Translations of
MATHEMATICAL
MONOGRAPHS

Volume 125

Theory of Commutative Fields

Masayoshi Nagata

American Mathematical Society

Recent Titles in This Series

125 **Masayoshi Nagata,** Theory of commutative fields, 1993

124 **Masahisa Adachi,** Embeddings and immersions, 1993

123 **M. A. Akivis and B. A. Rosenfeld,** Élie Cartan (1869–1951), 1993

122 **Zhang Guan-Hou,** Theory of entire and meromorphic functions: Deficient and asymptotic values and singular directions, 1993

121 **I. B. Fesenko and S. V. Vostokov,** Local fields and their extensions: A constructive approach, 1993

120 **Takeyuki Hida and Masuyuki Hitsuda,** Gaussian processes, 1993

119 **M. V. Karasev and V. P. Maslov,** Nonlinear Poisson brackets. Geometry and quantization, 1993

118 **Kenkichi Iwasawa,** Algebraic functions, 1993

117 **Boris Zilber,** Uncountably categorical theories, 1993

116 **G. M. Fel′dman,** Arithmetic of probability distributions, and characterization problems on abelian groups, 1993

115 **Nikolai V. Ivanov,** Subgroups of Teichmüller modular groups, 1992

114 **Seizô Itô,** Diffusion equations, 1992

113 **Michail Zhitomirskiĭ,** Typical singularities of differential 1-forms and Pfaffian equations, 1992

112 **S. A. Lomov,** Introduction to the general theory of singular perturbations, 1992

111 **Simon Gindikin,** Tube domains and the Cauchy problem, 1992

110 **B. V. Shabat,** Introduction to complex analysis Part II. Functions of several variables, 1992

109 **Isao Miyadera,** Nonlinear semigroups, 1992

108 **Takeo Yokonuma,** Tensor spaces and exterior algebra, 1992

107 **B. M. Makarov, M. G. Goluzina, A. A. Lodkin, and A. N. Podkorytov,** Selected problems in real analysis, 1992

106 **G.-C. Wen,** Conformal mappings and boundary value problems, 1992

105 **D. R. Yafaev,** Mathematical scattering theory: General theory, 1992

104 **R. L. Dobrushin, R. Kotecký, and S. Shlosman,** Wulff construction: A global shape from local interaction, 1992

103 **A. K. Tsikh,** Multidimensional residues and their applications, 1992

102 **A. M. Il′in,** Matching of asymptotic expansions of solutions of boundary value problems, 1992

101 **Zhang Zhi-fen, Ding Tong-ren, Huang Wen-zao, and Dong Zhen-xi,** Qualitative theory of differential equations, 1992

100 **V. L. Popov,** Groups, generators, syzygies, and orbits in invariant theory, 1992

99 **Norio Shimakura,** Partial differential operators of elliptic type, 1992

98 **V. A. Vassiliev,** Complements of discriminants of smooth maps: Topology and applications, 1992

97 **Itiro Tamura,** Topology of foliations: An introduction, 1992

96 **A. I. Markushevich,** Introduction to the classical theory of Abelian functions, 1992

95 **Guangchang Dong,** Nonlinear partial differential equations of second order, 1991

94 **Yu. S. Il′yashenko,** Finiteness theorems for limit cycles, 1991

93 **A. T. Fomenko and A. A. Tuzhilin,** Elements of the geometry and topology of minimal surfaces in three-dimensional space, 1991

92 **E. M. Nikishin and V. N. Sorokin,** Rational approximations and orthogonality, 1991

91 **Mamoru Mimura and Hirosi Toda,** Topology of Lie groups, I and II, 1991

(Continued in the back of this publication)

This page intentionally left blank

Theory of Commutative Fields

This page intentionally left blank

10.1090/mmono/125

Translations of
MATHEMATICAL
MONOGRAPHS

Volume 125

Theory of Commutative Fields

Masayoshi Nagata

Translated by
Masayoshi Nagata

American Mathematical Society
Providence, Rhode Island

可換体論

KAKANTAI RON (Theory of Commutative Fields)
by Masayoshi Nagata

Translated from the Japanese by Masayoshi Nagata

1991 *Mathematics Subject Classification*. Primary 12-01;
Secondary 12D15, 12F10, 12F20.

Abstract. This book presents various topics in the theory of commutative fields. After some preliminaries on set theory, we study, in Chapter I, basic properties of groups, rings, and fields. Chapter II contains the theory of algebraic extensions of finite degree, including Galois theory. Transcendental extensions are investigated in Chapter III. The theory of valuations is explained in Chapter IV. The theory of ordered fields and topics related to Hilbert's 17th Problem are introduced in Chapter V. Additional topics including Galois theory of algebraic extensions of infinite degree are stated in the final chapter.

Library of Congress Cataloging-in-Publication Data

Nagata, Masayoshi, 1927–
[Kakantairon. English]
Theory of commutative fields/ Masayoshi Nagata: translated by Masayoshi Nagata.
p. cm.—(Translations of mathematical monographs; v. 125)
Includes bibliographical references and index.
ISBN 0-8218-4572-1
1. Fields, Algebraic 2. Commutative law (Mathematics) I. Title. II. Series.
QA247.N2613 1993 93-6503
512′.74–dc20 CIP

This publication was typeset using $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX,
the American Mathematical Society's TEX macro system.

10 9 8 7 6 5 4 3 2 1 98 97 96 95 94 93

Contents

This page intentionally left blank

Preface to the English Edition

The theory of commutative fields is one of the basic areas in mathematics, particularly in algebraic theories including number theory, algebra, and algebraic geometry. Many books relating to algebraic theories contain some exposition on commutative fields, but very few books contain sufficient material on this area.

The author wrote the first edition of this book in 1966 (in Japanese), with the aim of producing a useful book on commutative fields containing many topics. In view of the progress made in the theory of commutative fields, the author added several new topics and reformulated some results for the new Japanese edition that appeared in 1985.

The author wishes to express his thanks to the American Mathematical Society for publishing this English edition, which closely follows the 1985 edition mentioned above.

Masayoshi Nagata
September 1992

This page intentionally left blank

Preface to the New Japanese Edition

It has been 18 years since the manuscript of the original Japanese edition was completed. After its publication, the author noticed several points that should be improved. Because of this and in view of the length of time since the publication of the original edition, the author proposed to write a revision. The author wishes to express his thanks to the publisher for accepting this proposal.

The main goal of this new Japanese edition is the same as that of the original and can be stated in three parts.

(1) The prerequisites should be as few as possible. (The prerequisite results on set theory are stated in Chapter 0 without proofs.)

(2) All results considered by the author to be important and fundamental in the theory of commutative fields are included.

(3) Chapter I consists of the basic results on group theory and the theory of commutative rings that are needed to achieve the purpose stated in (2).

In this new Japanese edition, the author has improved several points in the first edition and added some new topics.

Masayoshi Nagata
March 1985

This page intentionally left blank

Preface to the Original Japanese Edition

The theory of commutative fields is fundamental in modern algebra. Due to the fact that algebraic methods are employed not only in algebra but also in a wide variety of areas, the theory of commutative fields has become one of the basic areas in modern mathematics.

However, because of the lack of sufficient time in courses for mathematics students in universities, teachers cannot devote enough time to the theory of commutative fields, and often they must end with a brief introduction to the theory of algebraic extensions of fields.

Thus, the author aimed in writing this book to provide a treatise for those who wish to study the theory of commutative fields on their own and a reference for those attending lectures on the theory of commutative fields.

To achieve these aims, the author tried especially to have the prerequisites be as few as possible; the reader is required to have a fundamental knowledge of set theory and some knowledge of determinants. (These prerequisites are stated in Chapter 0 without proofs.) To make this book self-contained, the author included fundamental results on groups and commutative rings.

Thus, the main part of this book consists of what the author judges to be fundamental in the theory of commutative fields, preceded by a preparatory part on groups and commutative rings.

