$$S + (a_1 - a_2) \in T',\ S + a_1 a_2 \in T',$$

i.e.,

$$a_1 - a_2 \in T,\ a_1 a_2 \in T.$$

Thus T is a sub-ring of R containing S.

Also T' can be written as T/S, *i.e.*, each member of Σ' can be written as T/S for some sub-ring T of R containing S.

Now to show that the mapping is one-one. We shall now prove that

$$T_1/S = T_2/S \Longrightarrow T_1 = T_2,$$

where T_1/S, T_2/S are some two members of Σ'.

Let

$$t_1 \in T_1$$

so that

$$S + t_1 \in T_1/S = T_2/S.$$

There exists, $\therefore$, a member t_2 of T_2 such that

$$S+t_1=S+t_2.$$

$$\therefore \quad t_1 \in S+t_2.$$

$$\therefore \quad t_1 \in T_2.$$

$$\therefore \quad T_1 \subseteq T_2.$$

Similarly

$$T_2 \subseteq T_1.$$

$$\therefore \quad T_1=T_2.$$

Suppose now that T is an ideal of R containing S. We shall prove that T/S is an ideal of R/S. Let $S+a$ be any member of T/S so that a is a member of T and let $S+x$ be any member of R/S. We have

$$(S+x)(S+a)=S+ax \in S+T, \qquad \text{for } ax \in T.$$

$\therefore$ T/S is an ideal of R/S.

We may also easily show that if T/S is an ideal of R/S, then T is an ideal of R.

Consider now the natural homomorphisms :

$$R \simeq R/S=R',$$

$$R' \simeq R'/T'.$$

The resultant of two homomorphisms being a homomorphism, we have

$$R \simeq R'/T'.$$

The kernel of this homomorphism being the ideal T of R, we deduce, from the fundamental theorem of Homomorphism,

$$R/T \cong R'/T'.$$

Second law of isomorphism for rings. *If S is any ideal of a ring R and T any sub-ring of R then*

$$(S+T)/S \cong T/(S \cap T).$$

We shall firstly show that $S+T$ is a sub-ring of R.

Let

$$a \in S,\ b \in S\ ;\ \alpha \in T,\ \beta \in T,$$

so that

$$a+\alpha \in S+T,\ b+\beta \in S+T.$$

Now

$$(a+\alpha)(b+\beta)=ab+a\beta+\alpha b+\alpha\beta.$$

S being an ideal, we have

$$ab \in S,\ a\beta \in S,\ \alpha b \in S.$$

Also

$$\alpha\beta \in T.$$

$$\therefore \qquad (a+\alpha)(b+\beta) \in S+T.$$

Also

$$(a+\alpha)-(b+\beta)=(a-b)+(\alpha-\beta) \in S+T$$

Thus $S+T$ is a sub-ring of R. Also, we have

$$S \subseteq S+T \subseteq R.$$

Again, S being an ideal of R, it follows that S is an ideal of $S+T$. Thus $(S+T)/S$ is meaningful.

In the natural homomorphism

$$f : R \to R' = R/S,$$

each $a \in T$ is mapped on $(S+a) \in R'$

Clearly then

$$f(T)=(S+T)/S.$$

$$\therefore \qquad T \simeq (S+T)/S.$$

The kernel of this homomorphism being $T \cap S$, we have, by the fundamental law of Homomorphism,

$$T/(S \cap T) \cong (S+T)/S.$$

60. Relations compatible with ring structure. *A relation T defined in a ring R is said to be compatible with the ring structure of R, if*

$$aTb,\ cTd \Longrightarrow (a+c)T\,(b+d),\ ac\ T\ bd,$$

for every

$$a \in R,\ b \in R,\ c \in R,\ d \in R.$$

We now suppose that T is also an equivalence relation in the ring R, of course compatible with the ring structure of R. Then the following results may be easily established.

1. The equivalence class $\bar{0}$ determined by the element 0 of R is a two sided ideal S of the ring R. Also the equivalence class $\bar{a}$ determined by any element $a \in R$ is the residue class $S+a$ *of* S in R.

Finally the set of all equivalence classes is the same as the set of all residue classes modulo S.

2. If R' is a homomorphic image of a ring R; f being the corresponding ring homomorphism, then the relation in R defined by

$$aTb \Longleftrightarrow f(a)=f(b),$$

is an equivalence relation in R compatible with ring structure. Further the set of corresponding equivalence classes in R is such that

(*i*) any two elements of the same equivalence class have the same f-image,

(*ii*) no two elements of different equivalent classes have the same, f-image.

The proofs are left to the reader.

Ex. If S is a two sided ideal of a ring R, show that the relation T in R defined by

$$aTb \Longleftrightarrow a-b \in S,$$

is an equivalence relation in R compatible with the ring structure.

61. Algebra of ideals. Let Σ denote the totality of all the left ideals of a ring R. We shall now describe various useful binary compositions in this set Σ. Exactly similar considerations apply to the sets of all the right ideals and the two sided ideals of R.

61·1. The largest left ideal contained in each of two given left ideals. Theorem. *The intersection of any two left ideals of a ring is again a left ideal of the ring.*

Let I_1, I_2 be two left ideals of R.

We know (§ 22·1, page 58) that

$$I_1 \cap I_2$$

is a subgroup of the additive group of R. Again let

$$a \in I_1 \cap I_2.$$

We have

$$a \in I_1 \cap I_2 \Longrightarrow a \in I_1, a \in I_2$$

Since I_1, I_2 are left ideals,

$$\alpha \in R \Longrightarrow \alpha a \in I_1, \alpha a \in I_2.$$

Thus

$$\alpha a \in I_1 \cap I_2,$$

and accordingly $I_1 \cap I_2$ is a left ideal of R.

As may be easily seen, the left ideal $I_1 \cap I_2$ is the largest left ideal contained in I_1 as well as I_2.

Generalisation. *The intersection of any family of left ideals of a ring is a left ideal.*

The proof is immediate.

61·2. Smallest left ideal containing a given sub-set. It may be easily seen that the intersection of the family of left ideals containing a given sub-set L is the smallest left ideal containing L, in the sense that the same is a left ideal containing L and is contained in every left ideal containing L. The left ideal thus obtained is said to be generated by L and is denoted by (L).

61·3. Sum of two left ideals.

Theorem. *The left ideal generated by the union $I_1 \cup I_2$ of two left ideals is the set I_1+I_2 consisting of the elements of R obtained on adding any element of I_1 to any element I_2.*

By § 24, page 63, I_1+I_2 is a sub group of the additive group of R.

We have

$$a_1 \in I_1, a_2 \in I_2 \Longrightarrow a_1+a_2 \in I_1+I_2.$$

Then

$$\alpha \in R \Longrightarrow \alpha(a_1+a_2)=\alpha a_1+\alpha a_2 \in I_1+I_2.$$

Thus the set I_1+I_2 is a left ideal of R.

Again, we have

$$I_1+I_2 \supseteq I_1,\ I_1+I_2 \supseteq I_2$$

and also any left ideal which contains I_1 as well as I_2 must necessarily contain I_1+I_2.

Thus I_1+I_2 is the smallest left ideal containing the left ideals I_1 and I_2, *i.e.*, the union

$$I_1 \cup I_2.$$

Accordingly,

$$I_1+I_2=(I_1 \cup I_2).$$

61·4. The left ideal generated by a single element. If, a, be any element of R, then the set of elements

$$\alpha a+ma,\ \alpha \in R, m \in \mathbf{J},$$

constitute the left ideal generated by the element, a, of R, in as much as, as may be easily seen, this set is a left ideal and every left ideal containing, a, necessarily contains all the elements of the set in question.

The expression for the elements of the left ideal generated by a can be simplified i R is a ring with unity. In this case, we have

$$a=1\,a\ ;\ 1 \text{ being the unity of } R.$$

$$\therefore \quad \alpha a+ma=\alpha a+m1a$$

$$=(\alpha+m1)a=\beta a,\ \beta \in R.$$

Thus if R is a ring with unity, the left ideal generated by an element, a, consists of the elements

$$\alpha a,\ \alpha \in R.$$

61·5. The left ideal generated by any sub-set. If L be any given sub-set of R, then the set of elements of R expressible in the form

$$\sigma_1 a_1 + \ldots + \alpha_i a_i + m_1 b_1 + \ldots + m_j b_j,$$

where

$$\alpha_1, \ldots\ldots, \alpha_i \in R\ ;\ m_1, \ldots\ldots, m_j \in \mathbf{J},$$

and

$$a_1, \ldots\ldots, a_i,\ b_1, \ldots\ldots, b_j$$

range over the sub-set L is the left ideal (L) generated by L.

In case, however, R is a ring with unity, the left ideal generated by the sub-set L consists of elements of the form

$$\alpha_1 a_1 + \ldots\ldots + \alpha_i a_i,$$

where each, α, ranges over R and each, a, ranges over L.

The following results about right ideals and two sided ideals may now be easily established.

1. The right ideal generated by an element, a, consists of elements of the form

$$a\alpha + ma,\ \alpha \in R,\ m \in \mathbf{J}.$$

The two sided ideal generated by an element, a, consists of sums of elements of the form

$$\beta a \alpha + ma,\ \alpha \in R,\ \beta \in R,\ m \in \mathbf{J}.$$

The form when R is a ring with unity can now be easily stated. Also we may easily describe the elements of the left (two sided) ideal generated by an sub-set L of R.

62. Principal ideals and principal ideal rings. Any ideal of a ring generated by a single element thereof is called a *principal* ideal.

There exist commutative rings for which every ideal is principal. Such rings are known as *principal ideal rings*.

Theorem. *The ring* $\mathbf{J}$ *of integers is a principal ideal ring.*

This follows from § 21 2, page 57. Refer also to the illustration 1, on page 157.

63. Direct product of rings. Let R_1, R_2, be any two rings. We shall now define two compositions on the product set $R_1 \times R_2$ relatively to which, this product set acquires ring structure.

Let

$$(a_1, a_2), (b_1, b_2)$$

be any two elements of the product set $R_1 \times R_2$ so that

$$a_1 \in R_1, b_1 \in R_1, a_2 \in R_2, b_2 \in R_2.$$

We now define two compositions, addition and multiplication, in the product set as follows :

$$(a_1, a_2)+(b_1, b_2)=(a_1+b_1, a_2+b_2)$$
$$(a_1, a_2)(b_1, a_2)=(a_1b_1, a_2b_2).$$

It may be easily seen that the product set $R_1 \times R_2$ has the structure of a ring for the two compositions defined as above. The additive identity for the addition composition in $R_1 \times R_2$ is (0, 0) and the additive inverse of (a_1, a_2) is $(-a_1, -a_2)$. The rings R_1, R_2 may be referred to as the component rings of the product ring $R_1 \times R_2$.

The following facts may now be easily established :

(*i*) Denoting by R_1' the sub set of the elements of $R_1 \times R_2$ of the form $(a_1, 0)$ where a_1 is any arbitrary element of a_1, we may show that R_1' is a two sided ideal of the product ring $R_1 \times R_2$ isomorphic to R_1 ; an isomorphism being given by

$$(a_1, 0) \longleftrightarrow a_1.$$

We may similarly define the two sided ideal R_2' of $R_1 \times R_2$ isomorphic to the ring R_2.

(*ii*) $$R/R_1' \cong R_2', R/R_2' \cong R_1'.$$

(*iii*) Each element of $R_1 \times R_2$ is uniquely expressible as sum of an element of R_1' and an element of R_2'. In fact, we have

$$(a_1, a_2)=(a_1, 0)+(0, a_2).$$

(*iv*) The product of each element of R_1' with each element of R_2' is the (0, 0) of $R_1 \times R_2$. In fact, we have

$$(a_1, 0)(0, a_2)=(a_10, 0a_2)=(0, 0).$$

Generalisation. In a manner analogous to the above, we may also easily define the direct product

$$R_1 \times R_2 \times \ldots\ldots \times R_n \qquad (1)$$

of any finite number of rings

$$R_1, R_2, \ldots\ldots, R_n. \qquad (2)$$

Also we may define the two sided ideals,

$$R_1', R_2', \ldots\ldots, R_n'$$

of the direct product ring (1) respectively isomorphic to the rings (2).

63·1. A ring as direct sum of two sub-rings. Definition. *A ring R is said to be the direct sum of its two sub-rings R_1 and R_2, if*

(i) each element of R is uniquely expressible as sum of an element of R_1 and of an element of R_2 and $R=R_1+R_2$.

(ii) If $x \in R$, $y \in R$ are such that

$$x=x_1+x_2,\ y=y_1+y_2$$

where

$$x_1 \in R_1,\ y_1 \in R_1\ ;\ x_2 \in R_2,\ y_2 \in R_2,$$

then

$$xy=(x_1+x_2)(y_1+y_2)=x_1y_1+x_2y_2.$$

Also we then write

$$R=R_1\dot{+}R_2.$$

It may be shown that if $R=R_1\dot{+}R_2$, then

$$R/R_1 \cong R_2,\ R/R_2 \cong R_1.$$

Theorem. *Necessary and sufficient condition for a ring R to be the direct sum of its two sub-rings R_1 and R_2 are*

(i) R_1 and R_2 are two two-sided ideals of R,

(ii) The, 0, is only element common to R_1 and R_2,

(iii) $R=R_1+R_2$.

(iv) $R_1R_2=\{0\}$.

The conditions are necessary.

Let

$$R=R_1+R_2.$$

Let

$$x=x_1+x_2\ ;\ x \in R,\ x_1 \in R_1,\ x_2 \in R_2$$

Consider the mapping

$$x \longrightarrow x_1$$

of R onto R_1. In view of the fact shat each element of R is uniquely expressible as sum of an element of R_1 and an element of R_2, this mapping is well defined. This mapping, as may be easily seen, is also an homomorphism of R onto R_1 with R_2 as the kernel. Accordingly R_2 is a two sided ideal of R. Similarly R_1 is a two sided ideal of R. Thus we have *(i)*.

Again, *if* an element $a \neq 0$ belongs to R_1 as well as R, we would have

$$a=a+0=0+a,$$

so there exist atleast two ways of expressing an element, a, of R as sum of an element of R_1 and an element of R_2 and we accordingly arrive at a contradiction. Thus we have *(ii)*.

The condition (*iii*) is immediate.

If $$x_1 \in R_1, x_2 \in R_2,$$

we have,

$$x_1x_2=(x_1+0)(0+x_2)=x_10+0x_2=0,$$

and hence

$$R_1R_2=\{0\}$$

Hence (*iv*).

The conditions are sufficient.

By (*iii*) each element of R is expressible as sum of an element of R_1 and an element of R_2.

Let, if possible,

$$x=x_1+x_2=x'+x'', \text{ where } x_1 \in R_1, x' \in R_1, \quad x_2 \in R_2, x'' \in R_2.$$

$$\therefore \quad x_1-x'=x''-x_2 \in R_1 \cap R_2.$$

By (*ii*), $\therefore, x_1-x'=0=x''-x_2.$

$$x_1-x'=0 \Longrightarrow x_1=x',$$

$$x''-x_2=0 \Longrightarrow x_2=x'',$$

so that we have the uniqueness of expression as sum.

Finally

$$(x_1+x_2)(y_1+y_2)=x_1y_1+x_2y_2,$$

for, by (*iv*), $$x_1y_2=0, \ x_2y_1=0.$$

64. The ring of endomorphisms of an Abelian group.

Let G be any Abelian group. We suppose that the composition in G is additively denoted.

Let Σ denote the totality of *all* the endomorphisms of G. It will now be shown that with suitable definitions of addition and multiplication compositions in Σ, the same is equipped with the structure of a ring.

We recall that a mapping f of a group G into itself is an endomorphism, if

$$f(a+b)=f(a)+f(b) \ ; \ a \in G, b \in G.$$

Let f, g be any two endomorphisms of G, *i e*, members of Σ.

Addition Composition. The mapping denoted by $f+g$ of G into itself is defined as follows :

$$(f+g)(a)=f(a)+g(a) \ a \in G,$$

so that $f+g$ is the mapping which maps any element, a, into the sum of the f and g images of the same.

Firstly, we show that $f+g$ is also an endomorphism. We have, when $a \in G, b \in G,$

$$\begin{aligned}(f+g)(a+b)&=f(a+b)+g(a+b)\\&=[f(a)+f(b)]+[g(a)+g(b)]\\&=[f(a)+g(a)]+[f(b)+g(b)]\\&=(f+g)(a)+(f+g)(b),\end{aligned}$$

so that $f+g$ is an endomorphism.

Multiplication Composition.

The product mapping fg is by def., the same as the composite fog so that we have

$$(fg)(a)=f[g(a)].$$

To show that fg is an endomorphism, we have

$$\begin{aligned}(fg)(a+b)&=f[g(a+b)]\\&=f[g(a)+g(b)]\\&=f[g(a)]+f[g(b)]\\&=(fg)(a)+(fg)(b).\end{aligned}$$

Thus fg is an endomorphism.

We now establish the ring structure of the set Σ of endomorphisms of G.

We may recall that two mappings are said to be equal, if they map each element alike

Commutativity of addition.

We have

$$(f+g)(a)=f(a)+g(a)=g(a)+f(a)=(g+f)(a)$$

for every $a \in G$. Thus

$$f+g=g+f.$$

Associativity of addition.

$$\begin{aligned}[(f+g)+h](a)&=(f+g)(a)+h(a)\\&=[f(a)+g(a)]+h(a)\\&=f(a)+[g(a)+h(a)]\\&=f(a)+(g+h)(a)=[f+(g+h)]a\end{aligned}$$

so that

$$(f+g)+h=f+(g+h).$$

Existence of additive identity. We denote by, 0, the mapping of G which maps each element of G into the zero of G, *i.e.*,

$$0a=0 \qquad \text{for every } a \in G.$$

and show that 0 is an endomorphism of G.

Here the reader should notice the difference in the meanings attached to 0 on the left and to 0 on the right.

It may now be shown that

$$f+0=f. \qquad \text{for every } f \in \Sigma.$$

Existence of additive inverse. We define the mapping denoted by, $-f$, as follows :

$$(-f)(a) = -(f(a))$$

and show that $-f$ is itself an endomorphism.

We may now show that

$$f + (-f) = 0,$$

i.e.,

$$[f + (-f)](a) = 0(a) = 0$$

Associativity of multiplication. This has already been proved in § 3.61, page 10, for the multiplication of arbitrary mappings.

Distributivity of addition w.r.t. to multiplication.

We have

$$\begin{aligned}[f(g+h)](a) &= f\{(g+h)(a)\} \\ &= f(g(a) + h(a)) \\ &= f(g(a)) + f(h(a)) \\ &= (fg)(a) + (fh)(a) \\ &= (fg + fh)(a)\end{aligned}$$

so that

$$f(g+h) = fg + fh.$$

We may similarly show that

$$(g+h)f = gf + hf.$$

Thus, Σ, has a ring structure for the addition and multiplication compositions as defined.

The ring Σ of endomorphisms has unity which is the mapping denoted by 1 and defined by $a1 = a$. This ring Σ may not be commutative and may have proper zero divisors.

Illustration. *The ring of endomorphisms of the additive group J of integers is isomorphic to the ring J of integers.*

Let, f, be any endomorphism of the additive group J of integers and let

$$f(1) = a, \qquad 1 \in J, a \in J.$$

We shall firstly show that the f-image of each element of J is fixed as soon as that of 1 is fixed.

By note 3 on page 160,

$$f(0) = 0, f(-x) = -(f(x)).$$

Suppose that x is a positive integer,

$$\begin{aligned}f(x) &= f(1 + 1 + \ldots\ldots \text{ to } x \text{ terms}) \\ &= f(1) + f(1) + \ldots\ldots \text{ to } x \text{ terms}\end{aligned}$$

If x is a negative integer, we have

$$f(x) = f[-(-x)]$$

Thus we see that

$$f(1)=a \longrightarrow f(x)=xa \qquad \text{for each } x \in \mathbf{J}.$$

Thus to each endomorphism f of $\mathbf{J}$, there corresponds an integer a, given by $f(1)=a$. We may also see that to each $a \in \mathbf{J}$, there corresponds an endomorphism of $\mathbf{J}$ defined by

$$f(1)=a.$$

Thus we have a one-one mapping of Σ onto $\mathbf{J}$. The endomorphism associated to $a \in \mathbf{J}$ shall be denoted by f_a so that we write

$$a \longrightarrow f_a$$

defined by $f_a(1)=a$

We now show that

$$f_{a+b}=f_a+f_b,\ f_{ab}=f_a f_b.$$

We have

$$f_{a+b}(1)=a+b=f_a(1)+f_b(1)=(f_a+f_b)(1),$$

$$\therefore \quad f_{a+b}=f_a+f_b.$$

$$f_{ab}(1)=ab=a(f_b(1))=f_a(f_b(1))$$
$$=(f_a f_b)(1).$$

$$\therefore \quad f_{ab}=f_a f_b.$$

Thus the mapping

$$a \longrightarrow f_a$$

is an isomorphic mapping of the ring $\mathbf{J}$ of integers onto the ring Σ of endomorphisms of the additive group $\mathbf{J}$ of integers.

Ex. Determine the ring of endomorphisms of the group formed of 0, 1, 2 when the composition is addition reduced modulo 3.

Theorem. *Every ring with unity is isomorphic to a ring of endomorphisms of an Abelian group.*

This theorem may be thought of as the analogue for rings of Cayley's theorem for groups.

Let R be any ring with unity and let, a, be a member of R.

The mapping denoted by f_a and defined as

$$f_a(x)=ax,$$

is an endomorphism of the additive group of R. In fact, we have

$$f_a(x+y)=a(x+y)=ax+ay$$
$$=f_a(x)+f_a(y).$$

Thus to each given $a \in R$, there corresponds an endomorphism f_a of the additive group of R. We write

$$a \longrightarrow f_a.$$

We now show that

$$f_{a+b}=f_a+f_b,\ f_{ab}=f_a f_b.$$

We have, when $x \in$ the additive group of R,

$$f_{a+b}(x) = (a+b)x$$
$$= ax + bx$$
$$= f_a(x) + f_b(x) = (f_a + f_b)(x)$$

so that

$$f_{a+b} = f_a + f_b.$$

Also

$$f_{ab}(x) = (ab)x = a(bx)$$
$$= a[f_b(x)]$$
$$= f_a[f_b(x)] = (f_a f_b)(x)$$

so that

$$f_{ab} = f_a f_b.$$

This shows that the mapping

$$a \longrightarrow f_a$$

of the ring R into the ring of endomorphisms of the additive group of R is a homomorphism.

The kernel of this homomorphism is the ideal formed of those elements a of R for which $f_a = 0$, *i.e.*,

$$ax = 0 \qquad (1)$$

for every $x \in R$. Since R is a ring with unity, this means that, in particular $a1 = 0$, *i e.*, $a = 0$.

Thus the kernel consists of only one element *viz.*, 0 so that the homomorphism is actually an isomorphism.

65. Sub-fields. Let K denote any field. A sub-ring of K is called a sub-field if it has a field structure relative to the induced compositions. In this connection, we have the following theorem.

Theorem. *Necessary and sufficient conditions for a sub-set L of a field K to be a sub field thereof are that*

(*i*) $a \in L, b \in L \Longrightarrow a - b \in L,$

(*ii*) $a \in L, 0 \neq b \in L \Longrightarrow ab^{-1} \in L.$

The condition (*i*) is necessary and sufficient for the sub-set L to be a sub-group of the additive group of K and the condition (*ii*) is necessary and sufficient for the set formed of non-zero elements of L to be a sub-group of the multiplicative group formed of non-zero element of K.

Hence the theorem.

Theorem. *The intersection of two (or an arbitrary family of) sub-fields of a field K is itself a sub field of K.*

The proof which is an immediate consequence of the preceding theorem is left to the reader.

Sub-field generated by a sub-set S of a field K. The intersection of the family of sub-fields containing S is a sub-field which

we say is *generated by* S. *It is the smallest sub-field containing* the set S.

The sub-field of K generated by S is formed of all those elements of K which are obtainable as a result of a finite number of operations of addition, subtraction, multiplication and division performed on the elements of S; division by zero being of course excluded.

The reader may supply proofs to these statements.

A notation. If S be any sub-field and $a_1, a_2, \ldots\ldots, a_k$ be any elements of a field K, then the symbol

$$S(a_1, \ldots\ldots, a_k)$$

with *circular* brackets denotes the sub field of K generated by S and the elements $a_1, \ldots\ldots, a_k$. Also we say that this sub-field is obtained on *adjoining* elements $a_1, \ldots\ldots, a_k$ to S.

Ex. Explicity describe $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{2}, \sqrt{-1})$, $\mathbf{Q}(\pi)$, $\mathbf{R}(\sqrt{-1})$.

66. Homomorphism of fields.

Theorem I. *A field has no proper ideals.*

This theorem means that if I be any ideal of a field K, then we have

$$\text{either } I=(0) \text{ or } I=K.$$

Suppose that I *is a non-zero ideal of the field* K and, a, is any non-zero element thereof

Then

$$1=a^{-1}a \in I.$$

Again

$$x=x1 \in I \text{ ; } x \text{ being any member of } K,$$

so that

$$I=K.$$

Theorem II. *A non-zero commutative ring with unity is a field if it has no proper ideals.*

This is the converse of the preceding theorem.

Let K be any non-zero commutative ring with unity.

Let, a, be any non-zero member of K. Then *the set of* elements

$$xa$$

where, x, ranges over K is an ideal of K containing a. As this must coincide with K, we see that there must exist an element $b \in K$ such that

$$ba=1,$$

so that we see that each non-zero element of K possesses the *multiplicative* inverse.

Thus K is a field.

Ex. *A non zero ring with unity is a division ring if and only if* it has no proper left (right) ideals. Prove it.

Theorem III. *If f is a homomorphism of a field K into a ring A, then the sub-ring $f(K)$ of A is either a zero ring or a field isomrophic to K.*

The kernel I of the homomorphism being an ideal of the field K, we have

$$\text{either } I=(0) \text{ or } I=K.$$

Now $I=K$ implies that

$$f(x)=0 \text{ for every } x \in K,$$

so that (fK) is the zero ring.

If $I=(0)$, then the kernel consists of 0 alone and the homomorphism f is essentially an isomorphism. Thus in this case f is an isomorphism of the field K onto $f(K)$ which must therefore be a field.

Note. This theorem shows that the concept of the Homomorphic mappings of a field is rather trivial. A homomorphic image of a field is either the zero ring or a field isomorphic to the given field.

67. Maximal ideals.

Def. An ideal I of a ring A is called Maximal, if any ideal T of A containing I coincides with A.

This means that I is maximal if and only if

$$I \subset I' \subseteq A,\ I' \text{ is an ideal} \Longrightarrow I'=A.$$

Theorem. *An ideal I of a commutative ring A with unity is maximal if and only if the residue class ring A/I is a field.*

Since A is a commutative ring with unity, the residue class ring A/I is also commutative with unity.

Let I be maximal and let $I+b$ be any non zero member of A/I so that b does not belong to I.

The ideal generated by the maximal ideal I and the element b not belonging to I being the ring A, we have

$$I+(b)=A=(1).$$

There exist therefore an element $a \in I$ and $\alpha \in A$ such that

$$a+\alpha b=1.$$

We now have

$$\begin{aligned} a+\alpha b=1 &\Longrightarrow 1-\alpha b=a \in I \\ &\Longrightarrow I+1=I+\alpha b=(I+\alpha)(I+b) \\ &\Longrightarrow (I+b)^{-1}=I+\alpha. \end{aligned}$$

Thus $I+b$ is inversible.

The converse is also easy to prove.

Illustration. *The residue class ring* $\mathbf{J}/(p)$ *is a field, if* p *is any prime integer.*

By the preceding theorem, we have to show that (p) is a maximal ideal of $\mathbf{J}$. Let (q) be an ideal of the principal ideal ring $\mathbf{J}$ such that

$$(p) \subset (q) \subseteq \mathbf{J}.$$

This implies that q is a divisor of the prime p without being an associate of the same and we have thus a contradiction.

Thus (p) is a maximal ideal of $\mathbf{J}$ and accordingly $\mathbf{J}/(p)$ is a field.

Obviously $\mathbf{J}/(p)$ is a field with p elements.

Note. The elements

$$(p),\ (p)+1,\ (p)+2,\ \ldots\ldots\ldots,\ (p)+p-1$$

of $\mathbf{J}/(p)$ may as well be denoted by the symbols

$$[0],\ [1],\ [2],\ \ldots\ldots\ldots,\ [p-1]$$

or simply by

$$0,\ 1,\ 2,\ \ldots\ \ldots\ldots,\ p-1$$

where the addition and multiplication compositions are the ordinary addition and multiplication of numbers reduced modulo p.

We shall, in the following sometimes, write

$$\mathbf{J}_p \text{ in place of } \mathbf{J}/(p).$$

68. Characteristic of a field. Each element of a field has a certain order as a member of the additive group of the field. Consider the unity e of the field K. The order of e as a member of the additive group of K may be infinite or finite. If the order is finite, we denote the same by m.

If the order is infinite, then

$$ne=0 \Longleftrightarrow n=0,$$

and if the order, m, is infinite, then

$$ne=0 \Longleftrightarrow m \mid n.$$

We show that if the order is finite, then the finite order m must be some prime integer. Let, if possible,

$$m=m_1m_2,\ m_1\neq 1,\ m_2\neq 1.$$

We have

$$0=me=(m_1m_2)e$$
$$=(m_1e)(m_2e)$$

so that

$$\text{either } m_1e=0 \text{ or } m_2e=0.$$

This, however, is impossible for m is the least positive integer such that $me=0$. Thus m is prime.

Def. A field is said to be with characteristic 0, also sometimes infinity, if the order of the unity e as a member of the additive group is infinity, also the characteristic is said to be p if the order of e is finite and equal to p.

Thus the characteristic of a field is either 0 or a prime integer p.

Fields with non-zero characteristic are known as **Modular Fields.**

Ex. Show that each non-zero element of an integral domain, as a member of the additive group of the same, is of the same order and this order, if finite must be a prime integer. Show also that this result does not hold good for arbitrary rings.

Theorem. *The order of each non-zero element, as a member of the additive group of the field, is infinity or a prime integer p according as the characteristic of the field is zero or p.*

Let a be any non-zero element of the field.

Now

$$ma=0 \longleftrightarrow maa^{-1}=0 \longleftrightarrow me=0$$

so that if the characteristic of the field is 0, then we must necessarily have $m=0$ and if the characteristic is p, then the order of, a, must also be equal to p.

Illustration. The characteristic of the field of rational numbers is zero. In fact the characteristic of every field of numbers is zero.

The characteristic of the field $J/(p)$ is the prime integer p.

Note. *A field with characteristic zero is necessarily infinite* but a field with a non-zero characteristic may be finite or infinite.

69. Prime fields. *A field is said to be prime if it has no subfield other than itself.*

Illustration. The field of rational numbers is a prime field but the field of real numbers is not a prime field. (Prove).

The field $J/(p)$ is prime for each prime integer p. (Prove)

69·1. Structure of Prime fields. As stated above, the field of rational numbers and the field $J/(p)$ for each prime integer p are

prime fields. It will now be shown that, apart from isomorphisms, these are the only prime fields.

Let K be any prime field and let e denote the unit element of the same. Then the sub-field of K generated by e must necessarily coincide with K which is given to be a prime field.

Consider now the mapping f defined by

$$n \longrightarrow ne, \tag{1}$$

of $\mathbf{J}$ into K. This mapping is a homomorphism, for

$$n+m \longrightarrow (n+m)e = ne+me$$
$$nm \longrightarrow (nm)e = (ne)(me).$$

Let I denote the kernel of this homomorphism

Now I is an ideal of $\mathbf{J}$ and each ideal of $\mathbf{J}$ is a princip l ideal. Thus we have

$$I=(0) \text{ or } 1=(a),$$

where, a, is a non-zero member of $\mathbf{J}$.

In case $I=(0)$, the kernel consists of a single element 0 so that the mapping (1) is one-one. Then $f(\mathbf{J})$ is a sub-ring of K isomorphic to the integral domain $\mathbf{J}$. The prime field K, being now the quotient field of the integral domain $f(\mathbf{J})$ is isomorphic to the quotient field of $\mathbf{J}$, viz., the fie'd of rational numbers.

Now suppose that

$$I=(a),\ a\neq 0.$$

We now show that a is a prime integer.

Let, if possible,

$$a=bc\,;\ b\neq 1,\ c\neq 1.$$

We have

$$0=bce=(be)(ce),$$

so that either $be=0$ or $ce=0$ but this is not possible, for each integer x such that $xe=0$ is a multiple of a. Thus, a, is a prime.

We write

$$a=p.$$

We have in this case

$$f(\mathbf{J}) \simeq \mathbf{J}/(p).$$

As $\mathbf{J}/(p)$ is a field, $f(\mathbf{J})$ is itself a field necessarily identical with K. Thus in this case

$$K \simeq \mathbf{J}/(p),$$

so that the prime field K is isomorphic to the residue class field $\mathbf{J}/(p)$ of the ring of integers relative to the ideal generated by a prime p.

Exercises

1. G is an Abelian with additively denoted composition. Multiplication composition is defined in the set G by the rule

$$xy=0, x \in G, y \in G.$$

Show that G is a ring for the two compositions.

2. R is any arbitrary ring and J is the ring of integers. The compositions of addition and multiplication are defined in the product set $\mathrm{J}\times R$ by the rules

$$(m, x)+(n, y)=(m+n, x+y),$$
$$(m, x)(n, y)=(mn, my+nx+xy).$$

Show that the set $\mathrm{J}\times R$ is a ring for the two compositions.

[Here my and nx denote the multiples of the elements y and x of R].

3. Determine all the structures of a ring with n elements for $2\leqslant n\leqslant 6$. Which of these structures are fields ?

4. Show that for any arbitrary ring R, the set of elements commutative with each of its elements is a sub-ring of R. [This sub-ring of R is called the *central* of R].

5. Show that for any arbitrary ring R, and any sub-set S of R, the set of elements $x \in R$ such that $xy=0$ ($yx=0$) for each $y \in S$, is a left (right) ideal of R. [The left (right) ideal thus obtained is called the left (right) *annihilator* of S.]

6. Show that in a ring the left ideal generated by a right ideal is a two sided ideal.

7. Show that the ring of endomorphisms of the Four group is non-commutative and it admits of zero divisors.

Consider also the ring of endomorphisms of the cyclic group of order 4.

8. Show that the ring of endomorphisms of the infinite cyclic group is isomorphic to the ring J of integers.

9. Show that for any arbitrary ring R, the two sided ideal generated by the elements

$$xy-yx,$$

where x and y are arbitrary elements of R, is such that it is contained in every ideal I such that R/I is a commutative ring. [Refer to the theorem on page 98].

10 Show that the set A of all real-valued infinite sequences (a_n) forms a ring, if the operation of addition and multiplication are defined by

$$(a_n)+(b_n)=(a_n+b_n),$$
$$(a_n)(b_n)=(a_nb_n).$$

Given a sub-set E of positive integers, show that the set J_E of all the sequences (a_n) such that $a_n=0$ whenever n belongs to E is an ideal in A.

11. Let R be a ring. A new law of composition T is defined on R by setting

$$aTb=a+b-ab.$$

Show that T is associative. An element a of R is called quasi-regular, if there exists w in R for which

$$a\ T\ w=w\ T\ a=0.$$

Prove that the set Q of quasi-regular elements of R forms a group under T whose identity 0. If R has identity, show further that $a \in Q$ if and only if $1-a$ is an inverse in R.

12. Let $\mathbf{R}$ denote the field of real numbers and let c be a fixed positive real number. Let $\mathbf{S}$ be the set of real numbers x such that $|x| < c$. Prove that the compositions $\dot{+}$, $\dot{\times}$ given by

$$a \dot{+} b = \frac{a+b}{1+abc^{-2}}$$

$$a \dot{\times} b = c \tanh [\tanh^{-1}(ac^{-1}) \tanh^{-1}(bc^{-1})]$$

define internal laws of composition in $\mathbf{S}$ and that $\mathbf{S}$ is a ring with $\dot{+}$ and $\dot{\times}$ as the two ring compositions isomorphic to $\mathbf{R}$.

[**Hint.** You may use the fact that the correspondence

$$x \to c \tanh x$$

maps $\mathbf{R}$ onto $\mathbf{S}$.]

13. Show that the product set

$$\mathbf{R} \times \mathbf{R}$$

is a field for the two compositions defined as follows:]

$$(a, b) + (c, d) = (a+c, b+d),$$

$$(a, b)(c, d) = (ac+bd, ad+bc).$$

Show further that this field is isomorphic to the field $\mathbf{C}$ of complex members

14 Show that the correspondence

$$a + \sqrt{-1}\, b \longrightarrow \begin{bmatrix} a & b \\ -b & a \end{bmatrix}, \qquad a, b \in R,$$

is an isomorphism of the field $\mathbf{C}$ of complex numbers into the ring of 2×2 matrices over $\mathbf{R}$.

15. Show that the set of matrices

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$

is a sub-ring of the ring of 2×2 matrices over $\mathbf{R}$.

16. Show that each element x of the prime field J_p satisfies the equation

$$x^p = x$$

Show that the non-zero elements of the field form a multiplicative cyclic group.

17. Prove that a ring R such that $x^2 = x$ for each $x \in R$, is necessarily commutative.

18. The elements of a 2×2 matrix all belong to the field J_2. Show that there are six such non-singular matrices and that they constitute a group under multiplication. Is this group isomorphic to the symmetric group P_3 of degree 3?

Show that the non-singular 2×2 matrices with elements in J_p, $(p > 2)$ constitute a group G under multiplication of which those of determinant 1 constitute an invariant sub-group H.

What are the cosets of H in G?

If $p = 3$, show that the order of G is 48.

19. If I is an ideal of R, show how to construct a ring S and a homomorphism $x \to f(x)$ of R *onto* S such that

$$f(x)=0 \Longleftrightarrow x \in I.$$

Construct S if R is the ring of integers and I consists of all the multiples of 15. Show that S contains 6 zero divisors other than 0 and that the remaining non-zero element form a group with respect to multiplication.

20. Show that those elements of a group G which commute with the square of a given element, s, of G form a sub-group N and those which commute with, s, itself form a sub-group of N.

If G is the group of all non-singular 3×3 matrices whose elements belong to the field $\mathbf{J}_2$ and

$$s=\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix},$$

show that N consists of the matrices

$$\begin{bmatrix} 1 & a & a \\ b & c & c+1 \\ b & c+1 & c \end{bmatrix}$$

and no others ; a, b, c being any members of $\mathbf{J}_2$. Which of these matrices commute with s.

21. If A denote the matrix

$$\begin{bmatrix} 2 & -2 & 2 \\ 2 & -4 & 5 \\ -2 & 5 & -4 \end{bmatrix}$$

and A' its transpose, show that

$$AA'=I,$$

where I denotes the unit matrix ; the elements being members of the prime field of characteristic 11.

22. Obtain the six non-zero squares in $\mathbf{J}_{13}$.

23. *The symbols a, b denote arbitrary elements of the prime field $\mathbf{J}_p$ and d is a fixed element, not a square of the same field. Show that matrices of the form*

$$\begin{bmatrix} a & b \\ db & a \end{bmatrix}$$

form a field under the usual matrix operations.

Deduce, or otherwise prove, that

$$\begin{bmatrix} a & b \\ db & a \end{bmatrix}^p=\begin{bmatrix} a & -b \\ -db & a \end{bmatrix},$$

24. The elements of the field $\mathbf{J}_7$ are denoted, as usual, by the symbols

$$0, 1, 2, 3, 4, 5, 6.$$

Find the symbol in this set equal to the following :

$$\frac{2-1+4\cdot5+3\div2-2\div(-3)}{3\div4+5\div(-2)-(3\cdot2)+(-6)(-5)}.$$

25. Show that for any two elements a, b of an arbitrary field

$$(a+b)^n=\sum_{r=0}^{n}\frac{n(n-1)\ldots\ldots(n-r+1)}{r\,!}\,a^r b^{n-r}.$$

26. Show that for any two elements a, b of the field $\mathbf{J}_p$.

$$(a+b)^p=a^p+b^p.$$

27. Let I be any ideal of a ring R and A^* be the set of elements $a \in R$ for which some power a^n lies in A. Show that A^* is an ideal of R.

28. Let a and b be elements of a ring R containing a unit element and assume that the element a has a unique inverse in R.

(*i*) Show that all the transformations

$$y=ax+b,$$

form a group G.

(*ii*) Find a proper normal sub-group N of G and describe the quotient group G/N.

(*iii*) Assuming that R is the finite field $\mathbf{J}_p$, find the order of the group G.

29. Show that the direct sum of 2 fields cannot be a field.

30. Show that

$$\mathbf{J}/(6) \cong \mathbf{J}/(2)\dot{+}\mathbf{J}/(3),$$
$$\mathbf{J}/(15) \cong \mathbf{J}/(3)\dot{+}\mathbf{J}/(5).$$

31. Find all the ideals in the direct sum of two rings.

32. Find all the

(*i*) sub-rings, (*ii*) ideals, (*iii*) homomorphic images of

$$\mathbf{J}_6,\ \mathbf{J}_8,\ \mathbf{J}_{11},\ \mathbf{J}_{12}.$$

33. Show that the set of right (left and two sided) ideals in a ring form a *lattice* under the ordinary inclusion relation with the *l.u.b.* given by the sum and *g.l.b.* given by intersection.

34. If I_1, I_2, are two ideals of a commutative ring R with unity, then the set of all elements of R of the form

$$b_1b_2+c_1c_2+\ldots\ldots+l_1l_2$$

where

$$b_1, c_1, \ldots\ldots, l_1 \in I_1\ ;\ b_2, c_2, \ldots\ldots, l_2 \in I_2$$

is an ideal of R. Denoting this ideal by I_1I_2, show further that

$$I_1(I_2+I_3)=I_1I_2+I_1I_3,$$

I_3 being also an ideal of R

35. Show that a finite integral domain is necessarily a field.

36 Show that the set of all automorphisms of a field is a group for the resultant composition.

37. Show that identity is the only automorphism of a prime field.

38. Show that

$$a+bi \longrightarrow a-bi \longrightarrow, a \in \mathbf{R},\ b \in \mathbf{R},\ i=\sqrt{-1}$$

is an automorphism of the field **C** of complex numbers.

39. Find the groups of automorphisms of the following number fields :

(*i*) $\mathbf{Q}(\sqrt{2})$, (*ii*) $\mathbf{Q}(\sqrt{-1})$, (*iii*) $\mathbf{Q}(\sqrt{2}, \sqrt{3})$.

(*iv*) **Q** (ω), where (ω) denotes an imaginary cube root of unity.

40. Show that

$$\mathbf{J}[\sqrt{-3}]/(2)$$

is a field or order 4. Compute the composition tables for its additive and multiplicative groups.

41. Show that the following residue class rings are fields and determine their characteristics :

(*i*) $\mathbf{J}[i]/(3)$. (*ii*) $\mathbf{J}[i]/(1+i)$. (*iii*) $\mathbf{J}[i]/(3+2i)$.

42. Show that the following residue class rings are *not* fields :

(*i*) $\mathbf{J}[i]/(5)$. (*ii*) $\mathbf{J}[i]/(13)$.

43. A ring is called *Boolean* if each element x thereof satisfies the equation

$$x^2=x$$

Addition and multiplication compositions are defined on the set R of all sub-sets of an arbitrary set S as follows

$$AB=A \bigcap B,$$
$$A+B=(A \bigcap B') \bigcup (B \bigcap A')$$

where A, B are sub-sets of S and A' denotes the complement of A, *i.e*, the set of all those elements of S which do not belong to A and similarly B' denotes the complement of B.

Show that the set R of all sub-sets of S is a Boolean ring for the two compositions as defined.

44. In a commutative ring R with unity, an ideal $I \subsetneq R$ is called *prime*, if the residue class ring R/I is an integral domain.

Show that for a prime ideal I,

$$ab \in I \Longrightarrow \in I \text{ or } b \in I.$$

Show further that every maximal ideal is prime but not conversely.

45. R denotes any arbitrary ring and S denotes the systems

$$(a_0, a_1, \ldots\ldots, a_i, \ldots\ldots),$$

such that $a_i \in R$ and a finite number, at the most, of the members of each system is non-zero.

$$(a_0, a_1, \ldots\ldots, a_i, \ldots\ldots)+(b_0, b_1, \ldots\ldots, b_i \ldots\ldots)=(a_0+b_0, a_1+b_1, \ldots\ldots, a_i+b_i, \ldots\ldots)$$
$$(a_0, a_1, \ldots\ldots, a_i, \ldots\ldots)(b_0, b_1, \ldots\ldots, b_j, \ldots\ldots)=(c_0, c_1, c_2, \ldots\ldots)$$

where

$$c_k=\sum_{i+j=k} a_i b_j.$$

Show that the system S is a ring.

CHAPTER V

POLYNOMIAL RINGS

Factorisation in Integral Domains

70. Introduction. In various types of illustrations so far, we have already come across polynomials having numbers as coefficients. In relation to this, we have depended upon the knowledge of the reader acquired in his studies of classical Mathematics. In this chapter will be introduced for the first time the concept of Polynomials in a manner consistent with the spirit of the subject as being developed in this book.

