

UNIVERSAL
LIBRARY

OU_156480

UNIVERSAL
LIBRARY

OSMANIA UNIVERSITY LIBRARY

Call No. 512.8/H 35E Accession No. 32196

Author Helmut, Hasse . P. h . P

Title Exercises Higher algebra

This book should be returned on or before the date last marked below.

**EXERCISES TO
HIGHER ALGEBRA**

EXERCISES
TO
HIGHER ALGEBRA

BY
HELMUT HASSE, Ph.D.
Professor of Mathematics, University of Hamburg

and
WALTER KLOBE
Assistant Master, Lessing-Oberschule Erfurt

Translated from the second revised and enlarged German edition
by

THEODORE J. BENAC, Ph.D.
Associate Professor of Mathematics, U.S. Naval Academy

FREDERICK UNGAR PUBLISHING CO.
NEW YORK

Copyright 1954 by Frederick Ungar Publishing Co.

Printed in the United States of America

Library of Congress Catalog Card No. 54-7571

PREFACE

The volume of exercises is divided into two parts corresponding to the two volumes *Higher Algebra* 1 and 2, which will be referred to as Vol. 1 and Vol. 2. The organization of both parts into chapters and sections corresponds exactly to the organization of Vol. 1 and Vol. 2.

For each section of exercises it is always assumed that the entire corresponding section of Vol. 1 or Vol. 2 and all preceding sections are known to the reader. All quotations within a section of exercises without special reference to a section and volume refer to the like-designated sections of Vol. 1 or Vol. 2. In addition, all quotations in which the volume is not specified refer to the volume under consideration. Numbers annexed in square brackets to the number of a theorem or definition indicate the page numbers on which the theorem or definition in question appears.

A method of solution is always given in small print after the exercise in question. Frequently even the complete solution is introduced in a later exercise. Often the methods of solution are given intentionally only through reference to the theorems of Vol. 1 and Vol. 2 to be applied, or to earlier exercises, so that the solutions are not too obvious.

The co-author, as a student, solved all exercises of the first edition, and the experience thereby gained was extremely useful in the preparation of the second edition. The author expresses his special obligation to his co-author for his collaboration on this volume.

H. H.

CONTENTS

Volume I

Linear Equations

I. Rings. Fields. Integral Domains

1. Definition of Rings, Fields, Integral Domains	13
2. Subdomains. Congruence Relations. Isomorphism	15
3. The Quotient Field of an Integral Domain	18
4. The Integral Domain of Integral Rational Functions of n Indeterminates over $\mathbf{I}$ and the Field of Rational Functions of n Indeterminates over $\mathbf{K}$	20
5. Detailed Formulation of the Basic Problem of Algebra	22

II. Groups

6. Definition of Groups	24
7. Subgroups. Congruence Relations. Isomorphism	25
8. Partition of a Group Relative to a Subgroup	29
9. Normal Divisors. Conjugate Subsets of a Group. Factor Groups	31

III. Linear Algebra without Determinants

10. Linear Forms. Vectors. Matrices	38
11. Nonhomogeneous and Homogeneous Systems of Linear Equations	44
12. The Toeplitz Process	45
13. Solvability and Solutions of Systems of Linear Equations	47
14. The Case $m = n$	50
15. Importance of Linear Algebra without Determinants	51

IV. Linear Algebra with Determinants

16. Permutation Groups	53
17. Determinants	62
18. Minors and Cofactors. The Laplace Expansion Theorem	64
19. Further Theorems on Determinants	66
20. Application of the Theory of Determinants to Systems of Linear Equations in the Case $m = n$	73
21. The Rank of a Matrix	76
22. Application of the Theory of Determinants to Systems of Linear Equations in the General Case	84

Volume II

Equations of Higher Degree

I. The Left Sides of Algebraic Equations

1. The Fundamental Theorem of the Unique Decom- posability into Prime Elements in $K[x]$ and Γ	89
2. Residue Class Rings in $K[x]$ and Γ	102
3. Cyclic Groups	112
4. Prime Integral Domains. Prime Fields. Characteristic	119

II. The Roots of Algebraic Equations

5. Roots and Linear Factors	125
6. Multiple Roots. Derivative	129

III. The Fields of the Roots of Algebraic Equations

7. General Theory of Extensions (1). Basic Concepts and Facts	139
--	-----

CONTENTS

8. Stem Fields	143
9. General Theory of Extensions (2). Simple and Finite Algebraic Extensions	144
10. Root Fields	147
11. The So-called Fundamental Theorem of Algebra	154
 IV. The Structure of the Root Fields of Algebraic Equations	
12. Simplicity and Separability of the Root Fields of Separable Polynomials, More Generally, of Finite Algebraic Extensions with Separable Primitive System of Elements	157
13. Normality of Root Fields and of Their Primitive Elements. Galois Resolvents	158
14. The Automorphism Group of an Extension Domain	162
15. The Galois Group of a Separable Normal Extension of Finite Degree	164
16. The Galois Group of a Separable Polynomial	166
17. The Fundamental Theorem of Galois Theory	170
18. Dependence on the Ground Field	176
 V. Solvability of Algebraic Equations by Radicals	
19. Definition of Solvability by Radicals	180
20. Cyclotomic Fields. Finite Fields	181
21. Pure and Cyclic Extensions of Prime Degree	188
22. Criterion for the Solvability by Radicals	197
23. Existence of Algebraic Equations not Solvable by Radicals	202
 Index	211

Volume I.

Linear Equations

Vol. 1. Chapter I. Rings, Fields, Integral Domains

1. Definition of Rings, Fields, Integral Domains

1. Derive the following formulae from postulates (1) to (6):

$$\begin{aligned}(a+b)(c+d) &= ac + ad + bc + bd, \\ (-a)b &= -ab, (-a)(-b) = ab, (-a \text{ means } 0-a), \\ (a-b)(c-d) &= ac - ad - bc + bd.\end{aligned}$$

2. Derive the following formulae from postulates (1) to (7):

$$\frac{a \pm c}{b \pm d} = \frac{ad \pm bc}{bd}, \quad \frac{ac}{bd} = \frac{ac}{bd}, \quad \frac{a/c}{b/d} = \frac{ad}{bc},$$

($b, d \neq 0$; in the last case $c \neq 0$ is also assumed.)¹

3. Let the commutative law of addition (1) be dropped in postulates (c). Let the other postulates remain unchanged except that in (6), besides the existence and uniqueness of the solution b of $a+b=c$, the existence and uniqueness of the solution b' of $b'+a=c$ are also required. Show that the commutative law of addition (1) *can then be derived*.

Note that the proof of the existence of the unity element e (Theorem 3) is unaffected; compute $(a+e)(b+e)$ according to (2), (5) in two ways; then apply (6) and the indicated extension of (6) each once.

4. The set of couples (a_1, a_2) , where a_1, a_2 are elements of an arbitrary integral domain I , with the "equality" of couples defined by:

$$(a_1, a_2) = (a'_1, a'_2) \quad \text{if, and only if,} \quad a_1 = a'_1, a_2 = a'_2,$$

¹ Regarding this point, cf. Section 3, (1) to (5).

forms a ring with respect to the combinations:

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2).$$

What is the zero of this ring? Does this ring have a unity element? Show that it is, however, not an integral domain.

Conditions (a), (b), (c), (1) to (6) are satisfied; however, (7a) and Theorem 4 are not, as can be shown by examples.

5. The set of couples of the preceding exercise also forms a ring with respect to the following combinations:

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1).$$

Proof? What is the zero of the ring? Show that it also has a unity element and is even an integral domain.

Theorem 3 and Theorem 4 are satisfied. In addition to Theorem 4, prove that

$$a_1 b_1 - a_2 b_2 = 0$$

$$a_1 b_2 + a_2 b_1 = 0$$

implies either $a_1 = a_2 = 0$ or $b_1 = b_2 = 0$.

6. Next, replace the integral domain I in Exer. 4, 5, by a field K . Prove that the domain constructed in Exer. 4 is, just as before, only a ring, while the domain in Exer. 5 becomes a field. In the latter case represent the element

$$(a_1, a_2)$$

$$(b_1, b_2)$$

in the normal form (c_1, c_2) .

7. Prove the existence of a field of exactly *three* elements by setting up the multiplication and addition tables (analogous to the tables in Example 4 for a field of exactly two elements) and showing that postulates (1) to (7) are satisfied.

The three elements must necessarily be $0, e, -e$. For, if $-e = e$ (as in Example 4), the existence of a third element $a \neq 0, e$ would imply the existence of a fourth element $e + a \neq 0, e, a$.

8. Similarly, prove the existence of a field of exactly *four* elements.

In this case we must again (as in Example 4) have that $-e = e$. For, if $-e \neq e$, then either $-e \neq 2e$, so that $0, e, -e, 2e, -2e$ are already five different elements, or (as in Exer. 7) $-e = 2e$, so that the existence of a fourth element a would imply the existence of a fifth element $e + a$. Accordingly, take as elements $0, e, a, e + a$. If all elements are thereby exhausted, then a^2 must be one of these four elements. But it can be neither 0 nor a (Theorem 4); likewise, it cannot be e , since $(e + a)^2 = 0$ would then follow. Therefore $a^2 = e + a$ must be valid.

9. Prove: An integral domain containing only a finite number of elements must be a field.

See if necessary - the proof to Theorem 20 [64].

10. Consider the set of rational numbers of the form $\frac{g}{2^n}$, where g runs through all odd numbers in addition to 0, and 2^n runs through all integral powers of 2. Prove that this set forms an integral domain with respect to ordinary addition and multiplication.

Verify directly that the ring conditions (Def. 1) as well as the additional conditions (7a), (7b) or Theorems 3, 4 for an integral domain (Def. 3) are satisfied.

2. Subdomains, Congruence Relations, Isomorphism

1. What is wrong with the following argument: The reflexive postulate (α) follows from the symmetry postulate (β) and the transitive postulate (γ), because by (β) $a \sim b$ implies $b \sim a$, and by (γ) the relations $a \sim b, b \sim a$ thereby established further imply $a \sim a$.

Show that the indicated line of reasoning proves the relation $a \sim a$ only if a certain restriction is imposed on a , therefore not necessarily for *all* elements a of the set M under consideration.

2. Show by a counterexample that (α) does *not* (therefore neither by any other type of inference) follow from (β) and (γ) , that is, (α) is *independent* of (β) and (γ) .

A distribution of the symbols $\sim$, $\nmid$ between all pairs of elements of a set M has to be found whereby (β) and (γ) are valid throughout but (α) is not satisfied for at least one element. —This can be done for *any* set M ; in particular, also for the set consisting of only *one* element a .

3. Show analogously by counterexamples that (β) is independent of (α) and (γ) , and that (γ) is independent of (α) and (β) .

In order to form these counterexamples it is enough to use sets M of only two or only three elements.

4. Show that each of the four conditions $(\delta), (\delta'), (\epsilon), (\epsilon')$ for a one-to-one correspondence is independent of the remaining three, and illustrate the meaning of each one of these conditions.

It will help to make things clearer if the elements of the two sets M and M' are written in two vertical columns with the symbols $\longleftrightarrow$ as cross-connections between the elements under consideration; the symbols $\longleftrightarrow$ can be more simply represented merely by omitting the symbols $\leftarrow \rightarrow$.

5. Let a be an integer which is not the square of a rational number.¹ It is known that the two square roots of a are equal in magnitude but opposite in sign, and that they belong to the field A of all complex numbers (Section 1, Example 2). Let $\sqrt{a}$ be one of these two square roots.

¹ In this regard, cf. also Exer. 32 to Vol. 2, Section 1, given later.

Prove: The totality of all those complex (in the case $a > 0$, even real) numbers which can be obtained from the number $\sqrt{a}$ and $\left\{ \begin{smallmatrix} \text{integral rational} \\ \text{rational} \end{smallmatrix} \right\}$ numbers by the repeated application of the $\left\{ \begin{smallmatrix} \text{first three} \\ \text{four} \end{smallmatrix} \right\}$ elementary operations form an $\left\{ \begin{smallmatrix} \text{integral subdomain } \Gamma[\sqrt{a}] \\ \text{subfield } P(\sqrt{a}) \end{smallmatrix} \right\}$ of A . All its elements can be expressed (uniquely) in the form $u + v\sqrt{a}$ if u and v are allowed to run through, independently of one another, the elements of the $\left\{ \begin{smallmatrix} \text{integral domain } \Gamma \text{ of all integral} \\ \text{field } P \text{ of all rational} \end{smallmatrix} \right\}$ numbers (Section 1, Example 1).¹

By using the "if" statement in Theorem 6, first show that the $u + v\sqrt{a}$ form $\left\{ \begin{smallmatrix} \text{an integral subdomain} \\ \text{a subfield} \end{smallmatrix} \right\}$ of A . That this domain can also be characterized in the more general manner, specified above, follows from the "only if" statement of Theorem 6.

6. What is the intersection of the two fields $P(\sqrt{a})$ and $P(\sqrt{a'})$?

This depends on whether $\frac{a'}{a}$ is the square of a rational number (*special case*) or not (*general case*).

7. Prove: The composite of the subfields $K_1, K_2, \dots$ of the field K is the totality of all those elements of K which are generated by the repeated application of the four elementary operations on the elements of the union of the sets $K_1, K_2, \dots$

Apply Theorem 6 just as in Exer. 5.

8. Give a unique representation for the elements of the composite of the two fields $P(\sqrt{a})$ and $P(\sqrt{a'})$ in the general case (Exercise 6).

¹ This notation is adopted to conform with the general theory in Vol. 2, Sections 7, 8, ruling over this example.

See, if necessary, Vol. 2, Theorem 62 [220] and the proof to Vol. 2, Theorem 71 [228].

9. Prove: Every element a of a ring B determines a congruence relation based on the following convention:

$b \equiv c \pmod{a}$ if, and only if, $b - c = ha$ with an h in B .¹

10. Show that there are no congruence relations in a field except for the following two trivial ones:

(a). All elements are congruent to one another.

(b). Two elements are congruent to one another if, and only if, they are equal to one another.

Distinguish between the two cases (a) $0 \equiv e$ and (b) $0 \not\equiv e$.

11. Conversely, show that a ring is a field if only the two trivial congruence relations (a) and (b) of Exer. 10 exist in the ring.

Apply the alternative (a), (b) to the congruence relations of Exer. 9 determined by the individual elements a . It will follow that the division postulate, Section 1, (7) is valid.

12. How many types of fields are there of exactly two elements? three elements? four elements?

Note the cogency in the setup of the addition and multiplication tables in Section 1, Example 4 and Section 1, Exer. 7, 8.

3. The Quotient Field of an Integral Domain

1. Let $a (\neq 0)$ be an element of a ring B . We call a a (*proper*) *zero divisor* in B (cf. Section 1, Exer. 4) if there exists an element $b (\neq 0)$ in B such that $ab = 0$. This amounts to saying [cf. Section 1, (7a) and the remark after Theorem 4] that the division by a is not unique. The elements of B

¹ In this regard, cf. the theory in Vol. 2, Theorem 26 [189], Def. 10 [191].

which are not zero divisors—or, which amounts to the same thing, division by which is unique—are called *regular* in **B**.

Show that the construction in the proof to Theorem 10 can also be carried out if we start from a ring **B** without proper zero divisors [that is, a ring in which division is unique or a ring satisfying postulate Section 1, (7a)] instead of an integral domain.

We therefore have to show that we can manage even without the existence of the unity element [Section 1 (7b)—see also Def. 3, Addendum]. For this purpose instead of operating with the classes $\{a, e\}$, now use the classes $\{ac, c\}$. According to (1') these new classes are independent of c , and therefore determined by a alone.

2. Prove the following generalization of Theorem 4[18]: The product of two regular elements of a ring is not only different from zero but also regular.

This follows from the definition of regularity by a line of reasoning patterned after the proof of Theorem 4.

3. We will call a ring a *full ring*¹ if it contains all quotients $\frac{a}{b}$ with regular denominator b . This means that in a full ring division is unrestricted so far as it is unique. (Therefore, in this sense, full integral domain means the same as field.)—Show analogously to Theorem 10: An *arbitrary* ring **B** determines an extension full ring **V**, every element of which can be represented as a quotient $\frac{a}{b}$ (b regular in **B**) of elements of **B**. The extension type of **V** is determined uniquely by this requirement.

Operate with the set of all couples (a, b) over **B**, where b is regular in **B**, and in particular take Exer. 2 into account.

¹ The literature hitherto existing does not contain a nomenclature for such a ring.—For examples of full rings, which are not fields, cf. Exer. 6 to Vol. 2, Section 2, given later.

4. The Corollary to Theorem 10 can be adequately generalized only if the above extension full ring V^* of B has the property that elements regular in B remain regular, namely, do not become zero divisors. Show that the *quotient full ring* V constructed in Exer. 3 has this property.

5. Find the quotient full ring, in the sense of Exer. 3, to the ring of all even numbers (Section 1, Example 3).

4. The Integral Domain of the Integral Rational Functions of n Indeterminates over I and the Field of Rational Functions of n Indeterminates over K

1. Prove that $I[x_1, x_2]$ is isomorphic to $I[x_1][x_2]$ relative to I .

In this, think of $I[x_1, x_2]$ as defined by the array resulting from (1a) to (3a), $I[x_1][x_2]$ by two steps $I_1 = I[x_1]$, $I_2 = I_1[x_2]$ of the kind (1') to (3').—Set up the natural correspondence between the elements of the two domains and show that the isomorphism relations, Section 2, $(\delta), (\delta'), (\epsilon), (\epsilon'), (3), (4)$ are satisfied.

2. Show: If $f_0(x)$ is a fixed element of $I[x]$ not belonging to I and $f(x)$ runs through all elements of $I[x]$, then the correspondence $f(x) \longleftrightarrow f(f_0(x))$ represents an isomorphism relative to I between $I[x]$ and an integral subdomain $I[f_0(x)]$ of $I[x]$.

The crucial point is the confirmation of Section 2, (ϵ') , which amounts to the proof of $f(f_0(x)) \neq 0$ for $f(x) \neq 0$. For this purpose determine the term of highest degree in the normal representation of $f(f_0(x))$.

3. Find the necessary and sufficient condition on $f_0(x)$ in order that this integral subdomain $I[f_0(x)]$ coincide with $I[x]$. Accordingly, are there integral domains which are isomorphic to proper integral subdomains?

The necessary and sufficient condition easily follows from the fact that x can be represented in the form $f(f_0(x))$.

4. Show analogously to Exer. 2: If $\phi_0(x)$ is an element of $K(x)$ not belonging to K and $\phi(x)$ runs through all elements of $K(x)$, then the correspondence $\phi(x) \longleftrightarrow \phi(\phi_0(x))$ represents an isomorphism relative to K between $K(x)$ and a subfield $K(\phi_0(x))$ of $K(x)$.

The only case which is difficult to deal with is where f_0 and g_0 have the same degree. The crucial point in this case is handled (analogously to Exer. 2) by splitting the substitution $f(x) \rightarrow f\left(\frac{f_0(x)}{g_0(x)}\right)$ into two parts $f(x) \rightarrow f(x + \alpha) \equiv g(x)$, $g(x) \rightarrow g\left(\frac{h_0(x)}{g_0(x)}\right)$ according to the decomposition $\frac{f_0}{g_0} = \alpha + \frac{h_0}{g_0}$ (h_0 of lower degree than g_0 ; cf. Vol. 2, Theorem 13 [180]).

5. Show analogously to Exer. 3: In order that this subfield coincide with $K(x)$ it is in any case *sufficient*¹ that $\phi_0(x)$ have the form $\frac{a+bx}{c+dx}$ (a, b, c, d in K , $ad - bc \neq 0$).

6. Show that $K(x^n)$, for any $n \geq 2$, is a proper subfield of $K(x)$ isomorphic to $K(x)$.

It is easy to see that the equation $x \equiv \phi(x^n) \equiv \frac{f(x^n)}{g(x^n)}$ cannot be satisfied by every element $\phi(x) \equiv \frac{f(x)}{g(x)}$ of $K(x)$.

7. The integral rational function $x^2 + x \not\equiv 0$ over the field K of exactly two elements (Section 1, Example 4), but $\equiv 0$ for every x in K [proof to Theorem 12, d)], that is, $\equiv 0$ in the sense of analysis.—Show that the ring of integral rational functions in the sense of analysis over K is therefore not an integral domain.

Since Section 1 (7b) (existence of the unity element) is satisfied in any case, the proof can only depend on Section 1 (7a) (uniqueness

¹ For the *necessity* of this condition, cf. Exer. 30 to Vol. 2, Section 1, given later.

of division), that is, it must be proved that this ring contains proper zero divisors.

8. Construct similar examples for the fields of exactly three and exactly four elements (Section 1, Exer. 7, 8) as well as in general for *any* field containing only finitely many elements.

Note that in Exer. 7

$$x^2 + x \equiv x^2 - x \equiv (x - 0)(x - e)$$

is valid and $0, e$ are *all* elements of K .

5. Detailed Formulation of the Basic Problem of Algebra

1. Let a calculating process be given which is formed by means of the four elementary operations applied to the indeterminates $x_1, \dots, x_n$ and given elements of K , and let ϕ be its corresponding element in $K(x_1, \dots, x_n)$. This process consists of the successive application of the operations $O_1, \dots, O_n$; each operation O_ν is then an addition, subtraction, multiplication or division of two elements ψ_ν, χ_ν of $K(x_1, \dots, x_n)$ which leads to a new element ϕ_ν of $K(x_1, \dots, x_n)$; each of the elements ψ_ν, χ_ν is either one of the x_i or one of the given elements of K or one of the previous ϕ_μ ($\mu < \nu$); and finally $\phi_n = \phi$. Among the operations O_ν let there be exactly $O_{\nu_1}, \dots, O_{\nu_r}$ divisions, and let $\chi_{\nu_1}, \dots, \chi_{\nu_r}$ be the divisors (denominators) appearing therein. Then the indeterminates x_i in this process can be replaced by any system of elements of K for which neither χ_{ν_1} nor ... nor χ_{ν_r} are zero.—Show that there is (at least) one quotient representation $\phi = \frac{f}{g}$ in terms of two elements f, g of $K[x_1, \dots, x_n]$ whose denominator g is different from zero for all and only these substitutions.