For this reason, the presentation does not go more deeply into applications of commutative rings. In some cases where it seemed better, from the view point of commutative rings, to treat material under more general circumstances, the author chose to present the results under stronger conditions in order to simplify the presentation.

The author wishes to express his heartfelt thanks to several people for their help related to the writing and publishing of this book.

Masayoshi Nagata
December 1966

This page intentionally left blank

This page intentionally left blank

Answers and Hints

Chapter I

§**1. Exercise.** (1) $\binom{1\,2\,3\,4}{3\,4\,1\,2}$, (2) $\binom{1\,2\,3\,4}{3\,2\,1\,4}$, (3) $\binom{1\,2\,3\,4\,5}{3\,4\,5\,1\,2}$, (4) $\binom{1\,2\,3\,4\,5}{1\,2\,5\,3\,4}$.

§**7. Exercise.** When $H_1, \dots, H_r$ are submodules of a module G over a ring R, then the following is a necessary and sufficient condition for G to be the direct sum of $H_1, \dots, H_r$. $G = H_1 + \cdots + H_r$ and $(H_1 + \cdots + H_{i-1}) \cap H_i = \{0\}$ for $i = 2, \dots, r$.

Exercises

§1

2. Cf. exercise 1.2.4.
4. Symmetric group of degree 3.
7. Since $(ab)^m = b^m$, $\langle b^m \rangle = \langle b \rangle$, we have $\langle b \rangle \subseteq \langle ab \rangle$. Similarly, $\langle a \rangle \subseteq \langle ab \rangle$ and $\langle a, b \rangle \subseteq \langle ab \rangle$.
8. If $Z = \langle a \rangle$, $h = \#(Z)/q$, then the solutions of $x^q = 1$ in Z are a^h, $a^{2h}, \dots, a^{qh}$.

§2

9. Use exercise 1.2.8. Show that if G is solvable and N is a normal subgroup, then G/N is solvable. As for the solvability of N, consider $G_0 = G$, $G_i = [G_{i-1}, G_{i-1}]$, $N_0 = N$, $N_i = [N_{i-1}, N_{i-1}]$, then we can show $N_i \subseteq G_i$ by induction on i. Note that this proof can be applied to show that if N is a subgroup of a solvable group, then N is solvable.
10. The center $Z(G_1 \times \cdots \times G_n)$ of $G_1 \times \cdots \times G_n$ coincides with $Z(G_1) \times \cdots \times Z(G_n)$ and $(G_1 \times \cdots \times G_n)/Z(G_1 \times \cdots \times G_n) \cong (G_1/Z(G_1)) \times \cdots \times (G_n/Z(G_n))$.
11. If $\#(G/H) = 2$, then $\#(H\backslash G) = 2$; hence, $a \in G$, $a \notin H$ implies $G = H \cup Ha = H \cup aH$. Thus $aH = Ha$.
12. As for (1), use exercise 1.1.7. As for (2), use (1) and the hint.

§3

3. (1) (i) If I, J are ideals of a ring R, then $(I+J)(I \cap J) \subseteq IJ \subseteq I \cap J$.
(ii) $R = (I_1 + I_2)^2 \subseteq I_1^2 + I_2$ and $I_1^2 + I_2 = R$.
(2) Use (1) and an induction argument on n.

§4

2. The rational number field.

§5

1. (2) If $a, b, c, d \in R$, $a \neq 0$, $b \neq 0$, and $ab = 0$, then, setting $f = ax + c$, $g = bx + d$, we have $\deg fg \leq 1 < \deg f + \deg g$.
(3) $\deg(f_1 + f_2) \leq \max\{\deg f_1, \deg f_2\}$; if $\operatorname{def} f_1 \neq \deg f_2$, then $\deg(f_1 + f_2) = \max\{\deg f_1, \deg f_2\}$.

§6

4. See the proof of Theorem 1.6.4.

§7

2. $\mathbf{Z}/n\mathbf{Z}$ with a natural number n, or a module containing this as a submodule.
4. Cf. the Jordan-Hölder-Schreier theorem.
5. First take a composition series $R_i = R_{i0} \supset R_{i1} \supset \cdots \supset R_{ic(i)} = \{0\}$ of R_i-module R_i. Set $T_{ij} = R_{ij} + R_{i+1} + \cdots + R_n$ ($i = 1, 2, \ldots, n$; $j = 0, 1, \ldots, c(i)$). Then consider a refinement of $R = T_{10} \supset T_{11} \supset \cdots \supset T_{1c(1)} = T_{20} \supset \cdots \supset T_{2c(2)} = T_{30} \supset \cdots \supset T_{nc(n)} = \{0\}$.

REMARK 1. $\text{length}_S R_i = s_i c(i)$.

REMARK 2. By using T_{ij} as above, we can see that $\text{length}_R R = \sum c(i) = \sum \text{length}_{R_i} R_i$.

§8

1. The if part is obvious. As for the only if part, when τ, τ' are odd permutations, $\tau\tau'$, $\tau^{-1}\tau'$ are in A_n, and $\tau\tau' f = f$, $\tau f = \tau' f$. Thus, $g = f - \tau f$ is independent of τ, and $\tau g = \tau f - f = -g$. Hence, g is an alternating form. $h = f + \tau f$ is a symmetric form, and $f = (h/2) + (g/2)$.
6. g/f is expressed in the form k/h with h a symmetric form. Then k is also a symmetric form. If there is a common irreducible factor p, then the product of mutually distinct elements of $\{\sigma p | \sigma \in S_n\}$ is a common factor and k/h can be reduced. Here is another solution. $(\sigma g)/(\sigma f) = g/f$ (for all $\sigma \in S_n$), and we see that $\sigma f = c_\sigma f$, $\sigma g = c_\sigma g$ with $c_\sigma \in K$. For σ, $\tau \in S_n$, $c_{\sigma\tau} = c_\sigma c_\tau$. If σ is a transposition, then $c_\sigma = \pm 1$, which shows that either both of f, g are symmetric or alternating. The latter case is impossible by Theorem 1.8.2.

CHAPTER II. EXERCISES

§1

3. Cf. Theorem 2.1.4.
4. If $a \in M$, then there are $c_1, \dots, c_n \in L$, $a^n + c_{n-1}a^{n-1} + \cdots + c_n = 0$; hence, $[K(a, c_1, \dots, c_n) : K] = [K(a, c_1, \dots, c_n) : K(c_1, \dots, c_n)][K(c_1, \dots, c_n) : K] < \infty$. Thus, $K(a, c_1, \dots, c_n)$ is algebraic over K and every element of M is algebraic over K.
5. Cf. Theorem 2.1.3.

§2

1. (1) $\mathbf{Q}(\sqrt{5}, \sqrt{-3})$ [In finding the roots, the equality $x^4 - x^2 + 4 = (x^2 + 2)^2 - 5x^2$ is useful.] (2) $\mathbf{Q}(\sqrt{-3})$ (3) $(\mathbf{Q}(\sqrt{-3}, \sqrt[3]{2})$
2. (1) 4 (2) 2 (3) 6

§3

1. (1) It has a multiple root if the characteristic is 2 (1 is a 4-ple root); no multiple root otherwise. (2) It has a multiple root if the characteristic is 229 ($-4/3$ is a double root); no multiple root otherwise. (3) It has two double roots if the characteristic is 2 (square roots of two roots of $x^2 + x + 1$ are the double roots); one multiple root if the characteristic is 3 (1 is a 4-ple root); one double root if the characteristic is 139 (-7 is a double root); no multiple root otherwise. (4) No double root if $d \neq 0$; it has at least one multiple root of multiplicity $\geq p$, if $d = 0$.
3. Find a contradiction assuming that $t^{1/p} \in K(t)$.
6. If a is not separable, then the minimal polynomial for a is a polynomial in x^p, so (degree of a^p) $<$ (degree of a), and hence, $K(a^p) \neq K(a)$. Conversely, if $K(a^p) \neq K(a)$, then a is not separable over $K(a^p)$, and hence, a is not separable over K.