The second part of this chapter will be concerned with the problem of factorisation in integral domains. The reader may be aware of what is known as the Fundamental theorem of Arithmetic which states that every integer is uniquely expressible as a product of primes. In this part of the chapter, we shall lay down conditions under which a similar result holds good for an Abstract Integral domain. Naturally this will first involve the introduction of the relevant concepts of Divisibility, factors, primes, etc., as applicable to any domain. The case of an Abstract integral domain differs from that of integers in one basic aspect *viz.*, that the domain of integers is what is known as a totally ordered system whereas the same is not relevant for a general integral domain. The definitions of various concepts in the case of the Domain of integers will have to be modified so as to free the same from 'Order Notion' before the same can made available for general abstract integal domains.

71. Polynomial rings.—Let A be any arbitrary ring. By a polynomial over a ring A, is meant any ordered system

$$(a_0, a_1, a_2, \ldots\ldots),$$

of elements of A such that all except, at the most, a finite number of elements are zero.

Also two polynomials

$$(a_0, a_1, a_2, \ldots\ldots, a_i, \ldots\ldots)$$
$$(b_0, b_1, b_2, \ldots\ldots, b_i, \ldots\ldots)$$

will be said to be equal if and only if

$$a_i = b_i.$$

This definition of equality sets up an equivalence relation in the set of all polynomials over the ring A and is such that each of the corresponding equivalence classes consists of only a single member.

We shall now define Addition and Multiplication Compositions in the set of all polynomials and show briefly that the set acquires the structure of a ring relatively to the same.

Addition composition. By def.,

$$(a_0, a_1, a_2, \ldots\ldots) + (b_0, b_1, b_2, \ldots\ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots\ldots)$$

If $a_i = 0$ for $i > m$ and $b_i = 0$ for $i > n$, then

$$a_i + b_i = 0 \text{ for } i > \max.(m, n),$$

so that the sum, as defined, of two polynomials is again a polynomial.

Multiplication Composition. By def.,

$$(a_0, a_1, a_2, \ldots\ldots)(b_0, b_1, b_2, \ldots\ldots) = (c_0, c_1, c_2, \ldots\ldots),$$

where

$$c_0 = a_0 b_0,\ c_1 = a_0 b_1 + a_1 b_0,\ c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0,$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

$$c_i = a_0 b_i + a_1 b_{i-1} + \ldots\ldots + a_i b_0$$

$$= \sum_{j=0}^{i} a_j b_{i-j} = \sum_{j+k=i} a_j b_k.$$

If

$$a_i = 0 \text{ for } i > m,\ b_i = 0 \text{ for } i > n,$$

then

$$c_i = 0 \text{ for } i > m+n,$$

so that the product of two polynomials is again a polynomial.

The fact that the set of polynomials is an abelian group relatively to the addition composition may be easily verified by the reader. We only state that the polynomial

$$(0, 0, 0, \ldots\ldots)$$

is the additive identity and

$$(-a_0, -a_1, -a_2, \ldots\ldots) = -(a_0, a_1, a_2, \ldots\ldots).$$

Now we show that the multiplication is associative. Let

$$(a_0, a_1, a_2, \ldots\ldots),\ (b_0, b_1, b_2, \ldots\ldots),\ (c_0, c_1, c_2, \ldots\ldots)$$

be any three arbitrary polynomials.

Let

$$(a_0, a_1, a_2, \ldots\ldots)(b_0, b_1, b_2, \ldots\ldots) = (d_0, d_1, d_2, \ldots\ldots)$$

so that

$$d_i = \sum_{j+k=i} a_j b_k.$$

Again let

$$(d_0, d_1, d_2, \ldots\ldots)(c_0, c_1, c_2, \ldots\ldots) = (e_0, e_1, e_2, \ldots\ldots)$$

where

$$e_l = \sum_{i+m=l} d_i c_m = \sum_{i+m=l} \left(\sum_{j+k=i} a_j b_k \right) c_m$$

$$= \sum_{j+k+m=l} a_j b_k c_m.$$

Also, we may similarly see that

$$(a_0, a_1, a_2, \ldots\ldots)[(b_0, b_1, b_2 \ldots\ldots)(c_0, c_1, c_2, \ldots\ldots)] = (f_0, f_1, f_2, \ldots\ldots)$$

where

$$f_l = \sum_{j+k+m=l} a_j b_k c_m,$$

so that

$$e_l = f_l \text{ for every } l.$$

Thus we see that the multiplication is associative.

Distributivity of addition w. r. to multiplication. We have

$$(a_0, a_1, a_2, \ldots\ldots)[(b_0, b_1, b_2, \ldots\ldots) + (c_0, c_1, c_2, \ldots\ldots)]$$
$$= (a_0, a_1, a_2, \ldots\ldots)(b_0 + c_0, b_1 + c_1, b_2 + c_2, \ldots\ldots)$$
$$= (e_0, e_1, e_2, \ldots\ldots)$$

where

$$e_i = \sum_{j+k=i} a_j (b_k + c_k)$$
$$= \sum_{j+k=i} a_j b_k + \sum_{j+k=i} a_j c_k$$
$$= f_i + g_i, \text{ say.}$$

Also, as is obvious

$$(a_0, a_1, \ldots\ldots)(b_0, b_1, \ldots\ldots) = (f_0, f_1, \ldots)$$
$$(a_0, a_1, \ldots\ldots)(c_0, c_1, \ldots\ldots) = (g_0, g_1, \ldots\ldots)$$

Hence

$$(a_0, a_1, a_2, \ldots\ldots)[(b_0, b_1, b_2, \ldots\ldots) + (c_0, c_1, c_2, \ldots\ldots)]$$
$$= (a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots\ldots) + (a_0, a_1, a_2, \ldots\ldots)(c_0, c_1, c_2, \ldots\ldots).$$

Thus the set of polynomials, in question, is a ring known as **the Polynomial ring over the ring A.**

Further, we may verify that the mapping

$$a \longrightarrow (a, 0, 0, \ldots\ldots)$$

is a one-one isomorphic mapping of the ring A *into* the ring of polynomials.

In view of this isomorphic mapping, we shall find it covenient to identify the polynomial $(a, 0, 0, \ldots\ldots)$ with a.

We shall now see how it is possible to express polynomials in a form which is more usual. We write

$$x=(0, 1, 0\ 0, \quad ..),$$

so that x is a particular polynomial.

Thus we may easily verify that

$$x^2 = 0, 0, 1, 0, \ldots\ldots)$$
$$x^3=(0, 0, 0, 1, .. \ldots) \text{ and so on.}$$

Thus we have

$$\begin{aligned}(a_0, a_1, a_2, \ldots\ldots) &= (a_0, 0, 0, \ . \ \ldots) + (0, a_1, 0, \ \ldots.) \\ &\qquad + (0, 0, a_2, \ldots. \ ) + \ldots\ldots \\ &= (a_0, 0, 0, \ldots \ . \ ) + (a_1, 0, 0\ldots\ldots)\ x \\ &\qquad + (a_2, 0, 0, \ldots\ldots)\ x^2 + \ldots\ldots \\ &= a_0 + a_1 x + a_2 x^2 + \ldots\ldots\end{aligned}$$

in view of the identification.

Thus we see that each polynomial is expressible in the form

$$a_0 + a_1 x + a_2 x^2 + \ldots ..$$

The elements a_0, a_1 etc., are known as the *coefficients* of the polynomial and the polynomial x is known as an **Indeterminate.**

We may note that x is commutative with each element of the ring.

By the definition of the equality, two polynomials are equal if and only if the respective coefficients are separately equal.

The polynomial ring over a ring A will be denoted by the symbol $A[x]$. Also any member of the same will be denoted by some *such symbol as $f(x)$, which may be distinguished in* meaning from that of the same symbol employed earlier as denoting the f image of x.

A polynomial consisting of a single term a_0 of A is known as a *constant polynomial.*

71·1. Polynomial ring in two or more indeterminates. Just as we constructed the polynomial ring $A[x]$ over the ring A, we may now construct the polynomial ring

$$A[x]\ [y]$$

over the ring $A[x]$ and in an indeterminate y.

Here $A[x][y]$ denotes polynomials of the type

$$c_0+c_1y+c_2y^2+\ldots\ldots$$

where each of $b_0, b_1, b_2, \ldots\ldots$ belongs to $A[x]$.

This can clearly be re-written in the form

$$a_0+a_1x+b_1y+(a_2x^2+b_2xy+c_2y^2)+\ldots\ldots$$

Clearly

$$A[x][y]=A[y][x],$$

and we re-write the same as

$$A[x, y].$$

Similarly, we may set up polynomial rings over any finite number of indeterminates.

71·2. Degree of a polynomial member of $A[x]$. Consider any polynomial

$$f(x)=a_0+a_1x+a_2x^2+\ldots\ldots$$

Suppose that

$$a_i=0 \text{ for } i>n$$

and

$$a_n\neq 0.$$

We then say that n is the degree of the polynomial $f(x)$ and write

$$deg\, f(x)=n.$$

The degree of a non-zero constant polynomial is, according to our definition, 0. The degree of the zero polynomial however remains undefined.

71·3. Degree of the sum and the product of two polynomials. *If $f(x)$ and $\varphi(x)$ be two polynomial members of $A[x]$, then*

$$deg(f(x)+\varphi(x))\leqslant Max\ (deg\, f(x),\ deg\, \varphi(x)),$$
$$deg\ (f(x)\,\varphi(x))\leqslant deg\, f(x)+deg\, \varphi(x).$$

Let

$$f(x)=a_0+a_1x+\ldots\ldots+a_mx^m,\ a_m\neq 0$$
$$\varphi(x)=b_0+b_1x+\ldots\ldots+b_nx^n,\ b_n\neq 0,$$

so that

$$deg\, f(x)=m \quad deg\ \varphi(x) \quad n.$$

Then, as is easily seen.

$$deg\ (f\,x)+\varphi(x)=\begin{cases} max\ (m, n), & m\neq n \\ m \text{ if } m=n \text{ and } a_m+b_n\neq 0 \\ <m \text{ if } n \quad n \text{ and } a_m+b_n=0 \end{cases}$$

Also, we have

$$f(x)\,\varphi(x)=a_0b_0+(a_0b_1+a_1b_0)x+\ldots+a_mb_nx^{m+n}$$

so that

$$deg\, f(x)\, \varphi(x) = \begin{cases} m+n = deg\, f(x) + deg\, \varphi(x) \\ \qquad\qquad if\ a_m b_n \neq 0 \\ < m+n\ if\ a_m b_n = 0. \end{cases}$$

It may be noticed that since we have not imposed any restrictive conditions on the ring A which is perfectly arbitrary, we may have

$$a_m b_n = 0 \text{ even if } a_m \neq 0,\ b_n \neq 0.$$

We may note that if the underlying ring A is free from proper zero divisors so that if, in particular, it is an integral domain or a field, we shall have a more exact statement; *viz*, that

$$deg\ (f(x)\ \varphi(x)) = deg\ f(x) + deg\ \varphi(x).$$

Ex. 1. Show that the polynomial ring $A[x]$ is commutative if and only if the ring A is commutative.

Ex. 2. Show that the polynomial ring $A[x]$ is free from proper zero divisors if and only if A is free from the same.

Ex 3. Show that $A[x]$ is an integral domain if and only if A is an integral domain.

Ex. 4. Give an example to show that the degree of the product of two polynomials may be actually less than the sum of their degrees

71·4. Polynomial rings over a field. We shall now consider the polynomial ring $K[x]$ where the coefficient ring is a field K. In this context, we firstly have a simple theorem.

Theorem. *If A is an integral domain, then so is also the polynomial ring $A[x]$.*

The ring A being commutative, the polynomial ring $A[x]$ is also commutative. The proof is simple.

$A[x]$ is a ring with unity ; the unity of A being also the unity of $A[x]$.

We now show that $A[x]$ is free from proper zero divisors.

Let

$$f(x) \neq 0,\ \varphi(x) \neq 0,$$

be two polynomials of degrees m and n respectively.

Let

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m,\ a_m \neq 0$$
$$\varphi(x) = b_0 + b_1 x + \ldots + b_n x^n,\quad b_n \neq 0$$

Then

$$f(x)\ \varphi(x) \neq 0,$$

for atleast one coefficient thereof, viz :

$$a_m b_n$$

of x^{m+n} is $\neq 0$. Here $a_m b_n \neq 0$ for neither a_m is 0 nor b_n is 0 and A is an integral domain.

This theorem shows that K being a field, the polynomial ring $K[x]$ over the same is an integral domain.

The quotient field of the polynomial integral domain $K[x]$ over the field K will be denoted by the symbol $K(x)$ with *circular* brackets. Clearly this field $K(x)$ is infinite even if K is finite.

71·5. Division Algorithm for polynomials over a field. Let $K[x]$ be the polynomial ring over a field K. We shall now prove the following theorem which has reference to the division process in $K[x]$.

Theorem. *Corresponding to any two polynomials $f(x)$ and $\varphi(x) \neq 0$ belonging to $K[x]$, there exist uniquely two polynomials $q(x)$ and $r(x)$ also belonging to $K[x]$ such that*

$$f(x) = \varphi(x) q(x) + r(x),$$

where $r(x) = 0$ or deg $r(x) <$ deg $\varphi(x)$.

Let

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m,\ a_m \neq 0,$$
$$\varphi(x) = b_0 + b_1 x + \ldots + b_n x^n,\ b_n \neq 0.$$

If $m < n$, we write

$$f(x) = \varphi(x).0 + f(x),$$

so that $q(x) = 0$ and $r(x) = f(x)$.

Now suppose that $m \geqslant n$. We proceed by Mathematical induction assuming that the result holds good when $f(x)$ is replaced by any polynomial of degree $< m$.

We have

$$f(x) = a_0 + a_1 x + \ldots + a_m x^m = a_m b_n^{-1} x^{m-n}(b_0 + b_1 x + \ldots + b_n x^n) + (a_{m-1} - a_m b_n^{-1} b_{n-1}) x^{m-1} + (a_{m-2} - a_m b_n^{-1} b_{n-2}) x^{m-2} + \ldots$$
$$= a_m b_n^{-1} x^{m-n} \varphi(x) + r_1(x), \text{ say.}$$

Here

$$\text{deg } r_1(x) = m - 1.$$

On the assumed hypothesis, we see that there exist polynomials $q_1(x)$ and $r(x)$ such that

$$r_1(x) = q_1(x)\varphi(x) + r(x), \quad \text{where deg } r(x) < \text{deg } \varphi(x).$$

$$\therefore\ f(x) = a_m b_n^{-1} x^{m-n} \varphi(x) + q_1(x)\varphi(x) + r(x)$$
$$= [a_m b_n^{-1} x^{m-n} + q_1(x)]\varphi(x) + r(x)$$
$$= q(x)\varphi(x) + r(x), \quad \text{where deg } r(x) < \text{deg } \varphi(x)$$

We have now to show the uniqueness of $q(x)$ and $r(x)$.

Suppose that

$$f(x) = \varphi(x)q(x) + r(x),$$

where

$$r(x) = 0 \text{ or } deg\ r(x) < deg\ \varphi(x),$$

$$\therefore \quad \varphi(x)q(x) - \varphi(x)q'(x) = r(x) - r'(x),$$

or

$$\varphi(x)[q(x) - q'(x)] = r(x) - r'(x).$$

Now unless each side is 0, we have

$$deg[\varphi(x)(q(x) - q'(x))] \geq \varphi(x),$$

$$deg[r(x) - r'(x)] < \varphi(x),$$

and this latter possibility is absurd.

Thus

$$\varphi(x)[q(x) - q'(x)] = 0, \quad r(x) - r'(x) = 0.$$

Also

$$\varphi(x)[q(x) - q'(x)] = 0 \Longrightarrow q(x) = q'(x),$$

and

$$r(x) - r'(x) = 0 \Longrightarrow r(x) = r'(x).$$

Hence the result.

Theorem. *A polynomial domain $K[x]$ over a field K is a principal ideal domain.*

Let I be any ideal of $K[x]$ other than the null ideal (0).

Let $\varphi(x)$ be a polynomial of lowest degree belonging to the ideal I.

Also let $f(x)$ be any arbitrary member of I.

Now there exist two polynomials

$$q(x) \in K[x], \ r(x) \in K[x],$$

such that

$$f(x) = \varphi(x)\ q(x) + r(x),$$

where

$$r(x) = 0 \text{ or } deg\ r(x) < deg\ \varphi(x).$$

Now

$$f(x) \in I, \ \varphi(x) \in I \Longrightarrow f(x) - \varphi(x)q(x) = r(x) \in I.$$

Also, since $\varphi(x)$ is a polynomial of lowest degree belonging to I, we see that $deg\ r(x)$ cannot be less than that of $\varphi(x)$. Thus $r(x) = 0$ and we have

$$f(x) = \varphi(x)q(x)$$

so that we see that

$$I = (\varphi\ (x)).$$

Thus $K[x]$ is a principal ideal ring.

72. Factorisation in integral domains. The notion of divisibility is known to be an important one in our dealings with the domain of integers. In fact this notion plays a dominant part in the Classical Number theory and gives rise to the concepts of Prime and Composite integers and of the greatest common divisor and lowest common multiple. In the same context, we have also what is known as the Fundamental theorem of Arithmetic which states that every positive integer is uniquely expressible as a product of prime positive integers and this theorem is known to form the basis of all the developments in Classical Number Theory. An analogous situation concerned with the introduction of similar concepts arises also in connection with a polynomial domain when the coefficients belong to any field of numbers. Here also we have the notions of divisibility, greatest common divisor, lowest common multiple and prime polynomials which are usually known as irreducible or indecomposable polynomials.

Finally, we have a theorem for these polynomial domains analogous to the Fundamental theorem of Arithmetic for the domain of integers.

This part of the chapter will be concerned with the problem of introducing the basic concept of divisibility and other allied notions for Abstract integral domains. It will be seen, however, that the analogue of the Fundamental theorem of Arithmetic does *not* hold for every integral domain and we shall accordingly be concerned with the determination of sufficient conditions under which an integral domain may be what is known as a **Unique Factorisation domain**

72·1. Divisibility in an Integral domain. In the following, we shall use the symbol D to denote any arbitrary integral domain. Also we shall exclude, 0, the additive identity of D from the purview of all developments of the notion of divisibility so that any element of D which we may consider in the context of the same will essentially be non-zero and we may not always make a mention of it. Thus when we say that a is any element of D, it will mean that the same is non-zero. Of course, D being an integral domain, the product of any two non-zero elements of the same is again non-zero.

Def. An element $a \in D$ is said to be a divisor of $b \in D$, if there exists an element $c \in D$ such that

$$b = ac.$$

In symbols, we write

$$a \mid b$$

to denote that a is a divisor of b.

Further if a is a divisor of b, we say that b is a multiple of a.

We may show that *the relationship of divisibility in an integral domain is reflexive and transitive.*

We have

$$a=1\,a \text{ so that } a \mid a$$

and accordingly the relation is reflexive.

Again, let

$$a \mid b,\ b \mid c.$$

Then there exist two elements d and e of the domain D such that

$$b=ad,\ c=be.$$

$\therefore$ $$c=ade.$$

Also

$$c=ade \Longrightarrow a \mid c.$$

Thus

$$a \mid b,\ b \mid c \Longrightarrow a \mid c,$$

so tnat the relation is transitive.

72·2. Divisibility relation in terms of Inclusion relation between Principal ideals. We may easily see that

$$a \mid b \Longleftrightarrow (a) \supseteq (b),$$

so that if a is a divisor of b, then the principal ideal (a) includes the principal ideal (b) and vice versa.

Illustrations. 1. $2+\sqrt{-5}$ is a divisor of 9 in the integral domain $\mathbf{J}[\sqrt{-5}]$ formed of numbers $a+b\sqrt{-5}$; a, b being any integers.

2. $x+\sqrt{-1}$ is a divisor of x^2+1 in the polynomial domain $\mathbf{C}[x]$ over the field $\mathbf{C}$ of complex numbers.

3. Each element $a \neq 0$ is a divisor of each element $b \neq 0$ in a field K.

72·3. Units in an Integral Domain. The multiplicative identity, 1, of an integral domain is a divisor of each element of the same. In fact, we have

$$a=1a \text{ for every } a \in D,$$

so that $I \mid a$ for each $a \in D$.

Besides 1, there may also exist other elements which are divisors of each element of the domain. As, for example, in a field, each non-zero element is a divisor of every other non-zero element.

It can be seen that all inversible elements and these only are divisors of every element of the domain. In fact if, e, be any inversible element and a be any arbitrary element, we have

$$a=e(e^{-1}a) \text{ so that } e \mid a.$$

The inversible elements of an integral domain are known as its units. Thus each unit is a divisor of every element of the domain.

We see that the *set of all units of an integral domain is a group for the multiplication composition.* In fact if e, f be any two units, then their product ef is also a unit in as much as

$$(ef)^{-1}=e^{-1}f^{-1}.$$

Illustrations.

1. Each non-zero element of a field is a unit thereof.

2. ± 1 are the only two units in the domain J of integers.

3. The set of numbers $a+ib$ where a and b are any integers and $i=\sqrt{-1}$ is an integral domain relatively to the usual addition and multiplication of numbers as the two ring compositions.

This domain is known as the **Domain of Gaussian integers.**

The elements ± 1, $\pm i$ are the only four units in the domain of Gaussian integers.

Let $a+ib$ be any unit and let $c+id$ be its inverse. We have, then,

$$(a+ib)(c+id)=1.$$
$$\therefore \quad (a^2+b^2)(c^2+d^2)=1.$$
$$\therefore \quad a^2+b^2=1,$$

so that we have

$$a^2=1,\ b^2=0 \text{ or } a^2=0,\ b^2=1.$$

Thus ± 1, $\pm i$ are the only four possible units. That these are actually the units may be easily seen.

4. The number $3+2\sqrt{2}$ is a unit in the domain of numbers $a+b\sqrt{2}$; a, b being any integers.

Also every integral power of $3+2\sqrt{2}$ is a unit of the domain. Thus the domain, in question, has an infinite number of distinct units.

5. The non-zero elements of a field K are the only units of the domain $K[x]$ of polynomials over K.

If $f(x)$ be any unit and $\varphi(x)$ its inverse, we have

$$f(x)\,\varphi(x)=1,$$

so that

$$deg\, f(x)+deg\, \varphi(x)=0$$

and accordingly

$$deg\, f(x)=0,$$

so that $f(x)$ is a non-zero member of K.

Also, as is obvious, each non-zero member of K is essentially a unit of $K[x]$.

72·4. Associates. There may exist pairs of elements a, b each of which is a divisor of the other so that we simultaneouly have

$$a \mid b \text{ and } b \mid a.$$

As for example each of 3 and -3 is a divisor of the other in the domain J of integers.

Def. An element a is said to be an associate of b, if a is a divisor of b and b that of a. In symbols, we express this by writing

$$a \sim b.$$

Illustrations.

1. Each integer a is an associate of itself and of $-a$ ir the domain J of integers.

2. The Gaussian integer $a+ib$ is an associate of each of

$$a+ib,\ -a\ -ib,\ ia\ -b,\ -ia+b$$

in the domain of Gaussian integers.

3. In the polynomial domain $K[x]$ over a field K, each polynomial $af(x)$ is an associate of $f(x)$; a being any non-zero member of K.

Theorem. *The relation*

'a is an associate of b'

in any integral domain is an equivalence relation.

Reflexivity. We have

$$a \mid a \Longrightarrow a \sim a.$$

Symmetry. This is immediate.

Transitivity. Let

$$a \sim b,\ b \sim c$$

so that, we have

$$a \mid b, b \mid a, b \mid c, c \mid b.$$

Now

$$a \mid b, b \mid c \Longrightarrow a \mid c,$$
$$c \mid b, b \mid a \Longrightarrow c \mid a.$$

Thus

$$a \sim c.$$

Equivalence classes of Associates and their Structure. The relation 'a is an associate of b' being an equivalence relation, we have a partitioning of D into mutually exclusive classes such that

(i) any two elements of the same class are associates,

(ii) no two elements of different classes are associates.

Now if

$$a \sim b,$$

there exist two elements c, d such that

$$a = bc,\ b = ad,$$

so that

$$a = adc.$$

Thus

$$dc = 1,$$

so that d and c are units.

This shows that each of two associates differs from the other by some unit as a factor. Also conversely, an element

$$a = bc$$

where, c, is a unit is an associate of b.

This result shows *that the associates of an element can all be obtained on multiplying the same by the different units of the domain.* This result shows the simple manner in which any equivalence class of associates can be generated from any given member of the same.

We may also easily see that any two units are associates so that the totality of units in an integral domain is an equivalence class of associates determined by the unity.

The principal ideals generated by any two associates are the same.

In fact

$$a \mid b \Longleftrightarrow (a) \supseteq (b),$$
$$b \mid a \Longleftrightarrow (b) \supseteq (a),$$

so that

$$a \sim b \Longleftrightarrow (a)=(b).$$

Thus we can associate a single principal ideal to each equivalence class of associates of an integral domain.

We may also note that if a is a divisor of b without, however, being an associate of the same, we have

$$(a) \supset (b),\ (a) \neq (b).$$

Illustrations. 1. ± 1 being the only units in the domain $\mathbf{J}$ of integers, each equivalence class of associates consists of only two members.

Thus we have a class of associates consisting of a and $-a$.

2. The domain of Gaussian integers has four units ± 1, $\pm i$ and accordingly each class of associates contains 4 members. Thus the class of associates determined by $a+ib$ consists of the four elements

$$a+ib,\ -a-ib,\ ia-b,\ -ia+b,$$

obtained on multiplying $a+ib$ with $1, -1, i, -i$ respectively.

3. Each non-zero member of a field K being a unit of the polynomial domain $K[x]$ over the same, we see that the class of associates determined by any polynomial $f(x) \in K[x]$ consists of the polynomials $af(x)$; a being any non-zero member of K.

It may be seen that each class of associates in the domain $K[x]$ contains a single member with highest degree term coefficient unity. Such a polynomial is usually taken as the representative of the class and is known as *monic*.

Note. It may be noticed that associates have the same divisibility properties so that a divisibility relation will not change if any element in the same is replaced by an associate of the same.

Thus

$$a \mid b,\ a \sim a',\ b \sim b' \Longrightarrow a' \mid b'.$$

73. Greatest Common Divisor. *An element g is said to be a greatest common divisor of two elements a, b, if g is a divisor of a as well as of b and each common divisor h of a and b is as well a divisor of g.*

Thus if g is a greatest common divisor of a and b, we have

$$g \mid a,\ g \mid b$$

and

$$h \mid a,\ h \mid b \Longrightarrow h \mid g.$$

Of course for any given integral domain, a pair of elements may not have a greatest common divisor. It can be seen, however, that in case a greatest common divisor exists, it is unique apart from the distinction between associates. Thus if g_1, g_2 be two greatest common divisors of a and b we have, by def.,

$$g_1 \mid g_2 \mid \text{as well as } g_2 \mid g_1,$$

so that

$$g_1 \sim g_2.$$

73·1. Existence of greatest common divisor. Theorem. *Greatest common divisor exists for each pair of elements in a principal ideal domain.*

Let a, b be any two elements of a principal ideal domain D.

Consider the sum ideal

$$(a)+(b).$$

As D is a principal ideal ring, there exists an element g such that

$$(a)+(b)=(g). \tag{1}$$

It will now be shown that g is a greatest common divisor of a and b.

From (1), we have

$$(g) \supseteq (a),\ (g) \supseteq (b),$$

Also

$$(g) \supseteq (a) \Longrightarrow g \mid a,$$

and

$$(g) \supseteq (b) \Longrightarrow g \mid b,$$

so that g is a common divisor of a and b.

Now suppose that h is any common divisor of a and b so that

$$(h) \supseteq (a),\ (h) \supseteq (b).$$

$\therefore$ $(h) \supseteq (a)+(b) = (g)$. *Thus* $h \mid g$.

Hence the result.

Note I. The result obtained above shows that if in a principal ideal domain D, g is a greatest common divisor of a and b, so that

$$(g)=(a)+(b),$$

there exist two elements u, v of D such that

$$g=au+bv.$$

Note II. The domains J and $K[x]$; K being any field, are known to be principal ideal domains so that we see that the above theorem is applicable to these.

Note III. The notion of greatest common divisor can easily be generalised to that of any finite number of elements.

74. Lowest Common multiple. *In a domain D, an element, l is said to be a lowest common multiple of any two elements a, b thereof, if l, is a multiple of, a, as well as of, b, and any common multiple m of a and b is as well a multiple of l.*

Thus if l is a lowest common multiple of a and b, we have

$$a \mid l,\ b \mid l$$

and if m is an element such that

$$a \mid m,\ b \mid m$$

then we have

$$l \mid m.$$

It can be shown that lowest common multiple, in case it exists, is unique apart from the distinction between associates.

74·1. Theorem. *Lowest common multiple exists for each pair of elements of a principal ideal domain.*

Let a, b be any two elements of a principal ideal domain D. There exists an element l of D such that

$$(a) \cap (b) = (l). \qquad (1)$$

We now show that l is a lowest common multiple of a and b.

From (1), we have

$$(l) \subseteq (a),\ (l) \subseteq (b).$$

Also

$$(l) \subseteq (a) \Longrightarrow a \mid l,$$
$$(l) \subseteq (b) \Longrightarrow b \mid l.$$

Also if m be any common multiple of a and b, we have

$$(a) \supseteq (m),\ (b) \supseteq (m)$$

so that

$$(m) \subseteq (a) \cap (b) = (l),$$

and accordingly

$$l \mid m.$$

75. Prime and Composite elements of an Integral domain. *Any non-unit element of an integral domain is called prime, irreducible or indecomposable, if it has no divisors, other than its associates or units; otherwise it is called composite, reducible or decomposable.*

It may be noted that every associate of a prime (composite) element is prime (composite).

It will be seen that we have now learnt to distinguish between *four* types of elements of an integral domain, *viz.*,

(*i*) *Zero.* (*ii*) *Units.* (*iii*) *Primes.* (*iv*) *Composites.*

Illustrations. (1) In the domain $\mathbf{J}[i]$, of Gaussian integers, 5 is composite, for we have

$$5=(1+2i)(1-2i)$$

so that $1+2i$ is a divisor of 5 without being a unit or an associate of the same.

Also in the same domain, 3 is prime.

(2) x^3+1 is a prime element of the domain $\mathbf{R}[x]$ but a composite element of $\mathbf{C}[x]$.

(3) $2x+2$ is a prime of $\mathbf{R}[x]$ but a composite element of $\mathbf{J}[x]$.

It may be noted that 2 is a unit of $\mathbf{R}$ but not of $\mathbf{J}$.

Ex. If g is a common divisor of a, b in a domain D and there exist two elements u, v of D such that

$$g=au+bv,$$

then show that g is a greatest common divisor of a, b; the domain D being arbitrary.

76. Unique Factorisation domains. Let D be any integral domain and a any non-zero member of D. If a is not prime, then there exist two elements b, c, none of which is a unit such that

$$a=bc.$$

This process of decomposition i.e., expression of an element as a product of two non-unit members can be continued if either b or c is composite.

The question, now, is as to under what conditions, we shall, after a *finite* number of steps, arrive at an expression of, a, as product of prime elements. In addition to the question of the expression of any element as a product of prime elements, there is also the question of the uniqueness of this expression. Thus we are led to defining what are known as **unique Factorisation Domains.**

Def. *An integral domain is said to be a unique factorisation domain, if every non-zero non-unit element of the same is expressible as a product of prime elements of the domain and this factorisation, apart from order and associates, is unique.*

76·1. Some properties of unique factorisation domains. Let D be any unique factorisation domain.

Theorem I. *If a, b are two arbitrary elements of D and p is a prime element of D, then*

$$p \mid ab \Longrightarrow \text{either } p \mid a \text{ or } p \mid b.$$

Let

$$a = p_1 p_2 \ldots\ldots p_r,$$
$$b = p'_1 p'_2 \ldots\ldots p'_s$$

where each of $p_1, \ldots\ldots, p_r, p'_1, \ldots\ldots, p'_s$ is a prime element of D. Then, we have

$$ab = p_1 p_2 \ldots p_r p'_1 p'_2 \ldots\ldots p'_s. \tag{1}$$

By virtue of the fact, that expression as product of primes of each element of D is unique, we see that p must occur as a factor on the right side of (1) so that we have

$$\text{either } p \mid a \text{ or } p \mid b.$$

Theorem II. *Any two elements of a unique factorisation domain possess greatest common divisor as well as lowest common multiple.*

Let a, b be any two elements of D. Let

$$a = p_1^{e_1} p_2^{e_2} \ldots\ldots p_r^{e_r}, \tag{2}$$

$$b = p_1^{f_1} p_2^{f_2} \ldots\ldots p_r^{f_r}, \tag{3}$$

where we have arranged the expressions in such a manner that the same prime factors appear in both by employing the integer zero as index in any case, if necessary.

The elements $p_1, p_2, \ldots, p_r$ are all different primes and $e_1, \ldots\ldots, e_r$; $f_1, \ldots\ldots, f_r$ are all integers $\geqslant 0$.

We write

$$g_i = \max.(e_i, f_i),\ h_i = \min.(e_i, f_i).$$

It may then be easily verified that

$$p_1^{h_1} p_2^{h_2} \ldots\ldots p_r^{h_r}$$

and

$$p_1^{g_1} p_2^{g_2} \ldots\ldots p_r^{g_r}$$

are respectively the greatest common divisor and the lowest common multiple of a and b.

77. Theorem. *A principal ideal domain is a unique factorisation domain.*

EXISTENCE

Firstly we show that each element of a principal ideal domain is expressible as a product of prime elements.

Let a be any non-zero non-unit element of a principal ideal domain D.

If a is prime, we have finished.

If a is composite, there exist two non-unit elements b and c such that

$$a = bc.$$

Then we have

$$(b) \supset (a), \quad (b) \neq (a).$$

In case b, c are both prime, then again we have finished. In the alternative case, we continue as above. Thus two cases arise :

(*i*) After a finite number of steps, we arrive at an expression of a as a product of prime elements.

(*ii*) Howsoever far we may continue, we always have a composite element occurring as a factor in the expression of, a, as product of elements of D.

In case (*i*) we have finished.

In case (*ii*), there exists an infinite system of elements

$$a_1, a_2, \ldots\ldots, a_n, \ldots \ldots$$

such that

$$(a_1) \subset (a_2) \subset \ldots\ldots \subset (a_n) \subset \ldots\ldots, \qquad (1)$$

no two of these principal ideals being the same.

Consider now the union of all these principal ideals. This union is itself an ideal. In fact if x, y are any two members of this union, there exists an ideal member (a_k) of the system such that

$$x \in (a_k), \; y \in (a_k)$$

and accordingly

$$x - y \in (a_k), \; \alpha x \in (a_k) \text{ where } \alpha \in D$$

so that $x - y$ and αx also belong to the union.

The domain D being a principal ideal domain, there exists an element β of the same such that the union ideal is the principal ideal (β).

There exists, therefore, an ideal member (a_m) of the system such that

$$\beta \in (a_m).$$

and accordingly

$$\beta \in (a_n) \text{ for } n \geqslant m.$$

Thus,

$$(\beta) \subseteq (a_n) \text{ for } n \geqslant m.$$

Also since (β) is the union of the ideals, we have

$$(\beta) \subseteq (a_n) \text{ for all } n.$$

Thus

$$(\beta) = (a_n) \text{ for } n \geqslant m,$$

so that

$$(a_m) = (a_{m+1}) = \ldots\ldots$$

and accordingly we arrive at a contradiction.

This shows that case (*ii*) cannot arise.

Thus we have proved that *every non-zero non-unit element of a principal ideal domain is expressible as a product of prime elements.*

Uniqueness. Before proceeding to give the proof of uniqueness, we remark that by introducing units as factors, every decomposition can be altered. Thus

$$a = p_1 p_2 \ldots\ldots = (p_1 e_1)(p_2 e_1^{-1}) \ldots\ldots$$

where e_1 is some unit. Even in the domain **J** of integers, we have

$$6 = 2.3 = (-2)(-3).$$

It is thus important that we become clear as to the precise import of the theorem we have stated. Suppose that

$$a = \prod_{i=1}^{r} p_i = \prod_{q=1}^{s} q_k,$$

where each p_i and q_k is a prime and we have not allowed any unit to appear as a factor on either side. The theorem now states that

$$r = s,$$

and each p is an associate of some q and each q is an associate of some p.

Firstly we need to prove a lemma whose statement is as follows.

Lemma. *In a principal ideal domain, if a product, ab, is divisible by a prime p, then either a or b is divisible by p, i.e.,*

$$p \mid ab \Longrightarrow \text{either } p \mid a \text{ or } p \mid b.$$

Firstly we show that the ideal (p) is maximal. Let if possible (x) be an ideal containing the ideal (p) and different from D, *i.e.*,

$$D \neq (x) \supset (p), \quad (x) \neq (p).$$

This means that x is a non-unit element and is a divisor of p without being an associate of the same. Clearly this is not possible so that (p) is a maximal ideal.

Let a be *not* divisible by p. Then, a, does not belong to the ideal (p).

Thus the ideal (a, p) generated by a and p is the unit ideal D. There exist, therefore, two elements u, v of D such that

$$1=au+pv,$$

so that

$$b=abu+pbv.$$

Also since $p \mid ab$, there exists $c \in D$ such that

$$ab=cp.$$

$$\therefore \quad b=cpu+pbv=p(cu+bv),$$

so that

$$p \mid b.$$

Hence the lemma.

(The significance of the result proved in the lemma may become clearer if we consider a counter example. In the integral domain $J[\sqrt{-5}]$ of numbers $a+b\sqrt{-5}$, where a, b are any integers, we have

$$9=(2+\sqrt{-5})(2-\sqrt{-5})=3\cdot 3$$

It may now be seen that prime 3 is a divisor of the product

$$(2+\sqrt{-5})\ (2-\sqrt{-5})$$

without being a divisor either of $2+\sqrt{-5}$ or of $2-\sqrt{-5}$.

In terms of the lemma, we see that this domain of numbers $a+b\sqrt{-5}$, $a \in J$, $b \in J$ cannot be a principal ideal domain.

We now attend to the *main* theorem.

Let

$$a=p_1p_2\ldots p_r=q_1q_2\ldots q_s \tag{2}$$

where each p and each q is prime.

The result will be proved by induction on r.

The result is immediate if $r=1$. Suppose now that the result is true for each natural number $<r$.

As p_1 divides the product $q_1q_2\ldots q_s$, it must divide, by the lemma, atleast one of $q_1, q_2 \ldots, q_s$. Without any loss of generality, we may suppose that p_1 divides q_1. As q_1 is prime, we see that p_1, q_1 are associates. Let

$$q_1=e_1p_1, \tag{3}$$

where e_1 is a unit.

From (2) and (3), we have

$$p_2p_3\ldots p_r=(e_1q_2)\ q_2\ldots q_s \tag{4}$$

By the assumed hypothesis,

$$r-1=s-1$$

and each factor, on the right of (4) is an associate of some factor on the left and vice-versa.

Thus the result follows.

Note 1. It should be remembered that while principal ideal domains are unique factorisation domains, the converse is not true. Later on in § 79, we shall show that there exist unique foctorisation domains which are not, however, principal ideal domains.

Note 2. In the following section, we shall consider what are known as Euclidean Domains.

The introduction of these domains is motivated by the line of reasoning adopted for proving that (*i*) the domain **J** of integers and (*ii*) the domain $K[x]$ of polynomials over a field K are principal ideal domains.

In other words Euclidean domains are those to which the line of reasoning in question is applicable. Thus we abstract the fundamentals from this line of reasoning and give the definition of Euclidean Domains in the following section. It will then be proved that every Euclidean domain is a principal ideal domain and as such a unique factorisation domain. This quite often proves a useful method for showing that a domain in question is a principal ideal domain.

78. Euclidean Domains. Def. *An integral domain D is said to be Euclidean, if there exists a mapping f of the set of non-zero members of D into the set of positive integers such that if a, b be any two non-zero members of D,*

(*i*) $f(ab)=f(a)f(b)$,

(*ii*) *there exist members q and r of D such that*

$$a=bq+r,$$

where

$$r=0 \text{ or } f(r)<f(b).$$

Illustrations. 1. The domain **J** of integers is Euclidean, for the mapping f defined by

$$f(a)=|a|$$

satisfies the two properties in question.

2. The domain $K[x]$ of polynomials over a field K is Euclidean with the mapping f defined by

$$f(\phi(x))=deg\ \phi(x),$$

where $\phi(x) \in K[x]$.

3. The domain of Gaussian integers is Euclidean. We shall show that the mapping f of the set of non-zero Gaussian integers

into the set of positive integers defined as follows satisfies the two conditions in question. We write

$$f(a+ib)=a^2+b^2.$$

Then

$$f[(a+ib)(c+id]=(a^2+b^2)(c^2+d^2)=f[(a+ib)]f[(c+id)],$$

so that the condition (i) is satisfied.

We now write

$$\alpha=a+ib,\ \beta=c+id,$$

We have

$$\frac{\alpha}{\beta}=\lambda=p+iq, \text{ say}$$

where p, q are rational numbers.

There exist integers p', q' such that

$$|\ p'-p\ | \leq \tfrac{1}{2},\ |\ q'-q\ | \leq \tfrac{1}{2}.$$

We write

$$\lambda'=p'+iq',$$

so that λ' is a Gaussian integer.

We have

$$\begin{aligned}\alpha-\lambda'\beta&=(\alpha-\lambda\beta)+(\lambda-\lambda')\beta\\&=0+(\lambda-\lambda')\beta=(\lambda-\lambda')\beta,\end{aligned}$$

or

$$\alpha=\lambda'\beta+(\lambda-\lambda')\beta.$$

α, β, λ' being Gaussian integers, it follows that $(\lambda-\lambda')\beta$ is also a Gaussian integer.

Here

$$\begin{aligned}f[(\lambda-\lambda')\beta]&=[(p'-p)^2+(q'-q)^2]f(\beta)\\&\leq(\tfrac{1}{4}+\tfrac{1}{4})f(\beta)<f,\beta).\end{aligned}$$

Thus for every pair of Gaussian integers α, β, there exist Gaussian integers

$$\lambda' \text{ and } (\lambda-\lambda')\ \beta$$

such that

$$\alpha=\beta\lambda'+(\lambda-\lambda')\beta$$

where

$$f[(\lambda-\lambda')\beta]<f(\beta),$$

Thus the domain of Gaussian integers is Euclidean.

78·1. Theorem. *Every Euclidean domain is a principal ideal domain.*

Let D be any Euclidean domain and f a mapping referred to in the definition.

Let I be any ideal of D.

If I is the zero ideal, then it is a principal ideal. Now suppose that I is not the zero ideal so that it contains some non-zero members.

Consider the set of f images of the non-zero members of I which are all positive integers. Let $a \neq 0$ be a member of I so that $f(a)$ is the least of all the f-images.

Let b be any arbitrary member of I. There then exist two members q and r of D such that

$$b = aq + r,$$

where

$$\text{either } r = 0 \text{ or } f(r) < f(a).$$

The possibility $f(r) < f(a)$ is ruled out in respect of the manner of the choice of a so that $r = 0$ and we have

$$b = aq.$$

Thus

$$I = (a),$$

and I is accordingly a principal ideal.

Hence the theorem.

Cor. *Every Euclidean domain is a unique factorisation domain.* It follows from the preceding theorem and that of [illegible], page 204

Note. It follows from the preceding that the domain $J[i]$ of Gaussian integers is a principal ideal domain and hence also a unique factorisation domain.

79. Polynomial rings over unique factorisation domains. It will now be shown that *the polynomial ring $D[x]$ over a unique factorisation domain D is itself a unique factorisation domain.*

In the following, we shall also need to consider the quotient field of the integral domain D. This quotient field of D will be denoted by K.

Primitive polynomials. Def. *A polynomial member f of $D[x]$ is called primitive if the greatest common divisor of the coefficients of the polynomial is a unit.*

Thus, for example, $x^2 - 5x + 7$ is a primitive member of $J[x]$ whereas $3x^2 - 6x + 9$ is not primitive member of the same

Lemma I. *Each non-zero polynomial $f(x) \in D[x]$ is expressible as the product*

$$ag(x)$$

of a member $a \in D$ and a primitive member $g(x)$ of $D[x]$ and this expression is unique apart from the difference in associateness.

Let, a, denote the greatest common divisor of the coefficients of $f(x)$. Clearly then we have a relation of the form

$$f(x)=ag(x),$$

where $g(x) \in D[x]$ and is primitive.

Suppose also that we have

$$f(x)=bh(x),$$

where $b \in D$, $h(x) \in D[x]$ and is primitive.