Apply *mathematical induction on n* (conclusion from $n-1$ to n). Begin with $n = 0$, that is, with a process which requires *no* operation; here, we simply have that ϕ itself is either one of the x_i or one of the given elements of K . If we assume that the statement has already been proved to be valid for the process consisting of $n-1$ operations ($n \geq 1$) at most, then it is also true, in particular, for the processes leading to ψ_n, χ_n . We now distinguish between the four cases

$$\phi_n = \psi_n + \chi_n, \quad \phi_n = \psi_n - \chi_n, \quad \phi_n = \psi_n \chi_n, \quad \phi_n = \frac{\psi_n}{\chi_n}.$$

In the last case the denominator in the quotient representation of $\phi_n = \phi$ to be constructed should be made to involve the denominator, superfluous of itself, in the quotient representation of χ_n formed according to the induction assumption.

2. Give quotient representations in the sense of Exer. 1 for the following processes (K an arbitrary field):

$$\frac{e}{x}, \quad \frac{x-e}{x+e} - e, \quad \frac{\frac{e}{x-e} + e}{\frac{e}{x+e} - e}.$$

Use these representations to find the solutions of the equations obtained by setting these calculating expressions $\doteq 0$.

Note that those x in K , for which the calculating process in question is undefined due to one of the successive denominators becoming zero, are excluded as solutions *from the beginning*.

Vol. 1. Chapter II. Groups

6. Definition of Groups

1. Let an arbitrary geometric configuration be given in the plane (in space). Consider all *coincidence motions* of the configuration in the plane (in space), that is, those motions of the configuration by which it coincides with itself. Let these coincidence motions be characterized only by the terminal position relative to the initial position (therefore, neither by the intermediate positions nor by the absolute initial and terminal positions).—If the product of two coincidence motions is defined as the result of performing them in succession, show that the coincidence motions form a group with respect to this multiplication.

See the typical special case in Example 4.

2. Determine the order and the relations of combination for the groups of coincidence motions of the following configurations:

- (a) regular n -gon in the plane ($n \geq 2$) (*cyclic groups* $\mathfrak{Z}_n$)¹,
- (b) regular n -gon in space ($n \geq 2$) (dihedron = regular polyhedron with n vertices, n edges, 2 faces) (*dihedral groups* $\mathfrak{D}_n$),
- (c) regular tetrahedron in space (*tetrahedral group* $\mathfrak{T}$).

In (b) the case $n = 2$ means the configuration in space consisting of a line segment and a plane containing it. Instead of these we can also take a system of three mutually perpendicular lines of different colors through a point. What

¹ Cf. Vol. 2, Def. 12 [196].

advantage does the latter configuration have in reference to the group?

See again the typical special case in Example 4; and in addition the explanations to Section 7, Exer. 1 to 3.

3. Which of the groups obtained in Exer. 2 are Abelian?

4. Investigate the additive and multiplicative groups (in the sense of Example 1) of a field of two elements; three elements; four elements. Are any of these cyclic groups?

For this purpose see Section 1, Example 4, Section 1, Exer. 7, 8, and Section 2, Exer. 12.

5. Solve the equations

$$ABX \doteq BA, \quad YAB \doteq BA$$

according to their meaning in an arbitrary group (X the *right* and Y the *left commutator* of A and B). What relation exists between the commutators of A and B and those of B and A ? of A^{-1} and B^{-1} ? of B^{-1} and A^{-1} ?

See Theorem 15.

6. Show that the relation $A^n = E$ is valid for every element A in an Abelian group of finite order n .

Form the product of the elements AB specified in Theorem 16.—See, if necessary, the proof to Vol. 2, Theorem 29 [194].

7. Subgroups, Congruence Relations, Isomorphism

1. Determine all subgroups of the cyclic group $\mathfrak{Z}_n$ and illustrate the geometric meaning of the subgroups by the regular n -gon.

Let $\mathfrak{Z}_n$ be given by the elements A^ν ($\nu = 0, 1, \dots, n-1$) with the relation $A^n = E$. The consideration of the lowest power of A with a positive exponent which lies in a subgroup yields that the subgroups

are cyclic groups $\mathfrak{B}_d$ which correspond biuniquely to the divisors d of n .¹

2. Determine all subgroups of the dihedral group $\mathfrak{D}_n$ and again illustrate the geometric meaning of the subgroups by the regular n -gon in space (dihedron). Also classify the special case of Example 4.

If $\mathfrak{D}_n$ is given by the $2n$ elements

$$A^v, A^v B \quad (v = 0, 1, \dots, n-1)$$

with the relations

$$A^n = E, \quad B^2 = E, \quad BA = A^{-1}B,$$

then only the following types of subgroups can occur: subgroups $\mathfrak{B}_d$ of the cyclic subgroup $\mathfrak{B}_n$ formed by the A^v , their corresponding subgroups $\mathfrak{D}_d$, and subgroups of order 2 corresponding to the elements $A^v B$. The discussion is made a little easier by using Theorem 20.

3. Determine all subgroups of the tetrahedral group $\mathfrak{T}$.

Either the third or second power of the elements $\neq E$ of $\mathfrak{T}$ is $= E$, according as the element corresponds to a rotation axis through a vertex and the center of an opposite face or to a rotation axis through the midpoints of two opposite edges. This clearly shows which cyclic subgroups are contained in $\mathfrak{T}$. Furthermore, corresponding to the three mutually perpendicular rotation axes through the midpoints of the edges there is a dihedral group $\mathfrak{D}_2$ (*four-group*) in $\mathfrak{T}$. In order to show that all subgroups of $\mathfrak{T}$ have been enumerated, it is enough to establish that the entire group $\mathfrak{T}$ can be generated by a vertex- and center-of-face rotation A and a midpoint-of-edges rotation B (due to symmetry anyone of each kind may be chosen).

4. Prove:

(a) The integral multiples of an integer m form a subgroup of the additive group of all integers.—For which m is this a proper subgroup?

¹ In this regard see the general theory of cyclic groups in Vol. 2, Section 3.

(b) The integers form a subgroup of the additive group of all rational numbers.

(c) The positive real numbers form a subgroup of the multiplicative group of all real numbers $\neq 0$.

Theorem 20 is not enough here.

5. Prove that the following relations are congruence relations:

(a) (Additive group of all integers; *congruence mod m*)¹

$a \equiv b$, if $a - b$ is an integral multiple of m .

(b) (Additive group of all rational numbers; *congruence mod 1*)

$a \equiv b$, if $a - b$ is an integer.

(c) (Multiplicative group of all real numbers $\neq 0$)

$a \equiv b$, if a and b have the same sign.

Show how these congruence relations are related to the subgroups considered in Exer. 4. Give the types of the residue class groups belonging to the congruences in the cases (a) and (c). What property distinguishes the residue class group in case (b) from that in (a) and (c)?

See—if necessary—the general situation in Theorem 35 [75]. Case (a) has already occurred as a special case under Section 2, Exer. 9.

6. Prove: The totality of those elements of $\mathcal{G}$ which can be obtained from the elements of a subset M of $\mathcal{G}$ by the repeated application of multiplication and (two-sided) division form a subgroup of $\mathcal{G}$ (the *subgroup generated by M*).

Apply Theorem 19 as well as Theorem 15 [59].

7. What is the type of the subgroup generated by an element A of a group $\mathcal{G}$ (the *period* of A)?

¹ For this purpose cf. the general theory in Vol. 2, Section 2.

Distinguish between the case where all integral powers A^n are different from one another (one type) and the contrary case in which there must exist a smallest positive n for which $A^n = E$ (one type for each n). In this regard see—if necessary—the theory developed in Vol. 2, Section 3, especially Theorems 33, 34.

8. Two elements A, B of a group $\mathfrak{G}$ are said to *commute* if $AB = BA$ (in other words, if their commutator is equal to E).—Prove: The totality of those elements of $\mathfrak{G}$ which commute with all elements of $\mathfrak{G}$ form an Abelian subgroup of $\mathfrak{G}$ (the *centrum* of $\mathfrak{G}$).

9. Let $\mathfrak{B}_1, \mathfrak{B}_2$ be two cyclic subgroups of a group $\mathfrak{G}$ such that every element of the first subgroup commutes with every element of the second. Let the orders of these subgroups be m_1, m_2 , the order of their intersection $\mathfrak{D}$ be d , the order of their composite $\mathfrak{K}$ be k .—Show that the relation $dk = m_1 m_2$ is valid, whereby k is determined if d is known or d is determined if k is known.

Introduce generating elements D, A_1, A_2 for $\mathfrak{T}, \mathfrak{B}_1, \mathfrak{B}_2$ and represent the elements of $\mathfrak{K}$ in the form $D^\alpha A_1^{\alpha_1} A_2^{\alpha_2}$ with a range as small as possible for the exponents $\alpha, \alpha_1, \alpha_2$.

10. Determine the intersection and the composite of the two subgroups $\mathfrak{D}_d$ and $\mathfrak{B}_{d'}$ of the dihedral group $\mathfrak{D}_n$ (d and d' divisors of n).

The intersection depends on the greatest common divisor of d and d' ; the composite, on the least common multiple of d and d' . In this regard see—if necessary—the general theory in Vol. 2, Theorem 14 [182] and in Exer. 16 to Vol. 2, Section 1.

11. Determine the composite of the two subgroups $\mathfrak{B}_n$ and (E, B) , as well as that of the two subgroups (E, B) and $(E, A^k B)$, of the dihedral group $\mathfrak{D}_n$.

The latter depends on the greatest common divisor of n and the given exponent k .

12. Which of the groups obtained in Exer. 1 to 4, 7, and Section 6, Exer. 4 are isomorphic to one another? Therefore, what different types of groups have occurred in these exercises?

13. In an arbitrary group $\mathcal{G}$ prove that $A \longleftrightarrow A^{-1}$ gives a one-to-one correspondence of $\mathcal{G}$ to itself [therefore a permutation¹ of $\mathcal{G}$].—How is this correspondence related to the multiplication in $\mathcal{G}$? For which groups is it an isomorphism [therefore, an *automorphism*² of $\mathcal{G}$]?

Apply Theorems 15, 17 [59, 60].

14. Prove: If n is a fixed natural number, then the correspondence $a \longleftrightarrow na$ forms an automorphism in the additive group of all rational or all real numbers; furthermore, the correspondence $a \longleftrightarrow a^n$ forms an automorphism in the multiplicative group of all real positive numbers.

8. Partition of a Group Relative to a Subgroup

1. Show: If $S_1, S_2, \dots$ is a complete right residue system of $\mathcal{G}$ relative to $\mathfrak{H}$, then $S_1^{-1}, S_2^{-1}, \dots$ is a complete left residue system of $\mathcal{G}$ relative to $\mathfrak{H}$.

The relations $S \equiv S'(\mathfrak{H})$ and $S^{-1} \equiv S'^{-1}(\mathfrak{H})$ imply one another.

2. Set up the left and right partitions of the dihedral groups $\mathfrak{D}_n$, as well as of the tetrahedral group $\mathfrak{T}$, relative to their different subgroups.

For this purpose see Exer. 1 and the explanation to Section 7, Exer. 2, 3, as well as the special case typical of the dihedral groups in Example 2.

¹ See Def. 35 [117].

² See Vol. 2, footnote to Def. 32 [264].

3. Set up the partition into cosets relative to the subgroups found in Section 7, Exer. 4, (a), (b), (c).

Show that this exercise is identical with the last question in Section 7, Exer. 5. Even though there are infinitely many cosets in (b), a simple complete residue system can still be found for this case.

4. Let $\mathcal{G}$ be an arbitrary group of finite order n . Show that the relation $A^n = E$ is valid for every element A of the group.

Apply Theorem 25 to the cyclic subgroup of $\mathcal{G}$ generated by A (the period of A). For Abelian groups see also Section 6, Exer. 6, already given; in general, Vol. 2, Theorem 34 [198].

5. By the *order* of an element A of a group $\mathcal{G}$ we understand the order of its period.—Let A_1, A_2 be two commutative elements of a group $\mathcal{G}$ of finite orders m_1, m_2 . What can be said about the order of $A_1 A_2$?

By applying Section 7, Exer. 9 an upper bound (in the sense of a multiple) is obtained for the order.

6. Construct a case where the upper bound obtained in Exer. 5 is actually reached, and also a case where it is not reached.

For the former it is enough that m_1, m_2 have no common divisor; see Vol. 2, Theorem 35 [198]. For the latter apply, say, $AA^{-1} = E$.

7. Prove that a group of prime order is necessarily cyclic. For this purpose consider the period of any element $\neq E$.

8. Prove: If $\mathfrak{H}$ is a subgroup of $\mathcal{G}$, $\mathfrak{K}$ a subgroup of $\mathfrak{H}$, and S runs through a complete right residue system of $\mathcal{G}$ relative to $\mathfrak{H}$, while T runs through a complete right residue system of $\mathfrak{H}$ relative to $\mathfrak{K}$, then ST runs through a complete right residue system of $\mathcal{G}$ relative to $\mathfrak{K}$.

For arbitrary A, B in $\mathfrak{H}$ and U in $\mathcal{G}$ the relations $A \equiv B(\mathfrak{K})$ and $UA \equiv UB(\mathfrak{K})$ imply one another.

9. In Exer. 8 replace right residue systems by left residue systems.

Replace ST by TS .

10. What conclusions can be drawn from the data in Exer. 8 in regard to the indices of $\mathfrak{H}$ in $\mathfrak{G}$, $\mathfrak{K}$ in $\mathfrak{G}$, $\mathfrak{K}$ in $\mathfrak{H}$?

First, relationships can be drawn up according to the result of applying the alternative 'finite' or 'infinite' to the three indices; secondly, in the case where all three are finite a product relation can be derived.

11. Show that a coset of a group $\mathfrak{G}$ relative to a subgroup $\mathfrak{H}$ is a *subgroup* of $\mathfrak{G}$ if and only if it is the principal coset $\mathfrak{H}$ (cf. footnote 3 to Def. 18).

Otherwise the quotient condition of Theorem 19 [63], and especially the existence of the unity element according to Theorem 14 [58], would be violated.

9. Normal Divisors, Conjugate Subsets of a Group, Factor Groups

1. By a *subconfiguration* Ψ of a geometric configuration Φ we understand any subset of parts of Φ , therefore, for instance, a vertex, edge, face, axis, or a system of the same kind or of different kinds of such elements. Let $\mathfrak{G}$ be the group of coincidence motions of Φ (Section 6, Exer. 1).—Prove successively:

(a) The coincidence motions of Φ which—starting from a fixed initial position of Φ —are at the same time coincidence motions of Ψ form a subgroup $\mathfrak{H}$ of $\mathfrak{G}$.

(b) If the coincidence motion S of Φ takes the subconfiguration Ψ into the position of the subconfiguration Ψ' , then $\mathfrak{H}' = S^{-1}\mathfrak{H}S$ is the subgroup belonging to Ψ' in the sense of (a).

(c) Thus, to the entire system of subconfigurations generated from Ψ by the coincidence motions of Φ there corresponds the entire system of subgroups conjugate to $\mathfrak{S}$ in $\mathfrak{G}$. (Here it need not be true that different subconfigurations correspond also to different conjugate subgroups; cf. Exer. 6.)

(d) If the subconfiguration Ψ is carried into itself by all coincidence motions of Φ (*invariant subconfiguration*—special case $\mathfrak{S} = \mathfrak{G}$ in (a) to (c)), then those coincidence motions of Φ which leave Ψ unchanged form a normal divisor $\mathfrak{N}$ of $\mathfrak{G}$. Here it could be that $\mathfrak{N}$ coincides neither with $\mathfrak{E}$ nor with $\mathfrak{S} = \mathfrak{G}$. This can be seen, for instance, by the following example: Φ a regular tetrahedron, Ψ the system of the three midpoint-of-edges axes visualized as undirected lines.

(e) Likewise, a normal divisor of $\mathfrak{G}$ is formed by the coincidence motions of Φ which are at the same time coincidence motions for any one subconfiguration of the system in (c).

(a) follows from Theorem 19 [63]; (b) and (c) by Def. 21, Theorem 29; then (d) by Def. 19; (e) by Theorem 33.

2. Determine all systems of conjugate subgroups of the dihedral groups $\mathfrak{D}_n$ and of the tetrahedral group $\mathfrak{T}$; in particular, determine all normal divisors as well as the factor groups belonging to these normal divisors.

Illustrate the geometric meaning of the subgroups obtained in Section 7, Exer. 2, 3 by finding the associated subconfigurations, and use the result of Exer. 1.—In the dihedral case think of the top- and undersides of a face as two different subconfigurations (cf. Section 6, Exer. 2).

3. Determine the classes of conjugate elements in the dihedral groups $\mathfrak{D}_n$ and in the tetrahedral group $\mathfrak{T}$, and show that the normal divisor criterion in Theorem 32 is valid in these cases.

See the explanations to Section 7, Exer. 2, 3, as well as the special case typical of the dihedral groups given in Example 2.

4. There are other regular polyhedrons besides those considered in Section 6, Exer. 2, for example, the octahedron and hexahedron, as well as the icosahedron and dodecahedron.—Prove: The groups of coincidence motions of the first two configurations have the *same* group type (*octahedral group* $\mathfrak{D}$) and similarly for the last two (*icosahedral group* $\mathfrak{I}$).

Apply Exer. 1 (a) by noting that each polyhedron of a pair can be represented as an (invariant) subconfiguration of the other.

5. Determine the classes of conjugate elements in the octahedral group $\mathfrak{D}$ and in the icosahedral group $\mathfrak{I}$.

The elements are given by rotations around the following three kinds of axes: (a) through two opposite vertices; (b) through two centers of opposite faces; (c) through two midpoints of opposite edges. Let A be a rotation—starting from a fixed initial position—around the axis A through the angle α . Then form the rotation $A' = S^{-1}AS$, the transform of A by S . As in Exer. 1 (b), the latter is a rotation through the same angle α around the axis A' , the position to which the axis A is taken by the coincidence motion S .

6. Determine the normal divisors of the octahedral group $\mathfrak{D}$ and prove that the icosahedral group $\mathfrak{I}$ has no proper normal divisor (is *simple*). Illustrate the geometric meaning of the resulting normal divisors of $\mathfrak{D}$ by finding the associated subconfigurations of the octahedron in the sense of Exer. 1, (e).

Use Theorem 32, Exer. 5, and Theorem 25 [68] to determine the possible orders of subgroups by the additive combinations of the numbers specifying how many elements are in the classes of conjugate elements. This process is restricted from the beginning by the fact that the class consisting only of E must always be used.

7. Prove: A subgroup of index 2 of an arbitrary group must be a normal divisor.

This follows easily by Def. 19.

8. Prove: The centrum (Section 7, Exer. 8) of an arbitrary group is always a normal divisor.

This is again a simple consequence of Def. 19.

9. The mapping of the elements S of a group $\mathfrak{G}$ on the cosets $\mathfrak{S}S$ relative to a normal divisor $\mathfrak{S}$, that is, on the elements $\bar{S}$ of the factor group $\bar{\mathfrak{G}} = \mathfrak{G}/\mathfrak{S}$, is a unique (if $\mathfrak{S} > \mathfrak{E}$ it is not one-to-one) mapping of $\mathfrak{G}$ on $\bar{\mathfrak{G}}$ with the property:

$$S \rightarrow \bar{S}, T \rightarrow \bar{T} \text{ implies } ST \rightarrow \bar{S}\bar{T}.$$

A mapping with this property is called a *homomorphism* of $\mathfrak{G}$ on $\bar{\mathfrak{G}}$.—Show that conversely *every* homomorphism of $\mathfrak{G}$ on another group $\bar{\mathfrak{G}}$ is generated as above from a normal divisor $\mathfrak{S}$ of $\mathfrak{G}$; that is, associated with any such homomorphism there must exist a normal divisor $\mathfrak{S}$ of $\mathfrak{G}$ such that $\bar{\mathfrak{G}} \cong \mathfrak{G}/\mathfrak{S}^1$ and the given homomorphism comes about through $S \rightarrow \mathfrak{S}S$ and an isomorphism between $\mathfrak{G}/\mathfrak{S}$ and $\bar{\mathfrak{G}}$.

According to Theorem 35 we only have to show that the convention:

$$S \equiv T \text{ if } \bar{S} = \bar{T}$$

defines a congruence relation in $\mathfrak{G}$.

10. On the basis of Exer. 9 prove once more that to any invariant subconfiguration Ψ of Φ there corresponds a normal divisor $\mathfrak{S}$ of the group $\mathfrak{G}$ of coincidence motions of Φ [Exer. 1, (d)].

The coincidence motions of Φ are mapped homomorphically on the coincidence motions of ψ .

11. Let $\mathfrak{S}$ be a subgroup of the group $\mathfrak{G}$ and $\mathfrak{N}$ the totality of those elements S of $\mathfrak{G}$ for which $\mathfrak{S}S = S\mathfrak{S}$, or therefore $S^{-1}\mathfrak{S}S = \mathfrak{S}$ (the *normalizer of the subgroup $\mathfrak{S}$ in $\mathfrak{G}$*).—Prove successively:

¹ We use $\cong$ as a symbol for *isomorphism*.

(a) $\mathfrak{N}$ is a subgroup of $\mathfrak{G}$.

(b) $\mathfrak{H}$ is a normal divisor of $\mathfrak{N}$.

(c) If $\mathfrak{H}$ is a normal divisor of a subgroup $\bar{\mathfrak{H}}$ of $\mathfrak{G}$, then $\bar{\mathfrak{H}}$ is contained in $\mathfrak{N}$.

Briefly: The normalizer $\mathfrak{N}$ of $\mathfrak{H}$ in $\mathfrak{G}$ is the largest subgroup of $\mathfrak{G}$ which has $\mathfrak{H}$ as a normal divisor.

(a) follows from Theorem 19 [63]; (b) and (c) most simply from Def. 19.

12. Prove: The number of different conjugate subgroups of $\mathfrak{H}$ in $\mathfrak{G}$ is equal to the index of the normalizer $\mathfrak{N}$ of $\mathfrak{H}$ in $\mathfrak{G}$. Therefore, in particular, for finite $\mathfrak{G}$ this number is always a divisor of the order of $\mathfrak{G}$.

Show that the complete system of subgroups of $\mathfrak{G}$ conjugate to $\mathfrak{H}$ can be written in the form $S^{-1}\mathfrak{H}S$, where S runs through the representatives of a complete left residue system of $\mathfrak{G}$ relative to $\mathfrak{N}$.