§4

1. Take $a \in \mathbf{Z}$ such that $a + p\mathbf{Z}$ is a generator of the cyclic group consisting of nonzero elements of $\mathbf{Z}/p\mathbf{Z}$ (such an a is called a *primitive root* modulo p). Then the order of $a + p^n\mathbf{Z}$ (in the multiplicative group U of invertible elements of $\mathbf{Z}/p^n\mathbf{Z}$) is a multiple of $p - 1$. Hence, there is an $\alpha \in U$ of order $p - 1$. Set $\beta = (p + 1) + p^n\mathbf{Z} \in U$. Then the order of β is p^{n-1}. Since $\#(U) = p^{n-1}(p - 1)$, we see that $\alpha\beta$ generates U. If $p = 2$, then the group is the direct product of the cyclic group (or order 2) consisting of the residue classes of 1, -1 and the cyclic group (or order 2^{n-2}) generated by the residue class of 5.
2. Use exercise 1.2.12.
3. We define multiplication on the set of 8 elements, the identity 1, i, j, k,

$-1, -i, -j, -k$, as follows: $i^2 = j^2 = k^2 = -1$, $i^3 = (-1)i = -i$, $j^3 = (-1)j = -j$, $k^3 = (-1)k = -k$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$. Then these 8 elements form a group, in which the solutions of $x^3 = 1$ are 1 and -1 only.

§5

1. Let t, u be algebraically independent elements over a field k_0 of characteristic $p \neq 0$, and consider $k = k_0(t, u)$ and pth roots $t^{p^{-1}}$, $u^{p^{-1}}$ of t, u. Then $k(t^{p^{-1}}, u^{p^{-1}})$ is an extension of degree p^2 over k, and is not a simple extension. For the proof, first show that the extension is of degree p^2, and then adapt the last part of the proof of Theorem 2.5.5. For the degree part, cf. the hint for exercise 2.3.3 in the cases:
   (i) Apply it to $k_0(t, u) = k_0(t)(u)$ and obtain $[k_0(t, u^{p-1}) : k_0(t, u)] = p$,
   (ii) Apply it to $k_0(t, u^{p^{-1}}) = k_0(u^{p^{-1}})(t)$ and obtain
   $$[k_0(t^{p^{-1}}, u^{p^{-1}}) : k_0(t, u^{p^{-1}})] = p.$$
2. Let $L = K(a)$, and consider the minimal polynomial $f(x) = \prod_{i=1}^{n}(x - a_i)$ for a. For each intermediate field M, the minimal polynomial $f_M(x)$ for a over M is a factor of $f(x)$, and the set S_M of roots of f_M is a subset of $\{a_1, \ldots, a_n\}$. If $M \neq M'$, then $S_M \neq S_{M'}$, and therefore, the number of intermediate fields $\leq$ (the number of nonempty subsets of $\{a_1, \ldots, a_n\}) = 2^n - 1$.

§6

1. (2) Let t, u be algebraically independent elements over a field k_0 of characteristic $p \neq 0$, and set $K = k_0(t, u)$. For simplicity, we assume that $p \neq 2$. Set $L_s = K(\sqrt{t})$ and $L = L_s((\sqrt{t} + u)^{p^{-1}})$. Then L_s is a Galois extension of K and L is purely inseparable over L_s. But $(-\sqrt{t} + u)^{p^{-1}}$ is a conjugate of $(\sqrt{t} + u)^{p^{-1}}$ over K and is not in L. Thus L is not normal over K.
3. Assume that $L = K(a)$ and that the minimal polynomial for a over K is $f(x) = \prod_{i=1}^{n}(x - a_i)$. Then the degree of a_i over $K(a_1, \ldots, a_{i-1})$ is at most $n - i + 1$.
5. (1) $\mathbf{Q}(\sqrt{2})$, $\{1, \sigma\}$ $(\sigma\sqrt{2} = -\sqrt{2})$.
   (2) $\mathbf{Q}(\sqrt{2}, \sqrt{3})$, $\{1, \sigma, \tau, \sigma\tau\}$ $(\sigma^2 = \tau^2 = 1$, $\sigma\tau = \tau\sigma$; $\sigma\sqrt{2} = -\sqrt{2}$, $\sigma\sqrt{3} = \sqrt{3}$, $\tau\sqrt{2} = \sqrt{2}$, $\tau\sqrt{3} = -\sqrt{3})$.
   (3) $\mathbf{Q}(\sqrt[3]{2}, \sqrt{-3})$, $\{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ $(\sigma^3 = 1$, $\tau^2 = 1$, $\tau\sigma\tau = \sigma^{-1}$; $\sigma\sqrt{-3} = \sqrt{-3}$, $\sigma(\sqrt[3]{2}) = \omega(\sqrt[3]{2})$ with $\omega = (-1 + \sqrt{-3})/2$, $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, $\tau\sqrt{-3} = -\sqrt{-3})$
   (4) $\mathbf{Q}(\sqrt[4]{2}, \sqrt{-1})$, $\{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$ $(\sigma^4 = 1$, $\tau^2 = 1$,

$\tau\sigma\tau = \sigma^{-1}$; $\sigma\sqrt{-1} = \sqrt{-1}$, $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}\cdot\sqrt{-1}$, $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$, $\tau\sqrt{-1} = -\sqrt{-1}$)

§7

1. (1) $\{1\}$. (2) See exercise 2.6.5, (4). (3) $\{1\}$ in the characteristic 2 case: $\{1, \sigma\}$ ($\sigma^2 = 1$, $\sigma x = -x$); otherwise. (4) If K has a root $\omega \neq 1$ of $x^3 - 1$, then $\{1, \sigma, \sigma^2\}$ ($\sigma^3 = 1$, $\sigma x = \omega x$); otherwise $\{1\}$.
2. (1) $\mathbf{Q}(\sqrt[3]{2})$. (2) $\mathbf{Q}$. (3) $K(x)$ in the characteristic 2 case; otherwise $K(x^2)$. (4) $K(x^3)$ if K has a root $\omega \neq 1$ of $x^3 - 1$; $K(x)$ otherwise.
3. If we consider the matrix of the transformation with base $b'_1, \dots, b'_n$ instead of $b_1, \dots, b_n$, it is of the form $A^{-1}\rho(a)A$ with a regular matrix A of degree n. Therefore, the trace and determinant of the transformation matrix do not change (the invariance of the trace follows from that the trace of $\rho(a)$ is (the coefficient of x^{n-1}) × $(-1)^{n-1}$ of $\det(\rho(a) - xE)$ (where E is the unit matrix)). Therefore, we can choose a base $b_1, \dots, b_n$ as follows. Let $x^r + c_1x^{r-1} + \cdots + c_r$ be the minimal polynomial for a over K and let $d_1, \dots, d_v$ be a linearly independent base of L over $K(a)$ $(rv = n)$. Now, let $b_1, \dots, b_n$ be 1, $a, \dots, a^{r-1}, d_1, d_1a, \dots, d_1a^{r-1}, \dots, d_ia^j, \dots, d_v, d_va, \dots, d_va^{r-1}$.

(5) In the case where L is separable over K, if $[L : K]$ is not a multiple of the characteristic p of K, then, with nonzero element b of K, we have $\mathrm{Tr}_{L/K}\, b = nb \neq 0$. So we consider the case where $[L : K]$ is a multiple of p. Take a such that $L = K(a)$, and let $f(x) = x^n + c_1x^{n-1} + \cdots + c_n$ be the minimal polynomial for a over K. The conjugates of a are $\sigma_1 a = a_1, \dots, \sigma_n a = a_n$. Since a is separable, there is one i such that c_i is not 0 and i is not a multiple of p. Let j be the smallest such i. Set $p_k = a_1^k + \cdots + a_n^k$ for $k \leq j$. Then, by the relationship between elementary symmetric forms $s_1 = -c_1$, $s_2 = c_2, \dots, s_n = (-1)^n c_n$ and p_k (see exercise 1.8.5), we see that $p_k = 0$ if $k < j$ and $p_j \neq 0$. (We have another proof by using Lemma 2.9.9.)