We have

$$f(x)=ag(x)=bh(x).$$

Since b is a divisor of each coefficient of $f(x)$, we have

$$b \mid a.$$

Let

$$a=bc \qquad \text{where } c \in D.$$

$$\therefore \qquad cg(x)=h(x).$$

As $h(x)$ is primitive, we see that c is a unit so that

$$g(x) \sim h(x) \text{ and } a \sim b.$$

Lemma II. *The product of two primitive polynomials is primitive.*

Let

$$f(x)=a_0+a_1x+\ldots\ldots+a_ix^i+\ldots\ldots+a_mx^m,$$
$$g(x)=b_0+b_1x+\ldots\ldots+b_jx^j+\ldots\ldots+b_nx^n,$$

be two primitive members of $D[x]$.

Let

$$h(x)=f(x)g(x)=c_0+c_1x+\ldots\ldots+c_{m+n}x^{m+n}.$$

Let, if possible, a prime element, p, be the greatest common divisor of the coefficients of the product $f(x)g(x)$. Also let a_i and b_j be the first coefficients of $f(x)$ and $g(x)$ which are *not* divisible by p.

We have, now,

$$c_{i+j}=a_ib_j+a_{i-1}b_{j+1}+a_{i-2}b_{j+2}+\cdots \\ +a_{i+1}b_{j-1}+a_{i+2}b_{j-2}+\ldots\ldots$$

so that

$$a_ib_j=c_{i+j}-(a_{i-1}b_{j+1}+a_{i-2}c_{j+2}+\ldots\ldots)-(a_{i+1}b_{j-1}+a_{i+2}b_{i-2}+\ldots)$$

Since, p, is a divisor of each of the terms on the right, we have

$$p \mid a_ib_j$$

This implies that

$$\text{either } p \mid a_i \text{ or } p \mid b_j$$

so that we arrive at a contradiction.

Hence the lemma II.

Lemma III. *If $f_1(x)$, $f_2(x)$ are primitive members of $D[x]$ and are associates in $K[x]$, then they are also associates in $D[x]$; K being the quotient field of the domain D.*

Since $f_1(x)$, $f_2(x)$ are associates in $K[x]$, we have

$$f_1(x) = kf_2(x) \qquad \text{where } 0 \neq k \in K.$$

We have

$$k = ab^{-1} \qquad \text{where } a \in D,\ b \in D.$$

$$\therefore \qquad bf_1(x) = af_2(x).$$

By the lemma I, we see that

$$f_1(x) \sim f_2(x) \text{ in } D[x].$$

Lemma IV. *If $f(x)$ is an irreducible polynomial of positive degree in $D[x]$, it is also irreducible in $K[x]$.*

Let if possible, $f(x)$ be reducible in $K[x]$, so that, we have a relation of the form

$$f(x) = \phi_1(x)\phi_2(x)$$

where $\phi_1(x) \in K[x]$, $\phi_2(x) \in K[x]$ and the degree of each of $\phi_1(x)$, $\phi_2(x)$ is positive.

As may be easily seen, we have relations of the form

$$\phi_1(x) = a_1 b_1^{-1}\psi_1(x),$$
$$\phi_2(x) = a_2 b_2^{-1}\psi_2(x),$$

where a_1, b_1, a_2, $b_2 \in D$ and $\psi_1(x)$, $\psi_2(x)$ are primitive members of $D[x]$.

Thus we have

$$f(x) = a_1 a_2 b_1^{-1} b_2^{-1}\psi_1(x)\psi_2(x),$$

or

$$b_1 b_2 f(x) = a_1 a_2 \psi_1(x)\psi_2(x).$$

By the lemma II, $\psi_1(x)\psi_2(x)$ is primitive. Also, $f(x)$, being irreducible in $D[x]$, is primitive.

Thus by the lemma I,

$$f(x) \sim \psi_1(x)\psi_2(x).$$

On multiplication with a suitable unit, we may suppose that

$$f(x) = \psi_1(x)\psi_2(x).$$

Since $\deg \psi_1(x) > 0$, $\deg \psi_2(x) > 0$, we obtain a proper factorisation of $f(x)$ in $D[x]$ and thus arrive at a contradiction of what is given. Hence the lemma IV.

Theorem. *The polynomial ring $D[x]$ over unique factorisation domain D is itself a unique factorisation domain.*

Let $f(x)$ be any non-zero non-unit member of $D[x]$. We have

$$f(x)=af_0(x)$$

when $f_0(x)$ is a primitive polynomial $\in D[x]$ and $a \in D$.

Since D is a unique factorisation domain, we have

$$a=p_1p_2\ldots\ldots p_r,$$

where each of $p_1,\ldots\ldots, p_r$ is a prime member of D. If now $f_0(x)$ is reducible, we have

$$f_0(x)=f_{01}(x)\,f_{02}(x),$$

where deg $f_{01}(x)>0$ and deg $f_{02}(x)>0$; $f_0(x)$ being primitive. Also $f_{01}(x)$ and $f_{02}(x)$are both primitive.

Proceeding in this manner, we shall, after a finite number of steps, arrive at a relation of the form

$$f(x)=p_1p_2\ldots\ldots p_rf_1(x)\quad\ldots f_s(x),$$

where each factor on the right is irreducible.

Suppose also that we have

$$f(x)=p'_1\ldots\ldots p'_tf'_1(x)\ldots\ldots f'_m(x),$$

where each factor on the right is irreducible, each of

$$p'_1,\ldots\ldots, p'_t \in D$$

and the degree of each of

$$f'_1(x),\ldots\ldots, f'_m(x)$$

which $\in D[x]$ is positive.

Thus we have

$$p_1p_2\ldots\ldots p_rf_1(x)\ldots\ldots f_s(x)=p'_1\ldots\ldots p'_tf'_1(x)\ldots\ldots f'_m(x).$$

By the lemma II, the two products

$$f_1(x),\ldots\ldots f_s(x),\ f'_1(x)\ f'_2(x)\ldots\ldots f'_m(x)$$

are primitive. Further, by the lemma I

$$p_1p_2\ldots\ldots p_r \sim p'_1\ldots\ldots p'_t$$

$$f_1(x)\ldots\ldots f_s(x) \sim f'_1(x)\ldots\ldots f'_m(x).$$

On multiplying one of the $p_1,\ldots\ldots, p_r$ by a unit we can suppose that

$$p_1\ldots\ldots p_r=p'_1\ldots\ldots p'_t \qquad (1)$$

and accordingly also

$$f_1(x)\ldots\ldots f_s(x)=f'_1(x)\ldots\ldots f'_m(x)$$

By the lemma IV, each of,

$$f_1(x),\ldots\ldots,f_s(x)\ ;f'_1(x),\ldots\ldots,f'_m(x)$$

is irreducible in $K[x]$. Now $K[x]$, being a unique factorisation domain, we see that the two sets of polynomials

$$f_1(x),\ldots\ldots,f_s(x)\ ;f'_1(x),\ldots\ldots,f'_m(x)$$

are the same except for order and the difference in associateness. Thus by a possible change of notation, we have,

$$f_1(x)\sim f'_1(x), f_2(x)\sim f'_2(x),\ldots\ldots$$

in $K[x]$. By lemma III, this relation of associateness also holds good in $D[x]$.

Also D being a unique factorisation domain, we see from (1) that each p is an associate of some p' and vice versa.

Thus the two factorisations of $f(x)$ in $D[x]$ are the same except for the difference in order and associateness.

Cor. If D is any unique factorisation domain so that $D[x]$ is, as proved above; also a unique factorisation domain, we see, by employing the same theorem that

$$D[x]\ [y]=D[x, y]$$

is also a unique factorisation domain. This argument may be repeated any finite number of times.

Note. It has been seen in § 77 that every principal ideal domain is a unique factorisation domain.

This converse, however, is not true so that there exist unique factorisation domains which are not principal ideal domains.

Since the ring J of integers is a unique factorisation domain, it follows by the preceding theorem that $J[x]$ is also a unique factorisation domain. We shall, however, show by means of an example that $J[x]$ is not a principal ideal domain. Consider the ideal

$$(x, 2)$$

of $J[x]$ generated by the two elements x and 2. This ideal consists of all those members of $J[x]$ which have some even integer as the constant member thereof.

Since, 1, is a greatest common divisor of x and 2, we have, on the assumption that $J[x]$ is a principal ideal domain, by § 73·1 page 200.

$$(x, 2)=(1)=J[x].$$

Thus we arrive at a contradiction so that $J[x]$ is not a principal ideal domain even though it is a unique factorisation domain.

80. Irreducibility criterion. We shall now state and prove a criterion for irreducibility. **Eisenstein's theorem.** If

$$f(x)=a_0+a_1x+\ldots\ldots+a_nx^n \in D[x]$$

and p is a prime element of D such that

$$p \mid a_0,\ p \mid a_1,\ldots\ldots,\ p \mid a_{n-1}$$

whereas p is not a divisor of a_n and p^2 is not a divisor of a_0, then $f(x)$ is irreducible in $D[x]$ and hence also in $K[x]$.

Let, if possible,

$$a_0+a_1x+\ldots\ldots a_nx^n=(b_0+a_1x+\ldots\ldots+b_lx^l)(c_0+c_1x+\ldots\ldots+c_mx^m)$$

where $l>0$, $m>0$.

We have now

$$a_0=b_0c_0.$$

$$p \mid a_0 \Longrightarrow p \mid b_0 \text{ or } p \mid c_0.$$

Now since p^2 is not a divisor of a_0, therefore, p cannot be a divisor of both b_0 as well as c_0.

Suppose that $p \mid c_0$

Also, we have

$$a_n=b_lc_m$$

so that p is not a divisor of c_m.

Let $r \leqslant m$ be the smallest index such that each of

$$c_0,\ c_1,\ldots\ldots,\ c_{r-1}$$

is divisible by p and c_r is not divisible by p.

We have now

$$a_r=b_0c_r+b_1c_{r-1}+\ldots\ldots+b_rc_0.$$

Since neither b_0 nor c_r is divisible by p, and each of

$$c_0,\ c_1,\ldots\ldots,\ c_{r-1}$$

is divisible by p, we deduce that

$$a_r \text{ is not divisible by } p.$$

This shows that $r=n$ so that the degree of the second of the two factors is n and accordingly the polynomial is actually irreducible.

Ex. Show that

$$f(x)=x^{p-1}+x^{p-2}+\ldots\ldots+x^2+x+1$$

is irreducible over $J[x]$; p being a prime member of J.

[Apply Eisenstein's criterion to $f(x+1)$].

Exercises

1. Show that $J[\sqrt{-2}]$ is a Euclidean ring.

2. Prove that $R[\omega]$ is a Euclidean ring; ω denoting a complex cube root of unity.

3. Express the ideals

$$(1+2\omega, 3) \text{ and } (2+3\omega, 1+5\omega)$$

as principal ideals in the ring $R[\omega]$ of the preceding exercise.

4. Show that

$$J[\sqrt{-7}], J[\sqrt{-11}]$$

are Euclidean domains.

5. Find the greatest common divisor of

$$4-7i, 1-3i$$

in the ring $J[i]$ of Gaussian integers; $i=\sqrt{-1}$.

6. Factorise

$$78 \text{ and } 10+5i$$

into prime factors in $J[i]$; $i=\sqrt{-1}$.

7. Show that $J[\sqrt{-5}]$ and $J[\sqrt{-3}]$ are not unique factorisation domains.

8. Show that the subset of elements for which $a+b$ is even forms an ideal in the ring of numbers $a+b\sqrt{-3}$ where $a, b \in J$.

Prove that this ideal is not a principal ideal.

9. Prove that the set of numbers

$$a+b\sqrt{-3}$$

where a, b are either both integers or both halves of odd integers is a Euclidean ring relative to the usual addition and multiplication.

10. Show that there are 10 irreducible members of second degree in $J_3[x]$ and list the same.

What is the number of irreducible members of third degree in $J_2[x]$.

11. *Prove that if D is an integral domain that is not a field, then $D[x]$ is not a principal ideal domain.*

CHAPTER VI

VECTOR SPACES AND LINEAR TRANSFORMATIONS

81. Introduction. From the classical and concrete point of view, physical entities such as displacement, velocity, acceleration etc., which by virtue of their possessing direction besides magnitude are representable as Directed Line Segments and are further capable of addition by *Parallelogram law* are known as vectors. It is also found possible and useful to set up an Algebra of vectors (*i.e.*, directed line segments) which includes the operations of the Addition of vectors and of the multiplication of vectors by real numbers which are, in this context, known as *Scalars*. It also turns out that, relative to any choice of three suitable vectors as constituting a reference system, each vector is representable as an ordered *triad* of three real numbers and corresponding to the Algebra of Vectors there arises an Algebra of ordered triads of numbers in the manner given below. If a vector, α, is represented by a triad (a_1, a_2, a_3) so that if we write

$$\alpha \longrightarrow (a_1, a_2, a_3)$$

then

$$\alpha \longrightarrow (a_1, a_2, a_3),\ \beta \longrightarrow (b_1, b_2\ b_3) \Longrightarrow \alpha+\beta \longrightarrow (a_1+b_1,\ a_3+b_2,\ a_3+b_3)$$

and

$$\alpha \longrightarrow (a_1, a_2, a_3) \Longrightarrow a\alpha \longrightarrow (aa_1, aa_2, aa_3),$$

where a is any real number.

It is found that the addition of vectors and the multiplication of vectors by scalars obey the following laws :

$$\alpha+\beta=\beta+\alpha,\ \alpha+(\beta+\gamma)=(\alpha+\beta)+\gamma,$$
$$a(\alpha+\beta)=a\alpha+a\beta,\ (a+b)\alpha=a\alpha+b\alpha,$$
$$(ab)\alpha=a(b\alpha),\ 1\ \alpha=\alpha.$$

Here a, b are any real numbers and α, β are any vectors.

Now it is an interesting fact, that there exist quite a number of other mathematical systems (Refer illustrations on page 218) which have an Abstract Algebraic pattern similar to that of the vectors referred to above.

These considerations lead us to define Abstract Linear vector spaces to be referred to simply as vector spaces or Linear Spaces or sometimes only as spaces. Any element of a vector space will be known as a vector.

82. Vector Spaces. Before formulating the concept of an abstract space, we introduce the notion of *External composition* in one set over another as the same will be needed for the purpose in hand.

External Composition. *If E, F be any two given sets, then a mapping of the product set $E \times F$ into the set E is called an external composition in E over F*

Thus an external composition in a set E over a set F is a mapping which associates to each pair of members of E and F a member of E.

Multiplicative notation for external composition. If $\alpha \in E$ and $a \in F$, then the member of E associated to the pair a, α is usually denoted by the symbol $a\alpha$ so that we adopt the notation of scalar multiplication and call the members of F scalars.

Illustration. Let G be any group with multiplicatively denoted composition. Then if $n \in Z$ i.e., if n is any natural integer, then the mapping

$$(a, n) \longrightarrow a^n$$

is an external composition in G.

82·1. Vector Space over a field. Let K be any given field. Then a given set V is said to be a vector space or a Linear space over the field K, if

I. *There is defined a composition in V such that V is an Abelian group for the same* ; this composition will be denoted additively.

II. *There is defined an external composition in V over K* ; this will be denoted as a scalar multiplication.

III. *The two compositions satisfy the following laws* :

1. $a(\alpha+\beta)=a\alpha+a\beta$; $a \in K$, $\alpha \in V$, $\beta \in V$.
2. $(a+b)\alpha=a\alpha+b\alpha$; $a \in K$, $b \in K$, $\alpha \in V$.
3. $(ab)\ \alpha\ =a(b\alpha)$; $a \in K$, $b \in K$, $\alpha \in V$.
4. $1\ \alpha\ \ \ =\alpha$; $\alpha \in V$, 1 is the unity of K.

Also instead of saying that V is a vector space over a field K, we may simply say that $V(K)$ is a vector space. Further each

member of a vector space $V(K)$ will be referred to as a vector and each member of K as a scalar.

Note 1. It should be noted that we have a composition in V and a composition in K both of which have been denoted additively so that we have a zero member of V and a zero member of K, being the identities of the two compositions. Both these will be denoted by the symbol, 0, and it will be seen that no confusion thus arises and the context will always prove decisive as to which meaning does the symbol, 0, have.

Note 2. In dealing with a vector space $V(K)$, we are concerned with *four* compositions, *viz.*,

(*i*) Addition in V;
(*ii*) Scalar multiplication of elements of V with elements in K
(*iii*) Addition in K;
(*iv*) Multiplication in K.

Of the four laws given in III for the definition of a vector space we may see that

$$a(\alpha+\beta)=a\alpha+a\beta,$$

relates the compositions (*i*) and (*ii*),

$$(a+b)\alpha=a\alpha+b\beta,$$

relates (*iii*), (ii) and (*i*) and

$$(ab)\alpha=a(b\alpha),$$

relates (*iv*) and (*ii*)

Illustrations.

1. *The vector space of all polynomials over a field K.*

The set $K[x]$ of all polynomials in an indeterminate x over a field K is a vector space relative to the addition of polynomials as defined before and the product of a polynomial member of $K[x]$ by a member of K as the two vector space compositions.

2. *The vector space of all polynomials of degree $\leqslant n$ over a field K.* The set of all those members of $K[x]$ whose degree $\leqslant n$ is a vector space for the two compositions referred to in the illustration (1) above.

3. *The vector space of all real valued continuous (differentiable or integrable) functions defined in some interval* [0, 1].

If f, g be two such functions, then $f+g$, af are defined as follows:

$$(f+g)(x)=f(x)+g(x),\ (af)(x)=af(x),\ a \in R.$$

4. *The vector space of all n-tuples over a field K.*

Any ordered set

$$(a_1, a_2, \ldots\ldots, a_n)$$

of n-elements over a field K is called an n-tuple over K. The set of all n-tuples over a field K will be denoted by the symbol $V_n(K)$.

Equality. Two n-tuples

$$\alpha=(a_1, a_2, \ldots\ldots, a_n),\ \beta=(b_1, b_2, \ldots\ldots, b_n)$$

are said to be equal if and only if

$$a_i=b_i,\ 1\leqslant i\leqslant n.$$

Addition Composition. By definition

$$\alpha+\beta=(a_1+b_1, \ldots\ldots, a_n+b_n).$$

Scalar multiplication composition. By definition

$$a\alpha=(aa_1, aa_2, \ldots\ldots, aa_n)\ ;\ a\in K.$$

The fact that the set $V_n(K)$ is a vector space for the two compositions above defined may now be easily verified.

As a particular case of $V_n(K)$, we have the vector spaces of all ordered triads and tetrads over K.

5. *A field L can be regarded as a vector space over any subfield K of L* relative to the field addition in L and to the field multiplication of the elements of L with the elements of K as the two vector space compositions.

83. Some general properties of vector spaces.

The following properties of vector spaces can be easily established :

(*i*) $a0=0\ ;\ 0\in V,\ a\in K,$

(*ii*) $0\alpha=0\ ;\ 0$ on the left $\in K$ and that on the right $\in V,$

(*iii*) $a(-\alpha)=-(a\alpha)\ ;\ a\in K,\ \alpha\in V,$

(*iv*) $a(\alpha-\beta)=a\alpha-a\beta\ ;\ a\in K,\ \alpha\in V,\ \beta\in V.$

The proofs which are easy are left to the reader.

84. Vector Sub-spaces. Let W be any sub-set of a vector space $V(K)$. To each pair of members α, β of W regarded as members of V corresponds a member $\alpha+\beta$ of V which may or may not belong to W. In case W is such that

$$\alpha\in W,\ \beta\in W \Longrightarrow \alpha+\beta\in W,$$

we say that W is *stable* for the addition composition in V and that the addition composition in V has induced a composition in W and finally the composition in W given by

$$(\alpha, \beta)\longrightarrow \alpha+\beta,\ \alpha\in W,\ \beta\in W$$

is called the Induced addition composition in W.

Similarly if W is such that

$$\alpha \in W, a \in K \Longrightarrow a\alpha \in W,$$

we say that W is *stable* for the scalar multiplication composition in V and analogously define the induced scalar multiplication composition in W.

Def. *A sub-set W of a vector space $V(K)$ is said to be a vector sub-space or simply a sub-space of $V(K)$, if it is stable for the two compositions in $V(K)$ and is a vector space for the induced compositions.*

84·1. Criteria for a sub-set W of a vector space V(K) to be a sub-space thereof. *The necessary and sufficient conditions for a subset W of $V(K)$ to be a sub-space are that*

(*i*) $\alpha \in W, \beta \in W \Longrightarrow \alpha - \beta \in W,$

(*ii*) $a \in K, \alpha \in W \Longrightarrow a\alpha \in W.$

We may also state the result in another form.

The necessary and sufficient condition for a sub-set W of $V(K)$ to be a sub-space are that

$$\alpha \in W, \beta \in W, a \in K, b \in K \Longrightarrow a\alpha + b\beta \in W.$$

The proof is left to the reader.

Illustrations.

1. The vector space of all polynomials with coefficients in a field K and degree $\leqslant n$ is a sub-space of the vector space of all polynomials over K.

2. The set of ordered triads

$$(a_1, a_2, 0) \; ; \; a_1 \in K, a_2 \in K,$$

is a sub-space of the space $V_3(K)$ of triads over K.

Also the set of ordered triads

$$(a_1, 0, 0) \; ; \; a_1 \in K,$$

is a sub-space of $V_3(K)$.

85. Algebra of sub-spaces

85·1. Intersection of two sub-spaces. Largest sub-space contained in two sub-spaces. Theorem. *The intersection of any two sub-spaces of a vector space is again a sub-space.*

Let W_1, W_2 be two sub-spaces of $V(K)$.

Let

$$\alpha \in W_1 \cap W_2, \beta \in W_1 \cap W_2,$$
$$a \in K, b \in K.$$

We have

$$\alpha \in W_1 \cap W_2 \Longrightarrow \alpha \in W_1, \alpha \in W_2,$$
$$\beta \in W_1 \cap W_2 \Longrightarrow \beta \in W_1, \beta \in W_2.$$

Again

$$\alpha \in W_1, \beta \in W_1 \Longrightarrow a\alpha + b\beta \in W_1,$$
$$\alpha \in W_2, \beta \in W_2 \Longrightarrow a\alpha + b\beta \in W_2,$$

so that

$$a\alpha + b\beta \in W_1 \cap W_2.$$

Thus we see that

$$W_1 \cap W_2$$

is a sub-space of $V(K)$. It may be noted that

$$W_1 \cap W_2$$

is the largest sub-space contained in W_1 as well as in W_2 in the sense that it is contained in W_1 as well as W_2 and contains every sub-space contained in W_1 and W_2.

It may similarly be seen that *the intersection of* **any family** *of sub-spaces of a vector space is a sub-space.*

Illustration. If W_1 is a sub-space of $V_3(K)$ consisting of all the triads of the form $(a_1, a_2, 0)$ and W_2 be the sub-space consisting of all triads of the form $(b_1, 0, b_3)$, then $W_1 \cap W_2$ is the sub-space consisting of all triads of the form $(a, 0, 0)$.

85·2. Smallest sub-space containing any sub-set of V(K). Let S be any sub-set of $V(K)$. By the smallest sub-space containing S of $V(K)$ is meant the sub-space of $V(K)$ which contains S and is contained in every sub space containing S. It is quite easy to prove that the smallest sub space containing a sub set S exists and is unique. In fact it is the intersection of the family of sub spaces which contain the sub-set S. We may denote this sub-space by the symbol $\{S\}$ and say that S generates the sub space $\{S\}$. As an explicit expression for the elements of $\{S\}$, we may see that it is the totality *of all those elements of* $V(K)$ *which are expressible in the form*

$$a_1\alpha_1 + \ldots\ldots\ldots + a_m\alpha_m$$

where

$$\alpha_1, \alpha_2, \ldots\ldots\ldots, \alpha_m$$

is any arbitrary finite sub-set of S *and*

$$a_1, a_2, \ldots\ldots, a_m$$

is any arbitrary finite sub-set of K.

(*i*) this totality is a sub-space of $V(K)$,

(*ii*) this totality is necessarily contained in every sub-space containing S.

(*iii*) Each member α_i of S is a member of this totality for, we have

$$\alpha_i = 1\alpha_i.$$

Illustrations. 1. The sub-space of $V_3(K)$ generated by a sub-set containing of a single element (1, 0, 0) is the totality of elements the form $(a, 0, 0)$.

2. The sub-space of $V_3(K)$ generated by a sub-set consisting of the two elements (1, 0, 0), (0, 1, 0) is the totality of elements of the form $(a, b, 0)$.

3. Finally the sub set consisting of the three elements (1, 0, 0), (0, 1, 0), (0, 0, 1) generates the entire space $V_3(K)$.

4. The infinite set of polynomials

$$1, t, t^2, t^3, \ldots\ldots, t^n, t^{n+1}, \ldots\ldots$$

generates the entire space of polynomials over a field K.

85·3. Union. Sum of two-spaces. The union $W_1 \cup W_2$ of two sub-spaces W_1, W_2 of $V(K)$, unlike intersection, may *not* be a sub space of $V(K)$.

For example, the union of the sub-spaces of $V_3(K)$ consisting of the elements of the form $(a, 0, 0)$ and $(0, b, 0)$ is *not* a sub-space of $V_3(K)$.

In the case of union, we may however talk of the smallest sub-space

$$\{W_1 \cup W_2\}$$

containing $W_1 \cup W_2$ which is the same thing as the sub-space generated by the sub-set $W_1 \cup W_2$.

It is an interesting fact that the sub set

$$W_1 + W_2$$

of $V(K)$ which denotes the totality of elements obtained on adding each element of W_1 to each element of W_2 is a sub space and *in fact* the sub-space generated by the union $W_1 \cup W_2$, *i.e.*, we have

$$\{W_1 \cup W_2\} = W_1 + W_2.$$

Ex. Point out an analogous situation in group theory. (Refer § 24, page 83).

We now proceed to prove *this result.*

Let

$$\alpha_1 \in W_1, \beta_1 \in W_1 ; \alpha_2 \in W_2, \beta_2 \in W_2$$

so that

$$\alpha_1+\alpha_2 \in W_1+W_2,\ \beta_1+\beta_2 \in W_1+W_2.$$

We have

$$a(\alpha_1+\alpha_2)+b(\beta_1+\beta_2)=(a\alpha_1+b\beta_1)+(a\alpha_2+b\beta_2).$$

Now

$$\alpha_1 \in W_1,\ \beta_1 \in W_1 \Longrightarrow a\alpha_1+b\beta_1 \in W_1 ;$$

W_1 being a sub-space

$$\alpha_2 \in W_2,\ \beta_2 \in W_2 \Longrightarrow a\alpha_2+b\beta_2 \in W_2 ;$$

W_2 being a sub-space

$$\therefore \quad (a\alpha_1+b\beta_1)+(a\alpha_2+b\beta_2) \in W_1+W_2.$$

Thus W_1+W_2 is a sub-space.

We have now to show that the two sub-spaces

$$W_1+W_2,\ \{W_1 \cup W_2\}$$

are the same.

Now

$$W_1+W_2 \supseteq W_1,\ W_1+W_2 \supseteq W_2,$$

so that

$$W_1+W_2 \supseteq W_1 \cup W_2$$

$$\therefore \quad W_1+W_2 \supseteq \{W_1 \cup W_2\}.$$

Also, as is easy to see,

$$\{W_1 \cup W_2\} \subseteq W_1+W_2.$$

Thus

$$W_1+W_2=\{W_1 \cup W_2\}.$$

Note. It may be seen that the set of all sub-spaces of a vector space is a Lattice for the relation 'Included in'; the *g.l.b.* of two spaces being their sum and *l.u b.* their intersection.

86. Quotient space. We shall now consider the concept of the *Quotient Space* corresponding to that of *Quotient group* and *Difference ring*. It will be recalled that these two latter concepts had led to the introduction of distinguished types of sub-groups and sub-rings, *viz.*, Normal sub-groups and Ideals. The concept of Quotient Space, however, does not need the introduction of any distinguished type of sub-space.

Let W be any subspace of a vector space $V(K)$.

Considering the aspect of the set W as a subgroup of the additive group of V which is Abelian, we see that W is a normal subgroup of the additive group of $V(K)$. Then $W+\alpha$ is any coset of W in $V(K)$; α being any member of V.

We know that if $W+\alpha$, $W+\beta$ be any two cosets of W, we have

$$\text{either } W+\alpha=W+\beta \text{ or } W+\alpha \cap W+\beta=\phi,$$

where ϕ denotes the void set.

Also

$$W+\alpha=W+\beta \Longleftrightarrow \alpha-\beta \in W.$$

We shall now see that this set of cosets of W in $V(K)$ is equipped with the structure of a vector space over the field in terms of suitable definitions of addition and scalar multiplication.

Theorem. *If W is any subspace of a vector space $V(K)$, then the set V' of all cosets $W+\alpha$; α being any arbitrary member of V, is a vector space over K for the addition and scalar multiplication compositions defined as follows :—*

$$(W+\alpha)+(W+\beta)=W+(\alpha+\beta),$$
$$a(W+\alpha)=W+a\alpha\ ;\ a \in K.$$

It has firstly to be shown that these compositions are *well defined, i.e.*, are independent of the particular representatives chosen to denote a coset. This fact has already been seen twice for the case of the addition composition.

Suppose that

$$W+\alpha=W+\alpha'$$

so that

$$\alpha'-\alpha \in W.$$

We have then to see that

$$W+a\alpha=W+a\alpha'.$$

This is so for

$$\alpha'-\alpha \in W \Longrightarrow a(\alpha'-\alpha)=a\alpha'-a\alpha \in W$$

and

$$a\alpha'-a\alpha \in W \Longrightarrow W+a\alpha=W+a\alpha'.$$

Thus we see that

$$W+\alpha=W+\alpha' \Longrightarrow W+a\alpha=W+a\alpha'$$

so that

$$a(W+\alpha)=a(W+\alpha').$$

The set V' of cosets of W in K is an Abelian group for the Addition composition defined above in V'. (Refer § 36, page 94).

All that we have to do now is to show that the four laws as given in III of § 82, page 217 for the definition of a vector space hold good in the present case. We shall need only the def. of the sum of two cosets and of the product of a coset by a scalar to prove these laws.

1. We have, by def.,

$$\begin{aligned} a[(W+\alpha)+(W+\beta)] &= a[W+(\alpha+\beta)] \\ &= W+a(\alpha+\beta) \\ &= (W+a\alpha)+(W+a\beta) \\ &= a(W+\alpha)+a(W+\beta). \end{aligned}$$

$$\begin{aligned} (a+b)(W+\alpha) &= W+(a+b)\,\alpha \\ &= (W+a\alpha)+(W+b\alpha) \\ &= a(W+\alpha)+b(W+\alpha). \end{aligned}$$

$$\begin{aligned} (ab)(W+\alpha) &= W+(ab\alpha) \\ &= W+a(b\alpha) \\ &= a(W+b\alpha) \\ &= a[b(W+\alpha)]. \end{aligned}$$

4. $$1(W+\alpha)=W+1\alpha=W+\alpha.$$

Quotient Space. *The vector space V' formed of all the cosets in $V(K)$ of a vector sub-space W of the same is called the Quotient space of V relative to W and is denoted by V/W.*

87. Vector Space Homomorphisms. Linear Transformations. A mapping f of a vector space $U(K)$ into a vector space $V(K)$ is called a homomorphism, if

$$f(\alpha_1+\beta_1)=f(\alpha_1)+f(\beta_1)\ ;\ \alpha_1 \in U,\ \beta_1 \in U$$

$$f(a\alpha_1)=af(\alpha_1)\ ;\ a \in K,\ \alpha_1 \in U.$$

A homomorphism of a vector space into another vector space is also called a *Linear Transformation* and this latter name is one which is almost exclusively used in preference to homomorphism.

As an important illustration, we may see that if W is any sub-space of a vector space $V(K)$, then the mapping f of V onto W/V defined by

$$f(\alpha)=W+\alpha,\ \alpha \in V,$$

is a linear transformation.

Note 1. If f is a linear transformation of $U(K)$ into $V(K)$, then $f(U)$ which denotes the set of f-images of the members of U is a sub-space of V. The proof is simple.

Note 2. If f is a linear transformation of $U(K)$ into $V(K)$, then, as may be easily shown,

$$f(0)=0, \qquad (i)$$

and

$$f(-\alpha)=-f(\alpha). \qquad (ii)$$

The 0 on the left in (*i*) denotes the additive identity of U and that on the right the additive identity of V.

Note 3. The set of all those elements of $U(K)$ which are mapped onto the zero of $V(K)$ *i.e.*, the set of elements $\alpha \in U$ such that

$$f(\alpha)=0$$

is a subspace of U. This subspace is called the **Kernel** of the linear transformation.

Illustrations.

1. The mapping f defined by

$$f(a_1, a_2, a_3)=(a_1, a_2),$$

is, as may be easily shown, a linear transformation of $V_3(K)$ onto $V_2(K)$.

2. *Consider the vector space* $\mathbf{R}[x]$ *of all polynomials over the real field* $\mathbf{R}$.

The mapping f which associates to each $p(x) \in \mathbf{R}[x]$ its derivative $p'(x)$ also belonging to $\mathbf{R}(x)$ is a linear transformation of $\mathbf{R}[x]$ into itself. In fact, we have

$$\begin{aligned} f[p(x)+q(x)] &= [p(x)+q(x)]' \\ &= p'(x)+q'(x) \\ &= f(p(x))+f(q(x)), \\ f[ap(x)] &= [ap(x)]' \\ &= ap'(x)=af(p(x)). \end{aligned}$$

Thus differentiation is a linear transformation.

3. Let $p(x) \in \mathbf{R}[x]$ and let a mapping f be such that

$$f(p(x))=\int_0^x p(x)dx.$$

It is easy to verify that f, as defined here, is a Linear transformation of the vector space $\mathbf{R}[x]$ into itself.

Ex. 1. Examine which of the following mappings f of $V_3(R)$ into itself are linear transformations :

(1) $f(a_1, a_2, a_3)=(2a_1, 3a_2, 4a_3)$
(2) $f(a_1, a_2, a_3)=(a_1+1, a_2, a_3-1)$
(3) $f(a_1, a_2, a_3)=(a_2, a_1, a_3)$
(4) $f(a_1, a_2, a_3)=(a_1^2, a_2\ a_3^2)$.

2. $p(x)$ is any member of the vector space $\mathbf{R}[x]$ over the field R of real numbers. Show that

$$p(x) \longrightarrow p(2)$$

is a linear transformation of $R[x]$ into R looked upon as a vector space over the field R.

3. Which of the following mappings f of the vector space $R[x]$ are linear transformations of $R[x]$ into itself?

(i) $f(p(x)) = f(p(x)) + 1$.

(ii) $f(p(x)) = \frac{d^2p(x)}{dx^2}$.

(iii) $f(p(x)) = p(x) + \int_0^x p(x)dx$.

88. Isomorphisms. A special case of a linear transformation f of a vector space $U(K)$ into $V(K)$ arises, when f is a *one-one mapping of* $U(K)$ *onto* $V(K)$. In this case we say that $U(K)$ and $V(K)$ are isomorphic vector spaces.

As an illustration of an isomorphic mapping, we may see that if f is a linear transformation of a vector space U onto a vector space V and W denotes the Kernel of this linear transformation, then the quotient space U/W is isomorphic to V and an isomorphic mapping is defined by

$$W + \alpha \longrightarrow f(\alpha).$$

89. Direct sum of spaces. Let $U(K)$, $V(K)$ be any two vector spaces over the same field K. It may then be verified that the product set $U \times V$ which consists of the elements (α, β) where $\alpha \in U, \beta \in V$ acquires a vector space structure for the compositions defined as follows :

$$(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2)$$

$$a(\alpha, \beta) = (a\alpha, a\beta) \qquad a \in K.$$

This vector space $U \times V$ with elements (α, β) is known as the *Direct sum* of the vector spaces U and V is written as $U + V$.

The following facts may be verified.

1. The set U' of elements $(\alpha, 0)$, $\alpha \in U$ is a sub-space of $U + V$ isomorphic to U.

2. The set V' of elements $(0, \beta)$, $\beta \in V$ is a sub-space of $U + V$ isomorphic to V.

The quotient space $(U+V)/U'$ is isomorphic to V' and $(U+V)/V'$ is isomorphic to U'.

3. Each element of $U+V$ is uniquely expressible as sum of an element of U' and an element of V'

We have

$$(\sigma, \beta)=(\alpha, 0)+(0, \beta).$$

90. Vector space as a direct sum of sub-spaces. Def. *A vector space $V(K)$ is said to be a direct sum of its two sub-spaces W_1 and W_2, if each element of V is* **uniquely expressible** *as sum of an element of W_1 and an element of W_2.* Also we then write $V=W_1\dot{+}W_2$.

Illustration. 1. Consider the space $V_2(K)$ of 2-tuples over K. Clearly then the set of elements $(a, 0)$ and the set of elements $(0, b)$ are two sub-spaces of $V_2(K)$. Here a and b range over K. Denoting these sub-spaces by W_1 and W_2, we have

$$V_2=W_1\dot{+}W_2.$$

Theorem. *Necessary and sufficient conditions for*

$$V=W_1\dot{+}W_2$$

are that

(i) $$V=W_1+W_2$$

(ii) $$W_1\cap W_2=\{0\},$$

i.e., 0 is the only element common to the sub-spaces W_1 and W_2.

The conditions are necessary.

Since each element of V is expressible as sum of an element of W_1 and an element of W_2, we have

$$V=W_1+W_2.$$

Let if, possible $0\neq\alpha\in W_1\cap W_2$.

We have then

$$\alpha=0+\alpha,$$
$$\alpha=\alpha+0,$$

so that an element $\alpha\in V$ is expressible in atleast two ways as sum of an element of W_1 and an element of W_2 and accordingly

$$V=W_1\dot{+}W_2,$$

is contradicted.

The conditions are sufficient.

$$V=W_1+W_2$$

shows that each element of V is expressible as sum of an element of W_1 and an element of W_2.

Let, if possible,

$$\alpha=\alpha_1+\alpha_2,\ \alpha\in V,\ \alpha_1\in W_1,\ \alpha_2\in W_2,$$
$$\alpha=\beta_1+\beta_2,\ \alpha\in V,\ \beta_1\in W_1,\ \beta_2\in W_2.$$

Then

$$\alpha_1+\alpha_2=\beta_1+\beta_2$$

i.e.,

$$\alpha_1-\beta_1=\beta_2-\alpha_2$$

where

$$\alpha_1-\beta_1 \in W_1,\ \beta_2-\alpha_2 \in W_2.$$

Thus

$$\alpha_1-\beta_1=\beta_2-\alpha_2 \in W_1 \cap W_2,$$

By (*ii*), $\alpha_1-\beta_1=0=\beta_2-\alpha_2$.

Also

$$\alpha_1-\beta_1=0 \Longrightarrow \alpha_1=\beta_1,$$
$$\beta_2-\alpha_2=0 \Longrightarrow \alpha_2=\beta_2,$$

so that each element α of V is uniquely expressible as sum of an element of W_1 and an element of W_2. Hence

$$V=W_1+W_2.$$

91. Basis of a vector space. We shall now introduce the very important concept of the Basis of a vector space. For this purpose, we first state what is meant by a Linearly independent and a linearly dependent set of vectors.

Def. *A finite system of vectors*

$$\alpha_1, \alpha_2, \ldots\ldots, \alpha_m$$

of a vector space $V(K)$ is said to be a linearly independent (L.I.) system, if every relation of the form

$$a_1\alpha_1+a_2\alpha_2+\ldots\ldots+a_m\alpha_m=0, \qquad a_i \in K,\ 1 \leqslant i \leqslant m$$

implies that

$$a_i=0 \text{ for } 1 \leqslant i \leqslant m,$$

and otherwise it is said to be a linearly dependent (L.D.) system.

Also any infinite system of vectors is said to be linearly independent, if each *finite* sub-system of the same is linearly independent. In the alternative case, the system is said to be linearly dependent.

Ex. 1. Show that a system consisting of a single vector is *L.D.*, if and only if the vector is a zero vector.

Ex. 2. Show that the system of the three 3-tuples

$$(1, 0, 0),\ (0, 1, 0),\ (0, 0, 1)$$

of $V_3(\mathrm{R})$ is *L.I.*

Ex. 3. Show that any sub system of a *L.I.* system is *L.I.* and that any super-system of a *L.D.* system is *L.D.*

[A system S_1 is said to be a super-system of S_2 if $S_1 \supseteq S_2$].

91·1. Basis of a Vector Space. Def. *Any sub-set S of $V(K)$ is said to be a basis of $V(K)$, if*

(i) S is a linearly independent system,

(ii) S generates $V(K)$, i.e., $V(K)=\{S\}$.

Illustrations.

1. A system S consisting of the n vectors
$e_1=(1, 0, 0, \ldots\ldots, 0)$, $e_2=(0, 1, 0, 0, \ldots\ldots, 0), \ldots\ldots, e_n=(0, 0, \ldots\ldots, 1)$
is a basis of $V_n(K)$.

Firstly we show that S is a *L.I.* system.

Now, we have

$$a_1e_1+a_2e_2+\ldots\ldots a_ne_n=(a_1, a_2, \ldots\ldots, a_n)$$

so that

$$a_1e_1+a_2e_2+\ldots+a_ne_n=0 \longrightarrow a_1=0, a_2=0, \ldots\ldots, a_n=0.$$

Also the system S generates $V_n(K)$. In fact, if

$$(a_1, a_2, \ldots\ldots, a_n)$$

be any given member of $V_n(K)$, we have

$$(a_1, a_2, \ldots\ldots, a_n)=a_1e_1+\ldots\ldots+a_ne_n.$$

Hence the result.

2. A system consisting of the vectors

$$1, x, x^2, \ldots\ldots, x^n, \ldots\ldots$$

is a basis of the vector space $K[x]$ of all polynomials over the field K.

The verification is left to the reader.

It will be seen that nothing has so far been said about the possible existence of the basis of a given vector space. It is a *fact*, however, that for any given vector space there *exists a basis* and that any two bases of a vector space are such that there exists a *one-one* mapping of either onto the other. The proof this theorem in the general case being beyond the scope of the present book, we shall only restrict our attention to what are known as **Finitely Generated Spaces** as defined below.

92. Finitely generated spaces. Def. *A vector space is said to be a finitely generated space, if there exists a finite sub-system of the same which generates the whole space.*

Ex. 1. Show that the vector space $V_n(K)$ of n-tuples is a finitely generated space.

Ex. 2. Show that the vector space $K[x]$ of all polynomials in x over a field K is not a finitely generated space.

Ex. 3. Show that every element α of a vector space having as its basis a system of vectors

$$\alpha_1, \alpha_2, \ldots\ldots, \alpha_n$$

is uniquely expressible as

$$\alpha = a_1\alpha_1 + \ldots\ldots + a_n\alpha_n.$$

92·1. Cases of Finitely generated spaces. Theorem. *There exists a basis for each finitely generated space and any two bases of such a space have the same finite number of elements.*

We start with proving two lemmas.

Lemma I. If a system consisting of the vectors

$$\alpha_1, \alpha_2, \ldots\ldots, \alpha_m \qquad (1)$$

is L. D., then there exists a vector α_i of the system such that the same is a linear combination of the preceding vectors

$$\alpha_1, \alpha_2, \ldots\ldots, \alpha_{i-1}.$$

The system (1) being L. D., there exists a relation of the form

$$a_1\alpha_1 + a_2\alpha_2 + \ldots\ldots + a_m\alpha_m = 0, \qquad (2)$$

where, not all the coefficients $a_1, a_2, \ldots\ldots, a_m$ are zero. Let a_i be the last *non-zero* member of the ordered system of elements

$$a_1, a_2, \ldots\ldots, a_i, \ldots\ldots, a_m.$$

We may then re-write (2) as

$$\alpha_i = -a_1a_i^{-1}\alpha_1 - a_2a_i^{-1}\alpha_2 + \ldots\ldots - a_{i-1}a_i^{-1}\alpha_{i-1},$$

so that α_i appears as a linear combination of the system of vectors

$$\alpha_1, \alpha_2, \ldots\ldots, \alpha_{i-1}.$$

Lemma II. If β is a linear combination of the system of vectors

$$\alpha_1, \alpha_2, \ldots\ldots, \alpha_m$$

then the system of vectors

$$\beta, \alpha_1, \alpha_2, \ldots\ldots, \alpha_m$$

is L. D.

The proof is quite straight.

Now we come to the proof of the main theorem.

Existence of a basis. Let $V(K)$ be a finitely generated space and let a finite system S consisting of the vectors

$$\alpha_1, \alpha_2, \ldots\ldots, \alpha_m$$

generate S.

We may suppose that no member of S is 0. If S *is L. I.*, then S is already a basis.

Suppose now that S is L D. Then there exists a vector α_t which is a linear combination of the system of vectors

$$\alpha_1, \alpha_2, \ldots, \alpha_{t-1}.$$

Thus we see that the system of vectors

$$\alpha_1, \alpha_2, \ldots\ldots, \alpha_{t-1}, \alpha_{t+1}, \ldots\ldots, \alpha_m \qquad (2)$$

also generates $V(K)$. In fact each member of $V(K)$ is a linear combination of $\alpha_1, \ldots\ldots, \alpha_m$ and α_t is itself a linear combination of $\alpha_1, \ldots, \alpha_{t-1}$ so that we see that each member of $V(K)$ is also a linear combination of the system (2) of vectors.

