PURE AND APPLIED MATHEMATICS

A Series of Monographs and Textbooks

FIELD THEORY

Masayoshi Nagata

Field Theory

Masayoshi Nagata

Department of Mathematics
Kyoto University
Kyoto, Japan

MARCEL DEKKER, INC. New York and Basel

Library of Congress Cataloging in Publication Data

Nagata, Masayoshi, 1927-
Field theory.

(Pure and applied mathematics ; 40)
Includes index.
1. Fields, Algebraic. 2. Field extensions (Mathematics) I. Title.
QA247.N25 512'.32 76-11106
ISBN 0-8247-6466-8

MARCEL DEKKER, INC.

270 Madison Avenue, New York, New York 10016

Current printing (last digit):
10 9 8 7 6 5 4 3 2

PRINTED IN THE UNITED STATES OF AMERICA

PREFACE

The theory of fields has traditionally been considered a basic part of abstract algebra. In modern mathematics, however, the abundance of algebraic ideas which have been introduced has established the importance of the theory of fields not only in algebra but throughout all areas of mathematics as well. There are many topics that require discussion in the mathematics courses frequently offered in colleges and universities. Consequently, it is not unusual to have too few lecture hours devoted to the theory of fields.

In view of this, the author wished to publish a book on field theory, rich in topical variety, necessitating few prerequisites, and conveniently sized, that would allow any student to advance his study.

In this book, it is assumed that the reader is familiar with the basic definitions and results on set theory and determinants, and therefore these results are stated explicitly and without proof. In addition, some basic results on group theory and ring theory will be needed; proofs for these results are given.

Thus the main text of this volume initially consists of preliminaries on groups and rings (Chapters 1 and 2) and in subsequent chapters (Chapters 3 to 7) focuses on several important topics on fields, such as algebraic and transcendental extensions, valuations, ordered fields, and Galois theory of algebraic extensions.

M. Nagata

CONTENTS

CHAPTER 0

CONVENTIONS AND BASIC RESULTS ON SET THEORY

0.0 NOTATION

We assume that the reader is familiar with fundamental concepts in set theory such as sets, elements, subsets, the empty set, unions of sets and intersections of sets. We use the following symbols.

$\in$ $a \in M$ means that a is an element of M.

$\notin$ $a \notin M$ means that a is not an element of M.

$\subseteq$ $N \subseteq M$ means that N is a subset of M.

$\subset$ $N \subset M$ means that N is a proper subset of M, namely that $N \subseteq M$ and $N \neq M$. (Note that often in the literature $N \subset M$ means that N is a subset of M. The usage is different from ours.)

$\not\subseteq$ $N \not\subseteq M$ means that N is not a subset of M.

$\cup, \cap$ Union and intersection, respectively. Namely, the union and the intersection of sets $M_1, \ldots, M_n$ are denoted by $M_1 \cup M_2 \cup \cdots \cup M_n$ (or $\cup_{i=1}^{n} M_i$) and $M_1 \cap M_2 \cap \cdots \cap M_n$ (or $\cap_{i=1}^{n} M_i$) respectively. If a family of sets M_λ is indexed by a set Λ, then the union and the intersection of these M_λ are denoted by $\cup_{\lambda \in \Lambda} M_\lambda$ (or, simply, $\cup_\lambda M_\lambda$ or $\cup M_\lambda$) and $\cap_{\lambda \in \Lambda} M$ (or, simply, $\cap_\lambda M_\lambda$ or $\cap M_\lambda$), respectively.

$\{ \mid \}$ When P is a condition and M is a set, the set of elements of M satisfying the condition P is denoted by $\{a \in M \mid P\}$ or simply by $\{a \mid P\}$.

$-$ When B is a subset of a set A, we denote by $A - B$ the

complement of B in A (i.e., $\{a \in A \mid a \notin B\}$).

$\times, \Pi$ The product of sets $M_1, \ldots, M_n$, i.e., $\{(a_1, \ldots, a_n) \mid a_i \in M_i\}$, is denoted by $M_1 \times M_2 \times \cdots \times M_n$. For a family of sets M_λ $(\lambda \in \Lambda)$, the product of these sets M_λ is denoted by $\Pi_{\lambda \in \Lambda} M_\lambda$.