§8

1. The inseparable case is obvious. In the separable case, apply exercise 1.2.11 to the smallest Galois extension containing L.
2. (i) In the $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ case; the Galois group $G = \{1, \sigma, \tau, \kappa, \sigma\tau, \tau\kappa, \kappa\sigma, \sigma\tau\kappa\}$ is commutative and every element $\neq 1$ is of order 2. Therefore, there are 7 subgroups of order 2, and 7 subgroups of order 4. By adding the number of $\{1\}$, G, total number of subgroups, namely, the number of intermediate fields is $7 + 7 + 2 = 16$.

   (ii) In the $\mathbf{Q}(\omega\sqrt[3]{2})$ case, the Galois group is the symmetric group of degree 3, i.e., $\{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ ($\sigma^3 = 1$, $\tau^2 = 1$, $\tau\sigma\tau = \sigma^{-1}$). There are 3 subgroups of order 2 and there is only one subgroup of order

3. The total number of subgroups, namely, the number of intermediate fields is $3+1+2=6$.
(iii) In the $\mathbf{Q}(\sqrt[4]{2})$ case, the smallest Galois extension containing this field is $\mathbf{Q}(\sqrt[4]{2}, \sqrt{-1})$, whose Galois group G is $\{1, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$ ($\sigma^4 = 1$, $\tau^2 = 1$, $\tau\sigma\tau = \sigma^{-1}$; $\sigma(\sqrt{-1}) = \sqrt{-1}$, $\sigma(\sqrt[4]{2}) = \sqrt{-1}\cdot\sqrt[4]{2}$, $\tau(\sqrt{-1}) = -\sqrt{-1}$, $\tau(\sqrt[4]{2}) = \sqrt[4]{2}$). The subgroup H corresponding to $\mathbf{Q}(\sqrt[4]{2})$ is $\{1, \tau\}$. The subgroups containing H are H, G, and $\{1, \tau, \tau\sigma, \tau\sigma\tau\}$. Thus, the answer is 3.

§9

3. If we can prove this in the case $K = \mathbf{Q}$ (the rational number field), then the general case can be proved as in Theorem 2.9.4. The $K = \mathbf{Q}$ case follows from Theorem 2.9.5 and exercise 2.4.1. If $n = 2^s$ with natural number $s > 2$ and if $K = \mathbf{Q}$, then the extension is not cyclic.
4. Take a such that $L = K(a)$. Then $1, a, \dots, a^{n-1}$ form a linearly independent base of L over K. On the other hand, $\det(\sigma_i(a^j)) \neq 0$, because
$$\det\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix} = \prod_{i>j}(x_i - x_j).$$
6. (2) If $\sigma_1 u, \dots, \sigma_n u$ form a normal base, then $\sigma_1 u, \dots, \sigma_n u$ form a linearly independent base of L over K, and hence, $\det A \neq 0$ (cf. exercise 2.9.4). Conversely, if $\det A \neq 0$, then $\sigma_1 u, \dots, \sigma_n u$ form a linearly independent base; hence, $\sigma_1 u, \dots, \sigma_n u$ form a normal base. As for the existence of a normal base, see exercise 2.9.5.
7. (1) To prove the only if part, set $x_i = x\cdot(\sigma x)\cdots(\sigma^{i-1}x)$ ($i = 1, 2, \dots, n$). Then $\sigma x_i = x^{-1}x_{i+1}$ ($i < n$), $x_n = 1$, $\sigma x_n = 1 = x^{-1}x_1$. By Lemma 2.9.9, we see that $y = \sum x_i \sigma^i u \neq 0$ for some $u \in L$. Then $\sigma y = yx^{-1}$, $x = y/(\sigma y)$.

(2) To prove the only if part, set $x_i = x + \sigma x + \cdots + \sigma^{i-1}x$. Then $t = \sum \sigma^i u \neq 0$ for some $u \in L$. Set $z = \sum t^{-1}x_i\sigma^i u$. Then $z - \sigma z = \sum t^{-1}x_i\sigma^i u - \sum t^{-1}(x_{i+1} - x)\sigma^{i+1}u = x$.

§10

1. Use exercise 1.2.6.
3. (2) Let H_i be the subgroup of $G = G(L^*/K)$ that corresponds to K_i. Then $G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_r \supseteq \{1\}$ is a normal chain and $\bigcap_{a\in G} aH_r a^{-1} = \{1\}$. The solvability of G follows from this and the fact that H_i/H_{i-1} is a cyclic group for each i. An example of L^*, which is different from L, is obtained by taking $K = \mathbf{Q}$ (the rational number field), $L = \mathbf{Q}(\sqrt[4]{2}) = K_2$, $K_1 = \mathbf{Q}(\sqrt{2})$.

4. (1) The direct product of three cyclic groups of order 2.
(2) If $n = 2$, then it is a cyclic group of order 2. In the general case, let U_n be the group of invertible elements in $\mathbf{Z}/n\mathbf{Z}$ ($\mathbf{Z}$ being the ring of rational integers), and let $Z_n = \{1, b, \dots, b^{n-1}\}$ be the cyclic group of order n. Then the Galois group is isomorphic to the group generated by U_n and Z_n with defining relation $aba^{-1} = b^d$ if $a = d + n\mathbf{Z} \in U_n$.
(3) The symmetric group of degree 3. [The discriminant of the polynomial is 31, and therefore $\sqrt{31}$ = (the difference product of the roots) $\in$ the minimal splitting field. Hence, the Galois group cannot be the cyclic group of order 3. This fact and the irreducibility imply the answer.]
(4) The symmetric group of degree 3 by a similar reason as above.
(5) The cyclic group of order 2. [The minimal splitting field is $\mathbf{Q}(\omega)$ with an imaginary cubic root ω of unity.]
(6) The direct product of two cyclic groups of order 2. [The minimal splitting field is $\mathbf{Q}(\omega, \sqrt{-1}) = \mathbf{Q}(\sqrt{-1}, \sqrt{-3})$.]

§11

1. Use Theorem 2.11.5.
3. Consider a factor x^2+ax+b of x^4+x+1 with a, b in a splitting field. Then $x^4 + x + 1 = (x^2 + ax + b)(x^2 - ax + b^{-1})$; hence, $a^2 = b + b^{-1}$, $a^{-1} = b^{-1} - b$. Thus, $2b = a^2 - a^{-1}$, $2b^{-1} = a^2 + a^{-1}$ and therefore, $a^4 - a^{-2} = 4$, $a^6 - 4a^2 - 1 = 0$. This shows that the minimal polynomial for a^2 is $X^3 - 4X - 1$. Since a^2 is in the minimal splitting field, the order of the Galois group must be a multiple of 3.

§12

3. Take a natural number $n > 1$ and consider finite fields K_i such that $\#(K_i) = p^{n^i}$. Then $K_1 \subset K_2 \subset \cdots$, and $K = \bigcup_i K_i$ is a field such that $\#(K) = \infty$. Take a natural number $m > 1$ which is relatively prime to n, and let α be an element of degree m over π, then α is not in any K_i, consequently α is not in K. Thus, K is not algebraically closed.

Chapter III. Exercises

§2

3. To find a counterexample to (iv) implies (iii), take $L = K(\sqrt[n]{2})$, $M = K(\zeta \cdot \sqrt[n]{2})$ with the rational number field K, a primitive nth root ζ of unity and an odd number $n > 1$.

§3

2. One remark: It is not a right answer that, considering a prolongation D' of D to L, we take the restriction of D' to M, because $D'M \subseteq M$

may not be true.

If M has a separating transcendence base, then the existence of the required prolongation is obvious. So, the characteristic 0 case is finished, and we assume that the characteristic is $p \neq 0$. In general, if we fix a p-base B, then there is a one-to-one correspondence between derivations of L and elements of $\mathrm{Hom}_{\mathrm{set}}(B, L)$ (the set of mappings of B to L). Now, we choose B so that $L^p(K) = L^p(K \cap B)$, $L^p(M) = L^p(M \cap B)$. We define a prolongation D' of D by letting $D'b$ be Db if $b \in K \cap B$ and any element of M otherwise.