13. In Exer. 11 and 12 replace the subgroup $\mathfrak{H}$ by a single element A of $\mathfrak{G}$ so that $\mathfrak{N}$ now becomes the totality of those elements of $\mathfrak{G}$ which commute with A (the *normalizer of the element A* in $\mathfrak{G}$).—Prove similarly: $\mathfrak{N}$ is a subgroup of $\mathfrak{G}$; its index is equal to the number of different elements in $\mathfrak{G}$ conjugate to A . Therefore, in particular, for finite $\mathfrak{G}$ this number is always a divisor of the order of $\mathfrak{G}$. Furthermore: The period of A (Section 7, Exer. 7) is a normal divisor of $\mathfrak{N}$, and $\mathfrak{N}$ is a normal divisor of the normalizer of the period of A .

14. Let $\mathfrak{H}$ and $\mathfrak{J}$ be subgroups of a group $\mathfrak{G}$ such that $\mathfrak{J}$ is contained in the normalizer of $\mathfrak{H}$. Let $\mathfrak{K} = \{\mathfrak{H}, \mathfrak{J}\}$ be the composite, $\mathfrak{D} = [\mathfrak{H}, \mathfrak{J}]$ the intersection of $\mathfrak{H}$ and $\mathfrak{J}$.—Prove successively:

(a) $\mathfrak{H}$ is a normal divisor of $\mathfrak{K}$, $\mathfrak{D}$ is a normal divisor of $\mathfrak{J}$.

(b) For the factor groups we have $\mathfrak{K}/\mathfrak{H} \cong \mathfrak{J}/\mathfrak{D}$.

(c) If $\mathfrak{H}$ and $\mathfrak{J}$ are actually normal divisors of $\mathfrak{G}$, then $\mathfrak{K}$ and $\mathfrak{D}$ are also normal divisors of $\mathfrak{G}$.

(a) and (c) immediately follow from Def. 19 and the hypothesis. For (b) start with a complete residue system of $\mathfrak{J}$ relative to $\mathfrak{D}$ and show that it is also a complete residue system of $\mathfrak{K}$ relative to $\mathfrak{D}$.

15. Prove: If $\mathfrak{H}$ is a normal divisor of $\mathfrak{G}$ with finite index j , then S^j belongs to $\mathfrak{H}$ for every S of $\mathfrak{G}$.

Apply Section 8, Exer. 4.

16. Prove: The additive group of all rational (or all real) numbers and the multiplicative group of all real positive numbers have no proper subgroups of finite index.

Apply Exer. 15 as well as Section 7, Exer. 14.

17. Determine all subgroups $\mathfrak{H}$ of finite index in the multiplicative group $\mathfrak{G}$ of all real numbers $\neq 0$.

Such a subgroup is the group $\mathfrak{J}$ of the positive real numbers. For an arbitrary subgroup $\mathfrak{H}$ of finite index, consider the intersection $\mathfrak{D}$ with $\mathfrak{J}$ and apply Exer. 14, 16.

18. Prove: If C is the (let us say, right) commutator of A and B (Section 6, Exer. 5), then for arbitrary natural numbers m and n the (right) commutator $C_{m,n}$ of A^m and B^n is a product of transforms of C .

First calculate successively the commutators of $A, B^2; \dots; A, B^n$; then of $A^2, B^n; \dots; A^m, B^n$.

19. Prove: If C is the (let us say, right) commutator of A and B , then $S^{-1}CS$ is the (right) commutator of $S^{-1}AS$ and $S^{-1}BS$.

20. By the *commutator group* $\mathfrak{C}$ of a group $\mathfrak{G}$ we mean the subgroup of $\mathfrak{G}$ generated by the set of all commutators of every pair of elements of $\mathfrak{G}$ (Section 7, Exer. 6).—Prove successively:

(a) $\mathfrak{C}$ is a normal divisor of $\mathfrak{G}$.

(b) The factor group $\mathfrak{G}/\mathfrak{C}$ is Abelian.

(c) If $\mathfrak{H}$ is any normal divisor of $\mathfrak{G}$ with Abelian factor group $\mathfrak{G}/\mathfrak{H}$, then $\mathfrak{C}$ is contained in $\mathfrak{H}$.

Briefly: The commutator group $\mathfrak{C}$ is the smallest normal divisor of $\mathfrak{G}$ with Abelian factor group.

(a) follows most simply, according to Theorem 32, from Exer. 19; for (b) and (c) study the congruence relations corresponding to $\mathfrak{C}$ and $\mathfrak{H}$ according to Theorems 34, 35.

21. Determine the centrum and commutator group of the Abelian groups, the dihedral groups $\mathfrak{D}_n$, the tetrahedral group $\mathfrak{T}$, the octahedral group $\mathfrak{O}$, and the icosahedral group $\mathfrak{I}$.

For this purpose take into consideration Exer. 5, 6, as well as Section 6, Exer. 2, 3 and Section 7, Exer. 2, 3.

Vol. 1. Chapter III. Linear Algebra without Determinants

10. Linear Forms, Vectors, Matrices

1. Are the two linear forms

(a) x_1 and $x_1 + x_2$,

(b) $x_1 + x_2$ and $x_1 - x_2$

linearly independent?

Between these forms set up a linear relation with indeterminate coefficients c_1, c_2 and try to deduce that $c_1 = 0, c_2 = 0$ must be valid. Case (b) depends on whether $2e = 0$ or $2e \neq 0$ in the ground field K .¹

2. Show that, within the domain of all functions (in the sense of analysis) of $x_1, \dots, x_n$ over K , linear forms are characterized by the property of Theorem 44.

Apply the property in question to the linear combination $\mathbf{r} = \sum_{k=1}^n x_k \mathbf{e}_k$ of the vector $\mathbf{r} = (x_1, \dots, x_n)$ and the unit vectors $\mathbf{e}_k$, and also take Theorem 45 into consideration.

3. By the *product* of an (m, n) -rowed matrix $A = (a_{ik})$ by an $(n, \bar{o})$ -rowed matrix $B = (b_{ik})$ we mean the $(m, \bar{o})$ -rowed matrix $C = (c_{ik})$ with

$$c_{ik} = \sum_{l=1}^n a_{il} b_{lk} \quad (i = 1, \dots, m; k = 1, \dots, \bar{o})$$

¹ That is, whether the *characteristic* of K is equal to 2 or different from 2. Regarding this, see the general theory in Vol. 2, Section 4, especially Def. 14 [202].—This distinction will frequently be important in the following.

for which, therefore, c_{ik} is the inner product of the i -th row of A by the k -th column of B .—Show that this product matrix C results as the matrix of a system of linear forms in the following two ways:

(a) In the m linear forms $f_i(\mathfrak{x}) \equiv \sum_{l=1}^n a_{il} x_l$ ($i = 1, \dots, m$) with the matrix A substitute for the n indeterminates x_l the linear forms $\sum_{k=1}^o b_{lk} y_k$ ($l = 1, \dots, n$) with the matrix B in o new indeterminates y_k ; in doing so m new linear forms $g_i(\mathfrak{y})$ are derived (transformation of a system of linear forms to new indeterminates).

(b) From the n linear forms $f_l(\mathfrak{x}) \equiv \sum_{k=1}^o b_{lk} x_k$ ($l = 1, \dots, n$) with the matrix B form the m linear combinations $\sum_{l=1}^n a_{il} f_l$ ($i = 1, \dots, m$) with the matrix A ; in doing so m new linear forms $g_i(\mathfrak{x})$ are derived (transformation of a system of linear forms to a new system in the same indeterminates).

4. Prove that the matrix multiplication defined in Exer. 3 satisfies the associative law and, together with the matrix addition given by (2'), satisfies the distributive law; on the contrary, show that the commutative law of multiplication is not generally valid for matrix multiplication.

The associative and distributive laws are proved by writing out the expressions for $A(BC)$, $(AB)C$, $(A+B)C$, $AC+BC$, $C(A+B)$, $CA+CB$ resulting from the definitions (the two-sided distributivity must be shown) and applying the corresponding laws to the elements of the ground field. Naturally, it is implicitly assumed that the number of rows in each of the matrices A, B, C in question is such that the definitions of sum in (2') and product in Exer. 3 can be applied. For the commutative law we merely have to consider matrices A, B

with one and the same number of rows and columns n (n -rowed square matrices). Among such matrices it is easy to find examples in the case $n > 1$ for which $AB \neq BA$.

5. This means, in particular, that the n -rowed square matrices with a fixed number of rows n (over the ground field K) form a *non-commutative ring* (according to the generalization of the ring concept in Def. 1 [15]).—Prove: In this ring there is a uniquely determined unity element, that is, to every n there is one and only one n -rowed square matrix E_n with the properties:

$E_n A = A$ for all matrices A with n rows (and n columns or also any number of columns),

$A E_n = A$ for all matrices A with n columns (and n rows or also any number of rows),

(n -rowed identity matrix; when n is obvious from the context, it is also denoted simply by E).

The n -rowed square matrix E_n whose rows (or columns) are the n unit vectors $e_1, \dots, e_n$ satisfies the requirements. To prove the uniqueness apply either one of the above conditions to the case wherein E_n is an unknown n -rowed square matrix X and A is the matrix E_n just specified.

6. Construct the *transposition matrix* V_{ik} which by left multiplication interchanges the i -th row of an arbitrary matrix A with the k -th row. Next, construct the *multiplication matrix* $U_i(t)$ which again by left multiplication multiplies the elements of the i -th row of A by t but leaves all other rows unchanged. Finally, form the *addition matrix* W_{ik} which by left multiplication adds the k -th row of A to the i -th while leaving all other rows unchanged. What happens when A is multiplied on the right by these three matrices? From

$U_i(t)$ and W_{ik} also form a matrix which by left multiplication adds the k -th row of A multiplied by t to the i -th. (Naturally, the implicit assumption of Exer. 4, 5 must also be in force here.)

If the required matrix cannot be immediately found, it can be set up in the form (t_{ik}) with unknowns t_{ik} . On forming the product $(t_{ik}) \cdot A$ we obtain simple equations for the t_{ik} on the basis of the uniqueness (cf. (1)).

7. Let A be an n -rowed square matrix. If A_r^{-1} (or A_l^{-1}) is an n -rowed square matrix such that

$$AA_r^{-1} = E \quad (A_l^{-1}A = E),$$

then we say that A_r^{-1} is a *right* (A_l^{-1} a *left*) *inverse* to A .¹—Prove: If A_r^{-1}, B_r^{-1} are *right* (A_l^{-1}, B_l^{-1} *left*) inverses to the n -rowed square matrices A, B , then $B_r^{-1}A_r^{-1}$ is a right ($B_l^{-1}A_l^{-1}$ a left) inverse to AB .

Apply the associative law of matrix multiplication.

8. Prove: If an n -rowed square matrix A has a right (left) inverse, then there can be no more than one left (right) inverse to A . If right and left inverses to A exist, then they are equal to one another; in this case we use the simple notation A^{-1} .

The proof of both statements follows by multiplying the hypothetical equations $Y_1A = E$ and $Y_2A = E$ ($AX_1 = E$ and $AX_2 = E$) on the right by A_r^{-1} (on the left by A_l^{-1}).

9. Confirm the statement in footnote 3 to Def. 28 regarding the inner vector product. Use this matrix interpretation of the inner product of two vectors $a = (a_k)$ (one-rowed matrix)

¹ In this regard cf. also Theorem 18 [2], as well as Exer. 1, 3, 4, to Section 14, given later.

and $\mathbf{b} = (b_i)$ (one-column matrix) to determine the result of interchanging the factors.

The n -rowed square matrix $(b_i a_k)$.

10. Prove: The system of linear forms $f_i(\mathbf{x}) \equiv \sum_{k=1}^n a_{ik} x_k$ ($i = 1, \dots, m$) with the matrix $A = (a_{ik})$ can be written in the simple form $A\mathbf{x}$, where $\mathbf{x}$ represents a one-column matrix (x_i) .

This immediately follows from the definition of matrix product in Exer. 3.

11. Write the linear combination $\sum_{i=1}^m c_i f_i$ as a matrix product.

$\mathbf{c}A\mathbf{x}$, where $\mathbf{c} = (c_k)$ (one-rowed matrix).—According to Exer. 4 parentheses are not needed.

12. (a) Write the quadratic form

$$Ax_1^2 + 2Bx_1x_2 + Cx_2^2$$

as the product of three matrices.

(b) Similarly, write the known transformation formulae for the rotation of an orthogonal Cartesian system of coordinates through the angle α as the product of two matrices; do so in two ways.

(c) Carry out these transformations on the form (a) and express the new coefficients in terms of the product of matrices.

For (a). Among other things, we need the matrix $\begin{pmatrix} A & B \\ B & C \end{pmatrix}$.

For (b). $\mathbf{r} = \mathbf{x}'T$ or $\mathbf{x} = T'\mathbf{x}'$, where T is a two-rowed square matrix whose elements are formed from $\sin \alpha$ and $\cos \alpha$. (Cf. Exer. 10 for $m = n = 2$.)

For (c). Use the associative law (Exer. 4).

13. Prove the transposition rule $(AB)' = B'A'$. For square matrices A how does this rule tie the inverse of A' to that of A ?

The transposition rule is proved by writing out the expressions which are obtained by applying the definitions to both sides. It follows: If A_r^{-1} is a right [A_r^{-1} a left] inverse to A , then $(A_r^{-1})'$ is a left [$(A_r^{-1})'$ a right] inverse to A' .

14. Let $n = \nu_1 + \nu_2 + \cdots + \nu_r$ be a decomposition of n as a sum of positive integers $\nu_1, \nu_2, \dots, \nu_r$. Let the square array of the (n, n) -rowed matrix A be correspondingly subdivided into rectangular submatrices:

	ν_1	ν_2	$\dots$	ν_r
ν_1	A_{11}	A_{12}		A_{1r}
ν_2	A_{21}	A_{22}		A_{2r}
$\vdots$				
ν_r	A_{r1}	A_{r2}		A_{rr}

Prove: If

$$A = (A_{i\kappa}) \quad \text{and} \quad B = (B_{i\kappa}) \quad (i, \kappa = 1, 2, \dots, r)$$

are two matrices subdivided according to this scheme, then

$$AB = \left(\sum_{\lambda=1}^r A_{i\lambda} B_{\lambda k} \right)$$

in this division. Therefore, the multiplication of matrices A in terms of the matrices $A_{i\kappa}$ is carried out by a rule entirely analogous to the definition of ordinary matrix multiplication (Exer. 3).

On using the definition of multiplication given in Exer. 3 this rule easily follows by decomposing the sum, which represents the element in the i -th row and k -th column of the product matrix AB , into partial sums corresponding to the underlying division of the square array.

11. Nonhomogeneous and Homogeneous Systems of Linear Equations

1. Write the systems of linear equations (J), (H), (H') by means of matrix products.

See Section 10, Exer. 10.

2. The n -termed vectors over the field K form an Abelian group $\mathfrak{G}$ with respect to addition (Section 6, Example 1). The solutions of (H) (including the identical solution) form a subgroup $\mathfrak{H}$ of $\mathfrak{G}$. The solutions of (J) form a residue class relative to $\mathfrak{H}$ in $\mathfrak{G}$.

See Theorems 47, 46 and Theorem 19 [63].

3. Find a system of fundamental solutions for the homogeneous system consisting of the single equation

$$x_1 + \cdots + x_n = 0 \quad (n \geq 2).$$

The $n-1$ vectors $0, \dots, 0, e, -e, 0, \dots, 0$ are (a) linearly independent, (b) solutions of the equation, and (c) every solution is a linear combination of these.

4. Accordingly, represent the general solution of this equation by independent parameters.

$$x_1 = \xi_1, x_2 = \xi_2 - \xi_1, \dots, x_{n-1} = \xi_{n-1} - \xi_{n-2}, x_n = -\xi_{n-1}.$$

5. Accordingly, what is the general solution of the nonhomogeneous system consisting of the single equation

$$x_1 + \cdots + x_n = a?$$

A particular solution of this equation can be immediately given (if $ne \neq 0$ it can even be given in a symmetric form). Then apply Theorem 46.

6. By using a single product of matrices express the fact that the vectors $\xi_1, \dots, \xi_n$ are solutions of (H).

$AX = 0$, where A is the (m, n) -rowed matrix of (H) and X the (n, s) -rowed matrix formed from the $\xi_1, \dots, \xi_s$ as columns.

7. What restriction must be imposed on the right sides of the nonhomogeneous system

$$\begin{array}{rcl} x_1 & - & x_2 \doteq a_1 \\ x_2 & - & x_3 \doteq a_2 \\ \dots\dots\dots & & (n \geq 2) \\ x_{n-1} & - & x_n \doteq a_{n-1} \\ x_n & - & x_1 \doteq a_n \end{array}$$

due to the obvious dependence of the left sides?

Apply Theorem 48 and Exer. 3, 4.

12. The Toeplitz Process

1. Let C be an m -rowed square matrix with a left inverse C_l^{-1} (Section 10, Exer. 7). Through left multiplication by C the system of equations

$$(J) \quad Ax \doteq a$$

yields the system of equations

$$(J_C) \quad CAx \doteq Ca.$$

Any system (J_C) so generated will be said to be *linked* with (J) .—Show that a linkage is an equivalence relation in the sense of Section 2, (I), and that linked systems are equivalent in the sense of Def. 30.

Note that (J) can be regained from (J_C) through left multiplication by C_l^{-1} , and also take Section 10, Exer. 5, 7 into consideration.

2. Show that the equivalence relation between (J) and (J_0) constructed in the proof of the Theorem of Toeplitz is a linkage.

Due to the transitivity of linkages (Exer. 1) it is enough to establish this for the two steps of the Toeplitz process separately, that is, on the one hand, for (J) and $(\bar{J}_0)$, on the other hand, for $(\bar{J}_0)$ and (J_0) .

For the *first* step ($\bar{J}_0$) has to be interpreted as a formal m -termed system by the addition of $m - r$ zero equations. It must then be shown:

(a) (J) is generated from the new ($\bar{J}_0$) through left multiplication by a matrix of the type $\begin{pmatrix} E_r & 0 \\ C & E_{m-r} \end{pmatrix}$.—For this purpose take into consideration relations (5), (6) as well as Section 10, Exer. 3. (b).

(b) This matrix has a left inverse.—By taking Section 10, Exer. 14 into consideration it can be immediately written out, namely $\begin{pmatrix} E_r & 0 \\ -C & E_{m-r} \end{pmatrix}$.

Similarly, for the *second* step we only have to show that the matrix C on the right in (7) has a left inverse C_l^{-1} . Then the m -rowed square matrix $\begin{pmatrix} C & 0 \\ 0 & E_{m-r} \end{pmatrix}$ to be formed because of what was done at the first step (carrying along the $m - r$ zero equations) also has a left inverse, namely $\begin{pmatrix} C_l^{-1} & 0 \\ 0 & E_{m-r} \end{pmatrix}$. The existence of C_l^{-1} follows if each of the nonhomogeneous systems of linear equations formed with C and one of the unit vectors on the right side can be solved. This is certain by recursion (from lower to higher numbers); see the end of the proof to the Theorem of Toeplitz.

3. In the proof of the Theorem of Toeplitz we made special assumptions 'for reasons of notation only' regarding the ordering of the equations of Exer. 2. In order that these, too, may be subsumed, show: The equivalence relation resulting from an arbitrary rearrangement of the equations of a system is a linkage.

A rearrangement is generated through left multiplication by a matrix P which has the unity element e at exactly one position in each row and in each column, otherwise only zeros (cf. Section 10, Exer. 6). It is easy to find a left inverse of such a matrix P , namely, its transpose P' .

4. Carry the Toeplitz process through for the system of equations

$$x_1 + x_2 \doteq a_1$$

$$x_1 - x_2 \doteq a_2.$$

See the explanation to Section 10, Exer. 1 (b).

13. Solvability and Solutions of Systems of Linear Equations

1. Prove directly, without using the Theorem of Toeplitz, that the necessary condition for the solvability of (J) (Theorem 48 [92]) is sufficient (Theorem 49). Use mathematical induction on the number n of unknowns.

For the reduction from n to $n-1$ unknowns replace x_n by a suitable element ξ_n . In order to determine this ξ_n , there are two cases to be handled:

(a) x_n can be represented as a linear combination of the $f_i(x)$:

$$x_n \equiv c_1 f_1(x) + \cdots + c_m f_m(x).$$

In this case set

$$\xi_n = c_1 a_1 + \cdots + c_m a_m.$$

Due to the necessary condition for solvability, this ξ_n does not depend on the determination of $c_1, \dots, c_m$, which may possibly be done in many ways.

(b) x_n cannot be represented as a linear combination of the $f_i(x)$. Then ξ_n can be arbitrarily chosen (say $\xi_n = 0$).

Then consider the new system

$$a_{i1}x_1 + \cdots + a_{i, n-1}x_{n-1} \doteq a_i - a_{in}\xi_n \quad (i = 1, \dots, m)$$

with $n-1$ unknowns and establish that it, too, satisfies the necessary condition for solvability. This follows from the fact that a linear relation between the new left sides, which does not reduce to a linear relation between the old $f_i(x)$, gives rise to a representation of x_n as a linear combination of the $f_i(x)$, whence according to the determination of ξ_n in the case (a) the existence of this linear relation also can be inferred for the new right sides.

2. Prove directly, without using the Theorem of Toeplitz, that more than m m -termed vectors are always linearly dependent (Lemma 1): in other words, (H) can always be solved for $n > m$. For this purpose use mathematical induction on m .

In order to reduce the statement about (H) from m to $m-1$ equations we again distinguish the two cases (a) and (b) of the discussion in Exer. 1.

In the case (a) the left sides of the homogeneous system

$$a_{i1}x_1 + \cdots + a_{i, n-1}x_{n-1} \doteq 0 \quad (i = 1, \dots, m)$$

generated by the substitution $x_n = 0$ are linearly dependent; therefore, on omitting one linearly dependent equation this system is further reduced to $m-1$ equations in $n-1 > m-1$ unknowns.

In the case (b) the system

$$a_{i1}x_1 + \cdots + a_{i, n-1}x_{n-1} \doteq -a_{in}$$

generated by the substitution $x_n = e$ satisfies the necessary condition for solvability, and this brings us back to Exer. 1.

3. In the proof of Theorem 52 the trivial fact is established under (a) that if all $f_i = 0$, then all ξ are solutions of (H).—Show directly, without using the Theorem of Toeplitz and Theorem 52 proved with its help, that conversely if all ξ are solutions of (H) then all $f_i = 0$.