N The set of natural numbers, i.e., $N = \{1,2,3,\ldots\}$.

0.1 MAPPINGS

A mapping f of a set M into a set N is a correspondence which associates with each element of M a single element of N. If n $(\in N)$ is associated with m $(\in M)$ (the circumstance is often expressed by $m \rightsquigarrow n$) by f, then n is called the image of m under f. In expressing images, two types of notation are commonly used. One is fm and the other is m^f. If M_1 is a subset of M, then $fM_1 = \{fm \mid m \in M_1\}$ or $M_1^f = \{m^f \mid m \in M_1\}$ is called the image of M_1 under f. If $fM = N$ or $M^f = N$, then we say that f is a mapping of M onto N and that f is surjective. For a subset N' of N, $\{x \in M \mid fx \in N' \text{ (or } x^f \in N')\}$ is called the inverse image of N' under f and is denoted by $f^{-1}(N')$. If, for $n \in N$, $f^{-1}(\{n\})$ consists of a single element m, then m is also called the inverse image of n under f and m is denoted by $f^{-1}n$ or $m^{f^{-1}}$. If f is surjective and if every element n of N has the inverse image, then the mapping f^{-1} is well defined, which is called the inverse of f. Note that this condition is that f gives a one-one correspondence.

The projection of the product set $M_1 \times M_2 \times \cdots \times M_n$ into M_i is defined by the correspondence $(a_1, \ldots, a_n) \rightsquigarrow a_i$. Projections in the case of the product of an infinite number of sets M_λ are defined similarly. Note that projections are surjective unless some M_λ is empty.

Assume that f is a mapping of a set M into a set N and that g is a mapping of the set N into a set P. Then the composition of these mappings is defined by associating with each element m of M the image under g of the image of m under f. In case we are

using notation of type m^f, the product (i.e., the result of the composition) of the mappings f and g is denoted by fg. In case we are using notation of type fm, the product is denoted by gf. The reason is that, under the notation, we have $(m^f)^g = m^{fg}$ and $g(fm) = (gf)m$.

For each set M, there is defined the cardinality of M, which is denoted by $\#(M)$. If M consists only of a finite number of elements, then M is called a finite set, and $\#(M)$ is the number of elements of M. [If M is the empty set, then $\#(M) = 0$.] The cardinality of the set N of natural numbers is said to be countably infinite. (Countable means finite or countably infinite.) The cardinality of the set of real numbers is called the cardinality of continuum. Multiplication of cardinalities is defined by $\#(M) \times \#(N) = \#(M \times N)$. In the case of finite cardinalities, the multiplication coincides with that of numbers. But, as for infinite cardinalities, the multiplication is quite different from the case of numbers; cf. Theorem 0.1.3 below. In general, we define that $\#(M) = \#(N)$ if and only if there is a one-one correspondence between M and N. We define also that $\#(M) \geq \#(N)$ if and only if there is a subset M' of M such that $\#(M') = \#(N)$. Hence $\#(M) > \#(N)$ means that $\#(M) \geq \#(N)$ and $\#(M) \neq \#(N)$. Under the definition, we see obviously that $\#(M) \geq \#(N)$ and $\#(N) \geq \#(L)$ imply $\#(M) \geq \#(L)$. Furthermore, the following theorem holds.

THEOREM 0.1.1 (Bernstein) If M and N are sets, then either $\#(M) \geq \#(N)$ or $\#(N) \geq \#(M)$. If both of these inequalities hold, then $\#(M) = \#(N)$.

Some other important theorems on cardinality are:

THEOREM 0.1.2 For an arbitrary set M, let $S(M)$ be the set of all subsets of M. Then it holds that

$$\#(S(M)) > \#(M)$$

If $\#(M)$ is countably infinite, then $\#(S(M))$ is the cardinality of continuum. In particular, the set of real numbers is not countable.

THEOREM 0.1.3 If M is an infinite set, then

$$\#(M) = \#(M \times M)$$

We omit the proofs of these results.