§4

2. We can reduce the problem to the case where L_1, L_2 are finitely generated. Then we can use separating transcendence bases.
3. $[K_1 : K] \leq i(L/K)$ is easy by considering $L \otimes_K K_1$. $i(L/K) \leq [L : K(x_1, \dots, x_n)]_i$ follows from Theorem 3.4.3 and the fact that $[L(K^{p^{-\infty}}) : K^{p^{-\infty}}(x_1, \dots, x_n)] \geq [L : K(x_1, \dots, x_n)]_s$. For this last fact, use Theorem 2.7.3, (ii).

§5

2. To prove sufficiency, note that L is separable because $L \otimes_K L'$ is an integral domain for any purely inseparable extension L'. K is algebraically closed in L, because $L \otimes_K L'$ is an integral domain even when L' is separable over K. Cf. Theorem 3.5.2, (ii).
3. Use Corollary 3.4.5. (and Theorem 3.5.2, (ii)).
4. Use exercise 3.2.2.

§6

3. (i) For a counterexample, let x, y be algebraically independent elements over a field K, and set $R = K[x, y, y/x, y/x^2, \dots, y/x^n, \dots]$. Then, $y, y/x, \dots \in xR = I$, and $R/I \cong K$. (ii) For $(*)$ in the case $I^n = \{0\}$, we shall show that R/I^s is Noetherian by induction on s. It is so if $s = 1$, and we assume that $s > 1$. Let J be an ideal of R/I^s and let ϕ be the natural homomorphism of R/I^s to R/I^{s-1}. Then by our induction hypothesis, $J' = \phi J$ is finitely generated, and there exist $b_1, \dots, b_t \in J$, $J' = \sum \phi(b_i)(R/I^{s-1})$. Then $J = \sum b_i(R/I^s) + (J \cap (I^{s-1}/I^s))$. Since I^{s-1}/I^s is finitely generated as an R/I-module, its submodule $J \cap (I^{s-1}/I^s)$ is finitely generated. Thus, J is finitely generated.
4. I is not a primary ideal, because $xy \in I$, $x \notin I$, $y^n \notin I$ for all n.
5. M/I is the unique prime ideal of R/I. Hence, $x \notin M$ $(x \in R)$ implies $x \bmod I$ is invertible in R/I.
6. Let $I = Q_1 \cap \cdots \cap Q_n$ be a shortest expression of I as an intersection of primary ideals. For the only if part, $P = \sqrt{Q_1}$ implies there is $c \in$

$Q_2 \cap \cdots \cap Q_n$, $c \notin Q_1$. Then, $I : c = Q_1 : c$ and $\sqrt{(Q_1 : c)} = P$. Take d such that $d \in (Q_1 : c) : P$, but $d \notin Q_1 : c$. Then take $b = cd$. For the if part, $I : b = \bigcap(Q_i : b)$ and there exists i, $P = Q_i : b$.

7. (iii) For the only if part, take a set of generators $f_1, \dots, f_m$ of the ideal $M = \sum_{i=1}^{\infty} R_i$ such that every f_i is homogeneous. We show $R_j \subseteq R_0[f_1, \dots, f_m]$ by induction on j. This is obvious if $j = 0$. Assume that $j > 0$. $g \in R_j$ implies $g \in M \Rightarrow g = \sum f_i g_i$ with g_i homogeneous. Since $\deg g_i = j - (\deg f_i) < j$, we have $g_i \in R_0[f_1, \dots, f_m]$ and $g \in R_0[f_1, \dots, f_m]$.

   (iv) For the if part, we show that $f_i \in R_i$, $g_j \in R_j$, $(\sum_{i=c}^{c+s} f_i)(\sum_{j=d}^{d+t} g_j) \in Q$, $\sum f_i \notin P$ implies $\sum g_j \in Q$ by a double induction on s and t. Note that we may disregard those g_j which are in Q. The $s = 0$ case is easy, because $f_c g_j$ are in Q. The $t = 0$ case is similar. So, we assume that $s > 0$, $t > 0$. Since $f_c g_d \in Q$, $\sum_{j=d+1}^{d+t} f_c g_j \equiv \sum_{j=d}^{d+t} f_c g_j$ (mod Q). This implies that $(\sum_i f_i)(\sum_{j=d+1}^{d+t} f_c g_j) \in Q$. By our induction on t, we have $\sum_{j=d+1}^{d+t} f_c g_j \in Q$, which shows that each $f_c g_j \in Q$; hence $(\sum_{i=c+1}^{c+s} f_i)(\sum_{j=d}^{d+t} g_t) \in Q$. If $f_c \in P$, then we can use this last relation and an induction on s; otherwise, that $f_c g_j \in Q$ for every j.

   (v) Using the result (iv), adapt our proof of Theorem 3.6.10.

§7

1. If a prime ideal P of S contains I, then there is a P', a prime ideal of R, such that $P' \cap S = P$. Applying this to P such that $\operatorname{ht} I = \operatorname{ht} P$, we have $\operatorname{ht} I = \operatorname{ht} P = \operatorname{ht} P' \geq \operatorname{ht} IR$. Conversely, since $I \subseteq IR \cap S$, we have $\operatorname{ht} IR = \operatorname{ht}(IR \cap S) \geq \operatorname{ht} I$.
2. Take a prime ideal P_0' of height 0 and contained in P_n'. Then apply Theorem 3.7.12 to R/P_0'.
5. For the first half, $X^2 - 2$ is irreducible over $\mathbf{Z}[2\sqrt{2}]$. But $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ over its field of fractions. For the latter half, if $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$ with integral elements α_i over R and if $f = g(X)h(X)$ with monic polynomials g, h over its field of fractions, then the coefficients of g, h are integral over R, because they are expressed as polynomials in α_i.
6. For the first half, if $f(x) = (a_0 x^m + \cdots + a_m)(b_0 x^{n-m} + \cdots + b_{n-m})$ with $n > m > 0$, then $a_1, \dots, a_m, b_1, \dots, b_{n-m}$ are in pR, because $f(x) \equiv c_0 x^n (\bmod\ p)$. Then $c_n = a_m b_{n-m} \in p^2 R$, a contradiction.

§8

1. For the last part, we can choose $z_1, \dots, z_t$ from linear combinations of $a_1, \dots, a_n$ with coefficients in K.
2. For the first half, assume that $P \neq aR$. $x \in P$ implies $x = ax_1$ (for some $x_1 \in R$), so $x_1 \in P$ (because $a \notin P$). Thus, $P = aP$, and

$x = a^n x_n$ $(x_{n-1} = ax_n)$ (for some $x_n \in R$). $x_1R \subseteq x_2R \subseteq \cdots$ and for some m, $x_mR = x_{m+1}R$. Then $x_m = ax_{m+1} = ax_m z$ (for some $z \in R$) and $x_m(1-az) = 0$. Since $aR \neq R$, $1-az \neq 0$, and therefore, $x_m = 0$. Thus, $x = 0$. For the latter half, if $a = p_1 \cdots p_m$ with prime elements p_i, then there exists an i for which $p_i \in P$ and $P = p_iK[X_1, \dots, X_n]$.

3. It is advised to start with the latter half. If P is a maximal ideal, then consider the field $K[X_1, \dots, X_n]/P$. Let a_i be the residue class of X_i modulo P and set $K_i = K(a_1, \dots, a_{i-1})$. Let $f_i(X)$ be the minimal polynomial for a_i over K_i and let $g_i(X_1, \dots, X_i)$ be the monic polynomial in X_i obtained from f_i by replacing coefficients by their representatives in $K[X_1, \dots, X_{i-1}]$ and X by X_i. Then P is generated by $g_1, \dots, g_n$. For the first half, we can assume that $r > 0$. Let $Y_1, \dots, Y_n$ be the elements obtained by applying Theorem 3.8.2 to $K[X]$ and P. Then $K[X] = K[X_1, \dots, X_r, Y_{r+1}, \dots, Y_n]$ and $PK(Y_{r+1}, \dots Y_n)[X_1, \dots, X_r]$ is a maximal ideal. We apply the latter half to this maximal ideal.
4. If I' is a prime ideal, then $\operatorname{trans.deg}_K R'/I' = \operatorname{trans.deg}_K R/(I' \cap R)$, which implies $\operatorname{ht} I' = \operatorname{ht}(I' \cap R)$. In the general case, we can adapt our proof of Corollary 3.7.3.