The relation $A = 0$ to be proved follows columnwise by the substitution of the n unit vectors $e_1, \dots, e_n$ for ξ .

4. The totality of solutions of (H) can be described as the totality $\mathfrak{B}$ of those n -termed vectors b whose inner product with the m given vectors a_i (the rows of the matrix A of (H)), and consequently with the totality $\mathfrak{A}$ of linear combinations a of the a_i , yields the result $ab = 0$.—Show that this relation between the two vector sets $\mathfrak{A}$ and $\mathfrak{B}$ is reversible, that is, that $\mathfrak{A}$ is at the same time the totality of all n -termed vectors a whose inner product with all of the vectors b of $\mathfrak{B}$, or—which amounts to the same thing—only with the $n-r$ vectors b_j of a system of fundamental solutions of (H), yields the result $ab = 0$.—To achieve full symmetry and analogy, the set $\mathfrak{A}$ may also be described, in the statement first made, as the totality of linear combinations of the r vectors of $\mathfrak{A}$

maximal system of linearly independent vectors among the a_i (Lemma 2), or we can also assume from the beginning without loss of generality that $r = m$.

Let $\mathfrak{A}'$ be the totality of a with $ab = 0$ for all b in $\mathfrak{B}$. Then $\mathfrak{A}$ is in any case a subset of $\mathfrak{A}'$. Now, $\mathfrak{A}'$ can be thought of as the totality of solutions of the linear homogeneous system $rb_j = 0$ ($j = 1, \dots, n-r$). Apply Theorem 52 to this system in order to show that the already defined r vectors a_i form a system of fundamental solutions for this system, and consequently $\mathfrak{A} = \mathfrak{A}'$.

5. Show, for homogeneous systems in the first instance, that the converse to Section 12, Exer. 1 is valid, namely, that equivalent systems are linked.

According to the statements in the first step of the Toeplitz process in Section 12, Exer. 2 any homogeneous system $f_i(x) = 0$ is linked with that homogeneous system which is obtained by restricting oneself to a maximal system of linearly independent f_i ; in view of the statements made there regarding the connection between the first and second steps it can therefore be assumed without loss of generality that the two equivalent homogeneous systems are formed from linearly independent linear forms. Due to the equivalence they then have, according to Theorem 52, the same number r of equations. Next, apply Exer. 4, by which the r row vectors of the matrix of each of the two systems form a system of fundamental solutions of one and the same homogeneous system of equations (arising from the common totality of solutions of the original systems). From this we can easily deduce the linkage to be proved (proof to Theorem 51).

6. Conversely, show that the equivalence of nonhomogeneous systems (which can be solved) also implies their linkage.

If $Ax = a$, $Bx = b$ are the two systems, and x_0 is a particular solution, then the substitution $u = x - x_0$ yields two equivalent homogeneous systems $Au = 0$, $Bu = 0$; these are linked according to Exer. 5; consequently, the two original systems are linked on the basis of the same linking matrix.

7. Set up a system of fundamental solutions for the homogeneous system consisting of the single equation

$$x_1 + \cdots + x_n \doteq 0$$

by the method of the proof of Theorem 52 (Toeplitz process). Show how this is related to the system of fundamental solutions obtained in Section 11, Exer. 3, using the proof to Theorem 51 as a model (linear representation of two systems through one another).

14. The Case $m = n$

1. Prove: A has a right inverse if and only if A is regular.

Apply Theorem (46, 48, 49)a by noting: The existence of a right inverse to A is tantamount to the solvability of the system (J) belonging to A with each of the n unit vectors $e_1, \dots, e_n$ on the right, and therefore with any arbitrary vector a on the right.

2. Prove: A' is regular if and only if A is regular.

This follows immediately from Theorem (52, 53, 54)a.

3. Prove: A has a left inverse if and only if A is regular.

This follows by combining Exer. 1, 2, and Section 10, Exer. 13.

4. This means that right and left inverses to A exist simultaneously, if at all (namely, if A is regular), and are then uniquely determined and equal to one another (Section 10, Exer. 8).—Show that the resolvent matrix A^* of a regular A coincides with the inverse A^{-1} .

This is an immediate consequence of the matrix interpretation of part (a) of the proof of Theorem 55; see the discussion to Exer. 1.

5. What condition must the four coefficients of a two-rowed square matrix A satisfy if A is to be regular? In this case what is its resolvent matrix?

The condition says: $a_{11}a_{22} - a_{12}a_{21} \neq 0$. In order to establish its sufficiency as well as to answer the last question, see—if necessary—the remarks after Def. 38 [127] relative to the case $n = 2$. That it is necessary can be established, according to Theorem (52, 53, 54)a, by interpreting the relation $a_{11}a_{22} - a_{12}a_{21} = 0$, as far as possible, as either (H) or (H') being non-identically satisfied; the case where neither of the two is true is trivial.

15. The Importance of Linear Algebra without Determinants

1. In the field consisting of 0 and e alone (Section 1, Example 4) carry out the Toeplitz process in finitely many steps exactly in accordance to the scheme of Section 12 and thereby, in particular, also confirm that the necessary condition for solvability is satisfied in the case of the system of equations

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 + x_5 &\doteq 0 \\ x_1 \quad \quad + x_3 + x_4 + x_5 &\doteq 0 \\ x_1 + x_2 \quad \quad + x_4 &\doteq e \\ \quad \quad x_2 + x_3 \quad \quad + x_5 &\doteq e. \end{aligned}$$

Only 0 and e can be used as multipliers for the linear combinations and especially for the possible linear dependences. All combinations in question can be quickly checked for each step carried out according to the scheme.

2. The concept of *skew field* is generated by dropping the commutative law (2) of multiplication from the field axioms Section 1, (c) and supplementing (5), (6), (7), thereby becoming unsymmetrical, by analogous postulates with reversed sequence of factors.—Show that the results obtained in Sections 10 to 14 regarding systems of linear equations are also valid in a skew field K by properly fixing the sequence of factors.

By always regarding the sequence of the factors as essential, establish that Theorem 44 [86] remains valid if we take the multipliers c_i as *right* factors, corresponding to the obvious restrictions in Theorem 43 [85]. With this modification maintained throughout, Theorems 46, 47 [91] also remain valid. Furthermore, Theorem 48 [92] remains valid except that in its corollaries, as generally henceforth, (H') must be understood as written with the sequence of factors reversed (therefore, coefficients on the *right*). With the specified modifications all facts derived in Sections 12 to 14 are then valid. In Theorem 53 [109], with (H') suitably modified, r' has, of course, to be taken as the maximal number of linearly independent columns relative to linear combination with *right* factors, whereas r itself refers to the rows under *left* multiplication.

It is an open question whether there is a connection between (H) and the transpose system of equations with coefficients on the *left*, in other words, between the maximal numbers of linearly independent rows and columns in both cases relative to *left* multiplication.

Vol. 1. Chapter IV. Linear Algebra with Determinants

16. Permutation Groups

1. Let $\mathfrak{P}$ be an arbitrary n -termed permutation group, that is, an arbitrary subgroup of $\mathfrak{S}_n$. If a permutation of $\mathfrak{P}$ takes a numeral i into a numeral k , then k is said to be *connected* with i by $\mathfrak{P}$.—Prove: Connectedness is an equivalence relation.

It is easy to confirm that Section 2, (α) , (β) , (γ) are satisfied on the basis of the group properties of $\mathfrak{P}$.

2. Let the numerals $1, \dots, n$ be partitioned into r mutually exclusive classes (combinations) $\mathfrak{C}_1, \dots, \mathfrak{C}_r$ such that all numerals of a combination are connected with one another by $\mathfrak{P}$, while the numerals of different combinations are not.—Prove: Every permutation P of $\mathfrak{P}$ can be represented as the product of r permutations $P_1, \dots, P_r$, where P_ρ permutes the numerals of $\mathfrak{C}_\rho$ only among themselves and takes the numerals of all other $\mathfrak{C}_{\rho'}$ into themselves. The P_ρ commute with one another, and there is (apart from their arbitrary arrangement) only one partition of the specified kind.

This easily follows from

$$\begin{aligned} \left(\begin{array}{cc} i_1 \dots i_\nu & i_{\nu+1} \dots i_n \\ p_{i_1} \dots p_{i_\nu} & p_{i_{\nu+1}} \dots p_{i_n} \end{array} \right) &= \left(\begin{array}{c|c} i_1 \dots i_\nu & i_{\nu+1} \dots i_n \\ p_{i_1} \dots p_{i_\nu} & i_{\nu+1} \dots i_n \end{array} \right) \left(\begin{array}{c|c} i_1 \dots i_\nu & i_{\nu+1} \dots i_n \\ i_1 \dots i_\nu & p_{i_{\nu+1}} \dots p_{i_n} \end{array} \right) \\ &= \left(\begin{array}{c|c} i_1 \dots i_\nu & i_{\nu+1} \dots i_n \\ i_1 \dots i_\nu & p_{i_{\nu+1}} \dots p_{i_n} \end{array} \right) \left(\begin{array}{c|c} i_1 \dots i_\nu & i_{\nu+1} \dots i_n \\ p_{i_1} \dots p_{i_\nu} & i_{\nu+1} \dots i_n \end{array} \right), \end{aligned}$$

where $\mathfrak{C} = (i_1, \dots, i_r)$, $\mathfrak{C}' = (i_{r+1}, \dots, i_n)$ is a partition of $(1, \dots, n)$ into two mutually exclusive combinations, and $P = \begin{pmatrix} i \\ p_i \end{pmatrix}$ ($i = 1, \dots, n$) is a permutation which permutes the numerals of $\mathfrak{C}$ only among themselves, and likewise for the numerals of $\mathfrak{C}'$.

3. Prove: If the permutation P in Exer. 2 runs through the group $\mathfrak{P}$, then P_ρ runs through the permutation groups $\mathfrak{P}_\rho$, which are homomorphic (Section 9, Exer. 9) to $\mathfrak{P}$ on the basis of the correspondences $P \rightarrow P_\rho$.

It is easy to confirm the rule: If $P_1 \dots P_r$ and $P'_1 \dots P'_r$ are partitions of P and P' in the sense of Exer. 2, then $(P, P'_1) \dots (P_r, P'_r)$ is the partition of PP' .

4. An n -termed permutation group $\mathfrak{P}$ is said to be *transitive* if the number r of combinations $\mathfrak{C}_\rho$ in Exer. 2 is equal to 1, therefore, if any numeral i is connected by $\mathfrak{P}$ with any numeral k . For this it is sufficient, of course (Exer. 1), if every numeral i is connected by $\mathfrak{P}$ with a fixed numeral, say 1.—Show: The permutation groups $\mathfrak{P}_\rho$ in Exer. 3 are transitive if they are interpreted as permutation groups of the ν_ρ numerals of $\mathfrak{C}_\rho$ alone (therefore as ν_ρ -termed permutation groups), whereby all numerals remaining unchanged are omitted. The latter means merely an isomorphism.

The transitivity of $\mathfrak{P}_\rho$ is an immediate consequence of the property first used to characterize the combinations $\mathfrak{P}_\rho$ in Exer. 2.

5. Prove: The order of an n -termed transitive permutation group $\mathfrak{P}$ is a multiple of n .

For this purpose prove the existence of a subgroup in $\mathfrak{P}$ of index n by considering the totality $\mathfrak{U}$ of those permutations of $\mathfrak{P}$ which leave a fixed numeral unchanged, say the totality $\mathfrak{U}_1$ belonging to the numeral 1.

6. What subgroups of $\mathfrak{P}$ are conjugate to the subgroup $\mathfrak{U} = \mathfrak{U}_1$ just considered?

The transformation by a permutation P , that carries 1 into i , carries $\mathfrak{U}_1$ into the totality $\mathfrak{U}_i$ of those permutations which leave the numeral i unchanged. Due to the transitivity i can be any one of the numerals $1, \dots, n$.

7. Show: In a transitive n -termed permutation group $\mathfrak{P}$ every permutation leaves at least one numeral unchanged only in the trivial case $n = 1$.

Namely, the n conjugate subgroups $\mathfrak{U}_i$ taken together must exhaust the entire group $\mathfrak{P}$. If p, u are the orders of $\mathfrak{P}, \mathfrak{U}_i$, then the $\mathfrak{U}_i$, altogether, formally have $nu = p$ elements, therefore exactly as many as there are supposed to be different elements among them. But the $\mathfrak{U}_i$ have jointly the unity element in common. This is a contradiction except for $n = 1$.

8. In Exer. 2 to 4 we developed the concept of the *partition* of a permutation group into *transitive components*. Carry this partition through for the special n -termed permutation group $\mathfrak{P}$ which consists of the powers of a given n -termed permutation P (period of P ; Section 7, Exer. 7). Describe the factors P_ρ of the partition $P = P_1 \dots P_r$.

There are two possible cases:

(a) $\nu_\rho = 1$, that is, $\mathfrak{G}_\rho$ has only one numeral. Then $P_\rho = E$ and can be omitted from the product.

(b) $\nu_\rho > 1$. Then the numerals of $\mathfrak{G}_\rho$ can be arranged in an order $i_1, \dots, i_{\nu_\rho}$ such that P_ρ —by omitting the unchanged numerals in the sense of the statements in Exer. 4—has the form

$$P_\rho = \begin{pmatrix} i_1 & i_2 & \dots & i_{\nu_\rho} \\ i_2 & i_3 & \dots & i_1 \end{pmatrix}.$$

For this purpose we only have to apply the permutations $P, P^2, \dots$ of $\mathfrak{P}$ successively to a numeral $i = i_1$ of $\mathfrak{G}_\rho$.

9. A permutation of the form

$$P = \begin{pmatrix} i_1 & i_2 & \dots & i_\nu \\ i_2 & i_3 & \dots & i_1 \end{pmatrix}, \quad \text{briefly also} \quad P = (i_1 i_2 \dots i_\nu),$$

is called a ν -termed cycle (also a cycle of length or degree ν).—Form the powers $P^0, P^{+1}, P^{+2}, \dots$ of P . What is the order (Section 8, Exer. 5) of P ?

The positive (negative) powers are obtained by the 'cyclic' displacement of the lower row $i_1 \dots i_\nu$ of $P^0 = E = \begin{pmatrix} i_1 & \dots & i_\nu \\ i_1 & \dots & i_\nu \end{pmatrix}$ to the left (right) as many times as specified by the exponent.

10. According to Exer. 2, 8, 9 any permutation P has a uniquely determined *partition into mutually exclusive cycles*.—Carry this partition through for the permutations of $\mathfrak{S}_2, \mathfrak{S}_3, \mathfrak{S}_4$.

For instance, $\begin{pmatrix} 1234 \\ 4213 \end{pmatrix} = (143), \quad \begin{pmatrix} 1234 \\ 3412 \end{pmatrix} = (13)(24).$

11. Prove: Two n -termed permutations P, R are conjugate within the group $\mathfrak{S}_n$ if and only if the set of lengths ν_ρ of the cycles in the partition of the permutations into cycles is the same in both cases (with respect to a suitable arrangement of the cycles). Therefore, the set of numbers ν_ρ merely determines the classes of conjugate elements in $\mathfrak{S}_n$.

For this purpose it is appropriate to think of the numerals i which remain unchanged as also carried along as one-termed cycles (i) (number $\nu_\rho = 1$) so that $\sum_{\rho=1}^r \nu_\rho = n$ is always true. Then the assertion follows by means of the transformation formula in the proof of Theorem 62. According to this formula the transformation by $Q = \begin{pmatrix} i \\ q_i \end{pmatrix}$ takes $R = \begin{pmatrix} i \\ r_i \end{pmatrix}$ into $P = Q^{-1}RQ = \begin{pmatrix} q_1 \\ q_{r_1} \end{pmatrix}$, therefore can be carried out simply through replacing the original sequence of numerals $1, \dots, n$ by the new sequence of numerals $q_1, \dots, q_n$ as the objects to be permuted. If the sequences of numerals, as they appear in the (properly arranged) partitions of R and P into cycles, are written in two rows one under the other, and this is regarded as a symbol for a permutation Q , then $Q^{-1}RQ = P$ is valid. Example: $R = (123)(4), P = (142)(3), Q = \begin{pmatrix} 1234 \\ 1423 \end{pmatrix}$.

12. Accordingly, how large is the number of different classes of conjugate elements in $\mathfrak{S}_n$?

It is equal to the number of different ways in which the number n can be partitioned into an arbitrary number r of integral positive summands ν_ρ (without regard to their arrangement). If the number of summands $\nu_\rho = 1, 2, \dots, n$ is designated by $r_1, r_2, \dots, r_n$, it is also equal to the number of solutions of

$$1r_1 + 2r_2 + \dots + nr_n = n$$

in integral non-negative $r_1, r_2, \dots, r_n$.

13. Consider the classes of conjugate elements of $\mathfrak{S}_n$ determined by the numbers ν_ρ or better by the numbers $r_1, \dots, r_n$ defined above. How many elements are there in such a class?

Imagine a pattern of empty parentheses consisting of r_1 1-termed parentheses, $\dots, r_n$ n -termed parentheses. There are $n!$ ways in which the numerals $1, \dots, n$ can be distributed into the n blank spaces. Let each distribution be interpreted as the partition of a permutation P of $\mathfrak{S}_n$ into cycles. The following types of distributions will lead to the same permutation P : (a) the ν cyclic interchanges within a single ν -termed bracket; (b) the $r_\nu!$ interchanges by permuting with one another the r_ν parentheses with the same number of terms ν . The required number:

$$\frac{n!}{1^{r_1} \dots n^{r_n} r_1! \dots r_n!}$$

is thereby found.

14. Prove: Any permutation can be partitioned into (not necessarily mutually exclusive) cycles of length 2 (*transpositions*). Such a decomposition is possible in many ways.

If the act of permuting is visualized graphically as the displacement of objects placed in a row, then it consists in the successive interchange of adjacent objects.

15. Give a partition of the cycle $(12 \dots \nu)$ into transpositions.

Corresponding to the idea of the passage of 1 past $2, \dots, \nu$ we obtain, for instance, the partition

$$(12 \dots \nu) = (12)(13) \dots (1\nu).$$

Form another partition.

16. Prove: Even permutations can be constructed only from an even number of transpositions; odd permutations, only from an odd number of transpositions.

According to Theorem 60 it is sufficient to establish the relation $\text{sgn } T = -1$ for any transposition $T = (ik)$. This is easily done on the basis of Def. 37.

17. What is the value of $\text{sgn } P$ for a ν -termed cycle P ?

This easily follows from Exer. 15, 16.

18. Choose a permutation from each class of conjugate elements of $\mathfrak{S}_3, \mathfrak{S}_4, \mathfrak{S}_5$ and give its partition into cycles; also, find the number of elements contained in the class. What classes belong to the normal divisor $\mathfrak{A}_3, \mathfrak{A}_4, \mathfrak{A}_5$?

Apply Exer. 11, 13, 17.

19. A class of conjugate elements of $\mathfrak{S}_n$ belonging to $\mathfrak{A}_n$ is also a class of conjugate elements in $\mathfrak{A}_n$, if in the partition of its elements into cycles there appears a cycle with an even number of terms, or two cycles with the same odd number of terms (this number may also be equal to 1). However, if the lengths of the cycles are all different odd numbers, then the class of conjugate elements of $\mathfrak{S}_n$ is composed of two such classes in $\mathfrak{A}_n$.

Namely, if the partition of a permutation P into cycles contains a cycle with an even number of terms, then the class commutes with this cycle, which is an odd permutation (cf. Exer. 15); therefore, on prefixing this cycle to an odd transformer Q in $Q^{-1}PQ = P'$, the transformer is made even. Furthermore, if the partition of P

contains two different cycles of the same odd number of terms, say $(1, \dots, k), (k+1, \dots, 2k)$, then P commutes with the odd permutation $(1, k+1) \dots (k, 2k)$, and we can continue as above. However, if the lengths of the cycles of P are all different odd numbers, then it is easy to show that P commutes only with even permutations. On realizing that $Q^{-1}PQ = R^{-1}PR$ implies $P(QR^{-1}) = (QR^{-1})P$ we can immediately deduce our assertion.

20. A homomorphic mapping (Section 9, Exer. 9) of an arbitrary group $\mathfrak{G}$ on an n -termed permutation group $\mathfrak{P}$ is called a *representation* of $\mathfrak{G}$ by n -termed permutations. According to Exer. 2 to 4, $\mathfrak{P}$ can be assumed without loss of generality to be transitive (in the general case the representation reduces to a number of transitive components).--- Prove: If $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$ of index n , then the n right cosets $\mathfrak{R} = \mathfrak{H}R$ of $\mathfrak{G}$ relative to $\mathfrak{H}$ undergo permutations under right multiplication by the elements S of $\mathfrak{G}$:

$$P_S = \left(\begin{array}{c} \mathfrak{R} \\ \mathfrak{R}S \end{array} \right) \text{ (}\mathfrak{R} \text{ runs through the right cosets of } \mathfrak{G} \text{ relative to } \mathfrak{H}\text{)}.$$

These P_S form a transitive representation of $\mathfrak{G}$ by n -termed permutations.

We have to establish:

(a) The sets $\mathfrak{R}S$ generated from a right coset $\mathfrak{R}$ are again right cosets of $\mathfrak{G}$ relative to $\mathfrak{H}$.

(b) Distinct cosets $\mathfrak{R}, \mathfrak{R}'$ correspond to distinct cosets $\mathfrak{R}S, \mathfrak{R}'S$.

(c) To the successive application of the multiplications by S, S' there corresponds the successive application of the permutations $P_S, P_{S'}$.

(d) Any coset $\mathfrak{R}$ goes over into any other $\mathfrak{R}'$ under right multiplication by a suitable S in $\mathfrak{G}$.

21. Describe the above representation by permutations $\mathfrak{P}$ in the special case $\mathfrak{H} = \mathfrak{E}$ (therefore $\mathfrak{G}$ is a group of order n) (*regular representation* of $\mathfrak{G}$).

The permutation P_S is obtained by taking the n elements A of $\mathfrak{G}$ themselves as the objects to be permuted and multiplying them on the right by S :

$$P_S = \begin{pmatrix} A \\ AS \end{pmatrix} \quad (A \text{ runs through the elements of } \mathfrak{G}).$$

22. Prove the converse to Exer. 20: Every representation of $\mathfrak{G}$ as a transitive n -termed permutation group $\mathfrak{P}$ arises from a subgroup $\mathfrak{H}$ of $\mathfrak{G}$ as the group of permutations of the right cosets of $\mathfrak{G}$ relative to $\mathfrak{H}$ under right multiplication by the elements of $\mathfrak{G}$.