Thus $V(K)$ is as well generated by the system obtained on omitting the element α_t and consisting of $(m-1)$ elements. If this new system is L. I., it is a basis. Otherwise, we obtain, as above, a new system which consists of $(m-2)$ elements and generates $V(K)$. Thus proceeding, we shall, after a finite number of steps, obtain a L. I., sub-system of S which generates $V(K)$ and which is as such a basis of $V(K)$.

This proves the first part of the theorem concerning the existence of a basis.

Also we see that a finitely generated space has atleast one finite basis.

Invariance of the number of elements in a basis. Suppose that the two systems of vectors

$$\alpha_1, \ldots\ldots, \alpha_m$$

$$\beta_1, \ldots\ldots, \beta_n$$

are two bases of $V(K)$. We shall show that

$$m = n.$$

Consider the system of vectors

$$\beta_1, \alpha_1, \ldots\ldots, \alpha_m. \qquad (3)$$

This system is L. D. for β_1 is L. C. of the system of vectors $\alpha_1, \ldots\ldots, \alpha_m$. (Lemma 2)

Thus there exists a member $\alpha_t \neq \beta_1$ of the system such that α_t is a L. C. of

$$\beta_1, \alpha_1, \ldots\ldots, \alpha_{t-1}. \quad \text{(Lemma I)}$$

From this it follows, that $V(K)$ is generated by the system of vectors

$$\beta_1, \alpha_1, \ldots\ldots, \alpha_{t-1}, \alpha_{t+1}, \ldots\ldots \alpha_m. \qquad (4)$$

obtained on omitting α_t from the system (3).

Consider again the system of vectors

$$\beta_2, \beta_1, \alpha_1 \ldots\ldots, \alpha_{i-1}, \alpha_{i+1} \ldots\ldots, \alpha_m. \tag{5}$$

This system is L. D. for β_2 is a linear combination of the system of the vectors following. Proceeding as before, we see that there exists a member α_i different from β_1 and β_2 of the system such that the system obtained on eliminating α_i from (5) generates $V(K)$.

We may continue to proceed in this manner.

Here each complete step consists in the inclusion of a β and the exclusion of an α.

Clearly we cannot exhaust the α system before exhausting the β system, for that would mean that a proper sub-set of the β system of vectors generates $V(K)$. Thus we have

$$m \leqslant n.$$

Interchanging the roles of the two bases, we have also

$$n \not< m.$$

Thus

$$m = n.$$

Hence the theorem.

[Show also that no basis of a finitely generated space can be infinite].

Dimension of a finitely generated space. *The number of elements in a basis of a finitely generated space is called the dimension of the space.*

A vector space which is not finitely generated may be referred to as an infinite dimensional space.

Illustrations.

1. The vector space $V_n(K)$ of n-tuples over a field K is of dimension n.

2. The vector space $K[x]$ of all polynomials over a field K is infinite dimensional.

93. Some Properties of finite dimensional spaces. In this section $V(K)$ denotes a finite dimensional space.

1. *For each finite generating system S of vectors of $V(K)$, there exists a sub-system of S which is a basis of $V(K)$.*

The method of proof for the existence of the basis of a finitely generated vector space has already brought out the truth of this result.

II. *Any L. I. sub-system of $V(K)$ can be extended to a basis of $V(K)$.*

This result means that if

$$\alpha_1, \ldots, \alpha_m$$

constitute a L. I., system of $V(K)$, then we can supplement the same by adjoining $(n-m)$ vectors

$$\alpha_{m+1}, \ldots\ldots, \alpha_n$$

such that the complete system

$$\alpha_1, \ldots\ldots, \alpha_m, \alpha_{m+1}, \ldots\ldots, \alpha_n,$$

constitutes a basis of $V(K)$.

Let the vectors

$$\beta_1, \ldots\ldots, \beta_n$$

constitute any basis of the n-dimensional space $V(K)$ and consider the set

$$\alpha_1, \ldots\ldots, \alpha_m, \beta_1, \ldots\ldots, \beta_n.$$

which is clearly L. D.

Proceeding as in the case of the proof the existence of a basis of a finitely generated space, we may go on deleting elements of the β set so as to arrive at a basis of $V(K)$ containing the α set. It may be seen that at no stage shall we be omitting a member of the α set for no member of the α set can be a L. C. of the system of members preceding the same.

Ex. 1. If a system of n vectors

$$\alpha_1, \ldots\ldots, \alpha_n$$

of a finite dimensional space $V(K)$ of dimension n be *L. I.*, then the system is a basis of the space.

Ex. 2. If a system of n vectors

$$\alpha_1, \ldots\ldots, \alpha_n$$

of a finite dimensional space $V(K)$ of dimension n generates $V(K)$, then the system is a basis of the space.

III. *Each system of $(n+1)$ or more vectors of $V(K)$ of dimension n is L.D.*

If a system with $(n+1)$ or more vectors were *L.I.*, then we could supplement the same so as to arrive at a *basis* which would consist of only n members.

IV. *Each sub space W of a vector space $V(K)$ of dimension n is a finite dimensional space with dimension $\leq n$.*

Each system of $(n+1)$ or more vectors of W, being also a system of vectors of $V(K)$, is *L.D.*

Thus a *L.I.* system of vectors W can contain, at the most n members.

Consider now the totality of *L.I.* systems of W. Each member of this totality has at the most n members. Let S denote a *L.I.* system of W with a maximum number of elements. Then S is a basis of W for

(*i*) S is a *L.I.* system of W.

(*ii*) S generates W. In fact if S consists of the vectors

$$\gamma_1, \ldots\ldots, \gamma_m,$$

and α be any member of W, then the system

$$\alpha, \gamma_1, \ldots, \gamma_m$$

is *L.D.* and the system

$$\gamma_1, \ldots\ldots, \gamma_m$$

is *L.I.* From this it follows that α is a *L. C.* of the system of vectors

$$\gamma_1, \ldots\ldots, \gamma_m.$$

Hence the result.

V. *If W_1, W_2 are two sub-spaces of a finite dimensional vector space $V(K)$, then*

$$dim\ W_1 + dim\ W_2 = dim\ (W_1 + W_2) + dim\ (W_1 \cap W_2),$$

where $dim\ W_1$ denotes the dimension of the sub space W_1.

Let the system of vectors

$$\gamma_1, \ldots, \gamma_k \qquad \ldots (1)$$

be a basis of the sub-space $W_1 \cap W_2$.

The space $W_1 \cap W_2$ being a sub-space of W_1, we can supplement the system (1) so that the extended set is a basis of W_1. Thus let

$$\gamma_1, \ldots, \gamma_k, \alpha_1, \ldots, \alpha_l$$

be a basis of W_1. Similarly let

$$\gamma_1, \ldots \gamma_k, \beta_1, \ldots, \beta_m$$

be a basis of W_2. We have thus

$$dim\ (W_1 \cap W_2) = k,\ dim\ W_1 = k + l,\ dim\ W_2 = k + m.$$

We shall now show that the system of vectors

$$\gamma_1, \ldots, \gamma_k, \ldots, \alpha_1, \ldots, \alpha_l, \beta_1, \ldots, \beta_m$$

is a basis of $W_1 + W_2$.

Firstly, we shall show that this is a *L.I.* system. Let, if possible,

$$c_1\gamma_1 + \ldots + c_k\gamma_k + a_1\alpha_1 + \ldots + a_l\alpha_l + b_1\beta_1 + \ldots + b_m\beta_m = 0 \qquad (2)$$

$$\therefore \quad (c_1\gamma_1+\ldots+c_k\gamma_k)+(a_1\alpha_1+\ldots+a_l\alpha_l)=-(b_1\beta_1+\ldots+b_m\beta_m).$$

From this it follows that

$$b_1\beta_1+\ldots+b_m\beta_m \in W_1 \cap W_2,$$

so that we have a relation of the form

$$b_1\beta_1+\ldots+b_m\beta_m=d_1\gamma_1+\ldots+d_k\gamma_k.$$

i.e.

$$b_1\beta_1+\ldots+b_m\beta_m-d_1\gamma_1-\ldots-d_k\gamma_k=0$$

Since the system of vectors

$$\beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_k$$

is *L.I.*, it follows that we must have

$$b_1=0, b_2=0, \ldots b_m=0$$

The relation (2) now reduces to

$$c_1\gamma_1+\ldots+c_k\gamma_k+a_1\alpha_1+\ldots+a_l\alpha_l=0.$$

The system of vectors

$$\gamma_1, \ldots, \gamma_k, \alpha_1, \ldots, \alpha_l$$

being also *L.I.*, it follows that

$$c_1=0, \ldots, c_k=0, a_1=0, \ldots a_l=0.$$

Thus the system of vectors

$$\gamma_1, \ldots, \gamma_k, \alpha_1 \ldots \alpha_l, \beta_1, \ldots, \beta_m$$

is *L.I.*

Also, as may be easily seen, this system of vectors generates W_1+W_2.

Thus

$$dim\ (W_1+W_2)=k+l+m.$$

Hence it follows that

$$\begin{aligned} dim\ W_1+dim\ W_2&=(k+l)+(k+m)\\ &=(k+l+m)+k\\ &=dim\ (W_1+W_2)+dim\ W_1 \cap W_2. \end{aligned}$$

94. Dimension of a Quotient Space. Theorem. *If W is a sub-space of dimension m of a vector space $V(K)$ of dimension n, then the dimension of the quotient space V/W is $n-m$, i.e.,*

$$dim\ V=n, dim\ W=m \Longrightarrow dim\ V/W=n-m.$$

Let the system of vectors

$$\alpha_1, \ldots, \alpha_m$$

be a basis of W and let the system of vectors

$$\alpha_1, \ldots \alpha_m, \beta_1, \ldots \beta_l$$

be a basis of V so that $l+m=n$.

We shall now show that the system of l cosets

$$W+\beta_1, \ldots\ldots, W+\beta_l \qquad \ldots(1)$$

of W in V is a basis of the quotient space V/W.

Let

$$a_1(W+\beta_1)+ \ldots. +a_l(W+\beta_l)=0, \qquad \ldots(2)$$

where 0 on the right denotes the zero of the space V/W *i.e.*, the coset member W of the same. Then (2) gives

$$W+(a_1\beta_1+\ldots \ldots+a_l\beta_l)=0.$$

$$\therefore \quad a_1\beta_1+\ldots\ldots+a_l\beta_l \in W,$$

so that we have a relation of the the form

$$a_1\beta_1+\ldots\ldots+a_l\beta_l=c_1\alpha_1+\ldots\ldots+c_m\alpha_m. \qquad \ldots(3)$$

As, however, the system of vectors

$$\alpha_1\ldots\ldots, \alpha_m, \beta_1, \ldots\ldots, \beta_l$$

is *L.I.*, we deduce from (3) that

$$a_1=0, \ldots\ldots, a_l=0.$$

Thus the system (1) of vectors of V/W is *L.I.* Consider now any member

$$W+(b_1\beta_1+\ldots\ldots+b_l\beta_l) \text{ of } V/W.$$

As we have

$$W+(b_1\beta_1+\ldots \ldots+b_l\beta_l)=b_1(W+\beta_1)+\ldots\ldots+b_l(W+\beta_l),$$

we see that the system (1) generates V/W. Thus the system (1) is a basis of V/W and accordingly

$$dim(V/W)=l=n-m=dim\ V-dim\ W.$$

95. Dimension of a Direct Sum. Theorem. *If a finite dimensional vector space $V(K)$ is a direct sum of its two sub-spaces W_1 and W_2, then*

$$div\ V=dim\ W_1+dim\ W_2.$$

The space V being finite dimensional, the subspaces W_1 and W_2 thereof are also finite dimensional. Let

$$\dim W_1=l, \dim W_2=m.$$

Let the systems of vectors

$$\alpha_1, \ldots\ldots, \alpha_l$$

$$\beta_1 \ldots\ldots, \beta_m$$

be the bases of W_1 and W_2 respectively.

It will now be shown that the union

$$\alpha_1, \ldots\ldots, \alpha_l, \beta_1, \ldots\ldots, \beta_m \qquad (3)$$

of the two bases is a base of V.

Each vector of V being the sum of a member of W_1 and a member of W_2, we see that the same is the sum of a linear combination of $\alpha_1, \ldots\ldots, \alpha_l$ and a linear combination of $\beta_1, \ldots\ldots, \beta_m$ and accordingly a linear combination of the system (3). Thus the system (3) generates $V(K)$.

To show that the system (3) is L.I., consider the relation

$$a_1\alpha_1 + \ldots\ldots + a_l\alpha_l + b_1\beta_1 + \ldots\ldots + b_m\beta_m = 0$$

or

$$a_1\alpha_1 + \ldots\ldots + a_l\alpha_l = -(b_1\beta_1 + \ldots\ldots + b_m\beta_m).$$

This shows that

$$a_1\alpha_1 + \ldots\ldots + a_l\alpha_l \in W_1 \cap W_2,\ b_1\beta_1 + \ldots + b_m\beta_m \in W_1 \cap W_2.$$

As, 0, is the only vector common to W_1 and W_2, we have

$$a_1\alpha_1 + \ldots\ldots + a_l\alpha_l = 0,\ b_1\beta_1 + \ldots\ldots + b_m\beta_m = 0.$$

By virtue of the linear independence of the two systems of vectors, it follows that

$$a_1 = 0, \ldots\ldots, a_l = 0,\ b_1 = 0, \ldots\ldots, b_m = 0.$$

Thus the system (3) of vectors is L. I.

Hence the result.

Existence of Supplementary subspaces. Theorem. *Corresponding to each subspace W_1 of a finite dimensional vector space $V(K)$, there exists a sub-space W_2 such that V is the direct sum of the sub-spaces W_1 and W_2.*

Let a system of vectors

$$\alpha_1, \ldots\ldots, \alpha_l \qquad (1)$$

be a basis of W_1 By § 93, II, page 234, there exists a system of vectors

$$\alpha_{l+1}, \ldots\ldots, \alpha_n \qquad (2)$$

such that the union of the systems (1) and (2) is a basis of the space V.

Let W_2 be the sub-space generated by the system (2). We shall show that

$$V = W_1 \dot{+} W_2.$$

Every vector of V, being a linear combination of the system

$$\alpha_1, \ldots\ldots, \alpha_l, \alpha_{l+1}, \ldots\ldots, \alpha_n,$$

ifequal to the sum of a member of W_1 and a member of W_2.

Again, let a member

$$a_1\alpha_1+\ldots\ldots+a_l\alpha_l \text{ of } W_1$$

be equal to a member

$$a_{l+1}\alpha_{l+1}+\ldots\ldots+a_n\alpha_n \text{ of } W_2.$$

This gives

$$a_1\alpha_1+\ldots\ldots+a_l\alpha_l-a_{l+1}\alpha_{l+1}-\ldots\ldots-a_n\alpha_n=0,$$

so that by virtue of the L. I. of the system

$$\alpha_1,\ldots\ldots,\ \alpha_l,\ \alpha_{l+1},\ldots\ldots,\ \alpha_n,$$

we see that

$$a_1=0,\ldots\ldots,\ a_l=0,\ a_{l+1}=0,\ldots\ldots,\ a_n=0$$

so that, 0, is the only member common to W_1, and W_2.

Thus we have

$$V=W_1\dot{+}W_2.$$

Note. *The subspace W_2 such that*

$$V=W_1\dot{+}W_2$$

is said to be the **supplementary** of W_1 in V.

The theorem above establishes that there exists a supplementary of every sub space. The supplementary subspace of a subspace may not, however, be unique.

96. Isomorphism of finite dimensional vector spaces. Theorem. *Two finite dimensional vector spaces over the same field are isomorphic if and only if they are of the same dimension.*

Firstly suppose that $U(K)$ and $V(K)$ are two vector spaces over the same field K and with the same dimension n.

Let the systems of vectors

$$\alpha_1,\ldots\ldots,\ \alpha_n \qquad (1)$$

$$\beta_1,\ldots\ldots,\ \beta_n \qquad (2)$$

be the bases of U and V respectively.

Any member of U is uniquely expressible as

$$a_1\alpha_1+\ldots\ldots+a_n\alpha_n.$$

Consider now a mapping f of U into V defined by

$$f(a_1\alpha_1+\ldots\ldots+a_n\alpha_n)=a_1\beta_1+\ldots\ldots+a_n\beta_n.$$

Clearly f is such that

$$f(\alpha_i)=\beta_i \text{ for } 1\leqslant i\leqslant n.$$

It may be easily verified that f is a linear transformation (L.T.).

We shall now show that the L. T. f is one-one and onto.

Let

$$f(\Sigma a_i\,\alpha_i)=f(\Sigma a_i'\,\alpha_i)$$

$$\therefore \qquad \Sigma a_i\,\beta_i=\Sigma a_i'\,\beta_i$$

or

$$\Sigma(a_i - a_i')\,\beta_i = 0.$$

Since the system (2) is a basis of V, we have

$$a_i - a_i' = 0, \text{ for } 1 \leqslant i \leqslant n.$$

Thus we see that

$$f(\Sigma a_i\,\alpha_i) = f(\Sigma a_i'\,\alpha_i) \longrightarrow \Sigma a_i\,\alpha_i = \Sigma a_i'\,\alpha_i$$

so that f is one-one.

Finally since every member of V is expressible as $\Sigma b_i\beta_i$ and the same is the f-image of the element $\Sigma b_i\alpha_i$ of U we see that f is also onto.

Thus there exists an isomorphic mapping of U onto V.

Conversely suppose that there exists an isomorphic mapping f of a finite dimensional space $U(K)$ onto a vector space $V(K)$.

Let the system of vectors

$$\alpha_1, \ldots\ldots, \alpha_n \tag{1}$$

be a basis of the vector space U. We shall show that the system of vectors

$$f(\alpha_1), \ldots\ldots, f(\alpha_n) \tag{2}$$

is a basis of the space V.

Firstly, we show that this system (2) is L. I. Let

$$a_1 f(\alpha_1) + \ldots\ldots + a_n f(\alpha_n) = 0.$$

$\therefore$ f being a L. T., this is equivalent to

$$f(a_1\alpha_1 + \ldots\ldots + a_n\alpha_n) = 0.$$

As f is one one and $f(0) = 0$, we have

$$a_1\alpha_1 + \ldots\ldots + a_n\alpha_n = 0.$$

The system (1) being L. I., it follows that

$$a_i = 0 \text{ for } 1 \leqslant i \leqslant n.$$

Thus the system (2) is L. I.

Now to show that the system (2) generates V. Let $\beta \in$ The mappings f being onto, there exists $\alpha \in U$ such that

$$f(\alpha) = \beta.$$

Let

$$\alpha = b_1\alpha_1 + \ldots\ldots + b_n\alpha_n \in U.$$

We have

$$\begin{aligned}\beta &= f(\alpha)\\ &= f(b_1\alpha_1 + \ldots\ldots + b_n\alpha_n)\\ &= b_1 f(\alpha_1) + \ldots\ldots + b_n f(\alpha_n).\end{aligned}$$

so that the system (2) generates V.

The system (2), consisting as it does of n elements and being shown to be a basis of V, we see that

$$\dim V = n = \dim U.$$

Note. The theorem proved above shows that every space of dimension n over a field K is isomorphic to the space $V_n(K)$ of n-tuples over K; this latter space having been shown to be of dimension n in § 91·1. It also follows from above that over any given field K, there exists one and only one abstract finite dimensional vector space of given dimension n.

97. Co-ordinatisation of an abstract space. Let $V(K)$ be any finite dimensional vector space of dimension n. Also let the system of vectors

$$\alpha_1, \ldots\ldots, \alpha_n$$

be any basis of the space $V(K)$.

Every vector α of $V(K)$ is uniquely expressible in the form

$$\alpha = a_1\alpha_1 + \ldots\ldots + a_n\alpha_n,$$

i.e., corresponding to each $\alpha \in V(K)$ there exists and only one n-tuple

$$(a_1, \ldots\ldots, a_n)$$

over K such that

$$\alpha = \sum_{i=1}^{n} a_i \alpha_i.$$

Here we have a mapping of $V(K)$ onto $V_n(K)$ given by

$$\alpha \longrightarrow (a_1, a_2, \ldots\ldots, a_n).$$

We say that the n-tuple $(a_1, \ldots\ldots, a_n)$ is a coordinate of the member α of $V(K)$ or that the n elements of the n-tuple are the n coordinates of α. Of course the co-ordinate associated with a member of $V(K)$ is dependent upon the particular basis in the space. Thus the choice of a basis $V(K)$ leads to what we may say a manner of *coordinatisation* of the space.

A particular basis chosen may also be referred to as a particular coordinate system. The situation here exactly corresponds to the manner we coordinatize points in a plane and in three dimensional space in classical Geometry based on the choice of a system of coordinate axes and to the manner we coordinatize vectors in ordinary three dimensional space based on the choice of three non-coplanar vectors as constituting a basis.

Moreover we may easily see that the mapping

$$\alpha \longrightarrow (a_1, \ldots\ldots, a_n)$$

of $V(K)$ onto $V_n(K)$ is essentially an isomorphism in as much as
$\alpha \longrightarrow (a_1, \ldots, a_n)$, $\beta \longrightarrow (b_1, \ldots, b_n) \Longrightarrow \alpha+\beta \longrightarrow (a_1+b_1, \ldots\ldots, a_n+b_n)$.

and

$$\alpha \longrightarrow (a_1, \ldots, a_n) \Longrightarrow a\alpha \longrightarrow (aa_1, \ldots, aa_n).$$

It should of course be remembered that corresponding to different bases for a space, we have different co-ordinates assigned to the same vector.

Ex. What is the co-ordinate of the vector $(a_1, a_2, \ldots, a_n)$ of the space of n-tuples relative to the basis consisting of the vectors

$$e_1=(1, 0, \ , 0),\ e_2=(0, 1, 0, \ldots, 0),\ \ldots,\ e_n=(0, 0, \ldots, 0, 1).$$

98. Rank and Nullity of a linear transformation. Let f be a $L.T.$ of a vector space $U(K)$ into a vector space $V(K)$.

By the nullity of f to be denoted by $\nu(f)$, is meant the dimension of the sub-space of U formed by elements which are mapped by f on the zero of $V(K)$. Clearly the nullity of a $L.T.$ may also be described as the dimension of its Kernel.

Again by the rank of f is meant the dimension of the sub-space $f(U)$ of V We shall denote it by $\rho(f)$.

Theorem. *If f be a $L.T.$ of a finite dimensional space $U(K)$ into any space, then*

$$\nu(f) + \rho(f) = dim\ U.$$

Let W be the kernel of the $L.T.$ f of U so that, by def.,

$$\nu(f) = dim\ W.$$

Also we know that the sub-space $f(U)$ of V is isomorphic to the quotient space U/W whose dimension

$$= dim\ U - dim\ W.$$

$$\therefore \qquad \rho(f) = dim\ U - dim\ W.$$

or

$$dim\ U = \rho(f) + \nu(f).$$

99. Linear Equations. Let f be a liner transformation of a vector space $U(K)$ into $V(K)$ and let $y_0 \in V(K)$. Then an equation of the form

$$f(x) = y_0, \qquad x \in U$$

is called *linear* and x is called *unknown*. The equation is called *Linear* and *homogeneous* if $y_0 = 0$.

It can be easily shown that if x_0 is any solution of $f(x) = y_0$,

then the general solution of the same is given by $x+x_0$ where x ranges over the kernel of f *i.e.*, over the solutions of $f(x)=0$.

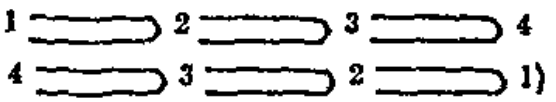
EXERCISES

1. If f be a *L.T.* of a finite dimensional space $U(K)$ into $V(K)$, show that
$$\rho(f) \leqslant min\ (dim\ U,\ dim\ V).$$
2. If f be a *L.T.* of a finite dimensional space $U(K)$ into $V(K)$, then
$$\rho(f)=dim\ U,$$
if and only if f is an isomorphic mapping of U into V *i.e.*, U maps distinct elements of U on distinct elements of V and,
$$\rho(f)=dim\ V,$$
if and only if f is a mapping of U onto V.

3. If f is an endomorphism of a finite dimensional space $U(K)$, i.e., a linear transformation of $U(K)$ into itself, show that the following properties are equivalent :

1. f is an automorphism of U,
2. f is a one-one mapping of U into U,
3. f is a mapping of U onto U,
4. f is of rank dim U,

(We may show that



4. In V_4 (Q), let W denote the subspace with basis,
$$(3, 2, -1, 1), (1, -1, 0, 1).$$
Describe the quotient space V_4 (Q)/W.

5. Show that the set
$$(3-i, 2+2i, 4), (2, 2+4i, 3), (1-i, -2i, 1)$$
is a basis for V_3 (C) and determine the coordinates of the vector
$$(1, 0, 0), (0, 1, 0), (0, 0, 1)$$
with respect to this basis.

6. Show that the set
$$(1, i, 0), (2i, 1, 1), (0, 1+i, 1-i)$$
is a basis for V_3 (C) and determine the coordinates of the vectors
$$(1, 0, 0), (0, 1, 0), (0, 0, 1)$$
with respect to this basis.

7. Show that the set of vectors (x_1, x_2, x_3) in V_3 (R) which satisfy
$$a_1x_1+a_2x_2+a_3x_3=0$$
is a subspace of V_3 (R) ; a_1, a_2, a_3 being given members of R.

8. Construct V_3 (J_2) and list all its sub-spaces. Find also the different bases of V_3 (J_2).

9. Show that V_3 (J_p) has $(p^3-1)/(p-1)=p^2+p+1$ distinct subspaces of dimension one ?

10. Let V_n (K) and V_m (K) denote vector spaces of n-tuples and m-tuples respectively over a field K. Show that the equations

$$\left.\begin{array}{l} x_1a_{11}+x_2a_{12}+\cdots\cdots+x_na_{1n}=y_1 \\ \cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots \\ \cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots \\ x_1a_{m1}+x_2a_{m2}+\cdots\cdots+x_na_{mn}=y_m \end{array}\right\} \text{(A)}$$

may be regarded as defining a linear transformation f of V_n into V_m which sends $(x_1, \cdots\cdots, x_n)$ into $(y_1, \cdots\cdots, y_m)$. Hence show that

(*a*) the solutions of the equations

$$\left.\begin{array}{l} x_1a_{11}+x_2a_{12}+\cdots\cdots+x_na_{1n}=0 \\ \cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots \\ \cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots \\ x_1a_{m1}+x_2a_{m2}+\cdots\cdots+x_na_{mn}=0 \end{array}\right\} \text{(B)}$$

form a subspace W of V_n of dimension equal to the nullity of f.

(*b*) If $b_1, b_2, \cdots\cdots, b_m$ are elements of K, not all zero, then the equations

$$\left.\begin{array}{l} x_1a_{11}+x_2a_{12}+\cdots\cdots+x_na_{1n}=b_1 \\ \cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots \\ \cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots \\ x_1a_{m1}+x_2a_{m2}+\cdots\cdots+x_na_{mn}=b_m \end{array}\right\} \text{(C)}$$

either have no solutions or else the totality of solutions form a coset of V_n modulo W.

CHAPTER VII

VECTOR SPACE OF LINEAR TRANSFORMATIONS

Linear Algebras

100. Introduction. This chapter will be devoted to an elementary discussion of the Algebraic Structure of the totality of all linear transformations from one vector space $U(K)$ into another vector space $V(K)$. It will be seen that this totality of linear transformations will have itself the structure of a vector space over the field K. In particular, we shall consider two cases which arise when

(*i*) $V(K)$ coincides with K regarded as a vector space over K,

(*ii*) $V(K)$ coincides with $U(K)$ itself.

The case (*i*) will lead us to the introduction of the important notion of **Dual Space** of a given vector space.

The case (*ii*) amounts to the consideration of the totality of endomorphisms of a vector space. It will be seen that this totality has the structure of what is known as a **Linear Algebra.** Thus we shall also define Linear Algebra and further give a number of examples of the same.

A linear transformation of $U(K)$ into $V(K)$ is a mapping

$$f : U \longrightarrow V$$

which preserves sums and products with members of K.

101. Vector Space of Linear transformations. Let $U(K)$, $V(K)$ be two vector spaces over the same field K. We shall denote by

$$L(U, V),$$

the totality of linear transformations of $U(K)$ into $V(K)$. It will be seen that it is possible to equip $L(U, V)$ with the structure of a vector space over the field K with suitable definitions of the sum of linear transformations and of the product of a linear transformation with any member of the field K.

101·1. Addition Composition in L(U, V). Let f and g be any two members of $L(U, V)$ to be briefly denoted by L.

Consider now a mapping of U into V denoted by $f+g$ and defined by

$$(f+g)(\alpha)=f\alpha)+g(\alpha)\ ;\ \alpha \in U.$$

This means that $f+g$ is defined as a mappping which maps any element α of U onto the sum, $f(\alpha)+g(\alpha)$, of the f and g images of α.

It will now be shown that $f+g$ is itself a member of L, *i.e.*, a linear transformation of U into V.

We have, when $\alpha \in U, \beta \in U, a \in K$,

$$(f+g)(\alpha+\beta) = f(\alpha+\beta)+g(\alpha+\beta), \text{ by the def. of } f+g$$
$$= [f(\alpha)+f(\beta)]+[g(\alpha)+g(\beta)]$$
$$= [f(\alpha)+g(\alpha)]+[f(\beta)+g(\beta)]$$
$$= (f+g)(\alpha)+(f+g)(\beta)$$
$$(f+g)(a\alpha) = f(a\alpha)+g(a\alpha)$$
$$= a[f(\alpha)]+a[g(\alpha)]$$
$$= a[f(\alpha)+g(\alpha)]$$
$$= a[(f+g)\alpha]$$

(The reader may supply the reason for each step).

Thus we see that $f+g$ is a linear transformation of U into V.

It can now be shown that *the set $L(U, V)$ is an Abelian group for the addition composition defined as above.*

The proof which is straight is being left to the reader. We shall only state that the mapping of $U(K)$ into $V(K)$, denoted by, 0, and defined by

$$0\alpha = 0,$$

is a linear transformation and is such that

$$f+0=f \text{ for every } f \in L(U, V).$$

Also we may state that the mapping denoted by, $-f$, and defined by

$$(-f)(\alpha) = -[f(\alpha)], \alpha \in U,$$

is a linear transformation and is such that

$$f+(-f)=0.$$

Ex. How many different meanings have been given to the symbol 0 in the discussion above.

101·2. Scalar multiplication. Let

$$\alpha \in U, a \in K, f \in L(U, V).$$

We define a mapping, denoted by af, of U into V as follows:

$$(af)(\alpha) = a[f(\alpha)].$$

Thus af is a mapping which maps any element α of U onto the product of $f(\alpha)$ by a.

We now show that af is a *L.T.*, *i.e.*, it belongs to $L(U, V)$.

We have

$$(af)(\alpha+\beta) = a[f(\alpha+\beta)]$$
$$= a[f(\alpha)+f(\beta)]$$
$$= a[f(\alpha)]+a[f(\beta)]$$
$$= af(\alpha)+af(\beta)$$
$$= (af)(\alpha)+(af)(\beta)$$
$$(af)(b\alpha) = a[f(b\alpha)]$$

$$=a\{b[f(\alpha)]\}$$
$$=(ab)f(\alpha)$$
$$=(ba)f(\alpha)$$
$$=b\{a[f(\alpha)]\}$$
$$=b[(af)(\alpha)]$$

Thus $af \in L(U, V)$.

(The reader may supply justification for each of the above steps).

101·3. Structure of $L(U, V)$ as a vector space.

To show that $L(U, V)$ is a vector space over the field K, we have only now to verify the various postulates of § 82·1 for a vector space.

In the following

$$\alpha \in U, a \in K, b \in K, f \in L, g \in L.$$

(*i*) We have

$$[(a+b)f](\alpha)=(a+b)[f(\alpha)]$$
$$=a[f(\alpha)]+b[f(\alpha)]$$
$$=(af)(\alpha)+(bf)(\alpha)$$
$$=(af+bf)(\alpha).$$

As this equality holds for each $\alpha \in U$, we have

$$(a+b)f=af+bf.$$

(*ii*) $$[a(f+g)](\alpha)=a[(f+g)\alpha]$$
$$=a[f(\alpha)+g(\alpha)]$$
$$=a[f(\alpha)]+a[g(\alpha)]$$
$$=(af)(\alpha)+(ag)(\alpha)$$
$$=(af+ag)(\alpha)$$

$$\therefore \quad a(f+g)=af+ag.$$

(*iii*) $$[(ab)f](\alpha)=(ab)f(\alpha)$$
$$=a[b(f\alpha)]=a[(bf)(\alpha)]$$
$$=[a(bf)](\alpha)$$

$$\therefore \quad (ab)f=a(bf).$$

(*iv*) $$(1f)(\alpha)=1f(\alpha)=f(\alpha)$$

$$\therefore \quad 1f=f.$$

Thus we see that the *set $L(U, V)$ of all linear transformations of a vector space $U(K)$ into another $V(K)$ is itself a vector space over K relative to the compositions defined as above.*

102. Dual space of a vector Space. Let $U(K)$ be any given vector space over a field K. *Then the vector space formed of all linear*

transformations of $U(K)$ into K regarded as a vector space over K is called the Dual of U and is denoted by U^*.

A linear transformation of $U(K)$ into K is also usually called a **Linear functional** on the space U. Thus a linear functional f on a space U is a mapping which assigns to each element $\alpha \in U(K)$ an element $f(\alpha) \in K$ and is such that

$$f(\alpha+\beta)=f(\alpha)+f(\beta),\ \alpha \in U,\ \beta \in U,$$
$$f(a\alpha)=a[f(\alpha)],\ a \in K,\ \alpha \in U.$$

Illustrations.

1. Consider the vector space $\mathbf{R}[x]$ of all polynomials over the field $\mathbf{R}$ of real numbers. Then, as may be easily verified, the mapping

$$f(x) \longrightarrow \int_0^1 f(x)\,dx\,;\ f(x) \in \mathbf{R}[x]$$

is a linear functional on $\mathbf{R}[x]$.

2. Consider the vector space $V_n(K)$ of all n-tuples over a field K. Also let

$$c_1, c_2, \ldots\ldots, c_n$$

be any given ordered set of n elements of K.

Then the mapping

$$(a_1, \ldots\ldots, a_n) \longrightarrow c_1a_1 + \ldots\ldots + c_na_n,$$

is a linear functional defined on $V_n(K)$.

Of course to different ordered sets

$$c_1, c_2, \ldots\ldots, c_n$$

there will correspond different linear functionals on $V_n(K)$.

102·1. Theorem. *The dual space V^* of a space $V(K)$ of finite dimension n is itself of dimension n.*

Let the system of vectors

$$(\alpha_1, \alpha_2, \ldots\ldots, \alpha_n) \qquad \ldots(1)$$

be a basis of $V(K)$.

We now define a set of n linear functionals

$$f_1, f_2, \ldots\ldots, f_n \qquad \ldots(2)$$

on $V(K)$.

Any element of $V(K)$ being uniquely expressible as

$$\sum_{i=1}^{n} a_i \alpha_i.$$

we define f_j by the relation

$$f_j\Big(\sum_{i=1}^{n} a_i\alpha_i\Big) = a_j,\ 1 \leqslant j \leqslant n.$$

It may be verified that f_j is a linear functional on $V(K)$ and that it is such that

$$f_j(\alpha_i) = \begin{cases} 1 \text{ if } j = i, \\ 0 \text{ if } j \neq i. \end{cases}$$

It will now be shown that the system (2) of linear functionals is a basis of V^*.

Let f be *any* linear functional on V and let

$$f(\alpha_i) = c_i, \quad 1 \leqslant i \leqslant n.$$

This equation completely defines f in as much as it follows that

$$f\Big(\sum_{i=1}^{n} a_i\alpha_i\Big) = \sum_{i=1}^{n} a_i c_i.$$

We shall show that

$$f = \sum_{i=1}^{n} c_i f_i$$

In fact, we have

$$f\Big(\sum_{i=1}^{n} a_i\alpha_j\Big) = \sum_{i=1}^{n} a_i c_i$$

and

$$\Big(\sum_{j=1}^{n} c_j f_j\Big)\Big(\sum_{i=1}^{n} a_i\alpha_i\Big) = \sum_{j=1}^{n}\sum_{i=1}^{n} a_i c_j f_j(\alpha_i)$$

$$= \sum_{i=1}^{n} a_i c_i.$$

Thus

$$f\Big(\sum_{i=1}^{n} a_i\alpha_i\Big) = \Big(\sum_{j=1}^{n} c_j f_j\Big)\Big(\sum_{i=1}^{n} a_i\alpha_i\Big)$$

so that

$$f = \sum_{j=1}^{n} c_j f_j.$$

Now to show that the system (2) is linearly independent, we consider a relation

$$\sum_{i=1}^{n} b_i f_i = 0.$$

We have, therefore

$$\sum_{i=1}^{n} b_i f_i(\alpha_j)=0, \text{ for } 1\leqslant j\leqslant n,$$

i.e.,

$$b_j=0 \text{ for } 1\leqslant j\leqslant n.$$

Thus the system (2) is also linearly independent.

Hence it follows that the system (2) is a basis of the dual space V^*.

The base consisting of the elements

$$f_1, \ldots\ldots, \ldots\ldots, f_n$$

of V^* is called the **dual** or the **transpose** of the base consisting of the elements

$$\alpha_1, \ldots\ldots, \ldots\ldots, \alpha_n$$

of V. These are such that

$$f_j(\alpha_i)=\begin{cases}1 \text{ if } i=j,\\ 0 \text{ if } i\neq j.\end{cases}$$

Ex. Show that the dual space of the space of n-tuples over a field K is isomorphic to the space of n-tuples over K.

Note. Let $\alpha \in V$ and $f \in V^*$. By the very definition of the zero linear functional, we know that if

$$f(\alpha)=0 \text{ for every } \alpha \in V,$$

then f is the zero linear functional so that we may write

$$f=0.$$

We shall now show that if

$$f(\alpha)=0 \text{ for every } f \in V^*,$$

then we must have

$$\alpha=0.$$

To prove this consider any base

$$(\alpha_1, \ldots\ldots, \alpha_n)$$

of V and the dual base

$$(f_1, \ldots\ldots, \ldots\ldots f_n)$$

of V^*. Let

$$\alpha=\sum_{i=1}^{n} a_i\alpha_i$$

be any given arbitrary element of V. We then have

$$f_j\left(\sum_{i=1}^{n} a_i \alpha_i\right)=0, \text{ for } 1\leqslant j\leqslant n$$

$$\therefore \qquad a_j=0 \text{ for } 1\leqslant j\leqslant n.$$

Thus $$\alpha=0.$$

102·2. Reflexivity of finite dimensional vector spaces. Let us now show interest in the dual V^{**} of the dual space V^* of K. By the theorem of § 102·1, it follows that if V is a space of dimension n so that V^* is also a space of dimension n, then V^{**} is as well a space of dimension n. By § 96, page 239 V and V^{**} are isomorphic spaces. We shall now exhibit a *Natural isomorphism* between V and V^{**}

Theorem. *The mapping*

$$\alpha \longrightarrow \bar{\alpha}, \qquad \alpha \in V,$$

where $\bar{\alpha}$ *is a linear functional on* V^* *defined by*

$$\bar{\alpha}(f)=f(\alpha), \qquad f \in V^*$$

is an isomorphism of V *onto* V^{**}.

Here

$$\alpha \in V \quad f \in V^*, \ \bar{\alpha} \in V^{**}$$

and

$$f(\alpha) \in K, \ \bar{\alpha}(f) \in K.$$

We may note that α is the linear functional on V^* which maps any given element f of the same exactly as α is mapped by f.

It may first be seen that α is linear. If $f_1 \in V^*$, $f_2 \in V^*$, we have

$$\begin{aligned}\bar{\alpha}\,(f_1+f_2)&=(f_1+f_2)(\alpha)\\ &=f_1(\alpha)+f_2(\alpha)=\bar{\alpha}(f_1)+\bar{\alpha}(f_2),\end{aligned}$$

and

$$\begin{aligned}\bar{\alpha}\,(cf_1)&=(af_1)(\alpha)\\ &=a(f_1(\alpha))=a(\bar{\alpha}\,(f_1))\end{aligned}$$

so that $\bar{\alpha}$ is linear.

Now to show that the mapping

$$\alpha \longrightarrow \bar{\alpha}$$

of V into V^{**} is linear.

We have for each $f \in V^*$,

$$\overline{(\alpha+\beta)}(f) = f(\alpha+\beta)$$
$$= f(\alpha)+f(\beta) = \bar{\alpha}(f)+\bar{\beta}(f)$$
$$= (\bar{\alpha}+\bar{\beta})(f)$$

$\therefore$ $$\overline{\alpha+\beta} = \bar{\alpha}+\bar{\beta}.$$

Also

$$(a\bar{\alpha})(f) = f(a\alpha)$$
$$= a(f(\alpha)) = a(\bar{\alpha}(f)).$$

Thus $\alpha \longrightarrow \bar{\alpha}$ is a linear mapping. Now to show that it is one-one i.e.,

$$\bar{\alpha} = \bar{\beta} \Longrightarrow \alpha = \beta.$$

Now for every f

$$\bar{\alpha} = \bar{\beta} \Longrightarrow \bar{\alpha}(f) = \bar{\beta}(f) \Longrightarrow f(\alpha) = f(\beta)$$
$$\Longrightarrow f(\alpha-\beta) = 0.$$

$\therefore$ By note on page 240,

$$\bar{\alpha} = \bar{\beta} \Longrightarrow \alpha-\beta = 0 \Longrightarrow \alpha = \beta.$$

Now since V and V^{**} have the same finite dimension and $\alpha \longrightarrow \bar{\alpha}$ is a linear mapping of V into V^{**} such that different elements of V are mapped differently, we deduce, that the mapping in question is an isomorphism.

Note. An element $\alpha \in V$ is also sometimes said to be *orthogonal* to $f \in V^*$ if $f(\alpha) = 0$.

103. Annihilator of a sub-space. Let W be any sub-space of a vector space $V(K)$. Then by the annihilator W' of the sub-space W of $V(K)$ is meant the totality of elements f of the dual space V^* such that

$$f(x) = 0 \qquad \text{for every } x \in W.$$

It can be shown that W' is a sub-space of V^*. Let $f_1 \in W'$, $f_2 \in W'$. We have

$$(f_1+f_2)(x) = f_1(x)+f_2(x) \qquad x \in W.$$
$$= 0+0 = 0$$
$$(af_1)(x) = a(f_1(x)) = a0 = 0, \qquad a \in K.$$

Thus W' is a sub-space of V^*

103·1. Theorem. *The annihilator of a sub-space W of dimension m of an n-dimensional space $V(K)$ is a sub-space of V^* of dimension $n-m$.*

Let

$$(\alpha_1, \ldots, \alpha_m)$$

be a basis of W and let

$$(\alpha_1 \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n)$$

be a basis of V obtained on supplementing that of W. Also let

$$(f_1, \ldots, f_m, f_{m+1}, \ldots, f_n)$$

be the dual basis of V^*.

We shall show that the annihilator W' of W is the sub-space of V^* with basis

$$(f_{m+1}, \ldots, f_n).$$

Suppose that

$$b_1 f_1 + \ldots + b_m f_m + b_{m+1} f_{m+1} + \ldots + b_n f_n$$

is any member of W'. We have then

$$(b_1 f_1 + \ldots + b_m f_m + b_{m+1} f_{m+1} + \ldots + b_n f)(\alpha_i) = 0 \quad \text{for } 1 \leqslant i \leqslant m$$

$$\therefore \qquad l_i = 0 \text{ for } 1 \leqslant i \leqslant m.$$

Thus every member of W' is of the form

$$b_{m+1} f_{m+1} + \ldots\ldots + b_n f_n.$$

Now, to show that for arbitrary values of $b_{m+1}, \ldots, b_n$, the element

$$b_{m+1} f_{m+1} + \ldots\ldots + b_n f_n$$

of V^* belongs to W', consider

$$(b_{m+1} f_{m+1} + \ldots\ldots + b_n f_n)\left(\sum_{i=1}^{m} a_i \alpha_i\right)$$

and see that the same is 0.

Thus the annihilator W' of W having as its basis a set of $(n-m)$ elements

$$f_{m+1}, \ldots\ldots, f_n$$

is an $(n-m)$ dimensional sub-space.

103·2. Theorem. *The annihilator of the sum (intersection) of two sub spaces of a finite dimensional space is the same as the intersection (sum) of the annihilators of the sub-spaces.*

Let W_1 and W_2 be two sub-spaces of a finite dimensional space $V(K)$.

Let α be any member $W_1 + W_2$ so that there exists a member

or as a row matrix

$$[a_1, a_2, \ldots\ldots, a_n].$$

We shall now show that any linear transformation f of an m-dimensional space $U(K)$ into an n-dimensional space $V(K)$ can relatively to the choice of fixed ordered bases in the two spaces be represented as an $m \times n$ matrix over the field K.