0.2 ORDERED SET

If a relation $\geq$ is defined on a set M (i.e., for each pair of elements a, b of M, it is well determined whether $a \geq b$ or not) and if the relation satisfies the following three conditions, then we say that $\geq$ is an order and that M is an ordered set:

(1) $a \geq a$ for every $a \in M$ (reflexive property).

(2) $a \geq b$, $b \geq a$ imply $a = b$ (asymmetric property).

(3) $a \geq b$, $b \geq c$ imply $a \geq c$ (transitive property).

$a > b$ means $a \geq b$ and $a \neq b$, and we say usually in such a case that a is larger (or greater) than b, or that b is smaller than a. $a < b$ (or $a \leq b$) means $b > a$ (or $b \geq a$, respectively). The notion of an ordered set is actually a pair of a set M and an order $\geq$ defined on it. Therefore, if a set M has two orders $\geq$ and $\propto$, then M with $\geq$ and M with $\propto$ are distinct from each other. Therefore in order to express that M is an ordered set with order $\geq$, we often say that $(M,\geq)$ is an ordered set.

For a set N, let $S(N)$ be the set of subsets of N. Then by the containment relation $\supseteq$, $(S(N),\supseteq)$ is an ordered set. When we deal with a subset of $S(N)$, we understand it as a subset of this ordered set.

Assume that $(M,\geq)$ is an ordered set. Then we can define another order $\propto$ on the same set M by defining

$$a \propto b \qquad \text{if and only if} \quad b \geq a$$

This new order is called the dual of the former.

We say that an ordered set $(M,\geq)$ is linearly ordered if for each pair of elements a, b of M, it holds either $a \geq b$ or $b \geq a$.

A subset of an ordered set is obviously an ordered set, and a subset of a linearly ordered set is a linearly ordered set.

Let S be a subset of an ordered set $(M,\geq)$, and let a be an

element of S. (i) If there is no b in S which is greater than a, then we say that a is a maximal element of S. (ii) If a is larger than any other elements of S, then we say that a is the largest (or greatest) element of S. An element y of M is called a lower bound of S if y is smaller than any element (except y in case y is in S) of S. If the set of lower bounds of S has the largest element, say z, then z is called the infimum of S and is denoted by inf S.

Considering the dual (hence, interchanging large and small), we define minimal elements, the smallest element, upper bound and the supremum of S. This last is denoted by sup S.

Note that S may not have any of minimal element, maximal element, infimum, supremum, etc. Even if S has the infimum, inf S may not be an element of S.

We say that the maximum condition (or the minimum condition) is satisfied by an ordered set M if every nonempty subset S of M has at least one maximal element (or minimal element, respectively). We say that the ascending chain condition holds in an ordered set $(M,\geq)$ if, for every ascending chain $a_1 \leq a_2 \leq \cdots \leq a_n \leq \cdots$ of infinite length in M, there is a natural number N such that $a_m = a_N$ for every $m > N$. This condition is equivalent to the statement that there is no properly ascending chain of infinite length in M. We define the descending chain condition in the dual way. Then we have:

THEOREM 0.2.1 The maximum conditon is equivalent to the ascending chain condition. Similarly, the descending chain condition is equivalent to the minimum condition.

PROOF: If there is a properly ascending chain $a_1 < a_2 < \cdots < a_n < \cdots$ of infinite length, then the set of all a_i has no maximal element. Conversely, if S is a nonempty subset which has no maximal element, then starting with an arbitrary element a_1 of S we have a properly ascending chain $a_1 < a_2 < \cdots < a_n$ of element of S. Then, since S has no maximal element, there is a_{n+1} $(\in S)$ which is larger than a_n. Thus we have such a chain of infinite length. This proves the theorem, taking account of the dual. QED

If the minimum condition holds in a linearly ordered set M, then we say that M is a well-ordered set and that the order of M is a well-order.

Let $(M_1,\geq), \ldots, (M_n,\geq)$ be ordered sets. Then we can define a new order $\geq$ in the product set $M_1 \times M_2 \times \cdots \times M_n$ as follows:

$(a_1,\ldots,a_n) > (b_1,\ldots,b_n)$ if and only if there is one i such that $a_i > b_i$ and such that, for every j smaller than i, it holds that $a_j = b_j$.

This new order is called the lexicographical order.