For this purpose consider the subgroup $\mathfrak{U} = \mathfrak{U}_1$ of $\mathfrak{P}$ defined in Exer. 5 and take $\mathfrak{H} = \mathfrak{H}_1$ as the totality of those elements of $\mathfrak{G}$ which are mapped in the subgroup $\mathfrak{U}$ of $\mathfrak{P}$ by the basic homomorphism of $\mathfrak{G}$ to $\mathfrak{P}$, therefore schematically

$$\mathfrak{G} \rightarrow \mathfrak{P},$$

$$\mathfrak{H} \rightarrow \mathfrak{U}.$$

We then have to establish:

(a) $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$ of index n .

(b) The homomorphism maps the n right cosets $\mathfrak{R}_i$ of $\mathfrak{G}$ relative to $\mathfrak{H}$ onto the n right cosets $\bar{\mathfrak{R}}_i$ of $\mathfrak{P}$ relative to $\mathfrak{U}$, where $\bar{\mathfrak{R}}_i$ is the totality of permutations of $\mathfrak{P}$ which carry the numeral 1 into a fixed numeral i .

(c) If
$$P_S = \begin{pmatrix} i \\ p_i \end{pmatrix} \quad (i = 1, \dots, n)$$

is the permutation of $\mathfrak{P}$ corresponding to an S of $\mathfrak{G}$ with respect to the homomorphism, then under right multiplication by P_S the $\bar{\mathfrak{R}}_i$ undergo the permutation

$$\begin{pmatrix} \bar{\mathfrak{R}}_i \\ \bar{\mathfrak{R}}_i P_S \end{pmatrix} = \begin{pmatrix} \bar{\mathfrak{R}}_{p_i} \\ \bar{\mathfrak{R}}_{p_i} \end{pmatrix} \quad (i = 1, \dots, n),$$

that is, the indices i of the $\bar{\mathfrak{R}}_i$ undergo exactly the permutation P_S . This is also valid for the indices i of the $\mathfrak{R}_i$.

23. Let $\mathfrak{N}$ be the normal divisor of $\mathfrak{G}$ determined by the homomorphic mapping of $\mathfrak{G}$ on $\mathfrak{P}$ (Section 9, Exer. 9),

therefore determined in such a way that this mapping is an isomorphism between $\mathfrak{G}/\mathfrak{H}$ and $\mathfrak{P}$.—Prove: $\mathfrak{H}$ is the intersection of the subgroups $\mathfrak{H}_i$ of $\mathfrak{G}$ conjugate to $\mathfrak{H}$.

$\mathfrak{H}$ is the totality of the elements of $\mathfrak{G}$ which are mapped on the unity element of $\mathfrak{P}$ by the underlying homomorphism (Section 9, Exer. 9). $\mathfrak{H}_i$ is the totality of elements of $\mathfrak{G}$ which are mapped on the elements of $\mathfrak{U}_i$ (Exer. 6). The intersection of the $\mathfrak{U}_i$ is the unity element.

24. Let Φ be a geometric configuration, $\mathfrak{G}$ the group of coincidence motions of Φ (Section 6, Exer. 1), Ψ a subconfiguration of Φ (Section 9, Exer. 1), and Ψ_i ($i = 1, \dots, n$) the system of the different subconfigurations of Φ which arise from Ψ through the coincidence motions of Φ .—Show that, in the coincidence motions of Φ , the Ψ_i bring about a transitive n -termed permutation representation $\mathfrak{P}$ of $\mathfrak{G}$.

It is easy to establish:

(a) Every coincidence motion S of Φ effects a permutation P_S of the Ψ_i .

(b) To the successive application of two coincidence motions S, S' corresponds the successive application of the permutations $P_S, P_{S'}$.

(c) Any subconfiguration Ψ_i goes over into any other Ψ_j by a suitable coincidence motion S of Φ .

25. How can the generation of the above representation by permutations $\mathfrak{P}$ through a subgroup $\mathfrak{H}$ of $\mathfrak{G}$ (Exer. 22) be characterized in terms of the configuration Φ and the subconfiguration Ψ ?

See Exer. 23 and Section 9, Exer. 1 (c), (e).

26. When is $\mathfrak{P}$ not only a homomorphism but also an isomorphism?

If and only if the normal divisor specified in Exer. 23 is $\mathfrak{H} = \mathfrak{G}$; therefore, by Exer. 25 and Section 9, Exer. 1, if and only if the

identity permutation alone is a coincidence motion for all subconfigurations Ψ , simultaneously.

27. Apply the results of Exer. 24 to 26 to the case where the configuration Φ is the regular n -gon or n -gonal dihedron or tetrahedron or octahedron or icosahedron, and the subconfiguration Ψ is a vertex or a face or an edge or an axis through a vertex or an axis through the center of faces or an axis through the midpoint of edges. Enumerate the resulting transitive permutation representations of the groups $\mathfrak{S}_n, \mathfrak{D}_n, \mathfrak{I}$ (Section 6, Exer. 2), $\mathfrak{Q}, \mathfrak{S}$ (Section 9, Exer. 4) according to their degree and the associated normal divisor $\mathfrak{N}$ in the sense of Exer. 23. In particular prove:

$\mathfrak{S}_3 \cong \mathfrak{A}_3, \mathfrak{D}_3 \cong \mathfrak{S}_3$ (see the remarks made in connection with Def. 36),

$\mathfrak{I} \cong \mathfrak{A}_4, \mathfrak{D} \cong \mathfrak{S}_4$.

28. Similarly, on the basis of a suitable subconfiguration of the icosahedron prove: $\mathfrak{I} \cong \mathfrak{A}_5$.

As a subconfiguration take a system of three mutually perpendicular axes through the midpoints of edges.

29. Show that the partition of $\mathfrak{D}_3, \mathfrak{I}, \mathfrak{D}, \mathfrak{S}$ into classes of conjugate elements, as obtained in Exer. 18, 19, 27, 28, is identical with the one obtained directly in Section 9, Exer. 3, 5.

17. Determinants

1. Compute the following 3-rowed determinants:

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix}, \quad \begin{vmatrix} 3 & -1 & -1 \\ -1 & 4 & -2 \\ -2 & -2 & 5 \end{vmatrix}, \quad \begin{vmatrix} 1 & 2 & 3 \\ 8 & 0 & 4 \\ 7 & 6 & 5 \end{vmatrix}, \quad \begin{vmatrix} a & 0 & b \\ 0 & t & 0 \\ c & 0 & d \end{vmatrix}$$

according to the rule of formation given in connection with Def. 38.

2. Write out the expansion of the determinant of the general 4-rowed square matrix $A = (a_{ik})$.

The permutation signs can be formed either directly by Def. 37 [122] or also by the partition into cycles according to Section 16, Exer. 16, 17.

3. Compute the following special 4-rowed determinants:

$$\begin{vmatrix} 1 & -2 & 1 & 0 \\ 0 & 3 & -2 & -1 \\ 4 & -1 & 0 & -3 \\ 1 & 2 & -6 & 3 \end{vmatrix}, \quad \begin{vmatrix} a & 0 & b & 0 \\ 0 & t & 0 & u \\ c & 0 & d & 0 \\ 0 & v & 0 & w \end{vmatrix}$$

by means of the general formula obtained above.

Later methods (Sections 18, 19) will emphasize the clumsiness of this direct computation.

4. Evaluate the following determinants:

$$\begin{vmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & & & \\ \vdots & & & \\ \vdots & & & \\ a_{n1} & \cdots & a_{n,n-1} & a_{nn} \end{vmatrix}, \quad \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & & & \\ \vdots & & & \\ \vdots & & & \\ 0 & \cdots & 0 & a_{nn} \end{vmatrix},$$

$$\begin{vmatrix} a_{11} & \cdots & a_{1,n-1} & a_{1n} \\ \vdots & & & 0 \\ \vdots & & & \\ \vdots & & & \\ a_{n-1,1} & \cdots & 0 & \end{vmatrix}, \quad \begin{vmatrix} 0 & \cdots & 0 & a_{1n} \\ \vdots & & & a_{2n} \\ \vdots & & & \\ \vdots & & & \\ 0 & \cdots & 0 & \end{vmatrix}$$

For the first determinant apply Def. 38 directly and note that in a permutation $P = \begin{pmatrix} i \\ p_i \end{pmatrix} \neq E$, $p_i > i$ must be valid for at least one i .

The value of the other determinants can then be obtained by means of Theorems 64, 65; or they too can be evaluated directly in the same manner as the first.

5. To every permutation $P = \begin{pmatrix} i \\ p_i \end{pmatrix}$ ($i = 1, \dots, n$) there corresponds a matrix A_P , namely, the coefficient matrix of the n linear forms x_{p_i} (cf. Section 12, Exer. 3).—What is the value of $|A_P|$?

The value follows immediately from Theorem 65.

6. In general, what is the value of the determinant of the coefficient matrix of the n linear forms $a_i x_{p_i}$?

This, too, can be easily deduced from Theorem 65 and the special determinant of this kind given in connection with Def. 38.

7. Let x_{ik} ($i, k = 1, \dots, n$) be a system of n^2 indeterminates over K . Prove that the determinant $|x_{ik}| \neq 0$.

Show that the formula (Def. 38) used to define the determinant $|x_{ik}|$ is, at the same time, its normal representation (Def. 9 [45]) as an element of $K[x_{11}, x_{12}, \dots, x_{nn}]$. On the basis of the principle of substitution it is also sufficient to point to the existence of n -rowed square matrices A with $|A| \neq 0$, for instance, $A = E$.

18. Minors and Cofactors. The Laplace Expansion Theorem

1. Let $\mathfrak{S}_{\{i_1, \dots, i_\nu\}}$ be the permutation group upon which the proof of Theorem 66 is based. What is its partition into transitive components (Section 16, Exer. 2 to 4)?

There are two transitive components corresponding to the reduction of $C_{R,S}$ to R and S . These are isomorphic to $\mathfrak{S}_\nu$ and $\mathfrak{S}_{n-\nu}$.

2. Compute the determinants given in Section 17, Exer. 1 to 3 through expansion by the elements of a row or column.

For this purpose it is appropriate to pick out a row or column which contains as many zeros as possible. For the 4-rowed matrices in Exer. 2, 3 the minors of degree 3 may be computed in a corresponding manner.

3. Prove by mathematical induction the formulae established in Section 17, Exer. 4.

For this purpose use the expansion by a row with $n-1$ zeros.

4. Compute the determinants given in Section 17, Exer. 2, 3 through expansion by the minors of a pair of rows or of columns.

Of the 6 cofactors of a pair of rows 4 have one sign, 2 the other sign (not, perhaps, 3 one sign and 3 the other sign).

5. In connection with the last determinants in Section 17, Exer. 1, 3, compute in general the determinant of a square matrix laid out like a checkerboard:

$$M = \begin{pmatrix} a_{11} & 0 & a_{12} & 0 & \cdot \\ 0 & b_{11} & 0 & b_{12} & \cdot \\ a_{21} & 0 & a_{22} & 0 & \cdot \\ 0 & b_{21} & 0 & b_{22} & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}.$$

By rearrangement of the rows and columns M can be converted into $M_0 = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$, where $A = (a_{ik})$ and $B = (b_{ik})$. If the number of rows of M is even and equal to $2n$, then A and B are both n -rowed; if the number of rows of M is odd and equal to $2n-1$, then A is n -rowed, B is $(n-1)$ -rowed. The determinant of M_0 can be immediately read off by the Laplace Expansion Theorem (expansion by the first row or column¹). Without previous rearrangement of the

¹ For this purpose also see Theorem 69 [141], given later.

rows and columns at the beginning we can also expand by the system of rows and columns occupied by the elements a_{ik} .

6. Evaluate the determinant

$$\begin{vmatrix} A_{11} & A_{12} & \cdot & \cdot & \cdot & A_{1r} \\ 0 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & A_{rr} \end{vmatrix},$$

where A_{ik} and 0 are to be understood as submatrices in the sense of a partition described in Section 10, Exer. 14.

Simply use mathematical induction on r (cf. Exer. 3) and expand, say, by the system of rows of A_{rr} .

7. Let $A = (a_{ik})$ be an n -rowed square matrix, $A = (\alpha_{ik})$ its complementary matrix, $u = (u_i)$ an n -termed column, $v = (v_k)$ an n -termed row. Prove the relation

$$\begin{vmatrix} A & u \\ v & 0 \end{vmatrix} = - \sum_{i,k=1}^n \alpha_{ik} u_i v_k.$$

First expand the $(n+1)$ -rowed determinant by its last row and then expand the resulting n -rowed determinants by their last columns.

19. Further Theorems on Determinants

1. Compute the numerical determinants in Section 17, Exer. 1, 3 by first making all elements of a column (row) 0 except for one element through row (column) combinations according to the Corollary to Theorem 71 and then expanding by this column (row).

It is again appropriate for the expansion to choose a row in which as many elements as possible are already 0. For instance, in the first determinant of Section 17, Exer. 1 we can subtract the first column multiplied by 2 from the second, and the first column multiplied by 3 from the third, and then expand by the first row.

2. In the same way compute the 5-rowed determinant

$$\begin{vmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{vmatrix}.$$

First, say, make all elements of the first column 0 except for the first and then continue in this way with the remaining 4-rowed determinant (in which all minus signs can be omitted according to the remark after Theorem 68).

3. That the first determinant of Section 17, Exer. 3 has the value 0 can also be easily seen by means of Theorem 71.

The sum of the columns is 0.

4. Evaluate the *Vandermonde determinant* of the elements $a_1, \dots, a_n$:

$$V(a_1, \dots, a_n) = |a_i^{n-k}| \quad (i, k = 1, \dots, n).$$

Subtract successively the second column multiplied by a_n from the first, ..., the n -th column multiplied by a_n from the $(n-1)$ -th and then expand by the n -th row. The evaluation of $V(a_1, \dots, a_n)$ is thereby reduced to that of $V(a_1, \dots, a_{n-1})$.—Result: $V(a_1, \dots, a_n) = \prod_{i < j} (a_i - a_j)$.—Use this to evaluate also $|a_i^{k-1}|$ (column permutation).

5. A square matrix $A = (a_{ik})$ is said to be *symmetric* if $A' = A$ (that is, $a_{ki} = a_{ik}$), *skew-symmetric* if $A' = -A$ (that is, $a_{ki} = -a_{ik}$).—Prove:

(a) If A is skew-symmetric with an odd number of rows n and K has the property $2e \neq 0$, then $|A| = 0$.¹

(b) For any even number of rows n there are skew-symmetric A with $|A| \neq 0$.²

(c) If A is symmetric, then all derived $A^{(v)}$ and complementary $A^{(v)}$ are also symmetric; on the contrary, if A is skew-symmetric, then the $A^{(v)}$ and $A^{(v)}$ of even degree are symmetric, those of odd degree are skew-symmetric.

For (a). Apply Theorem 64 [129] and the remark after Theorem 68 [141].

For (b). It is sufficient to take, say,

$$A = \begin{pmatrix} A_0 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & \ddots & & & & \cdot \\ \cdot & & \ddots & & & \cdot \\ \cdot & & & \ddots & & \cdot \\ \cdot & & & & \ddots & 0 \\ 0 & \cdot & \cdot & \cdot & 0 & A_0 \end{pmatrix} \quad \text{with} \quad A_0 = \begin{pmatrix} 0 & e \\ -e & 0 \end{pmatrix}$$

(Section 18, Exer. 6).

For (c). This is immediately clear on the basis of the given definitions.

6. Let A be an n -rowed square matrix and x an indeterminate. The integral rational function $|xE - A|$ is called the *characteristic polynomial* of A . By the *principal minor* of ν -th degree of A we understand a minor of the kind $a_{\{i_1, \dots, i_\nu\}, \{i_1, \dots, i_\nu\}}$, which therefore is formed with one and the same row and column combination $\{i_1, \dots, i_\nu\}$.—Prove:

¹ If $2e \neq 0$, namely, in general, if $2a = (2e)a \neq 0$ for $a \neq 0$ is valid in K , then the a_{ii} are 0; while if $2e = 0$ is valid in K , then the a_{ii} can be arbitrary elements of K and no distinction exists between symmetric and skew-symmetric matrices. Cf. the expositions after Theorem 70 [141]. For K with the property $2e = 0$, see Exer. 12 to Vol. 2, Section 4, given later.

² For even n see also Exer. 6 to Section 21, given later.

The coefficient of $(-1)^{\nu} x^{n-\nu}$ in the characteristic polynomial of A is equal to the sum of all principal minors of ν -th degree of A .

Corresponding to the decomposition of the rows of $x E - A$ into the two summands $x e_i$ and $-a_i$, we can additively decompose $|x E - A|$, according to Theorem 68, into 2^n determinants. Each such determinant is characterized by the combination $\{i_1, \dots, i_\nu\}$ of those rows, from which the summand $-a_i$ is obtained, whereas the summand $x e_i$ is obtained from the rows of the complementary combination $\{i_{\nu+1}, \dots, i_n\}$. The expansion of such a determinant by the row system $\{i_{\nu+1}, \dots, i_n\}$ yields the value

$$x^{n-\nu} (-1)^{\nu} a_{\{i_1, \dots, i_\nu\}, \{i_{\nu+1}, \dots, i_n\}}.$$

7. Let A and B be n -rowed square matrices. Evaluate the determinant

$$\begin{vmatrix} 0 & A \\ B & -E \end{vmatrix}$$

in two ways: First, analogously to Section 18, Exer. 6 (see also Section 17, Exer. 4); secondly, by bringing 0 to the position of B by column combination (Theorem 71, Corollary)—0 is thereby replaced by the matrix product AB —and then again applying Section 18, Exer. 6.

8. By comparing terms on both sides give a direct proof of the above formula $|AB| = |A| |B|$ for the determinant of the product of matrices.

Just as in Exer. 6, represent the determinant $|AB| = \left| \sum_{i=1}^n a_{ii} b_i \right|$ according to Theorem 68 as the sum of n^n determinants, corresponding to the linear combination $\sum_{i=1}^n a_{ii} b_i$ of its i -th row with the n -rows b_i of B . Such a determinant is characterized by the index system $i_1, \dots, i_n$ of the summands selected in the individual linear combinations of rows. It splits off the factor $a_{i_1} \dots a_{i_n}$. The complementary factor is the determinant of the matrix of the rows $b_{i_1}, \dots, b_{i_n}$ (in this order).

This complementary factor is 0, except when $l_1, \dots, l_n$ are different from one another, that is, are generated by a *permutation* L of $1, \dots, n$; in the latter case it has by Theorem 65 [130] the value $\text{sgn } L |B|$, so that the full determinantal summand has the value $\text{sgn } L a_{1l_1} \cdots a_{nl_n} |B|$. On combining the determinantal summands we obtain the statement by Def. 38 [127].

9. Similarly, prove by comparing terms the more general fact: If A is an (n, m) -rowed matrix and B an (m, n) -rowed matrix and $m > n$, then the determinant of the n -rowed square matrix AB is equal to the inner product of the vector of all $\binom{m}{n}$ minors¹ of n -th degree $a_{\{k_1, \dots, k_n\}}$ of A and the vector of all $\binom{m}{n}$ minors of n -th degree $b_{\{l_1, \dots, l_n\}}$ of B in a corresponding arrangement, therefore:

$$|AB| = \sum_{\{l_1, \dots, l_n\}} a_{\{k_1, \dots, k_n\}} b_{\{l_1, \dots, l_n\}},$$

where $\{l_1, \dots, l_n\}$ runs through all $\binom{m}{n}$ combinations of the numerals $1, \dots, m$ taken n at a time.

In the terminology of the previous explanation we again have that only those determinantal summands are left in which $l_1, \dots, l_n$ are different from one another, that is, correspond to the *combinations* of $1, \dots, m$ taken n at a time $\{l_1, \dots, l_n\}$. Every such combination appears in all $n!$ possible arrangements. The sum of these $n!$ terms contributes $a_{\{k_1, \dots, k_n\}} b_{\{l_1, \dots, l_n\}}$ to the determinantal sum. The statement follows from this.

10. The statement in Exer. 9 was established by using Exer. 8 as a model. Prove this statement by generalizing the proof in Exer. 7.

Evaluate the determinant $\begin{vmatrix} 0 & A \\ B & -E_m \end{vmatrix}$ in two ways: first, through expansion by the first n rows—this yields the right side of the

¹ For this purpose see Def. 41 [150], given later.

statement; and secondly again by replacing B by 0 through column combination and then making use of Section 8, Exer. 6—this yields the left side of the statement.

11. By means of Exer. 9 prove the rule: The ν -th derived (complementary) matrix of a product $AB = C$ is the product of the ν -th derived (complementary) matrices of the factors:

$$C^{(\nu)} = A^{(\nu)} B^{(\nu)}, \quad \Gamma^{(\nu)} = A^{(\nu)} B^{(\nu)}.$$

For the first rule apply Exer. 9 to a row combination $\{i_1, \dots, i_\nu\}$ of A as (ν, n) -rowed matrix, and a column combination $\{k_1, \dots, k_\nu\}$ of B as (n, ν) -rowed matrix. For the second rule proceed similarly, except that a simple discussion must still be made regarding the sign.

12. Express the extension of the Laplace Expansion Theorem, Theorem 72, in terms of two products of matrices.

$$A^{(\nu)} (A^{(\nu)})' = (A^{(\nu)})' A^{(\nu)} = |A| E_{\binom{n}{\nu}}.$$

13. Use this to prove: An n -rowed square matrix A has an inverse A^{-1} if and only if $|A| \neq 0$.¹ Then express A^{-1} in terms of the elements of A . (Cf. the special case in Section 14, Exer. 5.)

If $AX = E$ or $YA = E$, then $|A| \neq 0$ follows by the theorem for the determinant of the product of matrices (Exer. 7, 8). If $|A| \neq 0$, then $|A|^{-1}A'$ is a left and right inverse to A by Exer. 12.

14. In the case $|A| \neq 0$, $|B| \neq 0$ how can the second rule in Exer. 11 be deduced from the first?

By Exer. 12, 13, $|A| \neq 0$ also implies

$$|A^{(\nu)}| \neq 0 \quad \text{and} \quad (A^{(\nu)})' = |A| (A^{(\nu)})^{-1}.$$

Tie this in with the corresponding facts for B and take into consideration Section 10, Exer. 7, 13.