Let

$$(\alpha_1, \alpha_2, \ldots\ldots, \alpha_m)$$

and

$$(\beta_1, \beta_2, \ldots\ldots, \beta_n)$$

be the two bases of $U(K)$ and $V(K)$ respectively.

Since $\alpha_i \in U(K)$, $f(\alpha_i) \in V(K)$, we have a relation of the form

$$f(\alpha_i) = \sum_{j=1}^{n} s_{ij}\beta_{ij}, \qquad s_{ij} \in K$$

so that $f(\alpha_i)$ is expressed as a linear combination of the system of vectors $\beta_1, \beta_2, \ldots\ldots, \beta_n$. Here we see that

$$[\ s_{ij}\ ]$$

is a $m \times n$ matrix over the field K such that the n elements of the ith row of the same give the coordinates of the f-image $f(\alpha_i)$ of α_i relatively to the basis $(\beta_1, \beta_2, \ldots\ldots, \beta_n)$.

Conversely, if $[s_{ij}]$ be any $m \times n$ matrix over K, then relatively to two given bases $(\alpha_1, \ldots\ldots, \alpha_m)$, $(\beta_1, \ldots\ldots, \beta_n)$ of the two spaces $U(K)$ and $V(K)$, we have a linear transformation f defined by

$$f(\alpha_i) = \sum_{j=1}^{n} s_{ij}\beta_j.$$

We thus see that relatively to the choice of fixed bases in $U(K)$ and $V(K)$, a linear transformation f can be represented by a $m \times n$ matrix

$$[\ s_{ij}\ ],$$

over K, where m and n are the dimensions of $U(K)$ and $V(K)$ respectively.

105. Product of Linear transformations represented as Product of corresponding matrices.

Let

$$U(K),\ V(K),\ W(K)$$

be three vector spaces over the same field K with dimensions

$$m,\ n,\ p$$

respectively.

Let f, g be two linear transformations of $U(K)$ into $V(K)$ and $V(K)$ into $W(K)$ respectively.

We show that the product mapping fg is also a linear transformation of $U(K)$ into $W(K)$.

By def., $\quad (fg)(\alpha)=f[g(\alpha)], \qquad \alpha \in U.$

When $\alpha \in U, \beta \in U$, we have

$$\begin{aligned}(fg)(\alpha+\beta) &= f[g(\alpha+\beta)] \\ &= f[g(\alpha)+g(\beta)] = f[g(\alpha)]+f[g(\beta)] \\ &= (fg)(\alpha)+(fg)(\beta)\end{aligned}$$

and when $a \in K$,

$$\begin{aligned}(fg)(a\alpha) &= f[g(a\alpha)] \\ &= f[ag(\alpha)] = a[f(g(\alpha))] \\ &= a[(fg)(\alpha)].\end{aligned}$$

Thus fg is a linear transformation.

[The reader may supply reason for each of the above steps.]

Let

$$(\alpha_1, \ldots\ldots, \alpha_m), (\beta_1, \ldots\ldots, \beta_n), (\gamma_1, \ldots\ldots, \gamma_p) \qquad \ldots(1)$$

be three bases of the three spaces.

We write

$$f(\alpha_i) = \sum_{j=1}^{n} s_{ij}\beta_j,$$

$$g(\beta_j) = \sum_{k=1}^{p} t_{jk}\gamma_k$$

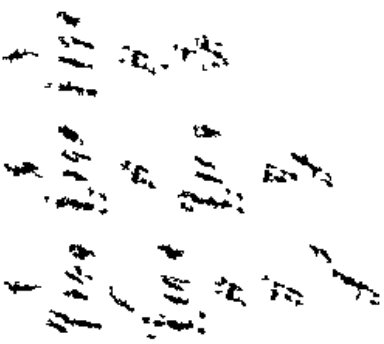
so that

$$[s_{ij}], \ [t_{jk}].$$

are the two matrices representing the two linear transformations f, g relatively to the bases in (1).

Then we have

$$\begin{aligned}(gf)(\alpha_i) &= g[(f(\alpha_i)] \\ &= g\left(\sum_{j=1}^{n} s_{ij}\beta_j\right) \\ &= \sum_{j=1}^{n} g(s_{ij}\beta_j)\end{aligned}$$



To write

[illegible]

and see that the matrix product

[illegible]

represents the product transformation

[illegible]

If we write

[illegible]

where $[a_{ik}]$ and $[b_{kl}]$ are the matrices representing the linear transformations f and g of $V_n(K)$ into $V_n(K)$ and $V_n(K)$ into $V_n(K)$ relatively to the bases

$$(\alpha_1, \ldots, \alpha_n), (\beta_1, \ldots, \beta_n)$$

and

$$(\beta_1, \ldots, \beta_n), (\gamma_1, \ldots, \gamma_n)$$

respectively, then we have

$$g' \longrightarrow [a_{ik}][b_{kl}]$$

so that the linear transformation g' of $V_n(K)$ into $V_n(K)$ is represented by the product matrix

$$[c_{il}][b_{kl}]$$

relatively to the bases

$$(\alpha_1, \ldots, \alpha_n), (\gamma_1, \ldots, \gamma_n)$$

106. Linear Algebra over a field. We shall now define what is meant by a *Linear Algebra* over a field K a very important illustration of which is provided by the set of all the linear transformations of a vector space into itself. A linear algebra is also often known as a **Hypercomplex system.**

Def. *A set E is said to be a Linear Algebra over a field K, if*

(i) there is defined in E an addition composition and also a scalar multiplication composition in E over K such that relative to these E is a vector space over K,

(ii) there is also defined in E a multiplication composition which is associative and right as well as left distribution with respect to addition referred to in (i) above and which is such that

$$a(\alpha\beta)=(a\alpha)\beta=\alpha(a\beta),$$

where $a \in K$, $\alpha \in E$, $\beta \in E$.

The reader would easily satisfy himself that if E be a Linear Algebra over a field K, then relative to the addition and multiplication compositions defined therein, it has the structure of a ring.

Alternatively a Linear Algebra over a field K may also be defined as follows :

A set E is said to be a *Linear Algebra* over a field K, if

(i) there are defined in E addition and multiplication compositions relative to which E is a ring,

(ii) there is defined in E an external composition over K, to be known as scalar multiplication such that

$$(a+b)\alpha=a\alpha+b\alpha,$$
$$a(\alpha+\beta)=a\alpha+a\beta,$$
$$(ab)\alpha=a(b\alpha),$$
$$1\alpha=\alpha.$$
$$a(\alpha\beta)=(a\alpha)\beta=\alpha(a\beta).$$

Here $a \in K$, $b \in K$, $\alpha \in E$, $\beta \in E$.

Note. What we have referred to here as Linear Algebra is also, sometimes, referred to in Literature as *Linear Associative Algebra* in view of the multiplication composition being assumed associative. No confusion would, however, arise in view of our dropping the adjective 'Associative', for we do *not* propose to consider systems with non-associative multiplication in this book.

106·1. Bases of an Algebra. Finite and infinite algebras. Let E be a Linear Algebra over a field K. Disregarding multiplication in E, we think of E as a vector space over the field K. As such, the vector space E will possess a basis which may be finite or infinite. Then the Algebra E is said to be finite or infinite over K, according as E, as a vector space over K, is finite or infinite dimensional. Also the dimension of the vector space E over K is known as the **degree** of the Linear Algebra E over K.

Let E be a finite Algebra of degree n over K and let

$$(\alpha_1, \alpha_2, \ldots\ldots, \alpha_n)$$

be a basis of the vector space E over K, to be also referred to as a **basis of the Algebra.**

Every member of E is expressible as

$$\sum_{i=1}^{n} a_i \alpha_i. \qquad a_1 \in K.$$

Consider now any two elements

$$\sum_{i=1}^{n} a_i \alpha_i, \quad \sum_{i=1}^{n} b_i \alpha_i,$$

of E. By using the various postulates for an Algebra, we have

$$\left(\sum_{i=1}^{n} a_i \alpha_i \right)\left(\sum_{j=1}^{n} b_j \alpha_j \right) = \sum_{j=1}^{n} \sum_{i=1}^{n} a_i b_j \alpha_i \alpha_j.$$

This shows that the product of any two elements of E is given if only the product in pairs of any two elements of a basis is given.

Now the product $\alpha_i \alpha_j$ like any element of E is expressible as a linear combination of the elements of the basis. Let

$$\alpha_i \alpha_j = \sum_{k=1}^{n} \gamma_{ijk} \alpha_k,$$

These n^3 elements γ_{ijk} which are members of the field K are known as the *Structure constants* of the Algebra for the basis in question.

It should however be noted that these n^3 Structure constants cannot be arbitrarily assigned and there exist relations between the same because of the associativity of multiplication.

We have

$$(\alpha_i \alpha_j)\alpha_k = \alpha_i(\alpha_j \alpha_k) \qquad \text{for } 1 \leqslant i, j, k \leqslant n.$$

Now

$$\begin{aligned} \alpha_i \alpha_j &= \Sigma_l \gamma_{ijl}\ \alpha_l, \\ (\alpha_i \alpha_j)\alpha_k &= \Sigma_l \gamma_{ijl} \alpha_l \alpha_k \\ &= \Sigma_m \Sigma_l \gamma_{ijl} \gamma_{lkm} \alpha_m \\ \alpha_j \alpha_k &= \Sigma_l \gamma_{jkl} \alpha_l, \\ \alpha_i(\alpha_j \alpha_k) &= \Sigma_l \gamma_{jkl} \alpha_i \alpha_l \\ &= \Sigma_m \Sigma_l \gamma_{jkl} \gamma_{ilm} \alpha_m \end{aligned}$$

$\therefore$ we have, by virtue of the uniqueness of expression as a linear combination of the elements of the basis,

$$\Sigma_l \gamma_{ijl} \gamma_{lkm} = \Sigma_l \gamma_{jkl} \gamma_{ilm},$$

for each system of values of i, j, k and m lying between 1 and n.

It will thus be seen that a finite algebra over a field is defined, if we are given a system of elements of the same constituting a basis and an associative multiplication table for the same.

106·2. An Algebra with a unit element. An algebra E over a field K is said to be one with unit element, if the multiplicative composition in E possesses a unit element. Let E be an algebra with a unit element which we denote by e. Consider the mapping

$$a \longrightarrow ae$$

of K *into* E. It may be shown that this mapping is actually an isomorphism. In view of this, it is usual to identify the unit element e of the algebra E with the unit element 1 of the field K and as such to identify any element ae of E with the element a of K.

It is clear that if E is an algebra with unit element; it possesses a sub-algebra isomorphic to K regarded as an algebra over itself.

106·3. Inversible elements of an Algebra with a unit element. Division Algebras. Any element of an Algebra with unit element is said to be *inversible* if it possesses a multiplicative inverse. Inversible elements are also known as *Regular* or *Non-singular*. An algebra with a unit element wherefor every non-zero element is inversible is known as a **Division Algebra.**

Note. It is not proposed to describe in details the various developments in connection with the concept of Linear Algebra. Only the basic concept is intended to be introduced here so that the reader may be able to recognise wherever he comes across a Linear Algebra. It may, however, be pointed out that taking his clue from developments in connection with Groups, Rings and Vector Spaces, the student may himself formulate the various concepts in connection with Linear Algebras such as those of

1. *Sub-Algebras.* 2. *Ideals.* 3. *Quotient Algebras.* 4. *Isomorphism of two Linear Algebras over the same field.* 5. *Homomorphic mapping of one Linear Algebra into another over the same field.* 6. *Direct Sum of two Linear Algebras.*

The reader may even be able to state and prove some of the basic theorems in respect of these concepts.

In the following, we give some illustrations of Linear Algebras.

Illustrations.

1. A field can be thought of as a linear algebra over any sub-field thereof and, in particular, over itself. The degree of a field as a linear algebra over itself is one.

2. The field **C** of complex numbers can be regarded as a linear algebra of degee 2 over the field **R** of real numbers.

3. The field **R** of real numbers can be regarded as a linear algebra of degree infinite over the field **Q** of rational numbers.

(The reader may explicitly state the three compositions in respect of which any given set is a linear algebra in the three cases above.)

4. The set $\mathbf{M}_n$ of all $n \times n$ matrices over the field **C** (**R**, **Q** or any abstract field K) is a linear algebra of degree n^2.

We define a $n \times n$ matrix E_{ij} such that each element of the same other than the (i, j)th element is 0 and the (i, j)th element is 1. These n^2 matrices E_{ij} form a basis of the linear algebra $\mathbf{M}_n$. As for the composition table for these n^2 matrices, we have

$$E_{ij}E_{kl} = \begin{cases} 0 & \text{if } j \neq k, \\ E_{il} & \text{if } j = k. \end{cases}$$

5. The set of all linear transformations of an n-dimensional vector space $U(K)$ into itself is a linear algebra of degree n^2 over the field K.

The reader may show that

$$f(g+h) = fg + fh$$
$$(f+g)h = fh + gh$$
$$a(fg) = (af)g = f(ag)$$

where f, g, h are any arbitrary linear transformations and a is any member of the ground field K.

Also the algebra of linear transformations of any n-dimensional vector space over a field K is isomorphic to the linear algebra of all the $n \times n$ matrices over K. [Refer § 105, page 255].

Ex. Show that the automorphisms of a vector space are the only invertible elements of the Linear algebra of the linear transformations of the same.

6. **Algebra of a group.** Let G be any finite group with multiplicatively denoted composition and let

$$\alpha_1, \ldots\ldots, \alpha_n$$

be the elements of the same. Also let

$$\alpha_i \alpha_j = \alpha_r,$$

so that r is uniquely determined corresponding to every ordered pair i, j where $1 \leqslant i, j, r \leqslant n$.

Consider now the set of *formal* symbols

$$a_1\alpha_1 + \ldots\ldots + a_n\alpha_n = \sum_{i=1}^{n} a_i\alpha_i ; \qquad a_i \in K.$$

Here K is any given field.

We give now various definitions in respect of these symbols ;

Equality. $\sum_{i=1}^{n} a_i \alpha_i = \sum_{i=1}^{n} b_i \alpha_i$ if and only if $a_i = b_i$ for each i.

Addition. $\sum_{i=1}^{n} a_i \alpha_i + \sum_{i=1}^{n} b_i \alpha_i = \sum_{i=1}^{n} (a_i + b_i) \alpha_i$.

Multiplication. $\left(\sum_{i=1}^{n} a_i \alpha_i \right)\left(\sum_{j=1}^{n} b_j \alpha_j \right) = \sum_{j}\sum_{i}\sum_{k} a_i b_j \gamma_{ijk} \alpha_k$.

$$\gamma_{ijk} = \begin{cases} 0 \text{ if } k \neq r \\ 1 \text{ if } k = r, \end{cases}$$

and where we agree to write $1\alpha_i = \alpha_i$; 1 being the unit element of K.

Scalar multiplication. $a\left(\sum_{i=1}^{n} a_i \alpha_i \right) = \sum_{i=1}^{n} a a_i \alpha_i \quad a \in K$.

It may now be shown that the set of elements

$$\sum_{i=1}^{n} a_i \alpha_i$$

has the structure of a Linear algebra over the field K relatively to the various definitions given above.

Its degree over K is n and it is known as the Algebra of the group G.

7. **Algebra of Quaternions over a field.** Let K be any given field. We shall now define an important linear algebra of degree four with a unit element. This linear algebra is defined as one with elements

$$1, i, j, k$$

as consisting a basis and with multiplication table as follows :

$$i^2 = -1, \; j^2 = -1, \; k^2 = -1,$$

$$ij = k, \; ji = -k \; ; \; jk = i, \; kj = -i \; ; \; ki = j, \; ik = -j.$$

Further 1 is the unit element of the algebra. It may be verified that the multiplication as defined is associative. (Refer note below).

Each element of the linear algebra thus defined is known as a *Quaternion* over the field K. Thus each quaternion over K is of the form

$$a + bi + cj + dk \; ; \; a, \; b, \; c, \; d \in K.$$

It can be shown that if the field K is such that

$$a^2 + b^2 + c^2 + d^2 = 0 \Longrightarrow a = b = c = d = 0,$$

then each non-zero quaternion is inversible.

In fact for such a field K, we have,

if

$$\alpha = a + bi + cj + dk \neq 0,$$

then

$$\alpha^{-1} = \left(\frac{a}{N} - \frac{b}{N} i - \frac{c}{N} j - \frac{d}{N} k \right),$$

where

$$N = a^2 + b^2 + c^2 + d^2.$$

Thus, in particular, we see that the algebras of quaternions over the fields of rational and real numbers are Division algebras whereas that over the field of complex numbers is not so.

Note. The fact that the multiplication table for $1, i, j, k$ is associative may also be seen as a result of the correspondence

$$1 \longrightarrow \begin{Bmatrix} 1 & 0 \\ 0 & 1 \end{Bmatrix}, \quad j \longrightarrow \begin{Bmatrix} 0 & 1 \\ -1 & 0 \end{Bmatrix},$$

$$i \longrightarrow \begin{Bmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{Bmatrix}, \quad k \longrightarrow \begin{Bmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 1 \end{Bmatrix},$$

and the fact that matrix multiplication is associative. [Refer the discussion about the Quaternion group as given on page 131].

EXERCISES

1. Consider the vector space of all polynomials of degree $\leqslant n$ over the field R of real numbers and show that differentiation is a linear transformation in the same.

Also obtain the matrix representing the same relative to the basis consisting of the polynomials $1, x, x^2, \ldots\ldots, x^n$.

2. Consider the vector space V_n (R) consisting of the n tuples

$$(x_1, \ldots\ldots x_i, \ldots\ldots, x_n).$$

and let

$$\begin{pmatrix} 1 & \ldots\ldots & i & \ldots\ldots & n \\ 1' & \ldots\ldots & i' & \ldots\ldots & n' \end{pmatrix}$$

be any given permutation of the n objects $1, \ldots\ldots i, \ldots\ldots n$. Show that the mapping

$$(x_1, \ldots\ldots, x_i, \ldots\ldots, x_n) \longrightarrow (x_1', \ldots\ldots, x_i', \ldots\ldots, x_n')$$

is a linear transformation in V_n (R) and represent the same matricially relative to the basis consisting of the vectors

$$(1, 0, \ldots\ldots, 0), (0, 1, 0, \ldots\ldots, 0), \ldots\ldots, (0, 0, \ldots\ldots, 0, 1).$$

3. An n-dimensional vector space $U(K)$ is the direct sum of its two vector sub-spaces $V(K)$, $W(K)$ so that each $\alpha \in U$ is uniquely expressible as

$$\alpha = \beta + \gamma, \qquad \beta \in V, \gamma \in W.$$

Show that the mapping f defined by

$$f(\alpha)=\beta,$$

is a linear transformation in $U(K)$. Show further that

(i) $f^2=f$. (ii) V and W are the sets of all solutions of the equations

$$f(\alpha)=\alpha, \quad f(\alpha)=0,$$

respectively.

If $(\beta_1, \ldots\ldots, \beta_l)$ is a basis of V and $(\gamma_1, \ldots\ldots, \gamma_m)$ is a basis of W, find the matrix representing the linear transformation, f relatively to the basis of U

$$(\beta_1, \ldots\ldots \beta_l, \gamma_1, \ldots\ldots, \gamma_m)$$

4. Show that the four vectors

$$(1, 2, 3, 0), (1, -1, 0, 1), (2, 0, -1, -1), (0, 1, -1, 2)$$

constitute a basis of $V_4(R)$ and find the martix relatively to this basis of the linear transformation σ in $V_4(R)$ defined by

$$\sigma(1, 0, 0, 0)=(2, -1, 1, 1); \quad \sigma(0, 1, 0, 0)=(1, 0, 1, 1)$$
$$\sigma(0, 0, 1, 0)=(1, 1, 1, 1); \quad \sigma(0, 0, 0, 1)=(1, -1, 1, -1).$$

5. E_1, E_2 are two algebras over the same field K. Show that the following definitions of the three compositions of addition, multiplication and scalar multiplication equip the product set $E_1 \times E_2$ with the structure of an algebra over K:

$$(\alpha_1, \alpha_2)+(\beta_1, \beta_2)=(\alpha_1+\beta_1, \alpha_2+\beta_2)$$
$$(\alpha_1, \alpha_2)(\beta_1, \beta_2) \quad =(\alpha_1\beta_1, \alpha_2\beta_2)$$
$$a(\alpha_1, \alpha_2)=(a\alpha_1, a\alpha_2).$$

Here $\alpha_1, \beta_1 \in E_1$, $\alpha_2, \beta_2 \in E_2$, $a \in K$.

(The algebra thus defined is known as the direct product of the two algebras E_1 and E_2).

6. Let there be given any sub-set of S of an Algebra E over a field K. Show that the sub-set of the elements of E permutable with each element of S is a sub-algebra of E.

Let f be a homomorphism of an algebra E onto an algebra F over the same field. Show that

(i) $I=f^{-1}(0)$ is a two sided ideal of the algebra E,

(ii) $f(E) \cong E/I$,

(iii) if G is a sub-algebra of E, then $f(G)$ is also a sub-algebra of F and

$$f(G) \cong G/(G \cap I).$$
$$f(G) \cong (G+I)/I.$$

7. Let f be a homomorphism of an algebra E onto an algebra F over the same field and let, γ_{ijk} be the structure constants for the algebra E so that

$$\alpha_i\alpha_j = \sum_{k=1}^{n} \gamma_{ijk}\alpha_k.$$

Show that

$$f(\alpha_i)f(\alpha_j)=\sum_{k=1}^{n} \gamma_{ijk}f(\alpha_k),$$

8. Consider the Linear algebra formed of the elements

$$\alpha u+\beta v+\gamma w, \qquad \alpha, \beta, \gamma \in \mathbf{R}$$

with the commutative associative multiplication table given by

$$u^2=u,\ v^2=-u,\ w^2=-u-v+w$$
$$uv=v,\ uw=u-v,\ vw=u+v.$$

Show that there are two idempotents of the Algebra of the form

$$\alpha u+v+w.$$

[An element a is said to be idempotent if $a^2=a$].

9. Let E be an Algebra of finite degree over a field K. Show that if an element $a \in E$ is neither a left nor a right zero divisor, then E admits a unit element and, a, is inversible.

Also deduce that E if does not contain any zero divisors, then it is a field.

10. Let K be a field with characteristic other than 2 and let E be an algebra of degree 2 over K with elements 1, u constituting a basis such that 1 is the unit element and

$$u^2=\gamma \text{ where } \gamma \in K.$$

Prove the following :

(*i*) E is a field if γ is not a square in K.

(*ii*) E is the direct product of two fields isomorphic to K if γ is a non-zero square member of K.

11. Let K be a field with characteristic $\neq 2$ and let E be an algebra of degree 4 with elements 1, i, j, k constituting a base. Also let

$$i^2=j^2=k^2=1\ ;\ ij=ji=k\ ;\ jk=kj=i\ ;\ ki=ik=j,$$

and let 1 be the unit element.

Show that E is the direct product of four fields isomorphic to K.

[Consider the base of E formed of the four elements $(1\pm i)$, $(1\pm j)$].

Also show that E is the algebra over K of the product of two cyclic groups of order 2.

12. Show that the centre of the algebra of quaternions over a field K whose characteristic $\neq 2$ is identical with K.

13. Show that the algebra of quaternions over the field of real numbers is isomorphic to the algebra of 2×2 matrices

$$\begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}; \qquad \alpha \in \mathbf{C},\ \beta \in \mathbf{C}$$

over R. Here $\bar{\alpha}$ denotes the complex conjugate of α.

CHAPTER VIII

FINITTE FIELD EXTENSIONS

Galois Theory

107. Introduction. This chapter will be devoted to a study of the Theory of Finite field extensions involving the introduction of the concepts of Algebraic extensions and of the special types of the same, *viz.*, Normal and Separable extensions. It is intended to lead to the Galois Theory of finite, normal and separable field extensions.

This study had originated with that of polynomial equations and in the following chapter will be developed the criteria for the solvability of polynomial equations by radicals as an application of Galois Theory.

The theory of finite fields as finite field extensions of prime fields of non-zero characteristic will also be taken up as an application of the theory of finite field extensions.

108. Field extensions. Let L be any given field and K any sub-field of the same.

We then say that L is an extension field or simply an extension of K. Consider any field L and the family of all its sub-fields. Let Γ denote the intersection of this family of sub-fields. Then Γ is obviously a prime field in the sense that it possesses no proper sub-field. As shown in § 69·1, page 179, a prime field is either isomorphic to the field $\mathbf{Q}$ of rational numbers or to the residue class field $\mathbf{J}_p$ for some prime p.

Thus we see that every field L can be thought of as an extension of a field Γ isomorphic to the field $\mathbf{Q}$ or $\mathbf{J}_p$ according as the characteristic of L is zero or the prime p.

109. Roots of a polynomial. Let L be any given field and let

$$f(x) = a_0 + a_1 x + \ldots\ldots + a_s x^s \in K[x],$$

and let $\alpha \in K$. Then the element

$$a_0 + a_1 \alpha + \ldots\ldots + a_s \alpha^s$$

of K is denoted by the symbol $f(\alpha)$.

It may be easily seen that if

$$f(x) \in K[x],\ \phi(x) \in K[x]$$

and if we write

$$\varphi_1(x)=f(x)+\psi(x),\ \varphi_2(x)=f(x)\ \psi(x),$$

then

$$\varphi_1(\alpha)=f(\alpha)+\psi(\alpha),\ \varphi_2(\alpha)=f(\alpha)\ \psi(\alpha).$$

If α is such that $f(\alpha)=0$, we say that α is a root of the polynomial $f(x)$ or of the polynomial equation $f(x)=0$.

Suppose that $\alpha \in K$ is a root of $f(x) \in K[x]$. Now there exist two polynomials $q(x)$ and $r(x)$ which $\in K[x]$ and are such that

$$f(x)=(x-\alpha)\ q(x)+r(x),$$

where $r(x)=0$ or $deg\ r(x)<deg\ (x-\alpha)$. Thus $r(x)$ is necessarily a member of K, say β We have thus

$$f(x)=(x-\alpha)\ q(x)+\beta,$$

so that

$$f(\alpha)=\beta.$$

We thus see that

$$f(\alpha)=0 \Longleftrightarrow (x-\alpha) \mid f(x).$$

It may thus be seen that if $f(x) \in K[x]$ has a root $\alpha \in K$, then $f(x)$ is not an irreducible member of $K[x]$ in as much as $(x-\alpha) \in K[x]$ is a factor of the same. The converse, however, is not true so that a reducible member of $K[x]$ may have no root in K. For example

$$x^4-5x^2+6 \in \mathbf{Q}[x],$$

is reducible without having any root in $\mathbf{Q}$.

Ex Show that a polynomial of the second or third degree is a reducible member of $K[x]$ if and only if the same has a root in K.

110. Polynomial equations and field extensions. The field $\mathbf{C}$ of complex numbers is known to be such that the only irreducible members of the polynomial ring $\mathbf{C}[x]$ over the same are those of degree one. In other words, every polynomial of the nth degree over the field $\mathbf{C}$ of complex numbers has n roots belonging to the field. This property is, however, not true of arbitrary fields. As an example, we may see that

$$x^3-2 \in \mathbf{Q}[x],$$

is an irreducible member of the same and has no root lying in $\mathbf{Q}$ and

$$x^2+1 \in \mathbf{R}[x],$$

is also an irreducible member of the same and has no root lying in $\mathbf{R}$.

While x^2-2 is an irreducible member of the ring $\mathbf{Q}[x]$ over the field $\mathbf{Q}$ of rational numbers, it is reducible as a member of the polynomial ring over the extension field $\mathbf{Q}(\sqrt{2})$ of $\mathbf{Q}$. Similarly while x^2+1 is an irreducible member of the ring $\mathbf{R}[x]$ over the field $\mathbf{R}$ of real numbers, it is reducible as a member of the polynomial ring over the extension field $\mathbf{R}(\sqrt{-1})=\mathbf{C}$ of complex numbers.

It has thus to be emphasised that the problem of the reducibility and irreducibility of polynomials and of the solution of polynomials equations is intrinsically related to the field in question and the answer to the problem changes on a change of the field.

To solve an equation $f(x)=0$ where $f(x) \in \mathrm{K}[x]$ amounts to constructing an extension field L of K such that $f(x)$ thought of as a member of $L[x]$ is expressible as a product of linear factors and as such has as many roots in L as is the degree of the same.

III. Finite field extensions.

An extension field L of a field can K be thought of as a* vector space over K relative to the field addition in L and the field multiplication of the elements of L with those of K as the two vector space compositions. As a vector space over K, the dimension of L my be finite or infinite. We say that L is a finite field extension of the field K or briefly that L is finite over K, if the vector space L over K is finite dimensional and this finite dimension is known as the *degree* of L over K and is denoted by the symbol

$$(L : K).$$

Illustrations. 1. The field $\mathbf{C}$ of complex numbers is a finite extension of the field $\mathbf{R}$ of real numbers and

$$(\mathbf{C} : \mathbf{R})=2.$$

2. The field $\mathbf{Q}(\sqrt{2})$ consisting of the numbers

$$a+b\sqrt{2}, \qquad a \in \mathbf{Q}, b \in \mathbf{Q}$$

if finite over $\mathbf{Q}$ and

$$(\mathbf{Q}(\sqrt{2}) : \mathbf{Q})=2.$$

3. The field $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ consisting of the numbers

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{2}\sqrt{3},$$

where $a, b, c, d \in \mathbf{Q}$, is finite over $\mathbf{Q}$ and

$$\left(\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}\right)=4.$$

4. The field $\mathbf{Q}(\pi)$ is *not* a finite field extension of $\mathbf{Q}$.

*In fact L can be thought of as a Linear Algebra over the field K.

111·1. Transitivity of finite extensions. Theorem. If K, L, M *are three fields such that*

$$K \subseteq L \subseteq M,$$

then M is a finite extension of K if and only if M is a finite extension of L and L a finite extension of K. Moreover, then,

$$(M : K) = (M : L)(L : K).$$

Let M be of finite degree over K.

Let L, being a sub-space of the finite dimensional vector space M over K, is itself finite dimensional. Further the finite set of elements constituting a basis of M over K is clearly a generating system of M over L and accordingly M is also finite dimensional over L.

Now suppose that

$$(L : K) = m, \ (M : L) = n.$$

Let

$$\alpha_i, \ 1 \leqslant i \leqslant m, \ \alpha_i \in L,$$
$$\beta_j, \ 1 \leqslant j \leqslant n, \ \beta_j \in M,$$

be the two sets of elements constituting the bases of L over K and of M over L respectively.

It will be shown that the set of mn elements

$$\alpha_i \beta_j$$

constitutes a base of M over K.

Let $\gamma \in M$. We have

$$\gamma = \sum_{j=1}^{n} b_j \beta_j, \qquad b_j \in L$$

Also, we have

$$b_j = \sum_{i=1}^{m} a_{ji} \alpha_i, \qquad a_{ji} \in K$$

Thus

$$\gamma = \sum_{j=1}^{n} \sum_{i=1}^{m} a_{ji} \alpha_i \beta_j \qquad \ldots(1)$$

so that $\gamma \in M$ is a linear combination over K of the set of mn elements $\alpha_i \beta_j$.

Thus the set of mn elements $\alpha_i \beta_j$ generates the vector space M over K.

Suppose now that

$$\sum_{j=1}^{n} \sum_{i=1}^{m} a_{ji}\, \alpha_i\, \beta_j = 0.$$

We have

$$\sum_{j=1}^{n} \sum_{i=1}^{m} a_{ji}\, \alpha_i\, \beta_j = 0 \Longrightarrow \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ji}\, \alpha_i \right) \beta_j = 0$$

$$\Longrightarrow \sum_{i=1}^{m} a_{ji}\, \alpha_i = 0 \text{ for each } j,$$

$$\Longrightarrow a_{ji} = 0 \text{ for each } i \text{ and } j.$$

Thus we see that the set of mn elements $\alpha_i\beta_j \in M$ is linearly independent over K.

Hence the set of mn elements $\alpha_i\beta_j$ constitute a basis of M over K so that

$$(M : K) = mn.$$

Hence the theorem.

112. Algebraic field extensions. Let L be any finite extensions field of degree n over K.

Let α be any arbitrary element of L. Then the $(n+1)$ elements

$$1, \alpha, \alpha^2, \ldots\ldots, \alpha^{n-1}, \alpha^n$$

of the vector space L of finite dimension n over the field K form a linearly dependent system and accordingly there exists a system of $(n+1)$ members

$$a_0, a_1, a_2, \ldots\ldots, a_{n-1}, a_n,$$

not all zero, of K such that

$$a_0 + a_1\alpha + a_2\alpha^2 + \ldots\ldots + a_{n-1}\alpha^{n-1} + a_n\alpha^n = 0.$$

This shows that, α, is a root of a non-zero polynomial equation

$$a_0 + a_1x + a_2x^2 + \ldots\ldots + a_{n-1}x^{n-1} + a_nx^n = 0,$$

over $K[x]$.

Thus we see that *if L is a finite field extension over K, each element of L is a root of some non-zero polynomial equation over $K[x]$.* This leads us to the following definition :

Algebraic field extension. Def. *An extension field L of a field K is said to be algebraic over K, if each element of L satisfies a non-zero polynomial equation over K.*

From the preceding discussion, we deduce that *every finite field extension L of K is algebraic over K.*

The converse of this result is, however, not true in as much as there exist algebraic extensions which are not finite. Also an infinite extension may not be algebraic.

Ex. 1. Show directly from definition that

$$\mathbf{Q}(\sqrt{2}),\ \mathbf{Q}(\sqrt{2}, \sqrt{3})$$

are algebraic over $\mathbf{Q}$.

Ex. 2. Show that $\mathbf{Q}(\pi)$ is an infinite non-algebraic extension of $\mathbf{Q}$.

113. Simple field extensions. A field extension L of a field K obtainable on adjunction of a *single* element to K is known as a *simple* extension of K. Thus a simple extension L of a field K is expressible as

$$L=K(\alpha),$$

where α is an element of L.

Illustrations. 1. The field $\mathbf{C}$ is a simple extension of the field $\mathbf{R}$ in as much as we have

$$\mathbf{C}=\mathbf{R}(\sqrt{-1}).$$

2. The field $K(x)$ of rational functions of an indeterminate x is a simple extension of the field K.

Ex. Show that

$$\mathbf{Q}(\sqrt{2}, \sqrt{3})=\mathbf{Q}(\sqrt{2}+\sqrt{3}),$$

and deduce that $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is a simple extension of the field $\mathbf{Q}$.

Note. The reader should carefully distinguish between finite and simple extensions in as much as a simple extension may *not* be finite. Thus, for example, the field $\mathbf{Q}(x)$ of rational functions is a simple but not a finite extension of $\mathbf{Q}$. Moreover, later on we shall obtain conditions under which a finite extension may be simple.

113·1. Structure of simple field extensions. Let $L=K(\alpha)$ be a simple field extension of K. It is proposed here to study the structure of $K(\alpha)$.

The symbol $K[\alpha]$ denotes the ring obtained on adjoining α to K. Clearly

$$K[\alpha] \subseteq K(\alpha).$$

It may be easily seen that $K[\alpha]$ consists of the elements

$$a_0+a_1\alpha+\ldots\ldots+a_n\alpha^n \qquad \ldots(1)$$

where n is a non-negative integer and $a_0, a_1, \ldots\ldots, a_n$ range over K.

The field $K(\alpha)$ is the quotient field of the integral domain consisting of the elements (1).

We proceed first to answer the following question :

'Is the representation of elements of $K[\alpha]$ by expressions of the form

$$f(\alpha)=a_0+a_1\alpha+a_2\alpha^2+\ldots\ldots+a_n\alpha^n,$$

unique ?'

Let, if possible,

$$f(\alpha)=\varphi(\alpha) \text{ where } f(x)\neq\varphi(x).$$

Then, we see that α satisfies a non-zero polynomial equation

$$\psi(x)=f(x)-\varphi(x)=0\ ;\ \psi(x)\in K[x].$$

We have thus two cases to distinguish in respect of, α, according as there exists or does not exist a non-zero polynomial $\psi(x)\in K[x]$ such that $\psi(\alpha)=0$.

In case there does *not* exist a non-zero polynomial $\in K[x]$ with α as a root, we see that

$$f(x)\longrightarrow f(\alpha),$$

is a one-one mapping $K[x]$ onto $K[\alpha]$.

Also we may see that if

$$f(x)\longrightarrow f(\alpha),\ \varphi(x)\longrightarrow\varphi(\alpha)$$

then

$$f(x)+\varphi(x)\longrightarrow f(\alpha)+\varphi(\alpha),\ f(x)\ \varphi(x)\longrightarrow f(\alpha)\ \varphi(\alpha).$$

We thus have

$$K[\alpha]\cong K[x]$$

and accordingly also

$$K(\alpha)\cong K(x).$$

Thus in this case the simple field extension $K(\alpha)$ is isomorphic to the field $K(x)$ of rational functions over K ; an isomorphism being given by $\alpha\longrightarrow x$, $a\longrightarrow a$ where $a\in K$.

Now suppose that there does exist a non-zero polynomial $\psi(x)\in K[x]$ such that

$$\psi(\alpha)=0.$$

It may be easily seen that in this case the set I of all those polynomials which $\in K[x]$ and which have α as a root is a non-zero ideal in $K[x]$.

In fact if

$$\psi_1(x)\in I,\ \psi_2(x)\in I,\ f(x)\in K[x],$$

so that

$$\psi_1(\alpha)=0,\ \psi_2(\alpha)=0,$$

we have

$$\psi_1(\alpha)-\psi_2(\alpha)=0,\ f(\alpha)\ \psi_1(\alpha)=0,$$

so that

$$\psi_1(x)-\psi_2(x)\in I,\ f(x)\ \psi_1(x)\in I.$$

As $K[x]$ is a principal ideal ring, there exists a non-zero polynomial $\varphi(x)\in K[x]$ such that

$$(\varphi(x))=I.$$

Thus the polynomials which $\in K[x]$ and which have α as a root are given by $f(x)\ \varphi(x)$; $f(x)$ being an arbitrary member of $K[x]$.

It may be seen that $\varphi(x)$ is the lowest degree polynomial which $\in K[x]$ and which has α as a root. Also $\varphi(x)$ is irreducible over $K[x]$.

In fact if

$$\varphi(x)=\varphi_1(x)\ \varphi_2(x),$$

where each of $\varphi_1(x)$, $\varphi_2(x)$ is of positive degree, we have

$$\varphi(\alpha)=0 \Longrightarrow \text{either } \varphi_1(\alpha)=0,\ \text{or } \varphi_2(\alpha)=0$$

so that α is a root of a polynomial equation over $K[x]$ with degree smaller than that of $\varphi(x)$. We thus arrive at a contradiction.

If a be any non-zero member of K, we have

$$(\varphi(x))=(a\varphi(x)),$$

so that we may suppose that $\varphi(x)$ is monic, *i.e.*, the co-efficient of the highest degree term is unity. Then $\varphi(x)$ is *uniquely* characterised as follows :

(*i*) $\varphi(x)\in K[x]$, (*ii*) $\varphi(\alpha)=0$,

(*iii*) $\varphi(x)$ *is irreducible over* $K[x]$,

(*iv*) $\varphi(x)$ *is monic.*

This polynomial $\varphi(x)$ is usually described as the *Monic minimal polynomial over K belonging* to α.

Consider now any element

$$f(\alpha)=a_0+a_1\alpha+\ldots\ldots+a_m\alpha^m\in K[\alpha].$$

There exist polynomials $q(x)$ and $r(x)$ such that

$$f(x)=\varphi(x)\ q(x)+r(x),$$

where $r(x)=0$ or $\deg r(x)<\deg \varphi(x)$.

$$\therefore \qquad f(\alpha)=r(\alpha).$$

Thus $f(\alpha)$ is expressible as $r(\alpha)$ where the degree of $r(x)$ is less than that of $\varphi(x)$. Also clearly no two elements $r_1(\alpha)$, $r_2(\alpha)$ such that

$$deg\ r_1(x) < deg\ \varphi(x),\ deg\ r_2(x) < deg\ \varphi(x)$$

can be equal. Thus we see that each element of the integral domain $K[\alpha]$ is uniquely expressible as

$$b_0 + b_1 x + \ldots\ldots + b_{n-1}\alpha^{n-1}, \qquad \ldots (2)$$

where $b_0, \ldots\ldots b_{n-1} \in K$ and n is the degree of $\varphi(x)$.

Consider now any element

$$F(\alpha)/G(\alpha) \in K(\alpha).$$

Since $G(\alpha) \neq 0$, $G(x)$ is not a multiple of the irreducible $\varphi(x)$. Thus the greatest common divisor of $G(x)$ and $\varphi(x)$ is unity.

Accordingly there exist polynomials

$$G_1(x),\ \varphi_1(x) \in K[x],$$

such that

$$G(x)\ G_1(x) + \varphi(x)\ \varphi_1(x) = 1.$$

$$\therefore \qquad G(\alpha)\ G_1(\alpha) = 1,$$

so that

$$\frac{F(\alpha)}{G(\alpha)} = F(\alpha)\ G_1(\alpha),$$

where $F(\alpha)\ G_1(\alpha)$ is a polynomial in α.

Proceeding as before, we may now express $F(\alpha)\ G_1(\alpha)$ in the form (2). This shows that each element of the field $K(\alpha)$ is as well expressible in the form (2) so that we have, in this case,

$$K(\alpha) = K[\alpha].$$

Also since each element of $K(\alpha)$ is uniquely expressible as

$$b_0 + b_1\alpha + \ldots\ldots + b_{n-1}\alpha^{n-1}$$

where $b_0, b_1, \ldots\ldots, b_{n-1} \in K$ and n is the degree of the minimal polynomial $\in K[x]$ with α as a root, we see that the n elements

$$1, \alpha, \ldots\ldots, \alpha^{n-1}$$

constitute a basis of the vector space $K(\alpha)$ over K and accordingly

$$[K(\alpha) : K] = n.$$

We have thus proved the following :

(*i*) If α is *not* a root of any non-zero polynomial $\in K[x]$, then the simple field extension $K(\alpha)$ is isomorphic to the field $K(x)$ of rational functions so that $K(\alpha)$ is an *infinite* non-algebraic extension of K. In this case α is said to be **transcendental** over K.

(*ii*) If α is a root of some non-zero polynomial $\in K[x]$, and the minimal polynomial $\varphi(x)$ belonging to α is of degree n, then the simple

field extension $K(\alpha)$ is of finite degree n over K and each element of the same is uniquely expressible as

$$b_0+b_1\alpha+\ldots+b_{n-1}\alpha^{n-1},$$

where $b_0, b_1, \ldots, b_{n-1} \in K$.

Thus $(K(\alpha) : K)=n=$degree of the minimal polynomial of α over K.

In this case α is said to be algebraic over K of degree n.

It follows that each element of a finite field extension L of degree n over K is algebraic over K ; degree of each element being $\leqslant n$. In fact the degree of each element of L is a divisor of n. If $\beta \in L$, we have

$$K \subseteq K(\beta) \subseteq L$$

so that

$$(L : K)=(L : K(\beta))\ (K(\beta) : K),$$

and accordingly $(K(\beta) : K)$ is a divisor of $(L : K)$ which is n.

Another presentation. We shall now investigate the structure of simple field extensions in a comparatively more advanced manner making use of the Homomorphism theorem for rings.

The mapping

$$f(x) \longrightarrow f(\alpha)$$

of $K[x]$ onto $K[\alpha]$ is, as may be easily seen, a homomorphism.

Let, I, denote the kernel of this homomorphism so that it is an ideal of $K[x]$ consisting of all those members of the same which have α as a root. As K is a field, $K[x]$ is a principal ideal ring and accordingly I is a principal ideal of $K[x]$.

Three cases are conceivable :

(*i*) $I=(0)$, (*ii*) $I=(1)$, (*iii*) $I\neq(0)$, $I\neq(1)$.

Case I. Let $I=(0)$. In this case, the kernel I consists of only the zero of $K[x]$ so that there is no non-zero polynomial having α as a root.

Thus the mapping $f(x) \longrightarrow f(\alpha)$ is in this case one-one so that we have

$$K[x] \cong K[\alpha].$$

From this it follows that

$$K(x) \cong K(\alpha),$$

so that the field $K(\alpha)$ is, in this case, isomorphic to the field $K(x)$ of rational functions of x over K.

Case II. Let $I=(1)$. This case is *not* possible, for this implies that the kernel consists of all the members of $K[x]$ and, in particular, the unity I of K is mapped on zero.

Case III. Let $I\neq(0)$, $I\neq(1)$. There then exists a polynomial $\varphi(x) \in K[x]$ of positive degree such that

$$I=(\varphi(x)).$$

We have

$$K[\alpha] \cong K[x]/(\varphi(x))$$

where α is mapped on $[x]$. [Refer note 2, page 159].

The polynomial $\varphi(x)$ is necessarily an irreducible member of $K[x]$, for $K[\alpha]$ is an integral domain.