In closing this section, we recall a well-known and important theorem, the Zorn lemma. For this purpose, we define the notion of an inductive set to be a nonempty ordered set M in which every nonempty well-ordered subset S has the supremum $\sup S$ in M. Now:

ZORN LEMMA If M is an inductive set, then there is a maximal element of M.

0.3 CLASSIFICATION

A classification on a set M means to express M as a disjoint union of nonempty subsets C_λ (λ runs through a set Λ), namely, (i) $M = \cup_\lambda C_\lambda$, (ii) if $C_\lambda \cap C_\mu$ is not empty then $C_\lambda = C_\mu$, and (iii) each C_λ is not empty. Each C_λ is called a class, and if a belongs to C_λ then a is called a representative of C_λ.

If a relation $\equiv$ defined on a set M satisfies the following three conditions, then we say that $\equiv$ is an equivalence relation:

(1) $a \equiv a$ for every $a \in M$ (reflexive property).

(2) $a \equiv b$ implies $b \equiv a$ (symmetric property).

(3) $a \equiv b$, $b \equiv c$ imply $a \equiv c$ (transitive property).

As is well known, the notion of classification is closely related to that of equivalence relation. Namely,

THEOREM 0.3.1 Assume that a set M is the union of nonempty subsets C_λ ($\lambda \in \Lambda$). Define a relation $\equiv$ by that $a \equiv b$ if and only

if there is λ such that both a and b are in C_λ. Then the relation $\equiv$ is an equivalence relation if and only if these C_λ give a classification on M.

The proof is easy.

EXERCISE 0.2

1. (<u>(Mathematical) induction</u>) Let M be an ordered set satisfying the minimum condition. Assume that there is given a statement P_a for each element a of M. Then all P_a $(a \in M)$ are true if the following is true :

   If $a \in M$ and if P_b is true for every b such that $a > b \in M$, then P_a is true.

2. Let W be a well-ordered set and let $\{M_w \mid w \in W\}$ be a set of ordered sets indexed by W. Generalize the definition of the lexicographical order to the product set ΠM_w.

3. Let $M_1, \ldots, M_n$ be ordered sets and consider the lexicographical order on $M_1 \times \cdots \times M_n$.

   (i) Prove that if $M_1, \ldots, M_n$ are linearly ordered, then $M_1 \times \cdots \times M_n$ is also linearly ordered.

   (ii) Prove that if $M_1, \ldots, M_n$ are well-ordered, then $M_1 \times \cdots \times M_n$ is also well-ordered.

CHAPTER 1

GROUPS

In this chapter, we recall some basic notions on groups which we need later. We assume that the readers are familiar with some elementary properties of rational integers.†

1.1 GROUPS AND SEMIGROUPS

A binary operation, often simply called an operation, on a set M is a mapping ψ of the product set $M \times M$ into M. The operation is said to be commutative if $\psi(a,b) = \psi(b,a)$ for every $(a,b) \in M \times M$. A binary operation is often called either a multiplication or an addition. If ψ is called a multiplication, then $\psi(a,b)$ is called the product of a and b; it is quite common that $\psi(a,b)$ is denoted by ab in this case, and we follow the custom. If ψ is called an addition, then $\psi(a,b)$ is called the sum of a and b and is denoted by $a + b$; it is quite common to assume that an addition is commutative, and we follow this too.

A semigroup is a set G with a binary operation, say a multiplication, satisfying associativity, i.e.,

$$a(bc) = (ab)c \qquad \text{for arbitrary } a,b,c \in G$$

If a semigroup G has an element e such that $ea = ae = a$ for every $a \in G$, then such e is unique (see Proposition 1.1.1

† As we shall study later in Chap. 3, there is the notion of algebraic integers. Therefore, integers $0, \pm 1, \pm 2, \ldots$ are called rational integers.

below) and is called the identity of G; it is denoted by 1 or more explicitly by 1_G. Assume that a semigroup G has the identity. If, for an element a of G, there is an element a' such that $aa' = a'a = 1$, then such a' is unique (Proposition 1.1.1) and is called the inverse of a; it is denoted by a^{-1}. An element a of G having its inverse is called an invertible element of G.