15. Eliminate the restrictions $|A| \neq 0$, $|B| \neq 0$ in Exer. 14 by considering the matrices of indeterminates.

¹ In this regard see also Section 14, Exer. 1 to 4, as well as Theorems 74, 79, 81 [145, 155].

If x_{ik}, y_{ik} ($i, k = 1, \dots, n$) is a system of $2n^2$ indeterminates over K , and the matrices $X = (x_{ik}), Y = (y_{ik})$ over $K[x_{11}, \dots, x_{nn}, y_{11}, \dots, y_{nn}]$ are formed from these indeterminates, then $|X| \neq 0, |Y| \neq 0$ (Section 17, Exer. 7). Therefore, the second rule in Exer. 11 is valid by Exer. 14 for X, Y . The validity for arbitrary matrices A, B over K then follows by the principle of substitution.

16. We designated by $A^{(\nu)}$ the ν -th complementary matrix to A , that is, the matrix of the $\binom{n}{\nu}^2$ cofactors of ν -th order of A . This must be distinguished from the ν -th derived matrix to A , that is, the matrix of the $\binom{n}{\nu}^2$ minors of ν -th degree of the (first) complementary matrix $A^{(1)} = A$ to A . We designate the latter by $A^{[\nu]}$.—What relation exists between $A^{(\nu)}$ and $A^{[\nu]}$?

Apply Exer. 11 to the special relation $AA' = |A|E$ established in Exer. 12, and compare it with the general relation of Exer. 12. The case $|A| = 0$ is handled as in Exer. 15.

17. By specializing to $\nu = 2$ prove the formulae

$$\begin{vmatrix} \alpha_{i_1 k_1} & \alpha_{i_1 k_2} \\ \alpha_{i_2 k_1} & \alpha_{i_2 k_2} \end{vmatrix} = |A| \alpha_{\{i_1, i_2\} \{k_1, k_2\}}.$$

18. Let (AB) be an $(m, m+r)$ -rowed matrix, where A is an m -rowed square matrix and B an (m, r) -rowed square matrix, in which all minors of m -th degree formed from $m-1$ columns of A and a column of B are equal to 0, while the minor formed from the m columns of A is $|A| \neq 0$. Prove that $B = 0$.—For this purpose make use of the $(m+1)$ -rowed square matrices

$$M_{ik} = \begin{pmatrix} A & b_k \\ a_i & 0 \end{pmatrix},$$

where a_i designates the i -th row of A and b_k the k -th column of B .

If $|M_{ik}|$ is expanded by the last row, then $|M_{ik}| = 0$ follows on the basis of the given assumption. If $|M_{ik}|$ is expanded by the last column, then $|M_{ik}| = \pm |A| b_{ik}$ follows by considering Theorem 70.

19. Let us assume that the ν -th derived matrix of an n -rowed square matrix A is $A^{(\nu)} = E_{\binom{n}{\nu}}$, for a fixed ν with $0 < \nu < n$.—Prove (on the basis of Exer. 18) that $A = \epsilon E$ with $\epsilon^\nu = e$.

In order to show that $a_{ik} = 0$ for $i \neq k$, consider the (ν, n) -rowed matrix of the ν -th and $\nu-1$ other rows $i_1, \dots, i_{\nu-1}$ of A . Then, by the assumption, exactly one of its $\binom{n}{\nu}$ minors of ν -th degree is different from zero (equal to e), namely, the one (principal minor of A) corresponding to the columns $i, i_1, \dots, i_{\nu-1}$. Therefore, by Exer. 18 it follows that $a_{ik} = 0$ for $k \neq i, i_1, \dots, i_{\nu-1}$. Due to $\nu < n$ we can, with $k \neq i$ given, always choose an $(\nu-1)$ -termed row system $i_1, \dots, i_{\nu-1}$ not containing i and k . Regarding the a_{ii} we now know that all ν -termed products of these with ν different indices i are equal to e . From this it immediately follows that all a_{ii} are equal to one another and satisfy the relation $a_{ii}^\nu = e$.

20. Prove the invariance of the *discriminant* $D = B^2 - AC$ of the quadratic form $Ax_1^2 + 2Bx_1x_2 + Cx_2^2$ with respect to rotations of the coordinate system (more general: with respect to a linear transformation with the determinant ± 1).

Note that $D = -\begin{vmatrix} A & B \\ B & C \end{vmatrix}$ and apply Section 10, Exer. 12 as well as Exer. 7, 8. (What is the significance of this fact in the theory of conic sections?)

20. Application of the Theory of Determinants to Systems of Linear Equations in the Case $m = n$

1. Solve the following systems of equations (relative to the field $\mathbb{P}$) by Cramer's rule:

$$\begin{aligned}
 \text{(a)} \quad & \begin{cases} 3x_1 + 2x_2 \doteq a_1 \\ 4x_1 + 5x_2 \doteq a_2, \end{cases} \\
 \text{(b)} \quad & \begin{cases} x_1 + 2x_2 + 3x_3 \doteq a_1 \\ 2x_1 + 3x_2 + 4x_3 \doteq a_2 \\ 3x_1 + 4x_2 + 5x_3 \doteq a_3, \end{cases} \\
 \text{(c)} \quad & \begin{cases} x_1 + x_2 & \doteq a_1 \\ & x_2 + x_3 & \doteq a_2 \\ & & x_3 + x_4 \doteq a_3 \\ -2x_1 & & & + x_4 \doteq a_4. \end{cases}
 \end{aligned}$$

2. Let the a_i ($i = 1, \dots, n$) be different from one another. In the system of equations

$$\sum_{k=1}^n a_i^{n-k} x_k \doteq b_i$$

determine the unknowns x_1 and x_n .

The determinant $|a_i^{n-k}|$ has already been evaluated in Section 19, Exer. 4. In order to evaluate the cofactors to the first and last columns use the same rule.¹

3. Form the inverse:

(a) of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $ad - bc \neq 0$,

(b) of the coefficient matrix A_P of the system of linear forms x_{p_i} ($i = 1, \dots, n$), where $P = \begin{pmatrix} i \\ p_i \end{pmatrix}$ is a permutation (cf. Section 17, Exer. 5),

(c) more general, of the coefficient matrix of the system of linear forms $a_i x_{p_i}$ ($i = 1, \dots, n$), where $a_i \neq 0$ (cf. Section 17, Exer. 6).

Apply Theorem 74.

¹ For the evaluation of *all* x_k see the determinant to be developed in Vol. 2, Section 23, Exer. 19.

4. Let B be an (m, n) -rowed matrix. Form the inverse of the $(m+n)$ -rowed square matrix

$$\begin{pmatrix} E_m & B \\ 0 & E_n \end{pmatrix}.$$

The determinant can be evaluated by Section 18, Exer. 6. For the evaluation of the cofactors apply the same rule as well as Theorem 69 [141]; in particular, in the case of the cofactor of an element of the null matrix of the lower left $[(m+i)$ -th row, k -th column], move the column of the cofactor containing b_{ki} to the left into the gap arising by striking out the k -th column, and then apply Section 18, Exer. 6. In order to show merely that

$$\begin{pmatrix} E_m & -B \\ 0 & E_n \end{pmatrix}$$

is the inverse—without deriving this matrix inductively—we simply have to use Section 10, Exer. 14.

5. Let A and D be square matrices with m and n rows, and determinants different from 0. Let B be an (m, n) -rowed matrix. By applying Exer. 4, form the inverse of the $(m+n)$ -rowed square matrix

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}.$$

Compare this result with that of Exer. 3 (a) in the special case $c = 0$.

Make use of the factorization

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \begin{pmatrix} E_m & A^{-1}B \\ 0 & E_n \end{pmatrix}$$

and Section 10, Exer. 7.

6. What is the value of the determinant of the complementary matrix A of an n -rowed square matrix A ?

In the case $|A| \neq 0$ it is easily obtained by Section 19, Exer. 12; for the rest, see also the remark after Theorem 81 [155]. The restriction $|A| \neq 0$ can be eliminated just as in Section 19, Exer. 15.

21. The Rank of a Matrix

1. Determine the rank of the first matrix in Section 17, Exer. 3, as well as the rank of the matrices (relative to the field P)

$$\begin{pmatrix} 1 & 1 & 2 & 5 & 7 \\ 1 & 2 & 3 & 7 & 10 \\ 1 & 3 & 4 & 9 & 13 \\ 1 & 4 & 5 & 11 & 16 \end{pmatrix}, \quad \begin{pmatrix} 2 & 4 & 8 & 10 \\ 3 & 6 & 12 & 15 \\ 5 & 10 & 20 & 25 \end{pmatrix}.$$

Instead of evaluating all individual minors according to Def. 42, it is much simpler to take into consideration the obvious column relations and apply Lemma 3.

2. Let $a = (a_i)$ be an $(m, 1)$ -rowed matrix and $b = (b_k)$ a $(1, n)$ -rowed matrix. What is the rank of the (m, n) -rowed matrix $ab = (a_i b_k)$?

The rank is 1 or 0 according as $a \neq 0$ and $b \neq 0$ is or is not true.

3. Conversely, prove: If an (m, n) -rowed matrix A has rank 0 or 1, then it has a representation $A = ab$ as the product of an $(m, 1)$ -rowed matrix a and an $(1, n)$ -rowed matrix b .

Apply Theorem 76.

4. Let $A = (a_{ik})$ be an n -rowed square matrix whose elements are real numbers with the properties:

(a) $a_{ii} > 0$,

(b) $a_{ik} \leq 0$ for $i \neq k$,

(c) $\sum_{k=1}^n a_{ik} > 0$.

(For instance, see the second matrix of Section 17, Exer. 1.) Give an indirect proof on the basis of Theorem 78 that $|A| \neq 0$.

If $\mathbf{r} = (x_k)$ is a solution of the system (H) associated to A , let i be so chosen that x_i has the greatest absolute value of the numbers x_k . Then the i -th equation of (H) yields a contradiction on the basis of (a), (b), (c).

5. The rank ρ of a matrix A will be designated by $\rho(A)$ to show that it is a function of A . Let A be an n -rowed square matrix with $|A| = 0$, therefore $\rho(A) \leq n - 1$, and let A be its complementary matrix.—Prove: $\rho(A) = 0$ or 1, according as $\rho(A) < n - 1$ or $= n - 1$.

The case $\rho(A) < n - 1$ is trivial. In the case $\rho(A) = n - 1$ determine the number of fundamental solutions of (H) according to Theorem 76 and Theorem 52 [106] and note that according to Theorem 72 [143] the rows of A are solutions of (H); the result can also be read immediately from Section 19, Exer. 17.

6. Let x_{ik} ($i, k = 1, \dots, n; i < k$) be a system of $\frac{n(n-1)}{2}$ indeterminates over K ($n \geq 2$), and set

$$x_{ik} = 0 \text{ for } i = k, \quad x_{ik} = -x_{ki} \text{ for } i > k,$$

so that $X = (x_{ik})$ ($i, k = 1, \dots, n$)

is a skew-symmetric matrix.—In connection with Section 19, Exer. 5, prove: For n even $|X|$ is the square of an integral rational function f of the x_{ik} over K :

$$|X| = f^2.$$

Show that any skew-symmetric matrix A over K can be obtained from X by substituting the elements a_{ik} of K for the indeterminates x_{ik} , provided that K has the property $2e \neq 0$.¹

¹ Cf. footnote 2 to Section 19, Exer. 5. For K with $2e = 0$ see also Exer. 13 to Vol. 2, Section 4, given later.

Prove this by mathematical induction on n . To do so—except for settling the case $n = 2$ —proceed as follows:

(a) Expand $|X|$ by the elements of the n -th row and column according to Section 18, Exer. 7.—The resulting coefficients are the cofactors of $(n-2)$ -nd degree

$$\xi_{\{i, n\} \{k, n\}} = \hat{\xi}_{ik} \quad (i, k = 1, \dots, n-1)$$

of X .

(b) On the basis of Section 19, Exer. 5, (c), prove that its matrix $\hat{\Xi} = (\hat{\xi}_{ik})$ is symmetric.

(c) On the basis of Exer. 5, prove the relations

$$\begin{vmatrix} \hat{\xi}_{ii} & \hat{\xi}_{ik} \\ \hat{\xi}_{ik} & \hat{\xi}_{kk} \end{vmatrix} = \hat{\xi}_{ii} \hat{\xi}_{kk} - \hat{\xi}_{ik}^2 = 0.$$

(d) Apply the induction assumption to the $\hat{\xi}_{,,}$. This gives $\hat{\xi}_{ii} = \eta_i^2$ with integral rational functions η_i of the x_{ik} over K . Then determine the signs of these η_i such that the relations $\hat{\xi}_{ik} = \eta_i \eta_k$ ($i, k = 1, \dots, n-1$) are valid.

For (a). According to the definition of the x_{ik} the expansion in question is given here by $|X| = \sum_{i, k=1}^{n-1} \hat{\xi}_{ik} x_{in} x_{kn}$, so that the proof (d)

yields the statement with $f = \sum_{i=1}^{n-1} \eta_i x_{in}$.

For (b). Here the assumption is used that n is even.

For (c). $\hat{\Xi}$ is the complementary matrix of that matrix $\hat{X}$ which arises from X by striking out the n -th row and column. By Section 19, Exer. 5, (a) it is known that $|\hat{X}| = 0$.

For (d). The $\hat{\xi}_{,,}$ are determinants of skew-symmetric $(n-2)$ -rowed submatrices of X ; therefore, by the induction assumption they are the squares of integral rational functions η_i of the x_{ik} over K . If the sign of η_1 is herein arbitrarily fixed [$\eta_1 \neq 0$ according to Section 19, Exer. 5, (b)] and the signs of $\eta_2, \dots, \eta_{n-1}$ are determined so that $\hat{\xi}_{ik} = \eta_i \eta_k$ ($k = 2, \dots, n$) [this is possible in accordance with the relations (c)], then the remaining relations specified in (d) are

automatically satisfied. This conclusion can be drawn from (b), (c) and the relations

$$\begin{vmatrix} \hat{\xi}_{11} & \hat{\xi}_{1k} \\ \hat{\xi}_{i1} & \hat{\xi}_{ik} \end{vmatrix} = \hat{\xi}_{11}\hat{\xi}_{ik} - \hat{\xi}_{i1}\hat{\xi}_{1k} = 0,$$

arising from the same source as (c).

7. For a given matrix A all the matrices which have the form $\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$, that is, which are generated from A by the addition of arbitrarily many zero rows at the bottom and zero columns at the right, may be called equal. In this sense matrices A and B of entirely arbitrary numbers of rows may be added to, and multiplied by, one another; in the same sense sums and products are independent of the number of zero rows and zero columns that must be adjoined to A and B in order to yield matrices that can be added to, and multiplied by, one another in the previous sense. Similarly, the rank of A is invariant in this sense. Furthermore, for arbitrary matrices A the derived matrices $A^{(\nu)}$ (but not the complementary matrices $A^{(\nu)}$) also are defined by extension to an equal square matrix and are invariant in the same sense (with respect to a suitable sequence of row and column combinations).

(a) How can the fact $\rho(A) = \rho$ be expressed by means of the derived matrices $A^{(\nu)}$?

(b) How can the fact $\rho(A) \leq \rho$ be expressed by means of the $A^{(\nu)}$?

(c) Use these expressions to prove the rule

$$\rho(AB) \leq \text{Min}(\rho(A), \rho(B)).$$

(a) is a consequence of $A^{(\rho)} \neq 0$, $A^{(\rho+1)} = 0$, as immediately follows from Def. 42.

(b) is a consequence of $A^{(\rho+1)} = 0$.

(c) is proved by applying Section 19, Exer. 11 and noting that $A^{(\sigma+1)} = 0$ or $B^{(\sigma+1)} = 0$, if $\sigma = \text{Min}(\rho(A), \rho(B))$.

8. Prove that the regular n -rowed square matrices form a group with respect to multiplication.

This immediately follows from Theorem 79 and Section 19, Exer. 7, 8.

9. Two (m, n) -rowed matrices A, B are called *equivalent*, if there exist a regular m -rowed square matrix P and a regular n -rowed square matrix Q such that $B = PAQ$.—Show that this relation of equivalence is an equivalence relation in the sense of Section 2, (I).

To prove Section 2, $(\alpha), (\beta), (\gamma)$ use the fact that regular matrices form a group (Exer. 8).

10. How are two systems of linear forms related if their matrices A and B are equivalent?

Let $f_i(x) = \sum_{k=1}^n a_{ik}x_k$ ($i = 1, \dots, m$) be the system of linear forms with matrix A . According to Section 10, Exer. 3 the system with matrix B can then be generated as follows: first, by carrying out in the f_i a linear substitution

$$g_j = \sum_{i=1}^m p_{ji}f_i \quad (j = 1, \dots, m)$$

with regular matrix $P = (p_{ji})$; and secondly, by carrying out in the indeterminates x_k a linear substitution

$$x_k = \sum_{l=1}^n q_{kl}y_l \quad (k = 1, \dots, n)$$

with regular matrix $Q = (q_{kl})$. Since P and Q are regular, both substitutions are uniquely invertible according to Theorems 79, 74 [145].

11. Prove: Equivalent matrices have the same rank.

Apply Exer. 7, (c) and Section 2, (β) .

12. Prove: If A is an (m, n) -rowed matrix of rank ρ , then A is equivalent to the (m, n) -rowed matrix $\begin{pmatrix} E_\rho & 0 \\ 0 & 0 \end{pmatrix}$.

First, by the rearrangement of the rows and columns of A a matrix A_1 can be generated in which the minor of the first ρ rows and columns is different from 0. This rearrangement can be brought about according to Exer. 10 by left and right multiplication by permutation matrices P_1 and Q_1 , and P_1 and Q_1 are regular (Section 17, Exer. 5):

$$A_1 = P_1 A Q_1 = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

with ρ -rowed square A_{11} and $|A_{11}| \neq 0$. Corresponding to the dependence of the last $m - \rho$ rows on the first ρ rows and of the last $n - \rho$ columns on the first ρ columns (Theorem 76) there then exist two more matrices

$$P_2 = \begin{pmatrix} E_\rho & 0 \\ 0 & E_{m-\rho} \end{pmatrix} \quad \text{and} \quad Q_2 = \begin{pmatrix} E_\rho & 0 \\ 0 & E_{n-\rho} \end{pmatrix}$$

such that

$$A_2 = P_2 A_1 Q_2 = \begin{pmatrix} A_{11} & 0 \\ 0 & 0 \end{pmatrix},$$

and P_2 and Q_2 are regular (Section 18, Exer. 6). Due to $|A_{11}| \neq 0$ we finally have

$$P_3 A_2 = \begin{pmatrix} E_\rho & 0 \\ 0 & 0 \end{pmatrix} \quad \text{with} \quad P_3 = \begin{pmatrix} A_{11}^{-1} & 0 \\ 0 & E_{m-\rho} \end{pmatrix},$$

and P_3 is again regular (Theorem 81).

13. Prove the theorem given in Exer. 12 by making full use of the Toeplitz process.

In the Toeplitz process it is established according to Section 12, Exer. 2, 3 that the (m, n) -rowed matrix A can be carried over into an (m, n) -rowed matrix B of the form

$$B = \begin{pmatrix} b_{11} & \dots & b_{1, k_1-1} & 1 & 0 & \dots & 0 \\ b_{21} & \dots & b_{2, k_1-1} & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ b_{r1} & \dots & \dots & \dots & b_{r, k_r-1} & 1 & 0 \dots 0 \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & \dots & \dots & \dots & \dots & 0 \end{pmatrix}$$

Since $P^{(v)}, Q^{(v)}$ are regular if P, Q are (Section 19, Exer. 12), by Exer. 11 we have

$$\rho_v = \binom{\rho}{v} \quad \text{for } v \leq \rho,$$

$$\rho_v = 0 \quad \text{for } v > \rho.$$

16. Use this to prove: For an n -rowed square regular matrix A all derived matrices $A^{(v)}$ and all complementary matrices $A^{(v)}$ are also regular, whereas for singular A all $A^{(v)}, A^{(v)}$ are also singular. What relation exists between $|A^{(v)}|$ and $|A^{(v)}|$?¹

For the latter apply Section 19, Exer. 12.

17. By means of the results just established give a new proof for the facts obtained in Exer. 5.

For this purpose note that $A = A^{(1)}$ and $A^{(n-1)}$ have the same rank for an n -rowed square matrix A .

18. Two n -rowed square matrices A, B are called *similar* if there exists a regular n -rowed square matrix P such that $B = P^{-1}AP$, namely, if B is generated from A through transformation by P .—Show that similarity is an equivalence relation in the sense of Section 2, (I).

To prove Section 2, (α), (β), (γ) use the fact that regular matrices form a group (Exer. 8), and Theorem 15 [59].

19. Prove: Similar matrices have the same characteristic polynomial (Section 19, Exer. 6).

Decompose the matrix $xE - B$ into three factors according to Section 10, Exer. 4 on the basis of $P^{-1}P = E$, and apply Section 19, Exer. 7, 8.

¹ For the complete determination of these determinants see Exer. 30 to 32 to Vol. 2, Section 2, given later; for $v = 1$, see Section 20, Exer. 6, already given.

20. An n -rowed square matrix A for which $A^2 = A$ is called *idempotent*.—Prove: If A is idempotent and has rank ρ , then A is similar to $\begin{pmatrix} E_\rho & 0 \\ 0 & 0 \end{pmatrix}$, and conversely.

The case $\rho = 0$ is trivial. For $\rho > 0$ it follows from

$$A^2 - A = (A - E)A = 0$$

that there is a transformation of A into the form

$$P^{-1}AP = \begin{pmatrix} E_\rho & X \\ 0 & Y \end{pmatrix},$$

where $Y = 0$ must be valid due to the rank (Exer. 11), and P is a regular matrix whose first ρ columns are formed from ρ linearly independent columns of A and whose last $n - \rho$ columns are formed from columns chosen suitably for this purpose (analogous to $\bar{A}$ in the proof of Theorem 76). The remaining matrix goes over into the stated form through transformation by $Q = \begin{pmatrix} E_\rho & -X \\ 0 & E_{n-\rho} \end{pmatrix}$. The converse follows simply from Section 10, Exer. 14.