Thus $(\varphi(x))$ is a maximal ideal of the principal ideal ring $K[x]$ and accordingly the residue class ring

$$K[x]/(\varphi(x))$$

is a field. Therefore, $K[\alpha]$, is in this case already a field, and we have

$$K(\alpha)=K[\alpha].$$

Thus the field $K(\alpha)$ is, in this case, isomorphic to the residue class field $K[x]/(\varphi(x))$; the ideal $(\varphi(x))$ consisting of all those polynomial members of $K[x]$ which have α as a root.

Canonical representation of the members of $K(\alpha)$. In case α is *not* algebraic over K, each element of $K(\alpha)$ *is uniquely* expressible as

$$f(\alpha)/g(\alpha)$$

where $f(x)$ and $0\neq g(x)$ are arbitrary polynomials of $K[x]$.

Consider now the case when α is algebraic over K and $(\varphi(x))$ is the ideal consisting of all those polynomials of $K[x]$ which have α as a root. Since

$$(\varphi(x))=(a\,\varphi(x)),$$

where a is any arbitrary non-zero member of K, we may regard $\varphi(x)$ as monic.

Consider any member $[f(x)]$ of $K[x]/(\varphi(x))$.

There exist two polynomials $q(x)$ and $r(x) \in K[x]$ such that

$$f(x)=\varphi(x)\,q(x)+r(x),$$

where $r(x)=0$ or $\deg r(x)<\deg \varphi(x)$.

Since

$$f(x)-r(x)=\varphi(x)q(x) \in (\varphi(x)),$$

we have

$$[f(x)]=[r(x)].$$

Thus we see that each member of $K[x]/\varphi(x)$, is representable as

$$[r(x)],$$

where $deg\ r(x)<n$; n being the degree of $\varphi(x)$. This representation is unique in as much as

$$[r_1(x)]=[r_2(x)] \Longrightarrow r_1(x)=r_2(x),$$

if $deg\ r_1(x)<n$, $deg\ r_2(x)<n$.

Thus each element of the field $K[x]/(\varphi(x))$ is representable as

$$[b_0+b_1x+.....+b_{n-1}x^{n-1}]; \qquad ...(1)$$

n being the degree of $\varphi(x)$. The member of $K(\alpha)$ corresponding to (1) in the isomorphic mapping of $K(\alpha)$ onto $K[x]/(\varphi(x))$ referred to above is

$$b_0+b_1\alpha+\quad ...+b_{n-1}\alpha^{n-1}.$$

Thus we arrive at the result in another manner.

It should be remembered that we compute with the members of $K(\alpha)$ as we do with the polynomials modulo the ideal $\varphi(x)$.

114. Existence of simple field Extensions. In the preceding section, we have investigated the structure of any arbitrary simple field extension $K(\alpha)$ of a field K on the assumptien that the same exists. We have seen that a simple field extension may be

(*i*) *transcendental* or (*ii*) *algebraic.*

We may note also that any two simple transcendental field extensions of a field K are isomorphic in as much as each is isomorphic to the field $K(x)$ of rational functions of an indeterminate x over the field K. Thus we may say that there exists *only one abstract simple transcendental extension of a given field.*

In the following, we shall make reference to the question of *existence* of the simple algebraic extensions and see as to what can said in respect of the same.

It will be shown below that every field K such that there exist irreducible members af $K[x]$ of degree greater than one admit of simple algebraic extensions.

115. Solution of algebraic equations. From an abstract point of view, the problem of solving an equation $\varphi(x)=0$ where

$$\varphi(x) \in K[x],$$

amounts to constructing an extension field L of K such that $\varphi(x)$ as a member of $L[x]$ is expressible as a product of first degree factors

which also $\in L[x]$ so that $\varphi(x)=0$ has as many roots in L as is the degree of $\varphi(x)$.

In this connection, we prove the following fundamental theorem.

Theorem. *If $\varphi(x)$ be any irreducible member of $K[x]$, then there exists an extension field L of K such that $\varphi(x)=0$ has a root in L.*

[It has been seen in § 113 that if $\varphi(x)$ is an irreducible member of $K[x]$, then the field $K(\alpha)$ obtained on adjoining a root α of $\varphi(x)=0$ to the field K is such that

$$K(\alpha) \cong K[x]/[\varphi(x)].$$

This result provides a clue for the construction of the field L as stipulated in the theorem].

We write

$$L=K[x]/(\varphi(x)),$$

and proceed to show that this L can be made into the required field.

Firstly, we see that $\varphi(x)$ being an irreducible member of the principal ideal ring $K[x]$, the residue class ring L is actually a field.

Secondly, we show that L contains a sub-field isomorphic to the field K.

Consider the mapping

$$a \longrightarrow [a],$$

of K into L.

Denoting by K' the sub-set of the elements $[a]$ of L where $a \in K$, we see that

$$a \longrightarrow [a]$$

is a mapping of K onto K'. This mapping is one-one. In fact

$$[a]=[b] \Longrightarrow a-b \in (\varphi(x))$$

and since the degree of each non-zero member of $(\varphi(x))$ is positive, we see that $a-b=0$ and accordingly $a=b$.

Thus $$[a]=[b] \Longrightarrow a=b.$$

Also we have

$$a+b \longrightarrow [a+b]=[a]+[b],$$
$$ab \longrightarrow [ab]=[a][b].$$

Thus the mapping, in question, is an isomorphism and we have

$$K \cong K'.$$

As a result of this isomorphism, we *identify* each element $[a]$ of K' with the corresponding element a of K so that we may regard K

actually as a sub-field of L, *i.e.*, the field $\mathfrak{L}$ as an extension of K.

As a second step, we show that

$$[x] \in L,$$

is a root of $\varphi(x)=0$ where we now regard $\varphi(x)$ as belonging to $L[x]$.

Let $$\varphi(x)=a_0+a_1x+\ldots\ldots+a_nx^n.$$

We have

$$\begin{aligned}\varphi([x]) &= a_0+a_1[x]+\ldots\ldots+a_n[x]^n \\ &= [a_0]+[a_1][x]+\ldots\ldots+[a_n][x]^n \\ &= [a_0+a_1x+\ldots\ldots+a_nx^n]=[\varphi(x)]=[0]=0\end{aligned}$$

so that $[x]$ is a root of $\varphi(x)=0$.

Thus we have proved the theorem as stated.

Note 1. By virtue of the result established in § 113, each element of the field $K([x])$ obtained on adjoining a root $[x]$ of

$$a_0+a_1x+\ldots\ldots+a_nx^n=0$$

to the field K is uniquely expressible as

$$b_0+b_1[x]+\ldots\ldots+b_{n-1}[x]^{n-1},$$

where

$$b_0, b_1, \ldots\ldots, b_{n-1} \in K,$$

and we manipulate with the same in respect of addition and multiplication as we do with polynomials modulo $\varphi(x)$.

Note 2. Root fields. A simple extension field of a field K containing a root of an irreducible member of $K[x]$ is called a root field of the polynomial.

Illustration. Consider

$$x^2+2x+2 \in J_3[x].$$

The three elements of J_3 may be taken as

$$0,\ 1,\ 2.$$

Since neither 0 nor 1 is a root of $x^2+2x+2=0$, we see that x^2+2x+2 *is an irreducible member of* $J_3[x]$.

Denoting a root of $x^2+2x+2=0$ by α, we see that the elements of the field $J_3(\alpha)$ are given by

$$a+b\alpha$$

where a, b range over the elements of J_3. Thus $J_3(\alpha)$ is a finite field

with 9 elements, *viz.*,

$$0,\ 1,\ 2,\ \alpha,\ 2\alpha,\ 1+\alpha,\ 1+2\alpha,\ 2+\alpha,\ 2+2\alpha.$$

It would be a good exercise for the reader to compute the inverses of the non-zero elements of the field.

Ex Show that the field **C** of complex numbers is incapable of algebraic extension.

116. Decomposition field of a polynomial. Def. *An extension field L of a field K is said to be a decomposition field of* $\varphi(x) \in K[x]$, *if* $\varphi(x) \in L[x]$ *is expressible as*

$$\varphi(x)=a(x-\alpha_1).....(x-\alpha_n),$$

where

$$a \in K,\ \alpha_1,....., \alpha_n \in L,$$

and if

$$L=K(\alpha_1....., \alpha_n).$$

116·1. Existence of a decomposition field. Theorem. *There exists a decomposition field for every* $\varphi(x) \in K[x]$.

The theorem will be proved by induction in respect of the degree of a polynomial.

Let the degree of $\varphi(x)$ be n.

The theorem is obviously true for polynomials of degree 1. Suppose that the theorem is true for polynomials of degree less than n.

Let

$$\varphi(x)=\varphi_1(x)\varphi_2(x).....\varphi_s(x),$$

where each of the polynomials on the right is an irreducible member of $K[x]$. Clearly K itself is a decomposition field of $\varphi(x)$ if each of $\varphi_1(x),....., \varphi_s(x)$ is of first degree. Suppose that at least one of them say, $\varphi_1(x)$, is of degree $\geqslant 2$. There then exists an extension field $K(\alpha_1)$ containing a root α_1 of $\varphi_1(x)=0$. Thus in the field $K(\alpha_1)$, we have a relation of the form

$$\varphi(x)=(x-\alpha_1)\psi(x),$$

where the degree of $\psi(x) \in K(\alpha_1)[x]$ is $n-1$.

By our supposition, there exists a decomposition field

$$K(\alpha_1)(\alpha_2,....., \alpha_n)=K(\alpha_1,....., \alpha_n),$$

of $\psi(x) \in K(\alpha_1)[x]$. Clearly then,

$$L=K(\alpha_1,....., \alpha_n),$$

is a decomposition field of $\varphi(x) \in K[x]$.

116·2. Uniqueness of the decomposition field. It will now be shown that the decomposition field of a polynomial is unique apart from isomorphism, *i.e.*, any two decomposition fields of a polynomial are abstractly identical.

Theorem. *Any two decomposition fields of a polynomial* $\varphi(x) \in K[x]$ *are isomorphic. Also the isomorphic mapping can be so chosen that each element of* K *is mapped on itself i.e., remains invariant and the set of roots of* $\varphi(x)$ *in one decomposition field is mapped one-one onto the set of roots of* $\varphi(x)$ *in the other.*

For the proof of this theorem, we need to introduce the notion of *Continuation of isomorphic mappings* and to prove a lemma.

Continuation of an isomorphic mapping. Def. *If*

$$K \subset L,\ K' \subset L'.$$

then an isomorphic mapping

$$g : L \longrightarrow L',$$

is said to be a continuation of the isomorphic mapping

$$f : K \longrightarrow K',$$

if

$$g(a) = f(a), \qquad \text{for each } a \in K.$$

Lemma. *If* f *is an isomorphic mapping of* K *onto* K' *and if*

$$p(x) = a_0 + a_1 x + \ldots + a_n x^n$$

is an irreducible member of $K[x]$ *so that*

$$f[p(x)] = f(a_0) + f(a_1)x + \ldots\ldots + f(a_n)x^n$$

is also an irreducible member of $K'[x]$, *then the mapping* f *can be continued to an isomorphism of the simple extension fields* L *and* L' *obtained on adjoining a root* α *of* $p(x) = 0$ *and a root* α' *of* $f[p(x)] = 0$ *to* K *and* K' *respectively such that* α *is mapped on* α'.

It may be easily seen that if $p(x)$ is an irreducible member of $K[x]$, then $f[p(x)]$ is also an irreducible member K'.

By § 113, we have

$$\tau : L = K(\alpha) \cong K[x]/[p(x)],$$
$$\tau' : L' = K'(\alpha') \cong K'[x]/[f(p(x))].$$

Also we have the isomorphic mapping

$$\eta : K[x]/[p(x)] \cong K'[x]/[f(p(x))]$$

given by

$$\eta[p(x)] = [f(p(x))].$$

Here

$$p(x) \in K[x].$$

Then, as will be shown, the mapping

$$(\tau')^{-1}\eta\tau$$

is the required continuation of f.

Firstly it is an isomorphic mapping of L onto L'. If a be any member of K, we have

$$\begin{aligned}[(\tau')^{-1}\eta\tau](a) &= [(\tau')^{-1}\eta][\tau(a)] \\ &= (\tau')^{-1}\{\eta[a]\} = (\tau')^{-1}[f(a)] = f(a)\end{aligned}$$

so that $(\tau')^{-1}\eta\tau$ is a continuation of f.

Finally, we have

$$\begin{aligned}[(\tau')^{-1}\eta\tau](\alpha) &= [(\tau')^{-1}]\eta[\tau(\alpha)] \\ &= (\tau')^{-1}\{\eta[x]\} \\ &= (\tau')^{-1}[f(x)] = \alpha'.\end{aligned}$$

Hence the lemma.

Cor. *If L_1 and L_2 are two simple extensions of a field K each containing a root of $p(x)$ which is an irreducible member of $K[x]$, then*

$$L_1 \cong L_2$$

and an isomorphism may be so chosen that each element of K is mapped on itself and one root is mapped on the other.

This follows from the preceding lemma on taking K' and K as the same field and f as the identity automorphism of K.

This corollary shows that any two root fields of the same irreducible member $\varphi(x) \in K[x]$ are isomorphic so that we may say that *apart from isomorphism there exists only one root field of an irreducible polynomial.*

It should be noted that this result holds good only for irreducible polynomials. The fields $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(-\sqrt{2})$ being the simple field extensions of $\mathbf{Q}$ each containing a root of the irreducible member x^2-2 of $\mathbf{Q}[x]$, are isomorphic. On the other hand the simple field extensions $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$ each containing a root of

$$(x^2-2)(x^2-3) \in \mathbf{Q}[x],$$

are not isomorphic.

Proof of the main theorem. Let $\phi(x) \in K[x]$ and let

$$L = K(\alpha_1, \alpha_2, \ldots\ldots, \alpha_n)$$
$$M = K(\beta_1, \beta_2, \ldots\ldots, \beta_n)$$

be two decomposition fields of the same.

Let $\varphi_1(x)$ be any irreducible factor of $\phi(x)$ in $K[x]$ of degree ≥ 2.

Note 3. Taking M the same as L in the theorem, we see that if L is a decomposition field of $\phi(x)$ over K, and if α, β are two roots of an irreducible divisor $\psi(x)$ of $\phi(x)$ over K, then the K-isomorphism of $K(\alpha)$ onto $K(\beta)$ which maps α on β can be continued to a K-automorphism of the L.

In fact we can think of M as the decomposition field of $\phi(x)$ as belonging to $K(\alpha)[x]$ as well as to $K(\beta)[x]$ and the σ of the lemma as the K-isomorphism of $K(\alpha)$ onto $K(\beta)$ which maps α on β.

117. Solution of Algebraic Equations. In the foregoing, it has been shown that *there exists a decomposition field for every given polynomial* $\phi(x) \in K[x]$ *and the same, apart from isomorphism, is unique.* From a pure algebraic point of view, the study of any given polynomial equation over a field K amounts to that of the structure of the decomposition field L of the same. In the following, when we come to the discussion of Galois theory, it will be seen that this study is intimately related to the study of intermediate fields between K and L. This algebraic study is, however, to be carefully distinguished from that we meet in Analysis. In Analysis, we have a special field $\mathbf{C}$ of complex numbers with a special role such that every number field can be thought of as a sub-field of the same and the study of polynomial equations consists in developing methods for approximating to the individual roots of the same.

118. Normal extension fields. We shall now introduce the notion of a particular type of algebraic extensions known as Normal.

Def. *An algebraic extension field L over K is said to be normal over K, if the decomposition field of the minimal polynomial $\phi(x) \in K[x]$ for each element $\alpha \in L$ is contained in L.*

This means that if L is normal over K and if $\alpha \in L$ and if $\phi(x)$ is the minimal polynomial of x over $K[x]$, then $\phi(x)$ can be expressed as a product of linear factors in $L[x]$ or in other words every polynomial $\phi(x) \in K[x]$ having one root in the field L has all its roots in L.

118·1. Structure of finite normal extensions. Theorem. *Every decomposition field extension is a normal extension.*

Let

$$L = K(\alpha_1, \ldots\ldots, \alpha_n)$$

be the decomposition field of $\psi(x) \in K[x]$; $\alpha_1, \ldots\ldots, \alpha_n$ being the roots of $\psi(x)$.

Let $\alpha \in L$ and let $\phi(x)$ be the minimal polynomial of x over $K[x]$.

Regarding $\phi(x)$ as a member of $L[x]$, we denote by M the decomposition field of the same so that we have

$$K \subset L \subseteq M.$$

Let α, β be any two roots of $\phi(x)$ in M. There exists a K-isomorphism, σ, say, of $K(\alpha)$ onto $K(\beta)$ mapping α on β.

This can be extended to an isomorphic mapping

$$K(\alpha)[x] \cong K(\beta)[x].$$

Regarding $\psi(x)$ as belonging to $K(\alpha)[x]$ and to $K(\beta)[x]$, we can continue the K-isomorphism of $K(\alpha)$ onto $K(\beta)$, to the K-isomorphism σ', say, of the decomposition fields

$$K(\alpha, \alpha_1, \ldots\ldots, \alpha_n),\ K(\beta, \alpha_1, \ldots\ldots, \alpha_n).$$

of $\psi(x)$.

In this latter isomorphism, α is mapped on β and the set $\alpha_1, \ldots\ldots, \alpha_n$ is mapped one-one onto itself. As

$$\alpha \in L \text{ and } \alpha_1, \ldots\ldots, \alpha_n \in L,$$

we see that α is a rational combination of a finite number of elements of K and of $\alpha_1, \ldots\ldots, \alpha_n$. Subjecting this relation to the isomorphism σ', we see that β is as well a rational combination of a finite number of elements of K and of $\alpha_1, \ldots\ldots, \alpha_n$. This shows that $\beta \in L$.

Hence the result.

118·2. Converse of the preceding theorem. *Every finite normal extension field is a decomposition field.*

Let

$$L = K(\beta_1, \ldots\ldots, \beta_r)$$

be a finite normal, extension of K. Each of $\beta_1, \ldots\ldots, \beta_r$ is algebraic over K. Let $\varphi_1(x), \ldots\ldots, \varphi_r(x)$ be the minimal polynomials over K belonging to $\beta_1, \ldots\ldots, \beta_r$ respectively. As L is normal over K and contains one root of each of $\varphi_1(x), \ldots\ldots, \varphi_r(x)$, we see that the decomposition field of each of these polynomials is contained in K. Thus L is the decomposition field of

$$\varphi(x) = \varphi_1(x) \ldots\ldots \varphi_r(x)$$

over K.

Note. From the preceding we see that so long as we deal with finite extension fields of a field K, the totality of normal extensions coincides with that of the decomposition fields of the polynomials over K so that the concept of finite normal extension field turns out to be equivalent to that of a decomposition field.

Theorem. *If L is a normal extension of K and M is an intermediate field so that*

$$K \subset M \subset L,$$

then L is also normal over M.

Let $\alpha \in L$ and let $\phi(x)$, $\psi(x)$ be the minimal polynomials belonging to α over the fields K and M respectively.

Now

$$\phi(x) \in K[x] \Longrightarrow \phi(x) \in M[x]$$

and $\psi(x)$ is the minimal polynomial over M satisfied by α, so that we see that

$$\psi(x) \mid \phi(x)$$

so that each root of $\psi(x)$ in L is as well a root $\phi(x)$ in L. Also each root of $\phi(x)$ belongs to L. Thus each root of $\psi(x)$ belongs to L. Thus L is normal over M. Hence the theorem.

Note. It should be seen that in the preceding case, M may not be a normal extension field of K.

Ex. 1. Show that every field extension L of degree 2 over K is necessarily normal over K.

Ex. 2. Show that $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is a decomposition field of

$$(x^2-2)(x^2-3) \in \mathbf{Q}[x]$$

and verify by considering the elements $\sqrt{2}+\sqrt{3}$, $(\sqrt{2}-\sqrt{3})$ that the same is a normal extension of $\mathbf{Q}$.

119. Separable polynomials, separable elements and separable field extensions. A slight complication arises in the course of the development of the theory of algebraic field extensions on account of the existence of what are known as *inseparable* polynomials over a field and accordingly the concepts of separable and inseparable polynomials over a field will now be introduced.

119·1. Multiple roots.

Let $\phi(x) \in K[x]$ and let L be the decomposition field of $\phi(x)$ or any extension field of K over the decomposition field L. Now, if $\alpha \in L$ is a root of $\phi(x)$, we have

$$(x-\alpha) \mid \phi(x) \text{ in } L[x].$$

It may, however, happen that a higher power of $(x-\alpha)$ than one is a factor of $\phi(x)$ in $L[x]$ Suppose that $r>1$ is a positive integer such that $(x-\alpha)^r$ but not $(x-\alpha)^{r+1}$ is a factor of $\phi(x)$. We then say that α is a multiple root of multiplicity, r, of $\phi(x)$. A non-multiple root is known as a *simple* root.

119·2. Separable and inseparable polynomials. Def. *An irreducible $\phi(x)$ over a field K is said to be separable over K, if the roots of $\phi(x)$ in its decomposition field are all simple. Also any arbitrary polynomial over K is said to be separable over K if each of its irreducible factors over K is separable. A polynomial which is not separable is known as inseparable.*

It is *not* correct to say that a polynomial over K is separable if it has only simple roots. Thus if $\psi(x)$ is irreducible and separable over K, $[\psi(x)]^3$ is also separable over K.

119·3. Characterisation of separability. To find the condition for separability or otherwise of a polynomial, we have to introduce a linear transformation in a polynomial domain which formally is the same as that of Derivation in Analysis.

Thus if

$$\phi(x)=a_0+a_1x+\ldots+a_nx^n \in K[x],$$

then, by def., we write

$$\phi'(x)=a_1+2a_2x+\ldots+na_nx^{n-1},$$

so that $\phi'(x)$ is also a member of $K[x]$. We say that $\phi'(x)$ is the derivative of $\phi(x)$. The mapping

$$\phi(x) \longrightarrow \phi'(x)$$

may be easily seen to be a linear transformation in $K[x]$. In fact, we may show that

$$f(x)=\phi(x)+\psi(x) \Longrightarrow f'(x)=\phi'(x)+\psi'(x),$$
$$g(x)=a\phi(x) \Longrightarrow g'(x)=a\phi'(x), \qquad a \in K.$$

Further, if

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

we may show that

$$h'(x)=\phi'(x)\,\psi'(x)+\psi(x)\,\psi'(x).$$

Since the product of $\phi(x)$ with $\psi(x)$ is a linear combination of powers of x, we need only prove the result for products of two powers of x. Thus consider

$$\phi'x)=x^r,\ \psi(x)=x^s,$$

so that

$$h(x)=x^{r+s}$$
$$\therefore \quad h'(x)=(r+s)x^{r+s-1}$$
$$=(rx^{r-1})x^s+(sx^{s-1})\,x^r$$
$$=\phi'(x)\,\psi(x)+\psi'(x)\,\phi(x).$$

This proves the result,

119·4. Condition for multiple roots. Theorem. *If α is a multiple root of $\phi(x)$, then it is also a root of $\phi'(x)$. Conversely, if α is a simple root of $\phi(x)$, then $\phi'(\alpha)\neq 0$.*

Let, α, be a multiple root of $\phi(x)$. Then we have a relation

$$\phi(x)=(x-\alpha)^r\,\psi(x),$$

where $\psi(x) \in K(\alpha)[x]$ and $r>1$.

$$\therefore \qquad \phi'(x)=r(x-\alpha)^{r-1}\,\psi(x)+(x-\alpha)^r\,\psi(x),$$

so that

$$\phi'(\alpha)=0.$$

Now suppose that α is a simple root of $\phi(x)$, so that we have

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

where $\psi(x) \in K(\alpha)[x]$ and $\psi(\alpha)\neq 0$.

$$\therefore \qquad \phi'(x)=\psi(x)+(x-\alpha)\,\psi'(x),$$

so that

$$\phi'(\alpha)=\psi'(\alpha)\neq 0.$$

Hence the result.

119·5. Condition for separability. Theorem. *Let $\phi(x)$ be irreducible over K. Then*

(i) if the characteristic of K is zero, $\phi(x)$ is separable over K;

(ii) if the characteristic of K is $p\neq 0$, $\phi(x)$ is separable over K except when it is expressible as $\psi(x^p)$.

Let $\qquad \phi(x)=a_0+a_1x+a_2x^2+\ldots\ldots+a_nx^n,\ a_n\neq 0.$

$$\therefore \qquad \phi'(x)= \quad a_1+2a_2x+\ldots\ldots+na_nx^{n-1}.$$

Let α be a multiple root of $\phi(x) \in K[x]$ so that α is also a root of $\phi'(x) \in K[x]$. As $\phi(x)$ is the minimal polynomial belonging to α, $\phi'(x)$ is necessarily a product of $\phi(x)$ with some member of $K[x]$. Since, however, the degree of $\phi'(x)$ is smaller than that of $\phi(x)$, we must have

$$\phi'(x)=0.$$

Thus we have

$$a_1=0,\ 2a_2=0,\ldots\ldots,\ na_n=0. \qquad \ldots(1)$$

For a field K of characteristic zero, this can only happen, if

$$a_1=0,\ a_2=0,\ldots\ldots,\ a_n=0$$

i.e., if the degree of $\phi(x)$ is non-positive.

Thus no irreducible polynomial over a field of characteristic zero can have multiple roots and accordingly *every polynomial over a field of characteristic zero is separable.*

Suppose now that the characteristic of K is p. From (1), we deduce that

$$a_k=0 \text{ if } k \text{ is not a multiple of } p$$

so that $\phi(x)$ is of the form

$$a_0+a_1x^p+a_2x^{2p}+\ldots\ldots$$

i.e., it is a polynomial in x^p.

It may very-well happen that $\phi(x)$ is a polynomial in x^{p^2} For the sake of generality, we suppose that $\phi(x)$ is a polynomial in $x^{(p^e)}$ but not in $x^{(p^{e+1})}$ Let

$$\phi(x)=\psi(x^{p^e})=\psi(y), \text{ say, where we write } y=x^{p^e}$$

We cannot have $\psi'(y)=0$ for if it were so, we would have

$$\psi(y)=\chi(y^p)=\chi(x^{p^{e+1}}),$$

which would be a contradiction of the hypothesis.

Thus $\psi(y) \in K[y]$ would have only simple roots in an extension field of K. Suppose that M is the decomposition field of $\psi(y)$ over K.

Let

$$\psi(y)=(y-\beta_1)\ldots\ldots(y-\beta_t)$$

where $\beta_1,\ldots\ldots,\beta_t$ are all *distinct* members of M.

$$\therefore \qquad \phi(x)=(x^{p^e}-\beta_1)\ldots\ldots(x^{p^e}-\beta_t).$$

In the decomposition field L of $\phi(x)$, there will exist roots $\alpha_1,\ldots\ldots\alpha_t$ of

$$x^{p^e}-\beta_1,\ldots\ldots, \quad x^{p^e}-\beta_t$$

respectively. We have

$$\alpha_1^{p^e}=\beta_1,\ldots\ldots, \quad \alpha_t^{p^e}=\beta_t.$$

$$x^{p^e}-\beta_1=x^{p^e}-\alpha_1^{p^e}=(x-\alpha_1)^{p^e}, \text{ etc.}$$

$$\therefore \qquad \phi(x)=(x-\alpha_1)^{p^e}\ldots\ldots(x-\alpha_t)^{p^e}$$

This shows that $\phi(x)=0$ has only t distinct roots and each root has multiplicity p^e. Thus

$$n = lp^e ;$$

n being the degree of $\phi(x)$.

The natural number e is known as the exponent of $\phi(x)$.

We have thus proved the following :

For a field K of characteristic $p>0$, an irreducible $\phi(x)$ over K has multiple roots if and only if it is a polynomial in x^p. Also if $\phi(x)$ is a polynomial in x^p, each root is of the same degree of multiplicity p^e ; e being some natural number. This e is such that $\phi(x)$ is a polynomial in x^{p^e} and not in $x^{p^{e+1}}$

119·6. Separable elements. Def. *An element α algebraic over K is said to be separable over K, if the minimal polynomial over K belonging to α is separable.*

119·7. Separable extensions. Def. *An algebraic extension L of K is said to be separable if each element of L is separable over K.*

In case an element or a field extension is not separable, we say that the same is *inseparable.*

It follows from the preceding that *every algebraic extension of a field of characteristic zero is necessarily separable over the same* so that inseparable extensions can occur only for fields of non-zero characteristic.

Thus in respect of number fields, the concept of inseparability becomes trivial.

Theorem. *If $K \subset M \subset L$ and L is a separable extension of K, then L is a separable extension of M and M is a separable extension of K.*

The proof which is very simple is left to the reader.

119·8. Characterisation of Separable elements. We have already in § 119·5 above, obtained a characterisation of separable polynomials over a field and shall here obtain that of separable elements over a field.

Theorem. *If α is separable over K, then the field $K(\alpha)$ has precisely $[K(\alpha) : K]$ distinct K-isomorphic images in the decomposition field L of the minimal polynomial $\phi(x)$ over K belonging to α and conversely.*

Let n be the degree of $\phi(x)$ so that, by § 113,

$$[K(\alpha) : K] = n.$$

Let, α, be separable over K so that the n roots say,

$$\alpha = \alpha_1, \alpha_2, \ldots\ldots, \alpha_n$$

of $\phi(x) = 0$ are all distinct.

By cor. to § 116·2, page 281 the field $K(\alpha)=K(\alpha_1)$ is K-isomorphic to each of the n fields

$$K(\alpha_1),\ldots\ldots, K(\alpha_n),$$

the isomorphisms being determined by

$$\alpha \longrightarrow \alpha_1,\ \alpha \longrightarrow \alpha_2,\ldots\ldots,\ \alpha \longrightarrow \alpha_n.$$

Thus these K-isomorphisms are all distinct.

Now suppose that some field $K_1 \subset L$ is K-isomorphic to $K(\alpha)$ and as a result α mapped on some $\alpha' \in L$. We then have

$$0=\phi(\alpha) \longrightarrow \phi(\alpha')=0$$

so that α' is itself a root of $\phi(x)$ in L and as such it coincides with some one of $\alpha_1, \alpha_2,\ldots\ldots, \alpha_n$.

Thus we have the first part of the theorem.

Conversely suppose that n distinct sub-fields

$$K_1,\ldots\ldots, K_n$$

are just the sub-fields of L which are K-isomorphic to $K(\alpha)$ and let, as a result, α be mapped on

$$\alpha_1, \alpha_2,\ldots\ldots, \alpha_n$$

Then $\alpha_1,\ldots\ldots, \alpha_n$ are the n distinct roots of $\phi(x)=0$. The degree of $\phi(x)$ being n, we deduce that the same is separable over K.

Thus we have proved the complete theorem.

Note 1. It is useful to note that if $M \supset L$, then the number of distinct K-isomorphic images of $K(\alpha)$ in M is the same as that in L.

Note 2. From the above, we deduce that α will be inseparable over K; if and only if the number of distinct K-isomorphic images of $K(\alpha)$ in L falls short of the degree of α over K which, by def., is the same as the degree of $K(\alpha)$ over K.

119·9. Separable extensions generated by separable elements. Theorem. *If α is separable over K, then so is $K(\alpha)$ separable over K.*

We have to show that every element β of $K(\alpha)$ is separable over K.

Let L be the decomposition field of the minimal $\phi(x)$ over K belonging to α.

Since L is normal over K and $\beta \in L$, it contains the decomposition field of the minimal polynomial for β, say $\psi(x)$, over K. We have

$$K \subset K(\beta) \subset K(\alpha) \subset L.$$

Let $K(\beta)$ have in all b distinct K-isomorphic images in L and let β be thus mapped on

$$\beta=\beta_1, \beta_2,\ldots\ldots, \beta_b$$

which are b distinct elements of L.

Also let $K(\alpha)$ have in all a distinct $K(\beta)$—isomorphic images in L and let α be thus mapped on

$$\alpha=\alpha_1, \alpha_2,\ldots\ldots, \alpha_a$$

which are a distinct elements of L.

Then the mappings

$$\beta \longrightarrow \beta_i, \ \alpha \longrightarrow \alpha_j, \qquad 1\leqslant i\leqslant b\ ;\ 1\leqslant j\leqslant a$$

determine ab distinct K-isomorphic images of $K(\alpha)$ in L. Also clearly every K-isomorphic images of $K(\alpha)$ in L is thus describable.

As α is separable over K, we have, by § 119·8,

$$[K(\alpha) : K]=ab.$$

Also

$$a\leqslant[K(\alpha) : K(\beta)],\ b\leqslant[K(\beta) : K].$$

Since

$$[K(\alpha) : K(\beta)]\ [K(\beta) : K]=[K(\alpha) : K]=ab,$$

we deduce that, we must have

$$[K(\alpha) : K(\beta)]=a,\ [K(\beta) : K]=b.$$

Thus β is separable over K and hence $K(\alpha)$ is a separable extension of K.

Cor. *The decomposition field of a separable polynomial* $\phi(x) \in K[x]$ *is a separable extension of the field* K.

120. Simplicity of finite separable extensions. Theorem of the primitive element.

Theorem. *Let* α, β *be separable over* K. *Then* $K(\alpha, \beta)$ *is a simple extension of* K.

We shall, in the following, assume that K is a field with an infinite number of elements. The case of a field with a finite number of elements will be taken up a little later in this chapter when we come to the consideration of finite fields.

Let $\phi(x)$, $\psi(x)$, be the minimal polynomials for α and β respectively over K and let L be the decomposition field of the polynomial

$$\phi(x)\psi(x).$$

We suppose that

$$\deg \phi(x)=m,\ \deg \psi(x)=n.$$

Let

$$\alpha=\alpha_1, \alpha_2, \ldots\ldots, \alpha_i, \ldots\ldots, \alpha_m$$

$$\beta=\beta_1, \beta_2, \ldots\ldots, \beta_j, \ldots\ldots, \beta_n$$

be the roots of $\phi(x)$ and $\psi(x)$ in L. These roots are all distinct as α and β are given to be separable over K.

Consider now the $m(n-1)$ linear equations

$$\alpha_i+x\beta_j=\alpha_1+x\beta_1,\ 1\leqslant i\leqslant m,\ 2\leqslant j\leqslant n$$

over L. For each i and each $j\neq 1$, this equation has a single root in L so that we obtain $m(n-1)$ elements of L, being the roots of these $m(n-1)$ equations. Some of these elements may belong to K. As K is assumed to contain an infinite of elements, there exists an element $c \in K$ different from those referred to here. We write

$$\theta=\alpha_1+c\beta_1=\alpha+c\beta$$

and see that

$$K(\theta) \subseteq K(\alpha, \beta).$$

Consider

$$\psi(x) \in K(\theta)[x],\ \phi(\theta-cx) \in K(\theta)[x].$$

It may be easily seen that the only root common to

$$\psi(x)=0,\ \phi(\theta-cx)=0$$

is β so that $x-\beta$ is the greatest common divisor of $\psi(x)$ and $\phi(\theta-cx)$. Since

$$\psi(x) \in K(\theta)[x],\ \phi(\theta-cx) \in K(\theta)[x],$$

we see that

$$x-\beta \in K(\theta)[x].$$

Thus

$$\beta \in K(\theta).$$

Thus also

$$\alpha=\theta-c\beta \in K(\theta).$$

$$\therefore \quad K(\alpha, \beta) \subseteq K(\theta).$$

Thus

$$K(\alpha, \beta)=K(\theta).$$

Cor. *Every finite separable extension is simple.* This follows from the preceding as a result of a finite number of successive applications.

As L is a finite normal extension of K, it is the decomposition field of some $\varphi(x)$ over K.

Let $\psi(x)$ be the minimal polynomial over K belonging to α. As L is normal over K and one root α of $\psi(x)$ belongs to K, each root of $\psi(x)$ belongs to L.

Then L is the decomposition field of

$$\varphi(x)\ \psi(x) \in K[x].$$

Let, if possible, the degree of $\psi(x)$ be $\geqslant 2$. As L is separable over K, the roots of $\psi(x)$ are all distinct.

There exists, therefore, an element $\beta \neq \alpha$ of L which is a root of $\psi(x)$. The elements α, β of L are both roots of the same irreducible polynomial $\psi(x)$ over K.

By cor. to § 116·2, page 282, there exists a K-isomorphism of $K(\alpha)$ onto $K(\beta)$ mapping α on β and the same can be continued to a K-automorphism of L. There exists, therefore, a member of the Galois group $G(K/L)$ which maps α on $\beta \neq \alpha$ so that we arrive at a contradiction. Thus the minimal polynomial $\psi(x)$ over K belonging to α is of the first degree and accordingly $\alpha \in K$.

Hence the theorem.

Note. The condition of the field L being a normal and separable extension of K is not only sufficient but also necessary in order to ensure that a member of L which remains invariant for each K-automorphism of L be necessarily a member of K. Sufficiency part has already been shown to be true and we shall now attend to the necessity part.

Let now L be any finite extension of K and let G be the group of *all* the K-automorphisms of L and let further any member of L which remains invariant for each member of G be necessarily a member of K.

We shall show that under this condition L is a separable and normal extension of K.

Let α be any *arbitrary* member of L and let

$$\alpha, f_2(\alpha), \ldots\ldots, f_h(\alpha)$$

be all the different members of L obtained as images of α by the members $f_1, f_2, \ldots\ldots, f_h$ of G. We write

$$\varphi(x) = (x-\alpha)(x-f_2(\alpha))\ldots\ldots(x-f_h(\alpha)).$$

Since each element of G simply permutes the set of elements

$$\alpha, f_2(\alpha), \ldots\ldots, f_h(\alpha),$$

we see that each coefficient of $\varphi(x)$ is kept invariant by each membe of G and is, thus a member of K. Thus $\varphi(x) \in K[x]$.

Let $\psi(x)$ be the minimal polynomial over K for α.

Since α is also a root of $\varphi(x)$ over K, we have

$$\psi(x) \mid \varphi(x).$$

Since $\alpha, f_2(\alpha), \ldots\ldots, f_n(\alpha)$ are also roots of $\psi(x)$, we have

$$\varphi(x) \mid \psi(x).$$

$$\varphi(x) = \psi(x).$$

Thus the roots of the minimal polynomial $\psi(x)$ for α are all distinct and members of L. Hence L is a separable and normal extension of K.

Theorem II. *The order of the Galois group $G(L/K)$ is equal to the degree of L over K.*

As L is a finite separable extension of K, it is as well a simple extension of K. There exists thus an element $\theta \in L$, such that

$$L = K(\theta).$$

The degree of the minimal polynomial, say $\varphi(x)$, over K belonging to θ is equal to the degree of L over K. Let

$$(L : K) = n.$$

As L is separable over K, the roots of $\varphi(x) = 0$ are all simple Let

$$\theta = \theta_1, \ \theta_2, \ldots\ldots, \theta_n$$

be the n roots of $\varphi(x) = 0$; which are all distinct and members of L.

Each K-automorphism of L is determined by its effect on the generator θ of the same.

Also any K-automorphism of L can map θ which is a root of $\varphi(x)$ only on another root of the same *i.e.*, one one of

$$\theta = \theta_1, \ \theta_2, \ldots\ldots, \theta_n.$$

Further we know that the K-mapping which maps θ_1 on θ_i actually determines a K-isomorphism of

$$L = K(\theta_1) \text{ on } K(\theta_i) = L,$$

i e., a K-automorphism of L. Denoting this K-automorphism of L by f_i, we see that

$$f_1, \ldots\ldots, f_i, \ldots\ldots, f_n$$

are just the n K-automorphism of L. Thus the order of $G(L/K)$ is equal to the degree n of L over K.

12. **Fundamental theorem of Galois Theory.** The fundamental theorem of Galois Theory aims to establish a one-one correspondence between the set of intermediate fields between K and L when L is a finite, separable and normal extension of K and the sub-groups of the Galois group of L over K.

If M is any intermediate field so that

$$K \subseteq M \subseteq L$$

then it is known that L is a finite, separable and normal extension of M so that there exists what we have called the Galois group of L over M. Since every K-automorphism of L is as well a K-automorphism of L, we see that

$$G_{L,M} \subseteq G_{L,K}.$$

Thus to each intermediate field M between K and L, there corresponds a sub-group $G_{L,M}$ of $G_{L,K}$. We shall find it convenient to refer to this as the Galois correspondence or mapping and shall show that this Galois mapping is one-one and onto. The result is formulated in the form of a theorem as follows

THEOREM. Fundamental Theorem of Galois Theory. *Let L be a finite, separable and normal extension of K. Then the mapping defined by*

$$M \longrightarrow G_{L,M},$$

is a one-one mapping of the set of intermediate fields M between K and L onto the set of sub-groups of the Galois group $G_{L,K}$ of L over K.

To each intermediate field M between K and L corresponds the sub-group of $G(L,K)$ formed of those K-automorphisms of L which are as well M-automorphisms of L.

We now start with any sub-group H of the Galois-group $G(L/K)$. Let the set of all those elements of L which remain invariant by each member of H be denoted by M. We show that M is a sub-field of L such that H is the Galois group of L over M.

Let

$$\alpha \in M, \beta \in M$$

so that

$$f(\alpha) = \alpha, f(\beta) = \beta \text{ for each } f \in H.$$

Then

$$f(\alpha \pm \beta) = f(\alpha) \pm f(\beta) = \alpha \pm \beta,$$
$$f(\alpha\beta) = f(\alpha) f(\beta) = \alpha\beta$$
$$f(\alpha\beta^{-1}) = f(\alpha) f(\beta^{-1}) = f(\alpha) [f(\beta)]^{-1} = \alpha\beta^{-1}, \beta \neq 0.$$

Thus M is a sub-field of L.

Since each member of H is an M-automorphism of L, we have

$$H \subseteq G(L/M). \tag{1}$$

Let

$$L=K(\theta),$$

and let

$$f_1, f_2, \ldots\ldots, f_h$$

be the members of the given sub-group H.

Consider the polynomial

$$\phi(x)=[x-f_1(\theta)][x-f_2(\theta)]\ldots\ldots[x-f_h(\theta)]: \tag{2}$$

Each co-efficient of this polynomial is such that the same remains invariant by each member of H and as such belongs to M

Thus the polynomial $\phi(x) \in M[x]$ and a root $\theta=\theta_1$ of the same lies in L. The degree of the element θ of L over M, being also the same as

$$[M(\theta) : M]=(L : M)$$

is therefore $\leqslant h$ which is the order of the sub-group H.

By theorem II, therefore the order of $G(L/M)$, being equal to the degree of L over M is $\leqslant$ the order h of H.

Thus we deduce that

$$H=G(L/M).$$

This shows that the mapping in question is onto.

Further it shows that the sub-field M is uniquely determined by any given sub-group H, so that two different sub-fields cannot correspond to the same sub-group. Thus the mapping is also one-one.

Hence the theorem.

Note. Galois correspondents. If L be any given finite, normal and separable extension of K, then the sub-group $H=G(L/M)$ of $G(L/K)$ which corresponds to any intermediate field M in the Galois correspondence may be referred to as the Galois correspondent of M.

Note. Since the number of sub-groups of a group of finite order is finite, it follows from the preceding theorem, that the number of intermediate fields between K and L, as defined above, is finite.

Further this sub-group H is such that any two elements belonging to the same right coset of H in G map α alike and conversely.

Thus if

$$G=H \cup f_2(H) \cup \ldots\ldots \cup f_i(H)$$

is the right coset decomposition of G relatively to H, then the class of elements conjugate over K to α consists of the elements

$$\alpha, f_2(\alpha), \ldots\ldots, f_i(\alpha)$$

(*ii*) *Two elements are conjugate over K if and only if the minimal polynomials belonging to them are the same*, i.e., are the roots of the same irreducible polynomial over K.

If β is conjugate to α, there exists a K-automorphism of L which maps β on α. From this it follows that α is as well a root of the irreducible polynomial over K satisfied by β.

If α, β are roots of the same irreducible polynomial over K, then there exists a K-isomorphism of $K(\alpha)$ on $K(\beta)$ mapping α on β and the same can be continued to an automorphism of L.

Hence the result.

123·2. Conjugate sub-fields. Def. *An intermediate field M is said to be conjugate over K to another intermediate field N, if there exists an $f \in G$ such that*

$$M=f(N) \qquad K \subseteq M, N \subseteq L.$$

It may be shown that the relationship of conjugacy over K in the set of all intermediate fields is an equivalence relation. It will now be shown that *two intermediate fields are conjugate over K if and only if their Galois correspondents are conjugate sub-groups of G.*

Suppose that M, is any intermediate field and the sub-group H is the Galois correspondent of M.

Let f denote any given element of G and g any arbitrary element of H.

Let α be an element of L. We have then

$$(fgf^{-1})(\alpha)=\alpha \longleftrightarrow g[f^{-1}(\alpha)]=f^{-1}(\alpha)$$
$$\longleftrightarrow f^{-1}(\alpha) \in M \longleftrightarrow \alpha \in f(M)$$

This shows that the sub-group fHf^{-1} is the Galois correspondent of the intermediate field $f(M)$ and *conversely*.

This proves the result as stated.

From this it further follows that *an intermediate field M is a normal extension of K if and only if the Galois correspondent $G(L/M)$ of M is a normal sub group of $G(L/K)$.*

Suppose now that an intermediate field M is a normal extension of K. We have

$$K \subseteq M \subseteq L.$$

Let G denote the Galois group of L over K and H that of L over M.