§9

1. $R[h] \subseteq a^{-1}R$ and $a^{-1}R$ is a finitely generated R-module.

§10

1. For the first half, use the zero-point theorem of Hilbert and the fact that $V(I(A_1) + I(A_2)) = A_1 \cap A_2$. For the last part, consider the polynomial ring $P = \mathbf{R}[x_1, \dots, x_n]$ $(n \geq 2)$ over the real number field $\mathbf{R}$. Then, with $A_1 = V(x_1)$, $A_2 = V(-x_1^2 + \sum_{i=2}^n x_i^2 + 1)$, we have $I(A_1) + I(A_2) = x_1P + (\sum_{i=2}^n x_i^2 + 1)P = \sqrt{I(A_1) + I(A_2)}$, but $A_1 \cap A_2$ is empty.
2. Let W be a component of $V \cap H$, and let h be an element which defines H. We apply Theorem 3.8.7 to $\Omega[X_1, \dots, X_n]/I(V)$, and we have $\operatorname{ht} I(W)/I(V) \leq 1$, because $I(W)/I(V)$ is a minimal prime divisor of the principal ideal generated by h modulo $I(V)$. Hence, $\operatorname{ht} I(W) \leq \operatorname{ht} I(V) + 1$ by Corollary 3.8.5.
4. (i) It has sufficiently many points in $\mathbf{R}$ if $r > 0$. If $r = 0$, then there is no $\mathbf{R}$-rational point. (ii) It has sufficiently many points in $\mathbf{R}$.

§11

1. Consider $x_1^2 + \cdots + x_n^2$.
2. Set $K = \mathbf{R}(t_1, \dots, t_i)$ and $L = \mathbf{C}(t_1, \dots, t_i)$ with algebraically independent elements $t_1, \dots, t_i$ over the real number field $\mathbf{R}$. Here $\mathbf{C}$ denotes the complex number field. K is not a C_n-field for any n and L is a C_i-field but not a C_{i-1}-field.

§12

1. Use exercise 3.12.1.
2. For the only if part, if (p, q) is a K-rational point, then $K(x, y) = K(t)$ with $t = (x-p)/(y-q)$. (Indeed, $x = p+t(y-q)$; hence, $a(p+t(y-q))^2 + by^2 = c = ap^2 + bq^2$. From this relation, we have $y \in K(t)$.) If (p, q) with $p \neq 0$ is a nontrivial solution of $ax^2 + by^2 = 0$, then $(qp^{-1}, 0)$ is a nontrivial solution of $a + bY^2 = cz^2$ (with $x = z^{-1}$, $y = xY$), we see the existence of similar t and $K(z, Y) = K(x, y)$. For the if part, assume that $x = f(t)/g(t)$, $y = h(t)/k(t)$ with polynomials f, g, h, k. If for some $p \in K$, $g(p) \neq 0$, $k(p) \neq 0$, then $(f(p)/g(p), h(p)/k(p))$ is a K-rational point. In the other case, factor g, k as $g(t) = t^s g_1(t)$, $k(t) = t^u k_1(t)$ with g_1, k_1 such that $g_1(0)$, $k_1(0)$ are different from 0. We can assume that $s \geq u > 0$ (> 0 follows from the nonexistence of p). Then $f(0) \neq 0$ and $a(f(t)/g_1(t))^2 + b(t^{s-u}h(t)/k_1(t))^2 = ct^s$. By setting $t = 0$, we have a nontrivial solution for $ax^2 + by^2 = 0$.

REMARK. The proof above shows that if $\#(K)$ is infinite, then $ax^2+by^2 = c$ has a K-rational point iff for some $t \in L$. $L = K(t)$.

3. Use the preceeding exercise and the fact that $K(z)$ is a C_1-field. (Consider the homogeneous form $f_1(z)X^2 + f_2(z)Y^2 - f_3(z)U^2$ in X, Y, U.)

§A

1. Take a valuation ring V_x of $K(x_1, \dots, x_r)$ containing K and such that V_x has prime ideals $P_1 \supset P_2 \supset \cdots \supset P_r \supset \{0\}$ with the property that $P_1 = x_i(V_x)_{P_i}$ for each i. Then adapt Lemma 3.A.2, considering $V_x \cap K'(x_1, \dots, x_{r-1})$.
2. Here is a proof of the theorem stated in the hint. If $n = r$, then there is nothing to prove. Assume that $n > r$. We use the normalization theorem for polynomial rings using exercise 3.8.1, and we see that there are linear combinations $y_1, \dots, y_{n-r}$ of $x_1, \dots, x_n$ with coefficients in K such that $L[x_1, \dots, x_n]$ is integral over $L[y_1, \dots, y_{n-r}]$. Choose $a_1, \dots, a_s \in L$ such that $L = K(a_1, \dots, a_s)$. Then, $x_1, \dots, x_n$ are integral over $K[a_1, \dots, a_s, y_1, \dots, y_{n-r}]$. There is $c \in K$ such that, when we write $a_1, \dots, a_s$ in fractional forms of $x_1, \dots, x_n$, no denominator is divisible by $y_1 - c$. Consider the ring $V = K[x_1, \dots, x_n]_{(y_1-c)K[x_1, \dots, x_n]}$. Since $a_1 \in V$, V contains $K[a_1, \dots, a_s, x_1, \dots, x_n]$. Set $P = (y_1 - c)V \cap K[a_1, \dots, a_s, x_1, \dots, x_n]$ and $Q = (y_1 - c)V \cap K[a_1, \dots, a_s, y_1, \dots, y_{n-r}]$. Since the field of fractions of $R = K[a_1, \dots, a_s, x_1, \dots, x_n]/P$ is $V/(y_1 - c)V$, we see that $\operatorname{trans.deg}_K R = n - 1$. R is integral over $S = K[a_1, \dots, a_s, y_1, \dots, y_{n-r}]$ and $\operatorname{trans.deg}_K S = n - 1$. Now for $T = K[a_1, \dots, a_s]/(Q \cap K[a_1, \dots, a_s])$, $\operatorname{trans.deg}_K T \geq (n - 1) - (n - r - 1)$, because $y_1 - c \in Q$. But, $\operatorname{trans.deg}_K K[a_1, \dots, a_s] = \operatorname{trans.deg}_K L = r$, and

we have $Q \cap K[a_1, \dots, a_s] = \{0\}$. Thus, L is regarded as a subfield of $V/(y_1 - c)V \cong K(x_1, \dots, x_{n-1})$.

Chapter IV. Exercises

§1

1. (i) $a \geq 1$. (ii) $c = 1$. (iii) $c \geq 0$.
2. If a is a nonzero element, then there is a natural number n such that $a^n = 1$.

§2

1. Similar to the proof of Theorem 4.2.1, (ii).
2. (ii) Assume that $a^n + c_1a^{n-1} + \dots + c_n = 0$, $v(c_i) \leq 1$. If $va > 1$, then $v(a^n) > v(c_ia^{n-i})$ and $0 = v(a^n + c_1a^{n-1} + \dots + c_n) = v(a^n) > 1$, which is a contradiction.

§3

1. (i) Let M be a set with at least two elements and let open sets on M be only the empty set and M itself.

   (ii) With M as above, let the open sets on M be M itself and all subsets not containing a fixed element a.

   (iii) Let M be a set containing infinitely many elements and define that a subset S is an open set iff either S is the empty set or the complement of S consists of a finite number of elements.