22. Application of the Theory of Determinants to Systems of Linear Equations in the General Case

1. Determine a system of fundamental solutions for the systems of homogeneous equations (H) and (H') which correspond to the two matrices last cited in Section 21, Exer. 1.

Apply Theorem 82.

2. Let (H) be a system of homogeneous equations with $(m, m+1)$ -rowed matrix A of rank m . Set up the simple rule by which a system of fundamental solutions can be formed in this case according to Theorem 82.

$x_k = \alpha_k$, where α_k is the minor with the sign factor $(-1)^{k-1}$ [or, naturally, also $(-1)^k$] formed by striking out the k -th column of A .

3. Accordingly, determine a system of fundamental solutions for the system of homogeneous equations (relative to the field P)

$$\begin{aligned}x_1 + 4x_3 + x_4 &\doteq 0 \\-2x_1 + 3x_2 - x_3 + 2x_4 &\doteq 0 \\x_1 - 2x_2 - 6x_4 &\doteq 0 \\-x_2 - 3x_3 + 3x_4 &\doteq 0\end{aligned}$$

(cf. Section 17, Exer. 3, and Section 21, Exer. 1).

4. Determine the totality of solutions of the two systems of nonhomogeneous equations (relative to the field P) (cf. Section 21, Exer. 1)

$$\begin{aligned}x_1 + x_2 + x_3 + x_4 &\doteq 0 & 2x_1 + 3x_2 + 5x_3 &\doteq 11 \\x_1 + 2x_2 + 3x_3 + 4x_4 &\doteq 2 & 4x_1 + 6x_2 + 10x_3 &\doteq 22 \\2x_1 + 3x_2 + 4x_3 + 5x_4 &\doteq 2 & 8x_1 + 12x_2 + 20x_3 &\doteq 44 \\5x_1 + 7x_2 + 9x_3 + 11x_4 &\doteq 4 & 10x_1 + 15x_2 + 25x_3 &\doteq 55 \\7x_1 + 10x_2 + 13x_3 + 16x_4 &\doteq 6\end{aligned}$$

(a) by the method of Theorem 83,

(b) by the method of Theorem 83, Corollary 1.

Thereby show that the necessary condition for solvability is satisfied,

(a) by the method of Theorem 48, Corollary 2 [93],

(b) by the method of Theorem 83, Corollary 2.

5. In Section 11, Exer. 3 to 5, 7, certain systems of equations without determinants were handled. Now do so by determinant-theoretic methods.

Volume II.

Equations of Higher Degree

Vol. 2. Chapter I. The Left Sides of Algebraic Equations

1. The Fundamental Theorem of the Unique Decomposability into Prime Elements in $K[x]$ and Γ

1. When is $f|g$ valid in a *field*? When is it not?

By Vol. 1, Section 1, (7) the *non*-divisibility relations introduced in Theorem 1 are the only ones.

2. Prove the divisibility law:

$$g_1 g_2 | f_1 f_2 \text{ and } f_1 | g_1 \ (f_1 \neq 0, g_1 \neq 0) \text{ imply } g_2 | f_2.$$

This follows from the rules in Theorem 2, or also directly on the basis of Def. 1.

3. The divisibility theory can also be developed in an arbitrary ring B . This being done, how must the divisibility laws expressed in Theorems 1 to 3 be modified?

Note that a unity element does not necessarily have to exist in B . Therefore, $e|f, f|f$ are in general dropped in Theorem 1. Furthermore, the conditions ' $\neq 0$ ' in Theorems 1, 2 are to be replaced by 'regular' (Vol. 1, Section 3, Exer. 1). If B has no proper zero divisors, then the modification last cited is dropped.

4. What is the meaning of divisibility in the ring of even numbers?

In the case of two even numbers f and g , $f|g$ does not have the same meaning in the ring of even numbers as in the ring of integers; for instance, here $2+2$.

5. What is the meaning of divisibility in a full ring (Vol. 1, Section 3, Exer. 3)?

Here the *non*-divisibility relations are possible only for zero divisors on the left of the divisibility sign.

6. What is the meaning of divisibility in the integral domain Γ_2 of all rational numbers of the form $\frac{g}{2^n}$ with odd g or $g = 0$ (cf. Vol. 1, Section 1, Exer. 10)?

The relation $\frac{g_1}{2^{n_1}} \mid \frac{g_2}{2^{n_2}}$ in Γ_2 amounts to $g_1 \mid g_2$ in Γ .

7. What are the units of this integral domain Γ_2 ? Accordingly, what is the meaning of associate in Γ_2 ?

The units are the numbers $\pm 2^n$ (n any integer).

8. Find a complete system of representatives for the classes of associates in Γ_2 .

The positive odd numbers, for instance, form such a system.

9. Are 2 and 6 prime elements in Γ_2 ?

It is just the reverse of Γ .

10. What are the units of the integral domain $l[x]$ of all integral rational functions of x over an arbitrary integral domain l ? Accordingly, what is the meaning of associate in $l[x]$? Furthermore, show that the prime elements of l are also prime elements in $l[x]$, and above all clarify the situation in the special cases $l = \Gamma, l = K[x_0]$ (Theorem 7) in view of the later Exer. 23 to 27 to Section 2.

Everything follows from formula (3) (valid also in $l[x]$).

11. Determine whether the elements $ax+b, ax^2+bx+c$ of $K[x]$ are prime elements.

Apply Theorems 6, 9 to narrow down the possible proper divisors. Result: $ax+b$ is a prime element if and only if $a \neq 0$. If $2c = 0$ in K , then ax^2+bx+c is a prime element if and only if $c \neq au^2+bu$ with u in K (cf. Exer. 33 and Section 7, Exer. 13). If $2c \neq 0$ in K , then ax^2+bx+c is a prime element if and only if b^2-4ac is not the square of an element of K .

12. By the Euclidean algorithm determine the greatest common divisor of the polynomials

$$(a) \quad x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1,$$

$$x^4 + x^3 + 3x^2 + 2x + 2, (K = P);$$

$$(b) \quad f(x), x - \alpha, (K \text{ arbitrary}, \alpha \text{ in } K).$$

In the latter case we must distinguish between $f(\alpha) \neq 0$ and $f(\alpha) = 0$.

13. How is the result in Exer. 12, (a) to be modified if the polynomials are taken over the field of exactly 2 elements $(0, e)$ or the field of exactly 3 elements $(0, \pm e)$ (cf. Vol. 1, Section 1, Example 4; Vol. 1, Section 1, Exer. 7; Vol. 1, Section 2, Exer. 12)?

In the first case, not at all; in the second case, however, by the linear factor $x - e$.

14. Prove the following rule for calculating with the symbol (f, g) for the greatest common divisor:

$$(af + bg, cf + dg) = (f, g) \quad \text{if} \quad ad - bc \text{ is a unit,}$$

$$\text{in particular,} \quad (f + hg, g) = (f, g)$$

is always valid.

Apply Theorem 14, (1), (2), and Theorem 3. Also show that the restriction regarding $ad - bc$ is essential.

15. Determine the greatest common divisor of

$$ax^2 + bx + c, \quad x^n + ax^2 + bx + c \quad (n > 2).$$

The results vary according as $c \neq 0$ or $c = 0, b \neq 0$ or $c = 0, b = 0, a \neq 0$ or $c = 0, b = 0, a = 0$.

16. From Theorem 14 derive the existence and uniqueness of the normalized *least common multiple* $v = \{f_1, f_2\}$ of f_1 and f_2 which is defined by

$$(a) \quad f_1 | v, f_2 | v;$$

$$(b) \quad f_1 | h, f_2 | h \text{ implies } v | h.$$

The uniqueness follows formally in analogy to the uniqueness of the greatest common divisor d . The existence can be deduced from the existence of d by using Theorem 14, (1), (2) to show that $\frac{f_1 f_2}{d}$ has the properties (a), (b).

17. Accordingly, what is the least common multiple of the polynomials in Exer. 12, (a), (b), and Exer. 13?

18. Analogous to Theorem 15, prove the rule

$$\{f_1, f_2\}g = \{f_1g, f_2g\}.$$

19. How can the fact that f_1 and f_2 are relatively prime be expressed by means of their least common multiple v ?

$$v = af_1f_2.$$

20. Show by a counterexample that in Theorem 16 the assumption, f and g_1 are relatively prime, is essential.

It is sufficient to take $g_2 = e$ and f as divisors of g_1 distinct from units.

21. Similarly, show that in Theorem 18 the assumption, p is a prime element, is essential.

It is sufficient to set g_1g_2 instead of p (where g_1, g_2 are not units).

22. Let the decomposition of two elements f_1 and f_2 into powers of distinct normalized prime elements be given. Use this decomposition to represent the greatest common divisor d and the least common multiple v of these two elements based on the fundamental theorem of the unique prime decomposition. What relation is generally valid between the maximal $\min(\nu_1, \nu_2)$ and the minimal $\max(\nu_1, \nu_2)$ of two integers ν_1, ν_2 corresponding to the relation $dv = af_1f_2$?

For this purpose it is appropriate to set f_i ($i = 1, 2$) in the form

$$f_i = a_i \prod_{k=1}^s p_k^{\nu_{ik}},$$

therefore as products of one and the same set of prime elements p_k ($k = 1, \dots, s$) by allowing the exponents v_{ik} to take on the value 0 also. The representation of d and r can then be found from this on the basis of Theorems 20, 21 and Theorem 14, (1), (2), or Exer. 16, (a), (b).

23. Let f_i ($i = 1, \dots, r$) be any r elements which are not all zero. Again prove the existence and uniqueness of the greatest common divisor $d = (f_1, \dots, f_r)$ and least common multiple $r = \{f_1, \dots, f_r\}$; also generalize the other facts regarding d given in Theorem 14 (representation as a linear combination), as well as Theorems 15, 16, 21 to 23 and, accordingly, the results of Exer. 14, 18, 19, 22.

The proof can be carried through either directly for exactly r elements f_i just as in the case $r = 2$ —in the proof of the uniqueness of the prime decomposition we are then spared the transition from Theorem 18 to Theorem 19—, or also, as before, by applying mathematical induction on r based on the relations

$$((f_1, \dots, f_{r-1}), f_r) = (f_1, \dots, f_r)$$

$$\{(f_1, \dots, f_{r-1}), f_r\} = \{f_1, \dots, f_r\},$$

to be used in this case as *definitions*. Prove these relations by the first type of proof.—The relation $dv = af_1f_2$ (Exer. 16) does *not* generalize to arbitrary r .

24. Prove the following rules for operating with the symbol (f, g) :

$$(a) (f_1, g_1)(f_2, g_2) = (f_1f_2, f_1g_2, g_1f_2, g_1g_2),$$

$$(b) (f, g)^n = (f^n, g^n).$$

(c) If $f_1, \dots, f_r$ are different from zero and *pairwise* relatively prime, then the $g_i = \frac{f_1 \cdots f_r}{f_i}$ ($i = 1, \dots, r$) are *altogether* relatively prime, that is, $(g_1, \dots, g_r) = e$.

What are the rules for the symbol $\{f, g\}$ corresponding to (a), (b)?

(a) follows by two applications of Theorem 15 (see also the explanation to Exer. 23). For (b) apply the fundamental theorem of the unique prime decomposition with the conclusion in Theorem 21, or also—after a slight reduction to the case $(f, g) = e$ —repeat Theorem 23. (c) is a consequence of the same facts as (a).

25. Due to *Zermelo*, the uniqueness proof F can be conducted as an indirect proof which is also very brief. In this case all that we need of the preliminaries in E is the division with remainder (Theorem 13) with the weaker condition $|h| < |g|$ instead of $|h| < |f|$, a modification whose proof is almost obvious.—Carry out this proof in detail according to the general directions given below.

Let $f \neq 0$ be an (hypothetical) element of smallest possible absolute value with a non-unique prime decomposition [principle (4)]:

$$f = ap_1 \dots p_r = bq_1 \dots q_s.$$

Show that $r \geq 2, s \geq 2$ and $p_i \neq q_k$ ($i = 1, \dots, r; k = 1, \dots, s$) must be valid. Then set up a contradiction by dividing p_1 by q_1 with remainder:

$$p_1 = q_1 g + h, \quad |h| < |p_1|$$

(in the above weaker form—therefore, for Γ it is sufficient to have $g = 1, h = p_1 - q_1$). Finally, discuss the relation

$$f_0 = ah p_2 \dots p_r = q_1 (b q_2 \dots q_s - a g p_2 \dots p_r),$$

namely, prove: For (any) decomposition of h and the expression in parentheses on the right into prime elements this relation represents two essentially different decompositions of an $f_0 \neq 0$ with $|f_0| < |f|$, since q_1 does not occur on the left.

26. Prove: If f, g are non-zero relatively prime units, we can actually find elements $\bar{f}, \bar{g}$ satisfying the relation $e = f\bar{f} + g\bar{g}$ in Theorem 14 such that $|\bar{f}| < |g|, |\bar{g}| < |f|$.

By Theorem 13 (division of $\bar{f}$ by $\bar{g}$ with remainder) $|f| < |g|$ can at any rate be reached at the expense of $\bar{g}$. Then in the case $K[x]$ $|\bar{g}| < |f|$ is also valid [by (2a)]; in the case Γ , too, with respect to one of the two possibilities for $\bar{f}$.

27. Prove: Any element ϕ of the quotient field P or $K(x)$ of Γ or $K[x]$, respectively, has a uniquely determined *reduced quotient representation*

$$\phi = \frac{f}{g}, \quad g \text{ normalized, } (f, g) = e,$$

from which all others are generated by multiplying the numerator f and the denominator g by an arbitrary h . What does the representation amount to in the special case $\phi = 0$?

The existence of the representation follows simply from Theorem 15 (dividing out the greatest common divisor in any quotient representation). According to Theorem 16 the uniqueness and the last statement follow on the basis of the equality criterion, Vol. 1, Section 3, (1) (it is best to operate with the *denominators* as divisors, since these are taken to be normalized).

28. Prove: Any element $\phi \neq 0$ of P or $K(x)$ can be represented uniquely in the form

$$\phi = a \prod_p p^\nu,$$

where the product extends formally over *all* normalized prime elements p of Γ or $K[x]$, a is a unit, and the exponents ν are any integers (≥ 0) of which only finitely many are different from zero.

Existence and uniqueness follow easily by prime decomposition of f and g in Exer. 27.

29. By the *degree* of an element $\phi \neq 0$ of $K(x)$ we understand the number $\max(m, n)$, if in the reduced quotient representation of ϕ the numerator f has the degree m and the denominator g has the degree n . If ϕ actually belongs to $K[x]$, then this amounts to the definition of degree given in Vol. 1, Section 5, (2).—Prove: The degree of $\phi(\phi_0(x))$ is the product of the degrees of $\phi(x)$ and $\phi_0(x)$.

Let $\phi = \frac{f}{g}$ (degree m, n), $\phi_0 = \frac{f_0}{g_0}$ (degree m_0, n_0) be the reduced quotient representations of ϕ, ϕ_0 . Since ϕ and $\frac{e}{\phi}$ have the same degree, we can take $m \geq n$ without loss of generality. Then

$$\phi(\phi_0(x)) \equiv \frac{f_1(x)}{g_0(x)^{m-n} g_1(x)} \quad \text{with} \quad \begin{cases} f_1(x) \equiv g_0(x)^m f(\phi_0(x)) \\ g_1(x) \equiv g_0(x)^n g(\phi_0(x)) \end{cases}.$$

First prove that $(f_1, g_1) = e$. To do this, starting from $\bar{f}\bar{f} + g\bar{g} = e$, show that (f_1, g_1) divides a power of g_0 without remainder, and apply $(f_1, g_0) = e$ due to $(f_0, g_0) = e$ (see the formula for f_1 , given below). This means that the reduced quotient representation of the above representation of $\phi(\phi_0(x))$ is obtained by going over to normalized denominators. Next, discuss the degree of

$$\begin{aligned} f_1 &= a_m f_0^m + a_{m-1} f_0^{m-1} g_0 + \cdots + a_1 f_0 g_0^{m-1} + a_0 g_0^m \\ g_0^{m-n} g_1 &= b_n f_0^n g_0^{m-n} + \cdots + b_1 f_0 g_0^{m-1} + b_0 g_0^m, \end{aligned}$$

where the a_i, b_k are the coefficients of f and g . For $m_0 > n_0$ no difficulty is encountered, since $a_m \neq 0, b_n (= e) \neq 0$. For $m_0 < n_0$ note that $a_0 = 0, b_0 = 0$ cannot be true simultaneously due to $(f, g) = e$. For $m_0 = n_0$ note that on applying the same reasons to the leading coefficient α of f_0 (that of g_0 is e due to the normality) $f(\alpha) = 0, g(\alpha) = 0$ cannot be true simultaneously.¹

30. In connection with Vol. 1, Section 4, Exer. 4, 5, show that $\phi_0(x) \equiv \frac{a+bx}{c+dx}$ ($ad-bc \neq 0$) is a necessary as well as sufficient condition for the relation $K(\phi_0(x)) = K(x)$.

Analogously to Vol. 1, Section 4, Exer. 3, the existence of a relation of the form $x \equiv \phi(\phi_0(x))$ is a necessary condition. Then apply the result of Exer. 29.

31. Show that the theorem of the unique decomposability into normalized prime elements is valid in the integral domain Γ_2 of Exer. 6 (cf. also Exer. 7 to 9).

¹ In this regard see—if necessary—Theorem 53 [210], given later, or Exer. 12, (b), already given.

This easily follows by starting from the unique prime decomposition already established in Γ .

32. Prove: If an element g of Γ or $K[x]$ is not an n -th power of an element of Γ or $K[x]$, then it is not an n -th power of an element of P or $K(x)$ either.—In the case Γ we describe this by saying that $\sqrt[n]{g}$ is *irrational* for integers g which are not n -th powers of integers.

On the basis of the fundamental theorem of the unique prime decomposition the assertion $g = \left(\frac{f_1}{f_2}\right)^n$, in a reduced quotient representation, leads in the form $gf_2^n = f_1^n$ to a contradiction of the assumption regarding g .—Show the details of this proof in the special cases $n = 2, g = -1$ and $g = p$ (prime number) relative to Γ .

33. For each of the finite fields of exactly 2, 3, 4 elements (cf. Vol. 1, Section 1, Example 4; Vol. 1, Section 1, Exer. 7, 8; Vol. 1, Section 2, Exer. 12) determine all the prime functions of degree 2, 3, 4.

The prime functions of degree 1 are known (see the remark in Section 1, D). If all prime functions up to the degree $n - 1$ are assumed as known, then all composite polynomials of degree n can be formed. The prime functions of degree n are those which are still lacking.

34. In Exer. 34 to 48 we will consider matrices A with elements from Γ or $K[x]$, briefly, *integral matrices*.—Give a necessary and sufficient condition that the inverse A^{-1} of an integral regular square matrix A be again integral.

A necessary condition is obtained from the formula for multiplying determinants (Vol. 1, Section 19, Exer. 7, 8; cf. also Def. 2). That this condition is sufficient then follows from the expansion of A^{-1} (Vol. 1, Section 19, Exer. 13).

35. Prove: The integral regular n -rowed square matrices A with the property investigated in Exer. 34 (*integral unimodular matrices*) form a group with respect to multiplication.

36. In order to refine the definition in Vol. 1, Section 21, Exer. 9, we call two integral (m, n) -rowed matrices A, B *arithmetically equivalent* if an m -rowed square matrix P and an n -rowed square matrix Q , both integral unimodular, exist such that $B = PAQ$.—Prove that the relation of arithmetical equivalence is an equivalence relation in the sense of Vol. 1, Section 2, (I).

37. Let A be an arbitrary integral matrix of rank ρ and d_ν ($\nu = 1, \dots, \rho$) the greatest common divisor of all ν -rowed minors of A (*determinantal divisors* of A).—In analogy to Vol. 1, Section 21, Exer. 11, prove:

(a) $d_1 | d_2 | \dots | d_\rho$, therefore

$$d_1 = e_1, \quad d_2 = e_1 e_2, \dots, \quad d_\rho = e_1 e_2 \dots e_\rho$$

with integral (normalized) e_ν (*elementary divisors* of A).

(b) Arithmetically equivalent matrices have the same determinantal divisors, therefore also the same elementary divisors.

(a) is a consequence of the Laplace Expansion Theorem; (b) follows from Vol. 1, Section 19, Exer. 11. In both cases use the symmetry of arithmetical equivalence [Vol. 1, Section 2, (β)].

38. Let $A \neq 0$ be an integral (m, n) -rowed matrix and $\bar{A} = (\bar{a}_{ik})$ a matrix arithmetically equivalent to A , where $\bar{a}_{11} \neq 0$ has the smallest possible absolute value.—Prove successively:

(a) $\bar{a}_{11}$ can be assumed to be normalized (with respect to a suitable choice of $\bar{A}$ among all matrices satisfying its defining condition).

(b) $|\bar{a}_{ik}| \geq |\bar{a}_{11}|$ or $\bar{a}_{ik} = 0$ is true throughout.

(c) $\bar{a}_{11} | \bar{a}_{i1}, \bar{a}_{11} | \bar{a}_{1k}$ ($i = 2, \dots, m; k = 2, \dots, n$).

(d) In the same sense as in (a) these can be assumed to be $\bar{a}_{i1}, \bar{a}_{1k} = 0$.

(e) Then $\bar{a}_{11} | \bar{a}_{ik}$ ($i = 2, \dots, m$; $k = 2, \dots, n$), therefore $\bar{a}_{11} = d_1 = e_1$.

For (a) use the operation of multiplying a row by a unit; for (b) the operation of interchanging two parallel rows; for (c), (d), (e), also the operation of adding a row multiplied by an integer to a parallel row. Note that each of these operations produces arithmetically equivalent matrices. In this regard, cf. Vol. 1, Section 10, Exer. 6.

39. On the basis of the recursive process sketched in Exer. 38, prove the following analogy to Vol. 1, Section 21, Exer. 12: Every integral matrix of rank ρ is arithmetically equivalent to a matrix

$$\begin{pmatrix} a_1 & a_2 & \dots & & & \\ & \ddots & & & & \\ & & a_\rho & 0 & \dots & \\ & & & \ddots & & \\ & & & & 0 & \end{pmatrix},$$

where the $a_\nu \neq 0$, are normalized and have the properties $a_1 | a_2 | \dots | a_\rho$.