Each K-automorphism f of L induces a K-automorphism, say, f', of M defined by

$$f'(\alpha)=f(\alpha), \qquad \alpha \in M$$

so that f is a continuation of f'.

Thus to each member of $G(L/K)$ corresponds a member of $G(M/K)$, *viz.*, the one induced. This correspondence, $f \longrightarrow f'$, is a homomorphism of $G(L/K)$ on $G(M/K)$ and the kernel of the same is the sub-group H of $G(L/K)$ which is the Galois group of L over M.

Then by the Homomorphism Theorem for groups, we see that

$$G(M/K) \cong G/H = G(L/K)/G(L/M).$$

Thus we have proved the following important theorem.

Theorem. *An intermediate field M, $K \subseteq M \subseteq L$, is a normal extension of K if and only if the Galois group H of L over M is a normal sub-group of the Galois group of L over K and in that case the Galois group of M over K is isomorphic to the quotient group G/H.*

Thus we have proved that if

$$K \subseteq M \subseteq L,$$

then

M is a normal extension of $K \Longleftrightarrow G(L/M)$ is a normal sub group of $G(L/K)$

and

$$G(M/K) \cong G/H.$$

124. Golois group of a separable polynomial.

Let $\phi(x)$ be a separable polynomial over a field K and let L be the decomposition field of the same. As seen in § 116·2, L is unique to within isomorphism and as seen in § 118·1 and cor. to § 119·9, it is a finite, normal and separable extension of K. Then the Galois field of L over K is known as the Galois field of the polynomial $\phi(x)$ over K. It will be seen in the following Chapter that the Galois field of a polynomial plays a very important role in respect of a type of problems which arise in connection with equations $\phi(x)=0$.

124·1. Galois group of a polynomial represented is a group of permutations of its roots. Let

$$L=K(\alpha_1, \ldots\ldots, \alpha_n)$$

be the decomposition field of a separable polynomial $\phi(x)$ of degree n over K ; $\alpha_1, \ldots\ldots, \alpha_n$ being the roots of $\phi(x)$. We suppose that $\phi(x)$ has no multiple roots. Each element of L is obtainable as the result of a finite number of operations of addition, subtraction, multiplication and division performed on the elements of K and on $\alpha_1, \ldots\ldots, \alpha_n$.

Each K-automorphism of L maps a root of $\phi(x)$ on a root of the same and different roots are mapped differently and accordingly, we see that each K-automorphism of L determines a permutation of the roots and is itself determined by it. Thus there exists a group of permutations of the roots of $\phi(x)$ isomorphic to the Galois group of the same.

Ex. *Find the Galois group of the equation*

$$x^3-2=0,$$

over the field of rational numbers.

The roots of the given equation in the field of complex numbers are

$$\sqrt[3]{2},\ \sqrt[3]{2}\omega,\ \sqrt[3]{2}\omega^2,$$

where $\sqrt[3]{2}$ denotes the real and positive cube root of 2 and ω denotes the primitive cube root of unity. Then

$$\mathbf{Q}(\sqrt[3]{2}, \omega)$$

denotes the decomposition field of the given equation.

Since the minimal polynomial over $\mathbf{Q}$ belonging to $\sqrt[3]{2}$ is $x^3-2=0$ which is of the third degree, we see that elements of the field $\mathbf{Q}(\sqrt[3]{2})$ are numbers of the form

$$a+b\alpha+c\alpha^2$$

where $a, b, c \in \mathbf{Q}$ and $\alpha=\sqrt[3]{2}$.

Again since the minimal polynomial over $\mathbf{Q}(\sqrt[3]{2})$ belonging to ω is $x^2+x+1=0$ which is of the second degree, we see that the elements of the field

$$\mathbf{Q}(\sqrt[3]{2})(\omega)=\mathbf{Q}(\sqrt[3]{2}, \omega)$$

are of the form

$$a+b\alpha+c\alpha^2+(d+e\alpha+f\alpha^2)\omega$$

i.e.

[illegible]

where

[illegible]

Thus we see that

[illegible]

so that the Galois group of the polynomial $x^3-2=0$ over the field C of rational numbers is of order 6.

We proceed now to determine the structure of this Galois group of order 6. (Refer also § 128).

Since $\alpha=\sqrt[3]{2}$ is a root of the irreducible cubic $x^3-2=0$ over C whose other roots are $\alpha\omega$, $\alpha\omega^2$, we see that there exist automorphisms of the Galois group which map α on α, $\alpha\omega$, $\alpha\omega^2$ respectively.

(Refer § 127.2)

Again since ω is a root of the irreducible quadratic $x^2+x+1=0$ over $\mathbf{Q}$ with roots ω, ω^2, we see that there exist automorphisms of the Galois group which map ω on ω and ω^2 respectively.

(Refer § 126.2)

Thus we have the following 6 different possibilities in respect of the images of the generators α, ω of the decomposition field :

$\alpha\longrightarrow$	α	$\alpha\omega$	$\alpha\omega^2$	α	$\alpha\omega$	$\alpha\omega^2$
$\omega\longrightarrow$	ω	ω	ω	ω^2	ω^2	ω^2

Since α, ω are two generators of $\mathbf{Q}(\alpha, \omega)$, every $\mathbf{Q}$-automorphism of the same is determined as soon as the images of α, ω are known.

Also further since the Galois group is necessarily of order 6, we see that the members of the same are as determined by the scheme given above in respect of the images α, ω. Rewriting the same thing in another form, we may say that the Galois group of $x^3-2=0$ over $\mathbf{Q}$ consists of $\mathbf{Q}$-automorphisms determined by the following :

$(\alpha, \omega) \longrightarrow (\alpha, \omega)$; $(\alpha, \omega) \longrightarrow (\alpha\omega, \omega)$, $(\alpha, \omega) \longrightarrow (\alpha\omega^2, \omega)$

$(\alpha, \omega) \longrightarrow (\alpha, \omega^2)$; $(\alpha, \omega) \longrightarrow (\alpha\omega, \omega^2)$, $(\alpha, \omega) \longrightarrow (\alpha\omega^2, \omega^2)$.

We proceed now to determine the permutation group of the roots isomorphic to the Galois group. We write

$$\beta=\sqrt[3]{2}\omega=\alpha\omega,\ \gamma=\sqrt[3]{2}\omega^2=\alpha\omega^2$$

so that α, β, γ denote the 3 roots. We may easily see that the six permutations of α, β, γ as determined by the six automorphisms referred to above are as follows :

$$\begin{pmatrix}\alpha & \beta & \gamma\\ \alpha & \beta & \gamma\end{pmatrix}, \begin{pmatrix}\alpha & \beta & \gamma\\ \beta & \gamma & \alpha\end{pmatrix}, \begin{pmatrix}\alpha & \beta & \gamma\\ \gamma & \alpha & \beta\end{pmatrix}$$

$$\begin{pmatrix}\alpha & \beta & \gamma\\ \alpha & \gamma & \beta\end{pmatrix}, \begin{pmatrix}\alpha & \beta & \gamma\\ \beta & \alpha & \gamma\end{pmatrix}, \begin{pmatrix}\alpha & \beta & \gamma\\ \gamma & \beta & \alpha\end{pmatrix}$$

or in cycle notation,

$$I, (\alpha\beta\gamma), (\alpha\gamma\beta), (\beta\gamma), (\alpha\beta), (\alpha\gamma).$$

Thus we see that *Galois group of* $x^3-2=0$ *over the field* $\mathbf{Q}$ *of rational numbers is isomorphic to the symmetric group* $\mathbf{P}_3$ *of degree 3.*

This also follows from § 124 and the fact that the order of the Galois group in question is 6.

Let us now examine the sub-field sub-group correspondence as enunciated in the Fundamental theorem of Galois Theorem. The following are the possible sub-groups of $\mathbf{P}_3$.

$$G_1 : I$$
$$G_{21} : I, (\alpha\beta)\ ;\ G_{22} : I, (\beta\gamma)\ ;\ G_{23} : I, (\gamma\alpha)$$
$$G_3 : I, (\alpha\beta\gamma), (\alpha\gamma\beta)$$
$$G_6 : I, (\alpha\beta), (\beta\gamma), (\gamma\alpha), (\alpha\beta\gamma), (\alpha\gamma\beta).$$

We shall now determine the intermediate sub-fields corresponding to these sub-groups.

We have

$$G_1 \longrightarrow \mathbf{Q}(\alpha, \omega).$$

The permutation $(\alpha\beta)$ is determined by the following :

$$(\alpha, \omega) \longrightarrow (\alpha\omega, \omega^2)$$

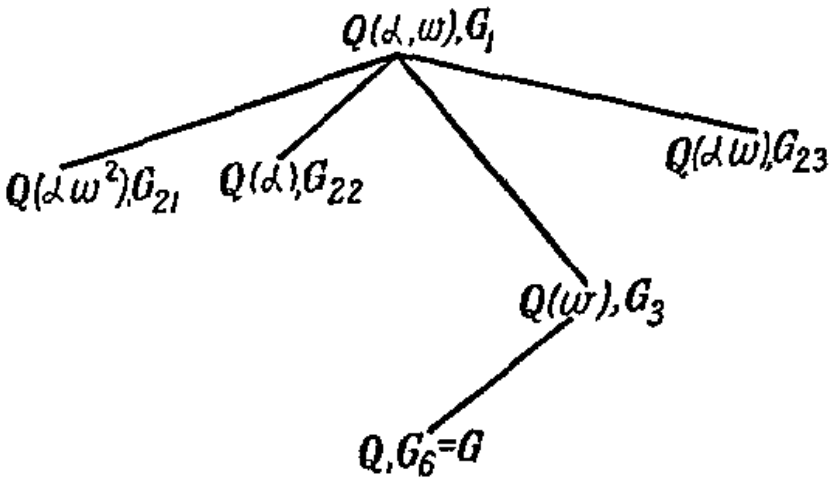
so that we need a sub-field of $\mathbf{Q}(\sigma, \omega)$ each element of which is mapped on itself, *i.e.*, remains fixed by this automorphism and by this only. By inspection, we may see that it is the sub-field $\mathbf{Q}(\alpha\omega^2)$. As a verification, we may see that

$$[\mathbf{Q}(\alpha, \omega) : \mathbf{Q}(\alpha\omega^2)]=2,$$

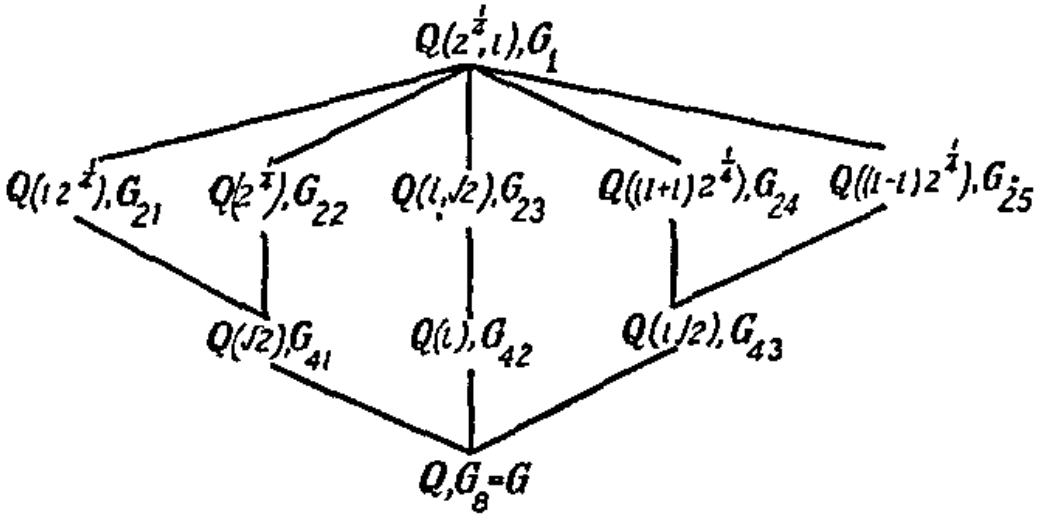
and the corresponding Galois group is also of order 2. Thus we may see that

$$G_{21} \longrightarrow \mathbf{Q}(\alpha\omega^2)\ ;\ G_{22} \longrightarrow \mathbf{Q}(\alpha)\ ;\ G_{23} \longrightarrow \mathbf{Q}(\sigma\omega)$$
$$G_3 \longrightarrow \mathbf{Q}(\omega)$$
$$G_4 \longrightarrow \mathbf{Q}(\alpha\omega).$$

This relationship may be diagrammatically exhibited as on the next page.



Ex. Show that the Galois group **G** of $x^4-2=0$ over **Q** is of order 8 isomorphic to the Dihedral group D_8 of order 8 show that the sub-field, sub-group Galois correspondence of the Fundamental theorem of the Galois theory is diagrammatically given as follows :



Determine the sub-groups G_{41}, G_{42}, G_{43}, ; $G_{21}, G_{22}, G_{23}, G_{24}, G_{25}$ of G.

125. Finite Fields. The remaining part of this chapter will be devoted to the investigation of the structure of fields with a finite number of elements to be also known as finite fields. Naturally the questions of existence and uniqueness will also be taken up. The reader is advised, however, to distinguish between finite fields and finite extension fields.

We have already come across finite fields J_p which are prime.

Finite fields are also known as Galois fields after the name of their discoverer.

Assuming existence, we shall start with a preliminary discussion of the properties which a finite field must possess. These properties will then lead us to the solution of the problems of existence and uniqueness in respect of finite fields.

126. Preliminaries.

Theorem I. *The characteristic of a finite field is necessarily non-zero.* This is a consequence of the fact that a field of characteristic zero already possesses a sub-field with an infinite number of elements, *viz.*, the prime sub-field isomorphic to the field of rational numbers.

Note. It may, however, be remembered that the converse of this theorem is not true, *i.e.*, a field with a non-zero characteristic may have an infinite number of elements, as for example, the field $\mathbf{J}_p(x)$ of rational functions in an indeterminte x over $\mathbf{J}_p$ has an infinite number of elements.

Theorem II. *The number of elements in a finite field of characteristic p is of the form p^n; n being some positive integer.*

Let L be a finite field of characteristic p and let K be the prime field in L. Then K contains, p, elements and L is a finite extension of K. Let

$$(L : K) = n$$

Let the n elements

$$\alpha_1, \alpha_2, \ldots\ldots, \alpha_n$$

constitute a basis of L over K. Then each element of L is uniquely expressible as

$$a_1\alpha_1 + \ldots\ldots + a_i\alpha_i + \ldots\ldots + a_n\alpha_n,$$

where $a_i \in K$. As each a_i is capable of assuming precisely, p, values, we duduce that the total number of elements in L is p^n.

Note. It may be remembered that if L is a finite field with p^n elements, then p, denotes the characteristic of L and n denotes the degree of the same over its prime sub-field.

Theorem III. *Each element of a finite field L with p^n elements satisfies the equation*

$$x^{p^n} = x.$$

The non-zero elements of L form a multiplicative group with, $p^n - 1$, elements so that for each such element x of L, we have

$$x^{p^n - 1} = 1.$$

Since

$$x^{p^n} - x = x\left(x^{p^n - 1} - 1\right),$$

we deduce that each element of L, zero or non-zero, satifies

$$x^{p^n} - x = 0 \text{ or } x^{p^n} = x.$$

127. Existence and uniqueness.

Theorem I. *For every prime integer p and every positive integer n, there* **exists** *a finite field with p^n elements.*

Let K denote the prime field of characteristic p. Consider

$$\phi(x)=x^q-x \in K\,[x], \text{ where } q=p^n,$$

and let L denote the decomposition field over K of x^q-x. It will be shown that L is a field with p^n elements.

Since

$$\phi'(x)=qx^{q-1}-1=-1,$$

we deduce by § 119·4, page 288, that the q roots of $\phi(x)=0$ are all distinct. Thus L contains atleast q elements, *viz.*, the q roots of $\phi(x)=0$. It will, however, be seen that the set of these q roots has a field structure so that L consists of just these q elements.

Let α, β be two roots of $\phi(x)=0$ so that

$$\alpha^q=\alpha,\ \beta^q=\beta.$$

We have

$$(\alpha\pm\beta)^q=\alpha^q\pm\beta^q=\alpha\pm\beta,$$

$$(\alpha\beta)^q=\alpha^q\beta^q=\alpha\beta,$$

$$(\alpha-\beta)^q=\alpha^q\div\beta^q=\alpha\div\beta. \qquad \beta\neq 0.$$

Thus we see that if α, β are two roots of the equation $\phi(x)=0$, then $\alpha\pm\beta$, $\alpha\beta$, $\alpha\div\beta$ are also the roots of the same ; β being assumed non-zero for the case of division. Thus L consists entirely of the q roots of $x^q-x=0$ and accordingly it is a field with $q=p^n$ elements.

Theorem II. *For each prime integer p and each positive integer n, a field with p^n elements is* **unique**, *apart from isomorphism.*

This follows from the following :

(*i*) A field with $q=p^n$ elements is a decomposition field of x^q-x over a prime field of characteristic p and consists, in fact, of the q roots of the same.

(*ii*) Any two decomposition fields of a polynomial are isomorphic.

(*iii*) Any two prime fields of characteristic p are isomorphic.

Note 1. It follows from above that there exists one and only one finite field with $q=p^n$ elements and the same consists of the q roots of $x^q-x \in J_p\,[x]$. Further, we may see that if $\alpha_1, \alpha_2, \ldots\ldots, \alpha_q$ denote the q elements of the field, we have

$$x^q-x=\prod_{i=1}^{q}(x-\alpha_i).$$

Note 2. The Galois field with p^n elements is often denoted by the symbol

$$GF(p^n).$$

128. Structure of the multiplicative group of a finite field. Theorem. *The multiplicative group of a finite field is cyclic.*

Let L denote a finite field with $q=p^n$ elements and let L^* denote the set of its, $q-1$, non-zero elements so that L^* is a multiplicative group of finite order $q-1$.

We write

$$h=q-1=\prod_{i=1}^{r} p_i^{m_i},$$

where $p_1, p_2, \ldots\ldots$ are all distinct prime integers each different from p.

There exists an element $\alpha_i \in L$ *not* satisfying

$$x^{h/p_i}=1,$$

for this equation has only, h/p_i, roots.

We write

$$\beta_i=\alpha_i^{h/p_i^{m_i}}$$

Now

$$\beta_i^{\left(p_i^{m_i}\right)}=\alpha_i^{h}=1,$$

$$\beta_i^{\left(p_i^{m_i-1}\right)}=\alpha_i^{(h/p_i)}\neq 1.$$

These show that the order of $\beta_i \in L^*$ is $p_i^{m_i}$. Thus we obtain a set of r elements

$$\beta_1, \beta_2, \ldots\ldots, \beta_r$$

of L^* with relatively prime orders

$$p_1^{m_1}, p_2^{m_2}, \ldots\ldots, p_r^{m_r}$$

$$\therefore \qquad \beta=\prod_{i=1}^{r} \beta_i$$

is an element of L^* with order

$$\prod_{i=1}^{r} p_i^{m_i}=h.$$

The order of L^* being h, we see that the same is a cyclic group with β as a generator.

Thus the $q-1$ elements of L^* can be denoted as

$$\beta, \beta^2, \ldots\ldots, \beta^{q-1}$$

so that we can write

$$GF(q) = \mathbf{J}_p(\beta),$$

and see that the *Galois field with $q=p^n$ elements is a simple extension of the prime field with characteristic p.*

Note. It follows from this that any finite extension L of a finite field K is a simple extension of K. In fact if β denote a generator of the multiplicative cyclic group of the non-zero elements of L, we have

$$L = K(\beta).$$

This completes the proof of the result as stated in § 120, page 292.

129. Construction of Galois fields. We shall now see how we may construct $GF(p^n)$. In this connection, we have the following theorem.

Theorem. *For each positive integer n, there exists an irreducible $f(x)$ of degree n over $\mathbf{J}_p$.*

We have seen that there exists $\beta \in GF(p^n)$ such that

$$GF(p^n) = \mathbf{J}_p(\beta).$$

Let $f(x)$ be the minimal polynomial for β over $\mathbf{J}_p$. Then we have

$$n = [\mathbf{J}_p(\beta) : \mathbf{J}_p] = \deg f(x),$$

so that the degree of $f(x)$ is n. Thus the irreducible polynomial $f(x)$ is of degree n over $\mathbf{J}_p$. Hence the theorem.

By § 113·1, page 271, we see that

$$GF(p^n) = \mathbf{J}_p(\beta) \cong \mathbf{J}_p[x]/[f(x)].$$

Thus to construct $GF(p^n)$, we need to determine an irreducible polynomial $f(x)$ of degree n over the field $\mathbf{J}_p$ so that

$$\mathbf{J}_p[x]/[f(x)]$$

is the required Galois field with p^n elements.

Ex. In the preceding theorem, show that

$$\beta, \beta^p, \beta^{p^2}, \ldots\ldots, \beta^{p^{n-1}}$$

are the n roots of $f(x)=0$ by showing that

$$[f(x)]^p = f(x^p).$$

130. Sub-fields of GF (p^n). We shall now examine the nature of the sub-fields of $GF(p^n)$. In this connection, we have the following result :

Theorem. *The number of elements in any sub field of $GF(p^n)$ is p^m where m is a divisor of n. Also to every divisor m of n, there corresponds one and only one sub-field with p^m elements.*

We shall prove it in two ways.

First method. Let M be any sub-field of GF (p so that we have

$$\mathbf{J}_p \subseteq M \subseteq GF(p^n).$$

By § 111·1, page 269,

$$n=[GF(p^n) : \mathbf{J}_p]=[GF(p^n) : M](M : \mathbf{J}_p)$$

so that

$$(M : \mathbf{J}_p) \mid n$$

Thus the degree of M over $\mathbf{J}_p$, say m, is a divisor of n and accordingly M contains p^m elements.

Now suppose that m is some divisor of n.

We have if $m \mid n$,

$$p^n-1=(p^m-1)(p^{n-m}+p^{n-2m}+\ldots\ldots+p^m+1)$$

so that

$$(p^m-1) \mid (p^n-1).$$

Also, therefore,

$$(p^{p^m-1}-1) \mid (x^{p^n-1}-1), \text{ in } \mathbf{J}_p[x].$$

[It may be seen that we have

$$x^{ab}-1=(x^a-1)[1+x^a+\ldots\ldots+x^{a(b-1)}].$$

Thus each root of

$$x^{p^m-1}=1,$$

is as well a root of

$$x^{p^n-1}=1,$$

so that $GF(p^n)$ contains the p^m roots of

$$x^{p^m}=x,$$

which constitute a field with p^m elements.

Second method. We shall now arrive at the same result by employing the Fundamental theorem of Galois Theory.

$GF(p^n)$ is a separable and normal extension of finite degree n over $\mathbf{J}_p$ so that the Galois group of $GF(p^n)$ over $\mathbf{J}_p$ is of order n.

We have, as shown in § 128,

$$GF(p^n)=\mathbf{J}_p(\beta).$$

Then, it may be seen, that

$$\beta \longrightarrow \beta^p,$$

is a $\mathbf{J}_p$-automorphism of $GF(p^n)$. Denoting this by f, we may see that

$$f:\beta \longrightarrow \beta^p\ ;\ f^2:\beta \longrightarrow \beta^{p^2}\ ;\ f^3:\ \beta \longrightarrow \beta^{p^3}\ ;.....$$

$$f^{n-1}:\beta \longrightarrow\ \beta^{p^{n-1}}\ ;\ f^n=I$$

are the n distinct $\mathbf{J}_p$-automorphism of $GF(p^n)$.

Then the n automorphisms are easily seen to be

$$I, f, f^2, ...f^{n-1}\ ;$$

I denoting the identity. Thus we see that *the Galois group of* $GF(p^n)$ *over* $\mathbf{J}_p$ *is cyclic and of order* n.

We have seen in § 27·3, page 72, that a cyclic group of order n possesses one and only one sub-group of index m, where m is any given divisor of n and each sub-group is cyclic. Thus by the Fundamental Theorem of Galois theory, it follows that to each divisor m of n, there corresponds one and only one sub-field of $GF(p^n)$ of degree m over $\mathbf{J}_p$, *i.e.*, a sub-field with p^m elements.

EXERCISES

1. Show that a finite integral domain is necessarily a field.
2. Show that identity is the only automorphism of a prime field.
3. Show that

$$a+bi \longrightarrow a-bi,\ a \in \mathbf{R},\ b \in \mathbf{R},$$

is a automorphism of the field $\mathbf{C}$ of complex numbers.

4. Show that the set of all automorphisms of a field is a group for the resultant composition. Also find the group of automorphisms of the following fields of numbers ; $\mathbf{Q}$ denoting the field of rational numbers ;

(*i*) the set of numbers $a+\sqrt{2}b$, $a \in \mathbf{Q}$, $b \in \mathbf{Q}$;

(*ii*) the set of numbers

$$a+\sqrt{2}b+\sqrt{3}c+\sqrt{2}\sqrt{3}d\ ;\ a, b, c\ d \in \mathbf{Q}.$$

5. Show that the group of automorphisms of the field consisting of the numbers

14. K is a commutative field and K^* is an extension of K. Prove

(i) that the elements of K^* which are algebraic over K form a field K';

(ii) that any element of K^* which is algebraic over K' is in K';

(iii) that if K^* is an extension of K of finite degree and if K is of characteristic zero, then K^* is a simple algebraic extension of K.

15. Show that x^2-x-1 is irreducible in $J_3[x]$. If $\lambda^2-\lambda-1=0$, show that $\lambda^r (r=1,\ldots,8)$ are the distinct non-zero elements of $J_3(\lambda)$.

16. Find a system of 3×3 matrices with elements in a field of order 3 which is isomorphic with the field of order 27.

17. $E=F(x)$ is the field of rational functions of an indeterminate x with coefficients in F. L is a sub-field of E containing F and differing from F. Prove that E is a finite extension of L and L is a simple transcendental extension of F.

18. Prove that if p is an odd prime number, the Galois field $GF(p^n)$ contains atleast one element that is not a square in $GF(p^n)$.

The letters a, b denote arbitrary elements of the prime field $GF(p)$ and d is a fixed element, not a square of $GF(p)$. Show that the matrices of the form

$$\begin{bmatrix} a & b \\ bd & a \end{bmatrix}$$

form a Galois field under the usual matrix operations.

Deduce or otherwise prove, that

$$\begin{bmatrix} a & b \\ db & a \end{bmatrix}^p = \begin{bmatrix} a & -b \\ -db & a \end{bmatrix}.$$

19. Let K be a field and $\phi(x)$ a polynomial over K. When is $\phi(x)$ is said to be irreducible over K ?

Is the polynomial

$$x^5+2x^3+4x-18,$$

irreducible over the field of rational numbers ? State reasons.

20. Write down all those quadratic polynomials over J_3 which are irreducible over J_3 (where J_3 is the field of three elements).

Show that the field generated by a root of any of these polynomials is always isomorphic with the Galois field $GF(3^2)$ consisting of nine elements.

Show that the transformation

$$\alpha \longrightarrow \alpha^3$$

is an automorphism in the field $GF(3^2)$.

21. Let L be an algebraic extension of F such that every polynomial in $F[x]$ splits completely into linear factors in $L[x]$. Prove that every polynomial $\phi(x)$ in $L[x]$ also splits completely into linear factors in $L[x]$.

[Let K be the field generated over F by the co-efficients of $\phi[x]$; let α be a root of $\phi(x)$ in a suitable extension of L. Considering the field $K(\alpha)$, show that α is a root of an irreducible polynomial in $F[x]$ of finite degree.]

$$a+b\sqrt[4]{2}+c\sqrt{2}+(d+e\sqrt[4]{2}+f\sqrt{2})\sqrt{-1}$$

is isomorphic to the Dihedral group $\mathbf{D}_8$; where $a, b, c, d, e, f \in \mathbf{Q}$.

6. Show that the group of automorphisms of the field consisting of the numbers

$$a+b\sqrt[3]{2}+c\sqrt[3]{4}+\sqrt{(-3)}\,(d+e\sqrt[3]{2}+f\sqrt[3]{4})\,;\ a, b, c, d, e, f \in \mathbf{Q}$$

is isomorphic to the symmetric group $\mathbf{P}_3$ of degree 3.

7. Identify the groups of automorphisms of the following fields of numbers

$$a+b\sqrt{2}+(c+d\sqrt{2})\sqrt{-1}\,,\ a, b, c, d \in \mathbf{Q}.$$

$$a+b\sqrt{5}+c\sqrt{7}+d\sqrt{5}\sqrt{7}\,;\ a, b, c, d \in \mathbf{Q}.$$

8. What are the degrees of the following fields over the field $\mathbf{Q}$ of all the rational numbers ; $a^{\frac{1}{n}}$ denoting the real nth root of the rational number a,

(*i*) $\mathbf{Q}(2^{\frac{1}{2}}, 5^{\frac{1}{2}})$, (*ii*) $\mathbf{Q}(2^{\frac{1}{3}}, 3^{\frac{1}{2}})$,

(*iii*) $\mathbf{Q}(2^{\frac{1}{4}}, 3^{\frac{1}{4}}, 5^{\frac{1}{5}})$, (*iv*) $\mathbf{Q}(6^{\frac{1}{2}}, 7^{\frac{1}{4}})$,

(*v*) $\mathbf{Q}(2^{\frac{1}{3}}, \sqrt{-1})$ (*vi*) $\mathbf{Q}(2^{\frac{1}{4}}, \sqrt{-1})$,

(*vii*) $\mathbf{Q}(2^{\frac{1}{3}}, \sqrt{-1})$.

Also give a basis over $\mathbf{Q}$ for each of these fields.

9. Show that $\mathbf{Q}(x)$ is an algebraic extension of $\mathbf{Q}(x^2)$; x being transcendental over $\mathbf{Q}$.

10. Find the permutation groups of roots isomorphic to the Galois groups over the field $\mathbf{Q}$ of the following equations :

(*i*) $x^3+1=0$. (*ii*) $x^3-9=0$.

(*iii*) $x^4-5x^2+6=0$. (*iv*) $x^4-3=0$.

(*v*) $x^4+x^2-6=0$. (*vi*) $x^4+4x^2+2=0$.

(*vii*) $x^4-10x^2+4=0$.

Exhibit also the sub-field, sub-group correspondence as formulated in the Fundamental theorem of Galois theory for these.

11. Prove that every finite extension of the field $\mathbf{R}$ of real numbers is either $\mathbf{R}$ itself or isomorphic to the field $\mathbf{C}$ of complex numbers.

12. If L is an extension of K of prime degree, prove that any element in L but not in K generates L over K.

13. A field E is an extension of a field F. Prove that the following two assertions are equivalent :

(*a*) There is a polynomial with coefficients in F, which is separable with respect to F and has E as its splitting field.

(*b*) There is a finite group of automorphisms of E which has F as its exact fixed field.

Assuming that these relations hold between E and F, prove that the group of all automorphisms of E over F is the only group of automorphisms of E which has F as its exact fixed field and show that the order of this group is equal to the degree of E over F

14. K is a commutative field and K^* is an extension of K. Prove

(*i*) that the elements of K^* which are algebraic over K form a field K';

(*ii*) that any element of K^* which is algebraic over K' is in K';

(*iii*) that if K^* is an extension of K of finite degree and if K is of characteristic zero, then K^* is a simple algebraic extension of K.

15. Show that x^2-x-1 is irreducible in $J_3[x]$. If $\lambda^2-\lambda-1=0$, show that $\lambda^r (r=1, \ldots, 8)$ are the distinct non-zero elements of $J_3(\lambda)$.

16. Find a system of 3×3 matrices with elements in a field of order 3 which is isomorphic with the field of order 27.

17. $E=F(x)$ is the field of rational functions of an indeterminate x with coefficients in F. L is a sub-field of E containing F and differing from F. Prove that E is a finite extension of L and L is a simple transcendental extension of F.

18. Prove that if p is an odd prime number, the Galois field $GF(p^n)$ contains atleast one element that is not a square in $GF(p^n)$

The letters a, b denote arbitrary elements of the prime field $GF(p)$ and d is a fixed element, not a square of $GF(p)$. Show that the matrices of the form

$$\begin{bmatrix} a & b \\ bd & a \end{bmatrix}$$

form a Galois field under the usual matrix operations.

Deduce or otherwise prove, that

$$\begin{bmatrix} a & b \\ db & a \end{bmatrix}^p = \begin{bmatrix} a & -b \\ -db & a \end{bmatrix}.$$

19. Let K be a field and $\phi(x)$ a polynomial over K. When is $\phi(x)$ is said to be irreducible over K ?

Is the polynomial

$$x^5+2x^3+4x-18,$$

irreducible over the field of rational numbers ? State reasons.

20. Write down all those quadratic polynomials over J_3 which are irreducible over J_3 (where J_3 is the field of three elements).

Show that the field generated by a root of any of these polynomials is always isomorphic with the Galois field $GF(3^2)$ consisting of nine elements.

Show that the transformation

$$\alpha \longrightarrow \alpha^3$$

is an automorphism in the field $GF(3^2)$.

21. Let L be an algebraic extension of F such that every polynomial in $F[x]$ splits completely into linear factors in $L[x]$. Prove that every polynomial $\phi(x)$ in $L[x]$ also splits completely into linear factors in $L[x]$

[Let K be the field generated over F by the co-efficients of $\phi[x]$; let α be a root of $\phi(x)$ in a suitable extension of L. Considering the field $K(\alpha)$, show that α is a root of an irreducible polynomial in $F[x]$ of finite degree.]

This shows that a pure extension obtained by adjoining a radical with any arbitrary exponent can as well be reached as a result of a finite series of pure extensions such that each member of the same is obtained on adjoining to its predecessor a radical with a prime exponent. In the following, we shall refer to solvability by radicals in this sense.

Note 1. It will be seen from above that equations of the type $x^n-a=0$ will play a fundamental role in respect of the contents of this chapter and such equations constitute building stones for the construction of the roots of an equation solvable by radicals.

Let

$$\alpha_1, \alpha_2, \ldots\ldots, \alpha_n$$

be the n roots of $x^n - a=0$, of course lying in the decomposition field of the same.

We suppose that they are all distinct. Then, none of these can be zero. As may be easily seen,

$$\frac{\alpha_1}{\alpha_1}, \frac{\alpha_1}{\alpha_2}, \ldots\ldots, \frac{\alpha_1}{\alpha_n}$$

are n distinct roots of

$$x^n=1,$$

and they lie in the decomposition field of $x^n-a=0$. This shows that the decomposition field of $x^n=1$ can be regarded as an intermediate field between K and the composition field of $x^n-a=0$. This remark points out the necessity for the study of equations of the type $x^n=1$.

Roots of $x^n=1$ are known as the nth roots of unity.

If we regard $x^n=1$ as belonging to the field of rational numbers and roots thereof as complex numbers and obtain points on a plane representing these complex numbers, then the n resulting points divide the circumference of the circle with centre at the origin and unit as radius into n equal parts. Accordingly the equation $x^n-1=0$ came to be known as cyclotomic in the classical theory.

Note 2. The theory in the present chapter will be developed only in respect of fields with characteristic zero and the corresponding results for fields of non-zero characteristic may only sometimes be given as exercises or in the form of notes.

132. Roots of unity. Cyclotomic equations and cyclotomic fields. Consider

$$x^n-1 \in K[x].$$

Def. *The decomposition field of* $x^n-1 \in K[x]$ *is known as the Cyclotomic field for* n *over* K or simply the cyclotomic field if no confusion may arise.

Illustrations. $\mathbf{Q}(w)$ where w is an imaginary cube root of unity is the cyclotomic field for $n=3$ over $\mathbf{Q}$ and $\mathbf{Q}(\sqrt{-1})$ is the coclotomic field for $n=4$ over $\mathbf{Q}$.

$GF(p^n)$ is the cyclotomic field for $n-1$ over $\mathbf{J}_p$.

Ex. Describe the cyclotomic field over $\mathbf{Q}$ for $n=5$.

132·1. Primitive nth roots of unity. We suppose that K is a field of characteristic zero. Exactly as in § 128, page 308, it may be shown that the n roots of $x^n-1=0$, thought of as elements of the decomposition field of the same, form a multiplicative cyclic group of order n. Any generator ξ of this cyclic group is such that the lowest power of ξ which is equal to 1 is n. Each such nth root of unity is known as *primitive*. Denoting, as is usual, by $\varphi(n)$, the number of integers which are less than n and prime to n, we see by § 27·2, page 72, that the number of primitive nth roots of unity is $\varphi(n)$ and if ξ is any primitive nth root then so is also ξ^m where m denotes any integer less than n and prime to the same.

If

$$\xi_1, \xi_2, \ldots\ldots, \xi_l ; \qquad l=\varphi(n)$$

denote the $\varphi(n)$ primitive nth roots of unity, we write

$$\varphi_n(x)=(x-\xi_1)(x-\xi_2)\ldots\ldots(x-\xi_l).$$

It will now be easily seen that $\varphi_n(x)$ belongs to the polynomial ring over the ground field K, *i.e.*,

$$\varphi_n(x) \in K[x].$$

Each nth root of unity is a primitive dth root of unity for one and only one divisor d of n and accordingly we have the result

$$x^n-1 = \prod_{d \mid n} \varphi_d(x). \qquad (1)$$

If we suppose that $\varphi_h(x) \in K[x]$ for each integer $h<n$, then by mathematical induction, it follows from (1) that

$$\varphi_n(x) \in K[x].$$

The polynomial $\varphi_n(x)$ is known as the *cyclotomic polynomial* for n. Herebelow, we give cyclotomic polynomials for a few n.

$$\varphi_1(x)=x-1,$$
$$\varphi_2(x)=x+1,$$
$$\varphi_3(x)=x^2+x+1,$$

$$\varphi_4(x)=x^2+1,$$
$$\varphi_5(x)=x^4+x^3+x^2+x+1,$$
$$\varphi_6(x)=x^2-x+1.$$

For any prime p, we have

$$\varphi_p(x)=x^{p-1}+x^{p-2}+\ldots\ldots+x+1.$$

Ex. 1. Show that

$$\varphi_{2n}(x)=\varphi_n(-x),$$

for any odd n.

Ex. 2. Show that if p is not a divisor of n,

$$\varphi_{pn}(x)=\frac{\varphi_n(x^p)}{\varphi_n(x)}.$$

Discuss also the case when $p \mid n$.

Ex. 3. Considering the case when K is a field of non-zero characteristic and x^n-1 is separable over the same, outline the results corresponding to those of § 132 for fields with zero characteristic.

132·2. Irreducibility of the cyclotomic polynomial over the prime field of characteristic zero. Without any loss of generality, we shall consider the prime field of characteristic zero to be the same as the field $\mathbf{Q}$ of rational numbers.

It can be shown that the cyclotomic polynomials $\varphi_n(x)$ are irreducible over the prime field of characteristic zero for every arbitrary n. Since, however, we do not need this result for an arbitrary n, we shall not give this general proof. Instead we shall give the proof for the case when the index is a prime and this is all that we shall need in the following. Irreducibility in this case is a simple consequence of the Eisenstein theorem as given in § 80, page 214.

We have, for $n=p$,

$$\varphi_p(x)=(x^p-1)/(x-1).$$

Now $\varphi_p(x)$ would be irreducible if and only if $\varphi_p(x+1)$ is irreducible. We have

$$\varphi_p(x+1)=[(x+1)^p-1]/(x+1-1)$$
$$=x^{p-1}+px^{p-2}+\frac{p(p-1)}{2!}x^{p-3}+\ldots\ldots+\frac{p(p-1)}{2!}x+p.$$

Since each co-efficient, other than the first, is *divisible* by the prime p, and the last one is not divisible by p^2, we deduce by the Eisenstein theorem that $\varphi_p(x+1)$ is irreducible over $\mathbf{Q}$. Thus $\varphi_p(x)$ is irreducible over $\mathbf{Q}$.

Note. It may be pointed out that $\varphi_n(x)$ may *not* be *irreducible* for fields with non-zero characteristic. As for example, in the *prime*

field J_{11}, of characteristic 11,

$$\varphi_{12}(x)=x^4-x^2+1=(x^2-5x+1)(x^2+5x+1).$$

Ex. Carry out the proof of the irreducibility of $\varphi_n(x)$ over $\mathbf{Q}$ when n is of the form p^m; p being any prime.

[We have, when $n=p^m$,

$$\varphi_n(x)=(x^{p^m}-1)/(x^{p^{m-1}}-1)].$$

133. Galois groups of cyclotomic fields over the prime field of characteristic zero. We shall now prove two theorems, the first of which will relate to arbitrary exponents and the second to prime exponents. The second one will give very precise information whereas the first one will only be partially informative.

Theorem I. *The Galois group of x^n-1 over any field of characteristic zero is Abelian.*

Let L denote the decomposition field of

$$x^n-1 \in K[x],$$

where K is the field of characteristic zero. We have, if ξ denotes a primitive nth root of unity,

$$L=K(\xi).$$

In every K-automorphism of L, ξ is mapped on some power ξ^a of the same and each such automorphism is determined by its effect on ξ.

We denote by f_a the automorphism which maps ξ on ξ^a so that we may write

$$f_a : \xi \longrightarrow \xi^a.$$

Also let f_b be a K-automorphism of L so that

$$f_b : \xi \longrightarrow \xi^b.$$

We have

$$\begin{aligned}(f_a f_b)(\xi)&=f_a(f_b(\xi))\\&=f_a(\xi^b)\\&=(f_a(\xi))^b\\&=(\xi^a)^b=\xi^{ab}=\xi^{ba}=(f_b f_a)(\xi),\end{aligned}$$

so that

$$f_a f_b=f_b f_a.$$

Thus the Galois group, in question, is Abelian.

Theorem II. *The Galois group of x^p-1 over the prime field of characteristic zero is the cyclic group of order $p-1$; p being any prime integer.*

We take the prime field of characteristic zero to be the same as $\mathbf{Q}$.

The decomposition field, say L, of $x^p-1 \in \mathbf{Q}[x]$ is the same as that of

$$\varphi_p(x)=x^{p-1}+x^{p-2}+\ldots\ldots+x+1,$$

and $\varphi_p(x)$ has been seen to be irreducible over $\mathbf{Q}$. If ξ denote any one of its roots, then

$$\xi, \xi^2, \ldots\ldots, \xi^{p-1}.$$

denote all the $(p-1)$ roots of $\varphi_p(x)$; of course all different. Clearly then there are $(p-1)$ $\mathbf{Q}$-automorphisms of L defined by

$$\xi \longrightarrow \xi\ ;\ \xi \longrightarrow \xi^2, \ldots\ldots, \xi \longrightarrow \xi^{p-1},$$

We denote by f_a the automorphism defined by

$$(f_a)(\xi)=\xi^a.$$

The mapping

$$f_a \longrightarrow a,$$

is, as may be easily seen, an isomorphism of the Galois group of automorphisms of order $(p-1)$ with the group of $(p-1)$ integers

$$1, 2, \ldots\ldots, p-1$$

for multiplication modulo p. In fact, we have

$$\begin{aligned}(f_af_b)(\xi) &= f_a(f_b(\xi))\\ &= f_a(\xi^b)\\ &= (f_a(\xi)^b)=(\xi^a)^b=\xi^{ab}\end{aligned}$$

so that

$$f_af_b \longrightarrow ab.$$

This latter group of integers, being just the multiplicative group of the prime field $\mathbf{J}_p$ of characteristic p is, as shown in § 128 cyclic of order $p-1$. Hence the result.

133·1. Galois group of x^p-1 over any arbitrary field of characteristic zero.

Let K denote any arbitrary field of characteristic zero and let L denote the decomposition field of $x^p-1 \in K[x]$. We have then

$$\mathbf{Q} \subseteq K \subseteq L.$$

By § 122·1, page 297, the Galois group of L over K is a subgroup of that of L over $\mathbf{Q}$. Since the Galois group of L over $\mathbf{Q}$ is cyclic of order $p-1$ and every subgroup of a cyclic group is cyclic, we deduce that the Galois group of L over K is also cyclic and its order is a divisor of $p-1$. Thus we have proved the following result:

134·2. Converse of the preceding theorem.

Theorem. *Let L be a normal extension of degree n over K and let the Galois group of L over K be cyclic. Finally, let K be of characteristic zero and contain the nth roots of unity. Then L is the decomposition field of a pure irreducible equation*

$$x^n - a = 0,$$

over K.

Since L is a separable, finite extension of K, there exists an element $\theta \in L$ such that

$$L = K(\theta).$$

Let ξ denote a primitive nth root of unity so that, as given, $\xi \in K$. Also let f be a generating element of the cyclic Galois group of L over K so that

$$f, f^2, \ldots\ldots, f^{n-1}, f^n = I$$

are the n elements of the Galois group.

Since $\xi \in K$ and f is a K-automorphism of L, we have

$$f(\xi) = \xi.$$

We now form what is usually called the **Lagrange resolvent** of θ:

$$\alpha = \theta + \xi^{-1} f(\theta) + \xi^{-2} f^2(\theta) + \ldots\ldots + \xi^{-(n-1)} f^{n-1}(\theta),$$

and compute the various conjugates of α.