   (iv) We fix a line L and a point A which is not on L, on the Euclidean plane P. Then, a new topology is defined on P by letting the following family C of subsets be a subbase of open sets. $C = B_1 \cup B_2 \cup B_3$, where $B_1 = \{\{x\} | x \in P,\ x \neq A,\ x \notin L\}$, $B_2 = \{U | U$ is an open set in the usual topology not containing $A\}$, $B_3 = \{P - (L \cup U) | U$ is the union of a finite number of circular disks$\}$. Then L is a closed set, and there is no pair of neighborhoods of L and of A separating each other.

   (v) On the plane P, we set $U(a, b, \varepsilon, \delta) = \{(x, y) \in P | a \leq x < a + \varepsilon,\ b \leq y < b + \delta\}$ with real numbers $a, b, \varepsilon, \delta$. We define a new topology on P by letting the family of all of such $U(a, b, \varepsilon, \delta)$ be a subbase of open sets. Then, on the line $L : y = -x$, the set E_1 of rational points (i.e., $E_1 = \{(a, -a) | a$ is a rational number$\}$) and the set E_2 of irrational points (i.e., $E_2 = L - E_1$) are closed sets. But there is no pair of neighborhoods of E_1 and of E_2 separating each other.
4. Use exercise 4.3.3.

§4

2. The space is not a T_1-space. Indeed, there is $P \in G$, such that $P \notin H$, and any neighborhood $U(P)$ of P meets H. This implies that any

neighborhood of $f(P)$ contains the identity element.

3. Consider the two-dimensional vector space $V = \{(a, b) | a, b \in \mathbf{R}\}$ over the real number field $\mathbf{R}$. This is a topological group under the usual topology (as a Euclidean space). $H = \{(0, b) | b \in \mathbf{R}\}$ is a closed normal subgroup. Then the mapping f defined by $f(a, b) = a$ is the one as stated. $F = \{(a, b) | 0 < a < 1, \ b = a^{-1}(1-a)^{-1}\}$ is a closed subset of V, but fF is not a closed set.
4. Each $sU = \{su | u \in U\}$ is an open set.

§5

3. (i) $a, b \in R$, $a-b \in \pi^s R$ $(s \geq 1)$ imply $a^p - b^p \in \pi^{s+1}R$, and therefore, $a^{p^n} - b^{p^n} \in \pi^{s+n}R$.

   (ii) If we take a_n, b_n for $\bar{a}$, $\bar{b} \in R/\pi R$, as in (i), then $a_n b_n$ is a representative of $(\bar{a}\bar{b})^{p^{-n}}$.

   (iii) is easy.

   (iv) is difficult, and the reader is advised to see some book, for instance, N. Jacobson, *Lectures on abstract algebra*, III.

REMARK. In general, Witt vectors and Witt rings are defined over an arbitrary commutative ring K with f_m, g_m in (iv), which define the addition and multiplication. It is known that the Witt ring of length infinity is a valuation ring if and only if K is a perfect field.

4. Show that $m_i = \sum_{j=1}^{n} a_{ij}u_j$ $(a_{ij} \in K)$ $(i = 1, 2, \ldots)$ form a Cauchy sequence which converges to 0 iff a_{ij} $(i = 1, 2, \ldots)$ form a Cauchy sequence which converges to 0, for each $j = 1, \ldots, n$. The if part follows from $\|\sum b_j u_j\| \leq \sum \|b_j u_j\| = \sum v(b_j)\|u_j\|$ (note that the inequality follows from the fact that M is a metric space). For the only if part, use an induction argument on n. Assume that $a_{11}, \ldots, a_{n1}, \ldots$ is not a Cauchy sequence converging to 0. Then there is a positive number ε such that $v(a_{i1}) \geq \varepsilon$ for infinitely many i. Choosing a suitable subsequence of $\{m_i\}$, we may assume that $v(a_{i1}) \geq \varepsilon$ for all i. Then $\{a_{i1}^{-1}m_i\}$ is a Cauchy sequence converging to 0, where the coefficient of u_1 in each term is 1. Thus, we may assume that $a_{11} = a_{21} = \cdots = 1$. Let $t(i)$ be natural numbers such that $t(1) < t(2) < \cdots$. Then $d_i = m_{t(i)} - m_i \in \sum_{j=2}^{n} Ku_j$, and $\{d_i\}$ is a Cauchy sequence converging to 0. Therefore, by our induction hypothesis, $\{c_{ij} = a_{t(i)j} - a_{ij} | i = 1, 2, \ldots\}$ is a Cauchy sequence converging to 0 for each $j \geq 2$. It follows now that $\{a_{ij} | i = 1, 2, \ldots\}$ is a Cauchy sequence. Set $a_j^* = \lim_{i\to\infty} a_{ij}$. Then $u_1 + a_2^*u_2 + \cdots + a_n^*u_n = \lim_{i\to\infty} m_i = 0$, which contradicts the linear independence of $u_1, \ldots, u_n$.

§6

1. Let B be a transcendence base of $\mathbf{C}$ over $\mathbf{Q}$. Since $\#(B)$ is infinite,

$\mathbf{Q}(B) \cong \mathbf{Q}(B, t)$. Hence, there is an injection of $\mathbf{C}(t)$ to $\mathbf{C}$.

2. Either its cardinality is greater than the cardinality of continuum or the characteristic is different from 0.

§7

1. Let R be such a valuation ring, and let P be a nonmaximal, nonzero prime ideal. Let $0 \neq a \in P$, and let b be an element of the maximal ideal that is not in P. Then $b^{-n}a \in R$ and $aR \subset b^{-1}aR \subset \cdots \subset b^{-n}aR \subset b^{-n-1}aR \subset \cdots$.
2. The intersection of integrally closed integral domains is an integrally closed integral domain.
3. $a - b \in P$ iff $a > b$.
4. For the first half, use Theorem 4.7.2, (vi) and the fact that $R \subseteq S \cap K \subseteq K$. For the latter half, show that if P is a prime ideal of R, then $\sqrt{PS} \cap R = P$.
6. Consider $P = \{a | va > h$ for all $h \in H\}$ for an isolated subgroup H.
7. (i) Use exercise 4.7.1 for the only if part.

(ii) For the only if part; take $a_i \in P_i$ such that $a_iR_{P_i} = P_iR_{P_i}$. For each element b of the field of fractions of R, let $m_1, \dots, m_n$ be the integers such that $bR_{P_i} = a_1^{m_1} \cdots a_i^{m_i} R_{P_i}$ $(i = 1, \dots, n)$. Then the mapping $wb \to (m_1, \dots, m_n)$ gives the required isomorphism.

8. (i) Use an induction argument on n. Let w_1 be the valuation defined by R_{P_1}. Let B be a subset of P_1 such that $\{w_1b | b \in B\}$ is maximal among linearly independent subsets of $w_1(P_1)$ over $\mathbf{Q}$. Consider the valuation v defined by R/P_1. Our induction hypothesis shows that there is an order isomorphism ϕ_1 from the value group of v into the $(n-1)$-ple direct sum $\mathbf{R} \oplus \cdots \oplus \mathbf{R}$. Then we define ϕ as follows. Let x be a nonzero element of K. Since w_1x is linearly dependent on $\{w_1b | b \in B\}$, there is a natural number m such $w_1(x^m) = w_1(b_1^{i_1} \cdots b_s^{i_s})$ with $b_i \in B$. Now $\phi(wx) = (w_1(b_1^{i_1} \cdots b_s^{i_s})/m, \ \phi_1(v(x^m/b_1^{i_1} \cdots b_s^{i_s}$ modulo $P_1))/m)$.
9. It suffices to show that $x_1, \dots, x_m$ $(\in R)$ are algebraically independent if (i) $wx_1 = \cdots = wx_r = 0$ and $x_1 \bmod P, \dots, x_r \bmod P$ are algebraically independent over k and if (ii) $wx_{r+1}, \dots, wx_m$ are linearly independent over the rational number field. Assume for a moment that $\sum c_{i_1 \cdots i_m} x_1^{i_1} \cdots x_m^{i_m} = 0$ $(c_{i_1 \cdots i_m} \in k)$. Denote by $\sum_* c_{i_1 \cdots i_m} x_1^{i_1} \cdots x_m^{i_m}$ the partial sum on the terms such that $w(c_{i_1 \cdots i_m} x_1^{i_1} \cdots x_m^{i_m})$ is the least. Then we have a contradiction from $w(\sum_* c_{i_1 \cdots i_m} x_1^{i_1} \cdots x_m^{i_m}) > w$ (one term in this partial sum) (this inequality follows from the fact that $wa < wb$ implies $w(a + b) = wa$).