A semigroup is called a group if (1) it is a semigroup with identity and (2) every element is invertible in the semigroup.

If the operation of a semigroup (or a group) is commutative, then the semigroup (or the group) is said to be commutative. A commutative group is sometimes called an abelian group.

If a set M is a group with addition $+$, then the identity is called zero, denoted by 0, and the inverse of an element a is called the minus of a and is denoted by $-a$. M itself is called a module or an additive group.

PROPOSITION 1.1.1 In a semigroup G with identity, there is only one identity; for each $a \in G$, the inverse a^{-1} is unique if it exists, and then $(a^{-1})^{-1} = a$.

PROOF: If $1'$ is another identity, the $1 = 11' = 1'$. If a' is another inverse of a, then $a^{-1} = a^{-1}(aa') = (a^{-1}a)a' = a'$. a is an inverse of a^{-1}, and hence $(a^{-1})^{-1} = a$. QED

If a subset H of a group G forms a group under the restriction of the operation of G to H, then we say that H is a subgroup of G. Submodules and subsemigroups are defined similarly.

If H_λ $(\lambda \in \Lambda)$ are subgroups of a group G, then the intersection of these H_λ is a subgroup. Therefore, when a subset S of a group G is given, the intersection D of all subgroups containing S is the smallest subgroup containing S. D is therefore called the group generated by S and is denoted by $\langle S \rangle$. If a subgroup H is generated by a subset S, then S is called a system of generators for H. A group generated by a single element is called a cyclic group. When H and K are subgroups of a group G, the subgroup generated by $H \cup K$ is denoted by $H \vee K$. Similar notation is employed for the subgroup generated by many subgroups.

THEOREM 1.1.2 For a nonempty subset H of a group G, each of the following two is necessary and sufficient for H to be a subgroup:

(1) $ab^{-1} \in H$ for arbitrary $a,b \in H$.

(2) $a^{-1}b \in H$ for arbitrary $a,b \in H$.

PROOF: Necessity is obvious. Assume that (1) holds good. Let $a \in H$. It holds that $a,a \in H$ which implies $1 = aa^{-1} \in H$ and then $1,a \in H$ which implies $a^{-1} \in H$. Now, if $a,b \in H$, then $a,b^{-1} \in H$; hence $ab = a(b^{-1})^{-1} \in H$. Sufficiency of (2) is similar. QED

If H, K are subsets of a group G, we denote by HK the set $\{hk \mid h \in H, k \in K\}$ (in case of an additive group, $H + K = \{h + k \mid h \in H, k \in K\}$). Hence, in particular, when H is a subgroup and a is an element of G, we denote by Ha the set $\{ha \mid h \in H\}$ and by aH the set $\{ah \mid h \in H\}$ (in the additive case, $H + a = \{h + a \mid h \in H\}$). Ha (or aH) is called the <u>right</u> (or <u>left</u>, respectively) <u>residue class</u> (or <u>coset</u>) of a <u>modulo</u> H. The set of all right (or left) residue classes of elements of G modulo H is denoted by $H\backslash G$ (or G/H, respectively).

PROPOSITION 1.1.3 Under the circumstances above,

(1) $aH = bH$ if and only if $b^{-1}a \in H$.

(2) $Ha = Hb$ if and only if $ab^{-1} \in H$.

(3) $aH \neq bH$ if and only if $aH \cap bH$ is empty.

(4) $Ha \neq Hb$ if and only if $Ha \cap Hb$ is empty.

PROOF: If $aH = bH$, then $a = bh$ with $h \in H$; hence $b^{-1}a \in H$. Conversely, if $b^{-1}a \in H$, then $a \in bH$ and $aH \subseteq bH$. Similarly, $bH \subseteq aH$ because $b = ah^{-1}$. (2) is similar. If $c \in aH \cap bH$, then by (1) we have $aH = cH = bH$. Since the converse is obvious, we have (3). (4) is similar. QED

The result stated above shows that G/H and $H\backslash G$ are giving classifications on G.

For a group G, $\#(G)$ is called the <u>order</u> of G. If $\#(G)$ is finite, we call G a <u>finite</u> group. For an element a of G, the order of the cyclic group $\langle a \rangle$ is called the <u>order</u> of the element a.