We have

$$\begin{aligned} f(\alpha) &= f(\theta) + \xi^{-1} f^2(\theta) + \xi^{-2} f^3(\theta) + \ldots\ldots + \xi^{-(n-1)} f^n(\theta) \\ &= \xi[\theta + \xi^{-1} f(\theta) + \xi^{-2} f^2(\theta) + \ldots\ldots + \xi^{-(n-1)} f^{n-1}(\theta)] \\ &= \xi\alpha. \end{aligned}$$

$$\therefore \quad f^2(\alpha) = f[f(\alpha)] = f(\xi\alpha) = \xi f(\alpha) = \xi^2\alpha,$$

$$f^3(\alpha) = \xi^3\alpha, \ldots\ldots, f^{n-1}(\alpha) = \xi^{n-1}\alpha, f^n(\alpha) = \alpha.$$

Thus

$$\alpha, \xi\alpha, \xi^2\alpha, \ldots\ldots, \xi^{n-1}\alpha$$

are the n different conjugates of α so that the minimal polynomial over K belonging to α is

$$\varphi(x) = (x-\alpha)(x-\xi\alpha)(x-\xi^2\alpha)\ldots\ldots(x-\xi^{n-1}\alpha),$$

which is of degree n.

$$\therefore \qquad [K(\alpha) : K] = n.$$

Now

$$K \subset K(\alpha) \subseteq K(\theta),$$

where $[K(\theta) : K] = n$.

$$\therefore \qquad K(\alpha)=K(\theta),$$

Also $K(\alpha)$ is the decomposition field of $\varphi(x)$ over K.

Again, we have

$$f(\alpha^n)=f(\alpha)^n=\xi^n\alpha^n=\alpha^n,$$

so that α^n remains invariant for f and therefore also for every member of the Galois group. Hence

$$\alpha^n \in K.$$

We write

$$\alpha^n=a \in K.$$

Thus α is a root of the nth degree polynomial

$$x^n-\alpha^n=x^n-a$$

over K. Hence, by § 113·1, page 271,

$$\varphi(x)=x^n-a.$$

Thus $K(\alpha)=K(\theta)=L$ is the decomposition field of the pure polynomial x^n-a which is irreducible over K.

Hence the theorem.

135. Solvability by radicals of cyclotomic fields.

Theorem. *The cyclotomic field for any prime p over a field of characteristic zero is solvable by radicals over the same.*

Let K denote any given field of characteristic zero and L denote the decomposition field of x^p-1 over K.

The Galois group of x^p-1 over K is cyclic whose order is some divisor d of $p-1$. We write

$$d=p_1^{a_1}\ p_2^{a_2}\ \ldots\ldots p_t^{a_t},$$

where $p_1, p_2, \ldots\ldots, p_t$ are distinct primes.

The theorem will be moved by induction on the exponent.

The theorem is clearly true for the exponent 2, for the roots ± 1 of x^2-1 already belong to K.

We assume the theorem true for each exponent less than p.

Firstly we successively adjoin, starting from K, the p_1 th, p_2-th, ..., p_t-th roots of unity. Under the assumed hypothesis this is possible by successive adjunction of radicals. Thus we arrive at a field say, M, of characteristic zero which contains the p_1-th, p_2-th, ..., p_t-th roots of unity and which is a tower over K.

Thus we have

$$K \subseteq M \subseteq L.$$

The Galois group of L over M being a sub-group of that of L over K which is cyclic of order

$$p_1^{a_1}\ p_2^{a_2}\ \ldots\ldots\ p_t^{a_t},$$

we see that the Galois group of L over M is cyclic whose order is of

the form

$$p_1^{b_1} p_2^{b_2} \ldots\ldots p_t^{b_t},$$

where

$$b_1 \leqslant a_1,\ b_2 \leqslant a_2, \ldots\ldots,\ b_t \leqslant a_t.$$

From § 27·3, page 72, we know that any given finite order cyclic group possesses a sub-group whose order is a given divisor of the order of the group. Then by the Fundamental theorem of Galois Theory there exists a finite sequences of fields

$$M,\ M_1',\ M_2', \ldots\ldots,\ M'_{b_1},$$

such that the Galois groups

$$G(M_1'/M),\ G(M_2'/M_1'), \ldots\ldots,\ G(M'_{b_1}/M'_{b_1-1})$$

are all cyclic of order p_1. Thus each of these fields is obtained from its predecessor on adjoining an irreducible radical of exponent p_1.

Thus

$$M'_{b_1}$$

is a tower over M and of degree

$$p_1^{b_1}$$

over the same. Proceeding in this manner adjoining successively radicals of exponent p_2, radicals of exponent p_3 etc., we shall arrive at the field L of degree

$$p_1^{b_1} p_2^{b_2} \ldots\ldots p_t^{b_t}$$

over M. Thus L is a tower over K.

Hence the theorem.

Ex. 1. If K is a field with non-zero characteristic p and contains the pth roots of unity and $p > n$, then the Galois field of the irreducible $x^n - a$ over K is cyclic of degree n.

Ex 2. Express the cyclotomic fields for all positive integers $\leqslant 12$ as towers ever the prime field of characteristic zero.

136. Solvability by Radicals. Fundamental Theorem.

We need the concept of Soluble (or Solvable) groups to state the condition for solvability by radicals of equations.

Soluble groups. Def. *A finite order group is said to be soluble (or solvable), if the composition factors thereof are all prime.*

Thus if G be a solvable group and

$$G,\ H_1,\ H_2, \ldots\ldots,\ H_k = \{e\}$$

be a composition series for the same, then the composition factor

groups

$$G/H_1,\ H_1/H_2,\ldots\ldots,\ H_{k-1}/H_k,$$

which are of prime orders are necessarily cyclic.

It may be easily shown that every finite order cyclic group is necessarily soluble.

Theorem. *A necessary and sufficient condition for a polynomial* $\phi(x) \in K[x]$ *where* K *is a field of characteristic zero to be solvable by radicals over* K *is that the Galois group of* $\phi(x)$ *over* K *is soluble.*

Let L denote the decomposition field of $\phi(x) \in K[x]$.

Firstly suppose that $\phi(x)$ is solvable by radicals over K. There exists, therefore, a finite chain of fields

$$K,\ K_1,\ K_2,\ldots\ldots,\ K_{t-1},\ K_t=L$$

such that each of these is a pure extension of prime degree of its predecessor. Let,

$$K_1=K(\sqrt[p_1]{a_1}),\ K_2=K_1(\sqrt[p_2]{a_2}),\ldots\ldots,\ K_t=K_{t-1}(\sqrt[p_t]{a_t})$$

where

$$a_1 \in K,\ a_2 \in K_1,\ldots\ldots,\ a_t \in K_{t-1}$$

We adjoin successively, to K, p_1-th, p_2-th,....., p_t-th roots of unity and thus obtain, starting from K, normal* cyclic extensions. Let M denote the field thus reached. Then M is normal over K. Starting from the series of fields between K and M thus obtained, we obtain another series of fields, also between K and M such that each member is a cyclic normal extension of *prime* degree of its predecessor.

We now adjoin to M successively the p_1-th roots of a_1 and of its conjugates over K and thus obtain a series of fields starting from M such that each is a cyclic normal extension of prime degree of its predecessor. Let us denote by M_1 the field thus reached. Then M_1 is normal over K.

Again we adjoin to M_1 successively the p_2-th roots of a_2 and of its conjugates over K and thus obtain a series of fields starting from M_1 such that each is a cyclic normal extension of prime degree of its predecessor. Let us denote by M_2 the field thus reached. Then M_2 is normal over K.

* A normal extension of a field K is called cyclic if the Galois group of the same over K is cyclic.

Proceeding in this manner and considering successively the elements $a_3, \ldots\ldots, a_t$ we obtain a field $M_t = N$, say such that

(*i*) N is normal over K,

(*ii*) there exists a chain of intermediate fields between K and N such that each is a cyclic normal extension of prime degree of its predecessor,

(*iii*) N contains the decomposition field L of $f(x)$ as a sub-field.

Let G denote the Galois group of N over K. To the chain of intermediate fields referred to in (*ii*) above, there corresponds, by the Fundamental theorem of Galois Theory, a chain of sub-groups

$$G \supset G_1 \supset G_2 \ldots\ldots \supset G_{t-1} \supset G_t = \{e\}$$

which constitute a composition series for G with composition factor groups

$$G/G_1,\ G_1/G_2, \ldots\ldots,\ G_{t-1}/G_t$$

cyclic of prime order. Thus G is a solvable group.

Let H denote the Galois correspondent of the intermediate field L between K and N. Since L is normal over K, therefore H is a normal sub-group of G.

By § 40, page 103, any composition series for G/H can be given in the form

$$G/H,\ G_1/H,\ G_2/H, \ldots\ldots,\ H/H$$

where G_1 is a normal sub-group of G, G_2 of G_1 and so on. Again, by § 40, page 103,

$$G/H_1 \cong (G/H)/(G_1/H)\ ;$$

$$G_1/G_2 \cong (G_1/H)/(G_2/H)\ ;\ \text{and so on.}$$

These results show that G_1 is a maximal normal sub-group of G, G_2 of G_1 and so on. Thus the series

$$G, G_1, G_2, \ldots\ldots, H$$

is a part of a composition series for G.

Let

$$H, H_1, \ldots\ldots H_t = \{e\}$$

be a composition series of H. Then

$$G, G_1, G_2, \ldots\ldots, H, H_1, \ldots\ldots, H_t = \{e\}$$

is a composition series for G. As G is soluble, all the composition factor groups and in particular,

$$H/H_1.\ H_1/H_2, \ldots\ldots,\ H_{t-1}/H_t$$

are cyclic of prime order.

Thus the group H is soluble. But H is the Galois group of the decomposition field L of $\phi(x)$ over K.

Hence the first part.

Now suppose that the Galois group H of $\phi(x)$ over K is soluble. Let L be the decomposition field of $\phi(x)$.

Let

$$H \supset H_1 \supset H_2 \ldots\ldots \supset H_{r-1} \supset (e) \qquad (1)$$

be a composition series for H. Since H is soluble, the composition factor groups

$$H/H_1, H_1/H_2, \ldots\ldots, H_{r-1}/H_r$$

are all cyclic of prime degree.

By the Fundamental theorem of Galois Theory, there corresponds to the series (1), a series of fields

$$K \subset L_1 \subset L_2 \ldots \subset L_{r-1} \subset L, \qquad (2)$$

being the Galois correspondents of those in (1), such that each of these is a normal cyclic extension of prime degree over its predecessor. This follows from the fact that H_i/H_{i-1} is isomorphic to the Galois group of L_i over L_{i-1} and H_i/H_{i-1} is cyclic of prime degree.

Let the primes involved in respect of above be

$$p_1, p_2, \text{ etc.}$$

We adjoin to K successively p_1-th, p_2-th, etc., roots of unity and reach a field say M which is solvable by radicals over K. (Refer § 135). By § 134·2, the generators of $L_1, L_2, \ldots\ldots$ can be expressed as radicals with prime exponents. We now suppose that the same are successively adjoined to M. Thus we reach L and see that L is solvable by radicals over K.

Hence the second part.

157. General equation of degree n and its Galois group.

Let

$$K = Q(u_1, u_2, \ldots\ldots, u_n),$$

where $u_1, u_2, \ldots\ldots, u_n$ are n indeterminates over the field Q of rational numbers. Then the equation

$$\phi(x) = x^n + u_1 x^{n-1} + u_2 x^{n-2} + \ldots\ldots + u_{n-1} x + u_n = 0$$

is known as the *General* (or *Generic*) equation of degree n over K. It is now proposed to find the Galois group of this polynomial over the field K. Let L denote the decomposition field of the polynomial and let

Replacing $y_1, \ldots\ldots, y_n$ by $x_1, \ldots\ldots, x_n$ respectively, we obtain

$$\psi[-(x_1+x_2+ \ldots\ldots +x_n), \ldots, (-1)^n x_1 x_2 \ldots x_n]=0$$

so that by virtue of (A),

$$\psi(u_1, \ldots\ldots, u_n)=0.$$

But since $u_1, \ldots\ldots, u_n$ are indeterminates are $\mathbf{Q}$, this must be only a trivial relation. Thus we arrive at a contradiction.

Now since

$$u_1, \quad \ldots, u_n$$

and

$$v_1, \ldots\ldots, v_n$$

are two sets of indeterminates over $\mathbf{Q}$, we have

$$K=\mathbf{Q}(u_1, \ldots\ldots, u_n) \cong \mathbf{Q}(v_1, \ldots\ldots, v_n)=\overline{K}$$

under the mapping

$$u_i \longrightarrow v_i, \qquad 1 \leqslant i \leqslant n.$$

Also $\overline{\phi(x)}$ is the image of $\phi(x)$ under this mapping. As L and $\overline{L}$ are the two splitting fields, they are isomorphic ; an isomorphism being a continuation of the isomorphism of K on $\overline{K}$ referred to above. Thus

$$G(L/K) \cong G(\overline{L}/\overline{K}),$$

so that we deduce that the Galois group of the general $\phi(x)$ of degree n over its coefficient field is isomorphic to the symmetric group $\mathbf{P}_n$ of degree n.

138. Abel's theorem. *The general equation of degree greater than 4 is not solvable by radicals.*

It has been seen that the Galois group of the general equation of degree n is isomorphic to the symmetric group $\mathbf{P}_n$. The theorem will, therefore, be proved if we show that $\mathbf{P}_n$ is not a solvable group for $n>4$. This will be established as a consequence of the following lemma :

Lemma. *The alternating group $\mathbf{A}_n$ $(n>4)$ is simple.* (Refer Def. § 34·2, page 91).

We have to prove that $\mathbf{A}_n$ possesses no proper normal sub-group when $n>4$.

Let, if possible, H be any proper normal sub-group of $\mathbf{A}_n$.

Each permutation of H leaves fixed none, one or more of the symbols permuted. We select a member σ of H which is different from the identity and which keeps fixed the largest possible number

$x_1, \ldots\ldots, x_n$

denote the n roots thereof in L. We have then

$$\left.\begin{aligned} u_1 &= -(x_1 + \ldots\ldots + x_n) \\ u_2 &= (x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n) \\ \ldots\quad &\ldots\quad \ldots\quad \ldots\quad \ldots \\ \ldots\quad &\ldots\quad \ldots\quad \ldots\quad \ldots \\ u_n &= (-1)^n x_1x_2\ldots\ldots x_n. \end{aligned}\right\}$$

Thus we have

$$L = K(x_1, \ldots\ldots, x_n) = \mathbf{Q}(u_1, u_2, \ldots\ldots, u_n ; x_1, \ldots\ldots, x_n)$$
$$= \mathbf{Q}(x_1, \ldots\ldots, x_n) \text{ ; by virtue of (A).}$$

The co-efficients of a general equation as defined above are indeterminates. We now proceed to compare this equation with another whose *roots* are indeterminates. We set

$$L = \mathbf{Q}(y_1, \ldots\ldots, y_n),$$

where $y_1, y_2, \ldots\ldots, y_n$ are indeterminates over $\mathbf{Q}$ and also set up

$$\bar{\phi}(x) = (x - y_1)(x - y_2)\ldots\ldots(x - y_n)$$
$$= x^n + v_1x^{n-1} + v_2x^{n-2} + \ldots\ldots + v_{n-1}x + v_n$$

where

$$\left.\begin{aligned} v_1 &= -(y_1 + \ldots\ldots + y_n) \\ v_2 &= (y_1y_2 + y_1y_3 + \ldots\ldots + y_{n-1}y_n) \\ \ldots\quad &\ldots\quad \ldots\quad \ldots\quad \ldots \\ \ldots\quad &\ldots\quad \ldots\quad \ldots\quad \ldots \\ v_n &= (-1)^n y_1y_1\ldots\ldots y_n. \end{aligned}\right\}$$

We write

$$\bar{K} = \mathbf{Q}(v_1, v_2, \ldots\ldots, v_n),$$

and see that $\bar{L}$ is the decomposition field of $\phi(x)$ over $\bar{K}$. Then n roots of $\bar{\phi}(x)$ are all distinct. The Galois group of $\bar{L}$ over $\bar{K}$ is isomorphic to the symmetric group of all the permutations on $y_1, \ldots\ldots, y_n$; for every such permutation is an automorphism of $\bar{L}$ wherefor each of $v_1, \ldots\ldots, v_n$ and accordingly each element of $\bar{K}$ remains invariant.

We now proceed to show that $v_1, \ldots, v_n$ are themselves indeterminates over $\mathbf{Q}$. Otherwise suppose that there exists some non-trivial relation

$$\psi(v_1, \ldots\ldots, v_n) = 0$$

over $\mathbf{Q}$. This gives

$$\psi(-(y_1 + y_2 + \ldots + y_n), \ldots\ldots, (-1)^n y_1y_2\ldots y_n) = 0.$$

As $y_1, \ldots, y_n$ are indeterminates over $\mathbf{Q}$, the relation would remain true irrespective of what we may substitute for the same.

Replacing $y_1, \ldots\ldots, y_n$ by $x_1, \ldots\ldots, x_n$ respectively, we obtain

$$\psi[-(x_1+x_2+ \ldots\ldots +x_n), \ldots, (-1)^n x_1 x_2 \ldots x_n]=0$$

so that by virtue of (A),

$$\psi(u_1, \ldots\ldots, u_n)=0.$$

But since $u_1, \ldots\ldots, u_n$ are indeterminates are $\mathbf{Q}$, this must be only a trivial relation. Thus we arrive at a contradiction.

Now since

$$u_1, \ldots, u_n$$

and

$$v_1, \ldots\ldots, v_n$$

are two sets of indeterminates over $\mathbf{Q}$, we have

$$K=\mathbf{Q}(u_1, \ldots\ldots, u_n) \cong \mathbf{Q}(v_1, \ldots\ldots, v_n)=K$$

under the mapping

$$u_i \longrightarrow v_i, \qquad 1 \leqslant i \leqslant n.$$

Also $\overline{\phi(x)}$ is the image of $\phi(x)$ under this mapping. As L and $\overline{L}$ are the two splitting fields, they are isomorphic ; an isomorphism being a continuation of the isomorphism of K on $\overline{K}$ referred to above. Thus

$$G(L/K) \cong G(\overline{L}/\overline{K}),$$

so that we deduce that the Galois group of the general $\phi(x)$ of degree n over its coefficient field is isomorphic to the symmetric group $\mathbf{P}_n$ of degree n.

138. Abel's theorem. *The general equation of degree greater than 4 is not solvable by radicals.*

It has been seen that the Galois group of the general equation of degree n is isomorphic to the symmetric group $\mathbf{P}_n$. The theorem will, therefore, be proved if we show that $\mathbf{P}_n$ is not a solvable group for $n>4$. This will be established as a consequence of the following lemma :

Lemma. *The alternating group* $\mathbf{A}_n$ $(n>4)$ *is simple.* (Refer Def. § 34·2, page 91).

We have to prove that $\mathbf{A}_n$ possesses no proper normal sub-group when $n>4$.

Let, if possible, H be any proper normal sub-group of $\mathbf{A}_n$.

Each permutation of H leaves fixed none, one or more of the symbols permuted. We select a member σ of H which is different from the identity and which keeps fixed the largest possible number

of symbols. *Suppose that σ displaces more than 3 elements. We express σ as a product of mutually exclusive cycles. Then we have the following two possibilities :*

(*i*) σ contains a cycle with atleast 3 symbols,

(*ii*) σ is a product of transpositions.

In respect of the first possibility, let

$$\sigma=(123.....).....$$

Take

$$\tau=(345) \in A_n.$$

We have

$$\tau^{-1}\sigma\tau=(125.....) \text{ ; Refer § 31, page 84}$$
$$=\sigma_1, \text{ say.}$$

Then $\sigma^{-1}\sigma_1$ leaves fixed more *symbols than σ does and is not* identity. This fact is opposed to the definition of σ. Thus first possibility cannot exist.

In respect of the second possibility, let

$$\sigma=(12)(34).....$$

and take as before

$$\tau=(345).$$

Then

$$\tau^{-1}\sigma\tau=(12)(53).....$$
$$=\sigma_1, \text{ say.}$$

Again, $\sigma^{-1}\sigma_1$ leaves fixed more symbols than σ does and is not the identity. This fact is again opposed to the definition of σ. Thus the second possibility cannot as well exist.

Thus σ as defined displaces exactly 3 symbols and leaves all the others fixed.

Let

$$\sigma=(123) \in H.$$

$$\therefore \quad \sigma^2=(132)=(213) \in H.$$

Choose

$$\tau=(12)(3k) \text{ where } k>3.$$

$$\therefore \quad \tau^{-1}\sigma^2\tau=(2k1)=(12k).$$

Thus *each permutation* $(12k) \in H$, for $k>3$. Then *by* (2), page 61 of § 23·1,

$$H=A_n,$$

and we arrive at a contradiction.

Hence A_n is simple for $n>4$.

Main Theorem. By the lemma above,

$$\mathbf{P}_n, \mathbf{A}_n, \{e\},$$

is a composition series for $\mathbf{P}_n$ for $n>4$, so that the composition factors of $\mathbf{P}_n$ for $n>4$ are

$$2, \tfrac{1}{2}n!$$

which are not both prime.

Thus $\mathbf{P}_n$ is not solvable for $n>4$.

139. Ruler and Compass Constructions. Numerous problems in Geometry relate to the determination through a finite series of steps of construction a set of points and line segments which are related to any given set of *points and line segments* in some given specified manner. Also Greeks and other mathematicians had interested themselves in examining whether or not any given problem of this nature can be solved with the help of *Ruler and Compass* alone. In this context the following three problems—known as the *Famous problems of Antiquity*—have been of very great interest to mathematicians.

(*i*) Duplicating a cube.

(*ii*) Trisecting an angle.

(*iii*) Squaring a circle.

It will now be seen that the theory developed so far provides us with a method for determining whether or not any such problem can be solved with the help of ruler and compass alone.

In any given problem, the data consists of a system of points and line segments and the *allowable* steps of construction, corresponding to the use of ruler and compass alone, are

(*a*) Drawing of a line through two points. [Use of a ruler]

(*b*) Drawing of a circle with any point as centre and any line segment as radius. [Use of compass].

(*c*) Determination of a point or points as the intersection of

(*i*) Two lines. (*ii*) A line and a circle. (*iii*) Two circles.

Thus starting from any given system of points and line segments, we have to determine, if possible, other points and line segments which bear to the given system some given relationship, making use of only the allowable steps of construction.

Analytical Formulation of the Problem. For the solution of the problems of the nature referred to above, we refer the given

system of points and line segments to a rectangular Cartesian system of axes so that

(1) a point is represented by a pair of real numbers which denote, the lengths of two line segments lying along the two coordinate axes,

(2) a line segment is represented by a single number which denotes the length of the same.

Thus any given system of points and line segments gives rise to a certain system of real numbers, say

$$a_1, a_2, \ldots\ldots, a_t.$$

Thus formulated analytically, *the problem consists in constructing a line segment with a length α on the basis of a certain number of given line segments with given lengths*

$$a_1, a_2, \ldots\ldots, a_t,$$

the means of construction restricted as explained. In the following we shall refer to α as being *constructible* if it can be constructed in the manner described.

We denote by K the field generated by the set of numbers

$$a_1, a_2, \ldots\ldots, a_t.$$

It is known from Elementary Geometry that it is possible to construct, by ruler and compass alone, a line segment whose length is given by any member of K. In fact, it may be seen that if a, b are the real numbers denoting the lengths of two given line segments, then it is possible to construct with the help of ruler and compass alone line segments with lengths

$$a+b,\ a-b,\ ab,\ a\div b.$$

any allowable step of construction, the corresponding field may change.

Suppose that at any stage of the process of construction, we have arrived at a system of points and line segments which we denote by S and the field corresponding to the same by K_s.

(i) The coefficients in the equation of a line through two points of S and that of the circle with any given point of S as centre and any given line segment of S as radius belong to the field K_s as defined.

The co-ordinates of the point of intersection of two lines whose coefficients belong to K_s again belong to K_s, since the process involves only the solution of two linear equations.

The determination of the co-ordinates of the points of intersection of circles reduces to that of the co-ordinates of the points of intersection of a circle and a straight line. Also this latter determination leads to the solution of a quadratic equation in one unknown with coefficients belonging to K_s. Thus the co-ordinates of these points of intersection either belong to K_s or to a quadratic extension of K_s of the form $K_s(\sqrt{\theta})$ where θ is a positive member of K_s but is not the square of a member of K_s. Thus in this latter case $\sqrt{\theta}$ is a real number and

$$(K_s(\sqrt{\theta}) : K_s) = 2.$$

Thus if we start with any given system of points and line segments and carry out successively any series of allowable constructions, we obtain a corresponding series of fields, being sub-fields of the field $\mathbf{R}$ of real numbers,

$$K \subseteq K_1 \subseteq K_2 \ldots\ldots\ldots \subseteq K_{s-1} \subseteq K_s \subseteq \ldots\ldots \subseteq K_t$$

such that

$$(K_{r-1} : K_r) \leqslant 2,$$

and accordingly, by § 111·1, page 269

$$(K_t : K) = 2^m,$$

where $m \leqslant t$.

Now suppose that we are required to determine whether or not a certain given segment of length, say α, can be determined from a given system of points and line segments which correspond to a field K. If α is thus constructible, then we must clearly have

$$K \subseteq K(\alpha] \subseteq K_t$$

for some t. The degree

$$(K(\alpha) : K),$$

that the sum, difference, product and quotient of two constructible numbers are themselves constructible.

This follows from the fact that

$$(a+ib)+(c+id)=(a+c)+i(b+d)$$

$$(a+ib)(c+id)=(ac-bd)+i(ad+bc)$$

$$(a+ib)\div(c+id)=[(ac+bd)\div(c^2+d^2)]+i[(bc-ad)\div(c^2+d^2)]$$

and the fact that the sum, difference, product and quotient of two constructible real numbers are themselves constructible.

Further, we have

$$\sqrt{a+ib}=\sqrt{[\tfrac{1}{2}(a+\sqrt{a^2+b^2})]}+i\sqrt{[\tfrac{1}{2}(-a+\sqrt{a^2+b^2})]}$$

so that a square root of a constructible complex number is construcible.

We now prove the following :

In order that α be constructible starting from a given system of points and line segments which correspond to a field K, it is necessary and sufficient that α belongs to a field which is a normal extension of K and whose degree over K is some power of 2.

The condition is necessary. Let α be constructible so that there exists, as shown before, a chain of fields of real numbers

$$K=K_0 \subset K_1 \subset K_2 \subset \ldots . \subset K_t \subset L$$

such that L contains α and each is obtained from its predecessor by adjoining a square root of the member of the same.

If after adjoining a square root at any stage, we also adjoin the square roots of the conjugate field elements, the field extensions remain of degree 2 and we obtain a normal extension of K containing α and of degree of the form 2^m over K. Thus the given condition is necessary.

Now to show that this condition is sufficient.

Suppose that $\alpha \in L$ where

$$(L : K)=2^m$$

and L is normal over K.

Let G denote the Galois group of L over K so that the order of G is 2^m.

being a divisor of the degree

$$(K_t : K)$$

must itself be a power of 2.

Thus we obtain the following necessary condition :

A necessary condition for a length α to be constructible starting from a given system of points and line segments which correspond to a field K is that the degree

$$(K(\alpha) : K)$$

is some power of 2.

The real number α may denote the length of a segment or either of the two co-ordinates of a point.

We now obtain a form of the condition for constructibility which is both necessary as well as sufficient.

In order that a length α be constructible starting from a given system of points and line segments which correspond to a field K, it is necessary and sufficient that there exists a field L containing α and a chain of fields, being sub-fields of **R**,

$$K=K_0 \subset K_1 \subset K_2 \ldots\ldots\ldots \subset K_t \subset L$$

such that the degree of each over its predecessor $\leqslant 2$.

That this condition is necessary follows from the preceding discussion.

Now to show that this condition is also sufficient. We suppose that the chain of fields of the above type exists. By § 134·2, page 322, we have a relation of the form

$$K_s=K_{s-1}(\sqrt{\alpha_{s-1}}).$$

where

$$\alpha_{s-1} \in K_{s-1}.$$

Also it is known from elementary geometry that a line segment whose length is the square root of the length of any given line segment is constructible. Thus proceeding step by step, we may see that α is constructible.

140·1. Use of Galois Theory. We have so far confined ourselves to real numbers. It is possible, however, to remove this restriction and make use of complex numbers, for the solution of the problem in hand.

We shall say that a complex number $a+ib$ is constructible if its real and imaginary parts a, b are constructible. It may be seen

that the sum, difference, product and quotient of two constructible numbers are themselves constructible.

This follows from the fact that

$$(a+ib)+(c+id)=(a+c)+i(b+d)$$

$$(a+ib)(c+id)=(ac-bd)+i(ad+bc)$$

$$(a+ib)\div(c+id)=[(ac+bd)\div(c^2+d^2)]+i[(bc-ad)\div(c^2+d^2)]$$

and the fact that the sum, difference, product and quotient of two constructible real numbers are themselves constructible.

Further, we have

$$\sqrt{a+ib}=\sqrt{[\tfrac{1}{2}(a+\sqrt{a^2+b^2})]}+i\sqrt{[\tfrac{1}{2}(-a+\sqrt{a^2+b^2})]}$$

so that a square root of a constructible complex number is construcible.

We now prove the following :

In order that α be constructible starting from a given system of points and line segments which correspond to a field K, it is necessary and sufficient that α belongs to a field which is a normal extension of K and whose degree over K is some power of 2.

The condition is necessary. Let α be constructible so that there exists, as shown before, a chain of fields of real numbers

$$K=K_0 \subset K_1 \subset K_2 \subset \ldots . \subset K_t \subset L$$

such that L contains α and each is obtained from its predecessor by adjoining a square root of the member of the same.

If after adjoining a square root at any stage, we also adjoin the square roots of the conjugate field elements, the field extensions remain of degree 2 and we obtain a normal extension of K containing α and of degree of the form 2^m over K. Thus the given condition is necessary.

Now to show that this condition is sufficient.

Suppose that $\alpha \in L$ where

$$(L : K)=2^m$$

and L is normal over K.

Let G denote the Galois group of L over K so that the order of G is 2^m.

Making use of the result established in Ex. 5, page 88, we may see that a group of order 2^m is solvable so that there exists a composition series

$$G \supset G_1 \supset G_2 \ldots\ldots \supset G_m = \{e\}$$

such that each of the quotient groups

$$G/G_1, G_1/G_2, \ldots\ldots$$

is of order 2.

Corresponding to this composition series, there corresponds, by the Fundamental Theorem of Galois Theary, the series of fields

$$K \subset M_1 \subset M_2 \ldots \subset M_s = L$$

such that each is of degree two over its predecessor. Accordingly, by § 134·2, each of these fields is obtainable from its predecessor on adjunction of a square root. Thus the given condition is also sufficient.

141. Illustration.

1. **Duplication of cube.** This problem consists in the determination of a line segment the cube of whose length is equal to the length of a given line segment. Taking the length of the given line segment as 1, we require to determine a length α which satisfies

$$x^3 = 2.$$

As seen in the Ex. on page 302, the smallest normal extension of $\mathbf{Q}$ containing α is of degree 6 over $\mathbf{Q}$. As 6 is not a power of 2, we deduce that the length α, in question, is *not* constructible by ruler and compass. This problem may also be solved by the first form of condition as given on page 334.

2. **Trisection of an angle.** Let φ be any angle. It may be seen that for any given φ, $\cos\varphi$ is given by means of the ratio of two line segments.

We have

$$\cos\varphi = 4\cos^3\tfrac{1}{3}\varphi - 3\cos\tfrac{1}{3}\varphi.$$

We write

$$a = \cos\varphi, \quad x = \cos\tfrac{1}{3}\varphi,$$

so that a is known and x unknown.

Thus we have

$$4x^3 - 3x - a = 0.$$

The polynomial $4x^3 - 3x - a$ is not red[illegible] $K = \mathbf{Q}(a)$ for arbitrary values of a. As for example, [illegible] Eis[illegible]

criterion (§ 80, page 214) see that $4x^3-3x-a$ is irreducible over

$$\mathbf{Q}(\tfrac{1}{3})=\mathbf{Q}, \qquad a=\tfrac{1}{3}.$$

The Galois group of $4x^3-3x-a$ over the field $\mathbf{Q}(a)$ is either 3 or 6 in the case of the irreducibility of the same.

Thus x is not constructible for arbitrary values of a. Accordingly every angle cannot be trisected by means of ruler and compass alone.

3. **Squaring a circle.** This problem consists in the determination of a square whose area is equal to that of a given circle. Suppose that the radius of a given circle is taken as *unity*. Then the problem requires the construction of a length x such that

$$x^2=\pi.$$

Now it has been shown that π cannot be the root of an equation whose coefficients belong to $K=\mathbf{Q}(1)=\mathbf{Q}$. Thus $\mathbf{Q}(\pi)$ is not algebraic over $\mathbf{Q}$ so that $\mathbf{Q}(\pi)$ is of infinite degree over $\mathbf{Q}$. Thus π and so also $\sqrt{\pi}$ are not constructible and accordingly the problem in question does not admit of a solution.

4. **Construction of a regular m-gon.** Let

$$m=p_1^{a_1}\ p_2^{a_2}\ \dots\dots\ p_r^{a_r},$$

where $p_1, p_2, \dots\dots, p_r$ are different primes.

It is clear that if an m-gon can be constructed, then we can also construct any d-gon ; d being any divisor of m.

Thus if m-gon can be constructed, then we can also construct regular polygons with $p_1^{a_1}$, $p_2^{a_2}$, $\dots\dots$, $p_r^{a_r}$ sides. *Conversely*, also, it may be shown that if regular polygons with $p_1^{a_1}$, $\dots\dots$, $p_r^{a_r}$ sides can be constructed, then a regular m-gon can also be constructed. The greatest common divisor of

$$\frac{m}{p_1^{a_1}}, \dots\dots, \frac{m}{p_r^{a_r}}$$

being unity, there exist integers,

$$b_1, \dots\dots, b_r$$

such that

$$\frac{mb_1}{p_1^{a_1}}+\dots\dots+\frac{mb_r}{p_r^{a_r}}=1$$

or

$$\frac{b_1}{p_1^{a_1}}+\cdots\cdots+\frac{b_r}{p_r^{a_r}}=\frac{1}{m}.$$

Thus the mth part of a circle consists of a sum of $p_1^{a_1}$-th, ..., $p_r^{a_r}$-th parts.

From the above it follows that we need only examine the constructibility of a regular polygon with sides p^n where p is some prime. We write

$$m=p^n$$

The construction of a regular m-gon requires that of $\cos(2\pi/m)$. Now the constructibility of $\cos(2\pi/m)$ is equivalent to that of $\sin(2\pi/m)$ and therefore also of the complex number

$$\xi=\cos\frac{2\pi}{m}+i\sin\frac{2\pi}{m}.$$

We have

$$\xi^m=1$$

so that ξ is a root of $x^m=1$. The cyclotomic polynomial

$$\varphi_m(x)=0,\ m=p^n$$

is irreducible over $\mathbf{Q}[x]$. The Galois group of $\varphi_m(x)=0$ over $\mathbf{Q}$ is of order

$$p^{n-1}(p-1).$$

Thus the regular m-gon will be constructible for only such values of p and n for which

$$p^{n-1}(p-1)=2^t,$$

for some t. Thus we can only have

$$p=2 \text{ or } n=1.$$

Thus except for 2, no power of a prime higher than the first can be admitted. Firstly, we see that a regular polygon with sides of the form 2^t is constructible.

Now suppose that $p\neq 2$ so that $n=1$. Then a regular polygon is constructible when only p is a prime number of the form

$$1+2^t.$$

Thus we are interested in all primes of the form

$$1+2^t.$$

If t has an odd divisor so that we may write, $t=u(2n+1)$, we have

$$1+2^t=1+2^{u(2n+1)}=(1+2^u)(.. ...)$$

so that $1+2^t$ is not prime in this case.

Thus the only allowable primes are of the form

$$1+2^{(2^k)}.$$

For $0\leqslant k\leqslant 4$, we obtain

3, 5, 17, 257, 65537

which are all prime.

For $k=5$,

$$1+2^{(2^k)}=1+2^{32},$$

is divisible by 641 so that

$$1+2^{(2^k)}$$

is not prime for every k.

Thus the only constructible m-gons are those for which m is a *product of powers of 2 with primes of the form*

$$1+2^{(2^k)}$$

BIBLIOGRAPHY

Albert, A. A. ; *Introduction to Algebraic Theories.* Chicago : The University of Chicago Press.

Albert, A. A. ; *Fundamental Concepts of Higher Algebra.* Chicago : The University of Chicago Press.

Artin, E. : *Galo s Theory.* Notre Dame Mathematical Lectures, Number 2, Notre Dame, Indiana.

Artin, E. ; *Lectures on Modern Higher Algebra, Part I, Galois Theory.* New York University Lectures.

Baumgartner, L. ; *Gruppentheorie.* Berlin, Walter de Gruyter.

Beaumont, R. A. ; Ball, R. W. ; *Introduction to Modern Algebra and Matrix Theory.* London : Constable and Co.

Birkhoff. G., and Maclane, S., *A survey of Modern Algebra.* New York. Macmillan.

Bourbaki, N. ; *Algebre,* Livre II. Paris : Hermann and Cie.

Carmichael ; *Introduction to the theory of groups of finite order.* New York : Ginn and company.

Dubreil, P. ; *Algebre, Vol. I.* Paris : Gauthier villars.

Halmos, P. R. : *Finite Dimensional Vector Spaces.* Princeton University Press.

Hasse, H. ; *Higher Algebra* (Translated from German). New York : Frederick Ungar Publishing Co.

Jacobson, N. : *Lectures in Abstract Algebra, Vol. I—Basic Concepts, Vol. II—Linear Algebra.* New York : D Van Nostrand Company, Inc.

Krull, W. ; *Elementare and Klassiche Algebra Vom modernen Standpunkt.* Berlin : Walter De Gruyter & Co.

Kurosh, A. G. ; *The theory of Groups* (Translated from Russian) New York : Chelsea.

Ledermann, W. ; *Introduction to the theory of Finite Groups* Edinburgh : Oliver and Boyd.

Levi, F. W. ; *Algebra.* Calcutta, University of Calcutta.

Macduffee, C. C. ; *An introduction to Abstract Algebra.* New York : Wiley.

McCoy, N. H. ; *Rings and Ideals.* The Carus Mathematical Monographs. New York : The Mathematical Association of America.

Speiser, A. *Die Thorie der Gruppen von endicher Ordnung.* New York : Dover Publications.

Steinitz, E. ; *Theorie Der Körper.* New York : Chelsea.

Tchebotarow, N. Schwerdfeger, H. ; *Grundzuge Der Galois' schen Theorie.* Groningen Djakarta : P. Noordhoff.

Waerden, B. L. Van Der ; *Modern Algebra, Vol. I.* (Translated from German). New York, Ungar Publishing Co.

INDEX

(Numbers refer to pages)

Abelian, 97
—Theorem 329
Abstract 1
Algebra, Linear, 245
—of complexes, 54
—of ideals 166
—of normal subgroups 92
—of subgroups 58
—of subspaces 220
—of quaternions 262
Algebraic field extensions 270
—structures 20
—systems 20
Algorithm, *Division* 192
Alternating group 31
Annihilator 252
Associates 197
Associative composition 21
Associativity of products of mappings 11
Automorphisms, of groups 110
—,Inner 113
—,Outer 113
Axiomatic 1

Basis, 229, 258
Binary relation 23

Cancellation law 143
Cayley's Theorem 51
Central of a group 83
Characteristic of a field 178
Classes, Equivalence 24
—of *conjugate elements* 83
Coincidence Rotations 75
Commutator of a group 97
Complexes 52
Composite, elements 201
—of subgroups 60
—of subrings 153
Composition, Associative 21
—,commutative 21
—factors 108
—*factor groups* 109
—Identity for 22
—Induced 63
—Inversible elements fo 22
—*tables* 8
Congruence 65
Conjugate, elements 82
—complexes 83
Co-ordinatisation 241
Cosets of a subgroup 65
Cyclic, groups 71
—permutations 13
Cyclotomic field extensions 316

Decomposition, field 280
—*Left coset* 68
—,Right coset 66
Degree of a polynomial 193
Difference ring 159
Dihedral groups 78
Dimension 233
Direct, product, 116, 118, 165, 169.
—sum 169, 227
Division Algebra 260
—algorithm 192
—rings 144
Divisibility 194
Dual of a space 245
Duplication of a cube 335

Eisenstein 214
Endomorphisms 111, 171
Equality of mappings 5
Equations, pure 314
—,Linear 242
Equivalence, classes 24
—relation 24
Euclidean domains 207
Even permutations 18
Extensions of a *field, 269*
—,Algebraic 270
External Direct product 11

Factor groups 109
Factorisation 194
Field 145
—,Characteristic 178
—,Cyclotomic 316
—,Decomposition 280
—*extensions* 268
—,*Finite 303*
—,Galois 305
—,*Prime* 179
—,*Normal extensions* 284
—,Root 279
—,Separable extensions 295
—,*Simple extensions* 271
—,*Skew* 146
Finite, fields 305.
—groups 29
—sets 5
Finitely generated spaces 235

Galois 305

Gaussian integers 196
Generators, of a group 60
—of a cyclic group 72
Greatest common divisor 199
Groups 28
—,Abelian 28
—,*Alternating* 31
—,Composition factor 109
—,Cyclic 71
—,Finite 29
—,Dihedral 78
—,Infinite 29
—*of* coincidence rotations 75
—of matrices 31
—of permutations 31
—of transformations 31
—of vectors 30
—,Symmetric 31
—,Order of 29
—,Quotient 96

Holder 107
Homomorphism 98, 195
—,Kernel of 100, 160
Hyper complex Systems 257

Ideals 154
—,*Maximal* 177
—,Null 157
—,Principal 168
—,*zero* 157
Identity, for a composition 22
—mappings 6
Implication, One way 1
—,Two way 1
Inclusion relation 3
Indeterminate 189
Infinite set 3
Integral domain 144
Internal direct product 118
Intersection of, sets 3
—subgroups *58*
Inverse of a mapping 8
Inversible elements 22
Irreducibility criterion 214
Isomorphism of, groups 43, 48
—rings *146*
—vector spaces 227

Jordan 107

Kernel 100, 226

Lagrange's Theorm 69
Lattice 26
Left cosets 65
Linear, algebras 245
—equations 212
—transformations 224
Lower bound 26
Lowest common multiple 201

Mappings, 5
—,Associativity of products of 11
—,Equality of 6
—,Identity of 6
—,into 6
—,many one 6
—,One one 6
—,onto 6
—,Inverse of 8
—,Inversible 6
—,Natural 26, 103
—,Non-singular 9
—,Product of 10
Matrices, Groups of 31
Maximal ideals 177

Natural mappings 162
Non-singular mappings 9
Normal subgroups 82, 91
Normaliser 86, 89
Notation, Additive 20, 39
—,Multiplicative 39
Nullity 242
Null, ideal 157
—set 2

Odd permutations 16
Order of, a finite group 29
—an element 40

Partial order relation 24
Permutations, 12
—,Cyclic 10
—,Degree of 12
—,Even 16
—,Groups of 31
—,Odd 16
—,Similar 85
Polynomials, Degree of 190
—rings 186
Prime, elements 201
—fields 179
Primitive polynomials 208
Product of, mappings 10
—sets 4
Pure equations 314

Quaternions 262
Quotient groups 96
—*field 148*
—rings 155
—set 26
—*space 223*

Radicals 314
Rank 242
Residue class rings 159
Relations, Binary 23
—*compatible with group structure* 107
—compatible with ring structure 165

—Equivalence 24
—Inclusion 3
—Partial order 24
—Reflexive 23
—Symmetric 23
—Transitive 23
Right cosets 65
Rings 138
—,Commutative 142
—of functions 139
—of matrices 139
—of polynomials 139,187
—,Principal ideal 168
—with cancellation law 142
—with unity 142
Root fields 179

Scalar multiplication 246
Self conjugate, elements 83
—subgroups 90
Set, Composition in a 17
—,Finite 3
—,Infinite 3
—,Intersection of 3
—,Null 2
—,Product of 3
—,Transformation of 12
—,Union of 3
—,Quotient 26
Similar permutations 85
Skew fields 146
Solvability 314
Space, Vector 216
Structure, Algebraic 20
—of cyclic groups 23
—,Transference of 50, 99
Subgroups, Normal 82
Subrings 152

Table, Composition 18
Theorem, Abelian 329
—,Cayley's 51
—,Eisensteins 214
—,Jordan Holders 107
—,Lagrange's 69
Transitive relation 23
Transformation, Groups of 31
Transference of structure 50, 99, 1
Transpositions 14
Trisecting an angle 325

Union of sets 3
Units 185
Unique factorisation domains 194
Upper bound 26

Vectors, Groups of 3
—space 216

Zero ideal 157