§8

1. If $i \neq j$, then $R_i[R_j] = K$. (In this case, we say that $R_1, \dots, R_n$ (or,

$v_1, \dots, v_n$) are *independent* of each other.)

§9

1. We fix an algebraically closed field Ω of characteristic 0 with sufficiently large cardinality. Consider a subfield M which has a discrete valuation v_M such that p generates the maximal ideal of the valuation ring R_M of v_M and such that there is a homomorphism ϕ_M from R_M to K whose kernel is pR_M. Let F be the set of all such (M, v_M, ϕ_M). We introduce an order $\geq$ on F by $(M, v_M, \phi_M) \geq (M', v_{M'}, \phi_{M'})$ iff $M \supseteq M'$, v_M is a prolongation of $v_{M'}$, and ϕ_M is a prolongation of $\phi_{M'}$. Then F is an inductive set and has a maximal member $(M^*, v_{M^*}, \phi_{M^*})$. Then the residue class field of v_{M^*} is isomorphic to K. Hence, the completion of v_{M^*} is the required one.

§10

1. Show, on the one hand, that we have a contradiction if there is a $v \in V_L$ such that no member of V' is equivalent to v. Show, on the other hand, if $V' = \{v^{t(v)} | v \in V_L\}$ contains v_1, v_2 such that $t(v_1) \neq t(v_2)$, then since the product formula holds with respect to $\{v^{t(v_1)} | v \in V_L\}$, we obtain another V' with no member equivalent to v_1.

§11

3. Adapt the proof of Theorem 4.11.5.
4. (i) Use Theorem 4.11.13.

(ii) Theorem 4.11.13 shows that such a valuation ring R' contains $R = K[[X]]$ or is contained in R. If R' contains R properly, then $R' = K((X))$. R', in the latter case, is obtained as $\{a_0 + a_1 X | a_0 \in R_0, a_1 \in R\}$ with a Hensel valuation ring R_0 of K.

Chapter V. Exercises

§1

1. When $b > 0$, $d > 0$, we have $a/b \geq c/d$ iff $ad \geq bc$.
3. $1 > 0$ because $1^2 = 1$. Consequently, every natural number > 0.
4. Cf. the proof of Theorem 4.7.5.
5. (i) $x \in K$, $a \in L$, $a > x < 0$ implies $x \in R$.

   (ii) $(a + P) < (b + P)$ implies there is a $d \in L$ such that $b - a > d > 0$.
7. Use Exercise 5.1.6.

§2

1. Cf. Theorem 5.2.9.
4. For the first half, let L and K be the real number field and $\mathbf{Q}(\sqrt{2})$ ($\mathbf{Q}$

being the rational number field). Let K be an ordered field with an order such that $\sqrt{2} < 0$.

§4

2. Adapt the proof of Theorem 5.4.2.

Chapter VI. Exercises

§3

2. Let x, y be algebraically independent elements over a field k of characteristic $\neq 3$, and set $K = k(x, y)$, $R = k[x, y]$. Let z be an algebraic element over K defined by $z^2+xz+y = 0$, and set $L = K(z) = k(x, z)$, $R_L = k[x, y, z] = k[x, z]$.
   (i) $P = (x-1)R_L$, $P' = (x-1)R_L + zR_L$.
   (ii) $P = (z - \alpha x)R_L$ with a root α of $X^2 + X + 1$, and we assume that $\alpha \in k$, $P' = xR_L + zR_L$.

§4

1. The condition (i) implies that the order of the Galois group G is a multiple of 3 and the condition (ii) implies that $\#(G)$ is an even number. Since G is a subgroup of S_3, we have $G = S_3$.

§5

2. An example is $f(x) = x^5+6x^4-12x^3+15x^2-17x+14$ from x^5+x-1 (mod 3), $x(x^4+x+1)$ (mod 2) and $(x^2-x+3)(x+1)(x-1)x($ mod 7$)$.

Index of Symbols

This page intentionally left blank

Subject Index

This page intentionally left blank

Recent Titles in This Series

(Continued from the front of this publication)

90 **S. L. Sobolev,** Some applications of functional analysis in mathematical physics, third edition, 1991

89 **Valeriĭ V. Kozlov and Dmitriĭ V. Treshchëv,** Billiards: A genetic introduction to the dynamics of systems with impacts, 1991

88 **A. G. Khovanskiĭ,** Fewnomials, 1991

87 **Aleksandr Robertovich Kemer,** Ideals of identities of associative algebras, 1991

86 **V. M. Kadets and M. I. Kadets,** Rearrangements of series in Banach spaces, 1991

85 **Mikio Ise and Masaru Takeuchi,** Lie groups I, II, 1991

84 **Đáo Trọng Thi and A. T. Fomenko,** Minimal surfaces, stratified multivarifolds, and the Plateau problem, 1991

83 **N. I. Portenko,** Generalized diffusion processes, 1990

82 **Yasutaka Sibuya,** Linear differential equations in the complex domain: Problems of analytic continuation, 1990

81 **I. M. Gelfand and S. G. Gindikin, Editors,** Mathematical problems of tomography, 1990

80 **Junjiro Noguchi and Takushiro Ochiai,** Geometric function theory in several complex variables, 1990

79 **N. I. Akhiezer,** Elements of the theory of elliptic functions, 1990

78 **A. V. Skorokhod,** Asymptotic methods of the theory of stochastic differential equations, 1989

77 **V. M. Filippov,** Variational principles for nonpotential operators, 1989

76 **Phillip A. Griffiths,** Introduction to algebraic curves, 1989

75 **B. S. Kashin and A. A. Saakyan,** Orthogonal series, 1989

74 **V. I. Yudovich,** The linearization method in hydrodynamical stability theory, 1989

73 **Yu. G. Reshetnyak,** Space mappings with bounded distortion, 1989

72 **A. V. Pogorelev,** Bendings of surfaces and stability of shells, 1988

71 **A. S. Markus,** Introduction to the spectral theory of polynomial operator pencils, 1988

70 **N. I. Akhiezer,** Lectures on integral transforms, 1988

69 **V. N. Saliĭ,** Lattices with unique complements, 1988

68 **A. G. Postnikov,** Introduction to analytic number theory, 1988

67 **A. G. Dragalin,** Mathematical intuitionism: Introduction to proof theory, 1988

66 **Ye Yan-Qian,** Theory of limit cycles, 1986

65 **V. M. Zolotarev,** One-dimensional stable distributions, 1986

64 **M. M. Lavrent′ev, V. G. Romanov, and S. P. Shishat·skiĭ,** Ill-posed problems of mathematical physics and analysis, 1986

63 **Yu. M. Berezanskiĭ,** Selfadjoint operators in spaces of functions of infinitely many variables, 1986

62 **S. L. Krushkal′, B. N. Apanasov, and N. A. Gusevskiĭ,** Kleinian groups and uniformization in examples and problems, 1986

61 **B. V. Shabat,** Distribution of values of holomorphic mappings, 1985

60 **B. A. Kushner,** Lectures on constructive mathematical analysis, 1984

59 **G. P. Egorychev,** Integral representation and the computation of combinatorial sums, 1984

58 **L. A. Aĭzenberg and A. P. Yuzhakov,** Integral representations and residues in multidimensional complex analysis, 1983

57 **V. N. Monakhov,** Boundary-value problems with free boundaries for elliptic systems of equations, 1983

(See the AMS catalog for earlier titles)

This page intentionally left blank

ISBN 0-8218-4572-1

9 780821 845721