40. Next, deduce: The a_ν are the elementary divisors of A . In addition to this we always have $e_1 | e_2 | \dots | e_\rho$, which sharpens Exer. 37, (a).

This follows immediately from Exer. 37, (b) by computing the determinantal divisors of the matrix obtained in Exer. 39.

41. To summarize, now prove in analogy to Vol. 1, Section 21, Exer. 14: Two integral matrices are arithmetically equivalent if and only if they have the same elementary divisors (determinantal divisors).

42. Determine the elementary divisors of the following integral matrices A and find integral unimodular matrices P, Q converting them into the normal form of Exer. 39, 40:

$$A = \begin{pmatrix} 6 & 9 & 12 \\ 4 & 5 & 6 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}, \quad \begin{pmatrix} 4 & 2 \\ 22 & 14 \end{pmatrix} \text{ over } \Gamma;$$

$$A = \begin{pmatrix} a-bx & a+bx \\ c-dx & c+dx \end{pmatrix} \text{ over } K[x] \text{ (} a, b, c, d \text{ in } K\text{)}.$$

In the latter case we must distinguish (a) whether $ad - bc \neq 0$ or $= 0$, and (b) whether $2e \neq 0$ or $= 0$ in K .

43. The theory of arithmetical equivalence for the case $K[x]$ can be used to study the concept of the similarity (Vol. 1, Section 21, Exer. 18) of n -rowed square matrices A over K . In Vol. 1, Section 21, Exer. 19 it was established that the characteristic polynomial $|xE - A|$ of A is an invariant relative to the similarity transformations $P^{-1}AP$ of A .—Prove that the determinantal divisors, and consequently the elementary divisors, of the integral matrix $xE - A$ (*characteristic matrix* of A) are also invariants relative to similarity transformations of A .

Note that a similarity transformation of A brings about an arithmetical equivalence relation for the characteristic matrix $xE - A$, and use Exer. 37, (b).

44. From now on let integral matrices over $K[x]$ be always specified by adjoining the indeterminate x , for instance, $A(x)$, in order to distinguish them from matrices over K which will be designated by capital Latin letters without adjoining x . By the *degree* of $A(x) \equiv (f_{ik}(x)) \neq 0$ we understand the highest degree in x appearing among the $f_{ik}(x)$. Therefore, the matrices A over K (and only these) have the degree 0; the characteristic matrix $xE - A$ of A has the degree 1; in general,

a matrix $A(x)$ of degree m can be represented in the form $A_0 + xA_1 + \cdots + x^mA_m$ ($A_m \neq 0$), where A_i is the matrix of the coefficients of x^i of the elements $f_{ik}(x)$.—Prove: To every integral n -rowed square matrix $P(x)$ there exist unique integral n -rowed square matrices $P_1(x), \bar{P}_1(x)$ and matrices $P, \bar{P}$ such that

$$P(x) \equiv P_1(x)(xE - A) + P$$

$$P(x) \equiv (xE - A)\bar{P}_1(x) + \bar{P}$$

(right and left division by $xE - A$). What is the expression for P and $\bar{P}$ in terms of $P(x)$ and A ?

Proceed [using as a basis the representation given above for $P(x)$ as an integral rational function of x with matrix coefficients] formally just as for ordinary division in the case of integral rational functions. The uniqueness, too, follows as in the latter; for instance, in the case of right division the uniqueness follows by considering the degree (highest term in x) of $(P_1(x) - P_2(x))(xE - A)$.

45. Let the n -rowed square matrices $xE - A$ and $xE - B$ have the same elementary divisors. Hence by the result of Exer. 41 there exist two integral unimodular n -rowed square matrices $P(x)$ and $Q(x)$ with

$$(xE - A)P(x) \equiv Q(x)(xE - B).$$

Show that a corresponding relation exists with matrices P and Q over K . For this purpose divide $P(x)$ on the right by $xE - B$ and $Q(x)$ on the left by $xE - A$, then take the degrees into consideration. Furthermore, show that in this case we must have $P = Q$.

Let $P_1(x), Q_1(x), P, Q$ be the quotients and remainders appearing in the divisions. Then, on considering the highest terms in x the relation

$$(xE - A)(P_1(x) - Q_1(x))(xE - B) \equiv Q(xE - B) - (xE - A)P$$

implies that $P_1(x) \equiv Q_1(x)$; consequently $P = Q$ must be valid, too.

46. Show that the matrix $P = Q$ in Exer. 45 is regular, by dividing $P(x)^{-1}$ on the right by $xE - A$, $Q(x)^{-1}$ on the left by $xE - B$ and taking the degrees into consideration.

Let $\bar{P}_1(x), \bar{Q}_1(x), \bar{P}, \bar{Q}$ be the quotients and remainders appearing in the latter divisions. Then $\bar{P}_1(x) \equiv \bar{Q}_1(x)$ is also valid, and we can obtain relations

$$E \equiv P(x)P(x)^{-1} \equiv R(x)(xE - A) + P\bar{P}$$

$$E \equiv Q(x)^{-1}Q(x) \equiv (xE - B)S(x) + Q\bar{Q}$$

with integral $R(x), S(x)$. By considering the highest terms in x these relations yield $R(x) \equiv 0, S(x) \equiv 0$.

47. To summarize, now deduce: Two n -rowed square matrices A and B are similar if and only if their characteristic matrices $xE - A$ and $xE - B$ have the same elementary divisors.

All that still has to be done in Exer. 45 is to set $x = 0$.

48. Decide whether the following matrices A and B over P are similar:

$$(a) \quad A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix};$$

$$(b) \quad A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix};$$

$$(c) \quad A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 1 & 0 \\ -1 & 0 & 0 \\ -1 & -1 & 1 \end{pmatrix}.$$

2. Residue Class Rings in $K[x]$ and Γ

1. Prove: If $g|f$, then every residue class mod g consists of complete residue classes mod f .

$$h_1 \equiv h_2 \pmod{f} \text{ implies } h_1 \equiv h_2 \pmod{g}.$$

2. Prove: If $g \mid f$ and $f \neq 0$, then in the case Γ every residue class $\text{mod } g$ has the same finite number of residue classes $\text{mod } f$. How large is this number?

Think of the residue class ring $\text{mod } f$ as a group with respect to its addition (*additive residue class group mod f*; Vol. 1, Section 7, Exer. 4, 5) and interpret the transition from the (finer) congruence $\text{mod } f$ to the (coarser) congruence $\text{mod } g$ as a homomorphism of this group on the additive residue class group $\text{mod } g$ (Vol. 1, Section 9, Exer. 9). The statements then follow from Vol. 1, Section 8, especially Vol. 1, Theorem 25 [68]; see also Vol. 1, Section 8, Exer. 8.

3. Decide whether the linear congruence

$$gy \equiv h \pmod{f} \quad (f \neq 0),$$

where g, h are given and y is to be found, can be solved, and in the case Γ determine the number of solutions. The solutions are to be counted as residue classes $\text{mod } f$, that is, only solutions y not congruent $\text{mod } f$ are to be counted as different.

It depends on the divisor of the residue class $g \pmod{f}$ (Theorem 30). The necessary and sufficient condition for solvability is that h also be divisible by this divisor (Theorem 3 [173], Theorem 31), and the number of solutions in the case Γ follows from its cancellation under consideration of Exer. 2.

4. Use this result to decide which of the linear congruences

(a) $2x \equiv 1 \pmod{5}$,

(b) $6x \equiv 5 \pmod{15}$,

(c) $6x \equiv 3 \pmod{15}$

can be solved, and determine the solutions of the congruences which can be solved.

5. How is the partition into regular elements and zero divisors (Vol. 1, Section 3, Exer. 1) represented in the residue class ring $\text{mod } f$?

The prime residue classes are regular (Theorem 31), the non-prime residue classes are zero divisors in case $f \neq 0$; however, the latter are also regular except for 0 in case $f = 0$.

6. Accordingly prove: The residue class ring mod f is a full ring (Vol. 1, Section 3, Exer. 3) for $f \neq 0$.

Apply the part of Theorem 31 still not taken into account in Exer. 5.

7. Let f_1, f_2 be relatively prime and different from zero. Furthermore, in the sense of Theorem 14 let

$$f_1 \bar{f}_1 + f_2 \bar{f}_2 = e,$$

therefore
$$\begin{aligned} f_2 \bar{f}_2 &\equiv e \bmod f_1 \equiv 0 \bmod f_2, \\ f_1 \bar{f}_1 &\equiv 0 \bmod f_1 \equiv e \bmod f_2. \end{aligned}$$

From this deduce a solution of the system of congruences

$$y \doteq y_1 \bmod f_1, \quad y \doteq y_2 \bmod f_2,$$

where y_1, y_2 are given and y is to be found. What modulus must be used in forming the residue classes in order that the solution be unique?

Multiply the previously given congruences by y_1 and y_2 and add.

8. Show that y in Exer. 7 runs through a complete system of representatives of the residue classes relative to the product modulus $f = f_1 f_2$ (*complete residue system mod f*), if y_1, y_2 run through such systems mod $f_1, \bmod f_2$.

In the case Γ we only have to carry through an enumeration based on Theorem 27 and Exer. 7; in the case $K[x]$, such an enumeration is not enough. However, the statement follows uniformly for both cases if in Exer. 7 we start with $y_1 = y, y_2 = y$.

9. In connection with Exer. 7, 8, prove that the one-to-one correspondence $y \longleftrightarrow (y_1, y_2)$ between the residue classes $y \bmod f$ and the pair of residue classes $y_1 \bmod f_1, y_2 \bmod f_2$

yields an isomorphism between the corresponding residue class rings, if the operations with the pairs y_1, y_2 are defined in terms of the components:

$$(y_1, y_2) + (y'_1, y'_2) = (y_1 + y'_1, y_2 + y'_2),$$

$$(y_1, y_2)(y'_1, y'_2) = (y_1 y'_1, y_2 y'_2)$$

(representation of the residue class ring $\text{mod } f$ as the *direct sum* of the residue class rings $\text{mod } f_1$ and $\text{mod } f_2$).

The isomorphism relations Vol. 1, Section 2, (3), (4) have to be proved for the specified correspondence with respect to the specified operations. These relations immediately follow on expressing the correspondence in a computational form according to Exer. 7:

$$y \equiv y_1 f_2 \bar{f}_2 + y_2 f_1 \bar{f}_1 \text{ mod } f.$$

10. Investigate the behavior of the prime residue classes with respect to this isomorphism.

y is prime to f if and only if y_1 is prime to f_1 and y_2 is prime to f_2 .

11. Under the assumptions of Exer. 7, what relation is obtained from this in the case Γ for the numbers $\phi(f) = \phi(f_1 f_2)$ and $\phi(f_1), \phi(f_2)$ of prime residue classes?

12. Generalize Exer. 7 to 11 to the case of a product f of an arbitrary number r of pairwise relatively prime factors $f_1, \dots, f_r$ different from zero.

In connection with Section 1, Exer. 23, Exer. 24, (c), start here from the relation

$$g_1 \bar{g}_1 + \dots + g_r \bar{g}_r = e, g_i = \frac{f}{f_i} \quad (i = 1, \dots, r).$$

13. Use this to solve the system of congruences

$$y \equiv 3 \text{ mod } 4, \quad y \equiv 2 \text{ mod } 5, \quad y \equiv 2 \text{ mod } 3.$$

Generally, if we wish to obtain in Exer. 12 the basic solution of

$$g_1 \bar{g}_1 + \dots + g_r \bar{g}_r = e,$$

not by trial and error but by a systematic calculating process, we must first of all determine by the Euclidean algorithm a solution h_1, h_2 of $g_1 h_1 + g_2 h_2 = (g_1, g_2)$, then a solution h'_1, h'_2 of

$$(g_1, g_2) h'_1 + g_3 h'_2 = (g_1, g_2, g_3), \text{ etc.}$$

14. On the basis of Exer. 12, prove the formula for the Euler function $\phi(f)$ found in connection with Theorem 31.

Take as a basis the decomposition of f into powers p^v of different prime numbers p and determine $\phi(p^v)$ directly from the fact that here the non-prime residue classes are exactly the residue classes of the divisor p , the number of which is known by Exer. 2 (or can also be easily derived from the complete residue system of Theorem 27).

15. In connection with Vol. 1, Section 6, Exer. 6 clarify the group-theoretic nature of the proof for the Fermat Theorem (Theorem 29 and remarks after Theorem 31).

16. For which natural numbers f as moduli is

$$(a) \phi(f) = 4, \quad (b) \phi(f) = f - 1, \quad (c) 2\phi(f) = f,$$

$$(d) \phi(f) \mid f, \quad (e) 2\phi(f) \mid f?$$

For (a) distinguish cases according as the (proper or improper) factorizations of 4 correspond to the decomposition of f into powers of different prime numbers, and apply the formula for $\phi(f)$ explicitly given by Theorem 31. (b) is easily answered directly (Theorem 28); (c), (d), (e) again on the basis of the explicit formula. Results for (d): $f = 2^\nu 3^\nu$ ($\nu > 0$, in case $\nu' > 0$); for (e): $f = 2^\nu$.

17. Classify the above f with $\phi(f) = 4$ into two classes according as to which of the two (no other) group types $\mathfrak{Z}_4$ or $\mathfrak{D}_2$ of order 4 (Vol. 1, Section 6, Exer. 2) the prime residue class group $\mathfrak{P}$, belongs.

From a *practical point of view* this is easily decided by the explicit construction of the residue classes and their combinations. From a *theoretical point of view* have recourse to the direct sum representation of the ring Γ , given in Exer. 9. By Exer. 10 this yields a *direct product*

representation¹ of the group $\mathfrak{P}_f$. If two of these components have the type $\mathfrak{B}_2$, then $\mathfrak{P}_f$ has the type $\mathfrak{D}_2$; however, if one has the type $\mathfrak{B}_4$, the other the type $\mathfrak{B}_1 = \mathfrak{C}$ (or the other is missing entirely), then $\mathfrak{P}_f$ has the type $\mathfrak{B}_4$.

18. In Exer. 2 we determined the number of those residue classes relative to a natural number f whose divisor is *divisible* by g . Determine also the number of those residue classes mod f whose divisor is *exactly* g .

Note that g prime residue classes relative to the resulting modulus must be generated on cancelling out the divisor.

19. Accordingly, prove the relation

$$\sum_{d \mid f} \phi(d) = f$$

for any natural number f , where the sum is to extend over all different (proper and improper) normalized divisors d of f .

Enumerate all f residue classes mod f ordered according to their divisors.

20. Construct finite fields by combining Theorems 27, 28 for the case Γ ; using the same theorems, then do this for the case $K[x]$ (with suitable K).²

If $f(x)$ is a prime function of degree n over $\mathbf{P}_p$, then the residue class ring mod $f(x)$ is a finite field of p^n elements.

21. Establish that the field of 4 elements constructed in Vol. 1, Section 1, Exer. 8 can be generated in this way.

The only prime function of degree 2 in $\mathbf{P}_2$ is $x^2 + x + e$ (Section 1, Exer. 33).

22. Prove the existence of finite fields of p^2 elements for any prime number p .

¹ In this regard see also the general theory given later in Section 3, Exer. 9 ff.

² For Exer. 20 to 22 see the general theory given later in Section 20.

The number of different *reducible* polynomials over P_p of degree 2 can be easily found by using the fact that they can all be expressed in the form $(x-a)(x-b)$. We have to show that it is smaller than the number of *all* different polynomials over P_p of degree 2. Note that $(x-a)(x-b) \equiv (x-a')(x-b')$ is permissible only for $a = a', b = b'$ (or the other way around) (Theorem 12 [178]).

23. Let $I = \Gamma$ or $K[x]$, and consider the integral domain $I[x_1]$ (cf. Section 1, Exer. 10). To every non-zero element

$$f(x_1) \equiv a_0 + a_1x_1 + \cdots + a_nx_1^n$$

of $I[x_1]$ there corresponds a definite greatest common *divisor* of its coefficients $a_0, \dots, a_n$ in I , briefly, the *divisor* of f . f is called *primitive* if its divisor is e . The divisor of f is always unique:

$$f = df_0 \text{ (} f_0 \text{ primitive in } I[x_1], d \text{ normalized in } I\text{)}.$$

For a normalized prime element p of I the highest power p^v dividing d without remainder is called the *p-divisor* of f , and f is called *p-primitive* if its *p-divisor* is e . The *p-divisor* of f is always unique:

$$f = p^vf_p \text{ (} f_p \text{ p-primitive in } I[x_1]\text{)}.$$

Besides the facts just specified, prove successively (*Gauss's Theorem*):

(a₀) If f_1 and f_2 are *p-primitive*, then f_1f_2 is also *p-primitive*.

(b₀) If f_1 and f_2 have the *p-divisors* p^{v_1} and p^{v_2} , then f_1f_2 has the *p-divisor* $p^{v_1+v_2}$.

(a) If f_1 and f_2 are primitive, then f_1f_2 is also primitive.

(b) If f_1 and f_2 have the *divisors* d_1 and d_2 , then f_1f_2 has the *divisor* d_1d_2 .

(b₀) and (b) easily follow from (a₀) and (a). (a) and (b) follow from (a₀) and (b₀) according to the fundamental theorem of the unique

prime decomposition in l by taking into account *all* prime elements p of l . The crucial statement (a_0) amounts to the trivial Vol. 1, Theorem 4 [18] if we go over from $l[x_1]$ to the residue class ring $l_p[x_1]$, relative to the prime element p (Section 1, Exer. 10). For, ' p -primitive' thereby goes over into ' $\neq 0$ ', and the residue class ring is an integral domain (not a field—Theorem 28 is not proved for $l_p[x_1]$; in fact it is not valid), namely, is isomorphic to the integral domain $l_p[x_1]$ over the residue class field $l_p \bmod p$ of l . The latter is proved by setting up an obvious correspondence. It represents the main conclusion of the proof.

24. Let $\bar{K} = P$ or $K(x)$ designate the quotient field of $l = \Gamma$ or $K[x]$, respectively. Exer. 23, (a) implies: If an element $f \neq 0$ in $l[x_1]$ has a decomposition $f = a\bar{f}_1\bar{f}_2$ into two normalized factors $\bar{f}_1, \bar{f}_2$ of $\bar{K}[x_1]$ and a in l , then it also has a decomposition $f = cf_1f_2$ into two primitive factors f_1, f_2 of $l[x_1]$ which are associates of $\bar{f}_1, \bar{f}_2$ in $\bar{K}[x_1]$, and c in l . In particular, if f is normalized (polynomial in x_1), therefore $a = 1$, then $\bar{f}_1, \bar{f}_2$ already belong to $l[x_1]$ (this, too, is often called *Gauss's Theorem*).

By introducing suitable quotient representations of the $\alpha_0, \dots, \alpha_{n-1}$ in $\bar{K}$, any normalized

$$\bar{f}(x_1) \equiv \alpha_0 + \alpha_1 x_1 + \dots + \alpha_{n-1} x_1^{n-1} + x_1^n$$

in $\bar{K}[x_1]$ can be uniquely expressed in the form

$$f(x_1) \equiv \frac{a_0 + a_1 x_1 + \dots + a_n x_1^n}{a_n} \equiv \frac{f(x_1)}{a_n},$$

where $a_0, \dots, a_n$ (the latter normalized) are relatively prime elements in l (a_n the normalized *least common denominator* of $\alpha_0, \dots, \alpha_{n-1}$). Therefore $f(x_1)$ is a primitive element of $l[x_1]$.

25. In connection with this prove the validity in $l[x_1]$ of the fundamental theorem of the unique prime decomposition based on its validity in l and in $\bar{K}[x_1]$.

The *possibility* of the decomposition follows analogously as in Section 1, D. For this purpose set here $|f| = k^n$, if $f (\neq 0)$ has degree n (in x_1). For $|f| = 1$ there exists an element of l for which the possibility of the prime decomposition in $l[x_1]$, too, is already known (Section 1, Exer. 10). For the *uniqueness* of the prime decomposition proceed from the unique prime decomposition of an $f (\neq 0)$ of $l[x_1]$ in the extension domain $\bar{K}[x_1]$; from this derive according to Exer. 24 a decomposition into primitive (but not normalized in $\bar{K}[x_1]$) prime elements of $\bar{K}[x_1]$ belonging to $l[x_1]$, and a unit factor of $\bar{K}[x_1]$ (associate of the divisor of f) belonging to l . The uniqueness of the prime decomposition in the extension domain $\bar{K}[x_1]$ together with the uniqueness of the prime decomposition of the last-specified unit factor in l guarantees the uniqueness of the prime decomposition in the subdomain $l[x_1]$ just obtained (except for the ordering and the normalization of the prime elements by units of $l[x_1]$ [units of l]). In this regard clearly show that among all associates of a prime element $\bar{p}(x_1)$ of $\bar{K}[x_1]$ in $\bar{K}[x_1]$ only the associate $p(x_1)$ (and its associates in $l[x_1]$) constructed according to the discussion to Exer. 24 belongs to $l[x_1]$ and, at the same time, is a prime element there.

26. Find a normalization rule for the prime elements of $l[x_1]$ on the basis of which the prime decomposition is completely unique except for the ordering.

It is sufficient to require that the leading coefficient in x_1 be normalized in l .

27. According to the same scheme as before, prove by mathematical induction that the fundamental theorem of the unique prime decomposition in $\Gamma[x_1, \dots, x_n]$ and in $K[x_1, \dots, x_n]$ is valid.

In the latter case it is better to base the induction proof on $K[x, x_1, \dots, x_n]$, since the basic steps of the mathematical induction then correspond in both cases as follows:

$$\begin{aligned} &\Gamma, \Gamma[x_1], \dots, \Gamma[x_1, \dots, x_n] \\ &K[x], K[x, x_1], \dots, K[x, x_1, \dots, x_n]. \end{aligned}$$

The first two steps are obvious. The passage from the $(n-1)$ -th step to the n -th step is accomplished by the very same scheme as the passage from the first to the second step.—A suitable normalization rule is obtained by the following *inductive definition* adapted to the inductive proof: An element $f \neq 0$ of $I[x_1, \dots, x_n]$ is said to be normalized in $I[x_1, \dots, x_n]$ if its leading coefficient in x_n is normalized in $I[x_1, \dots, x_{n-1}]$. This rule refers to the fixed basic ordering $x_1, \dots, x_n$ of the indeterminates.

28. Let I be any of the previously studied integral domains $\Gamma[y_1, \dots, y_m]$ or $K[y_1, \dots, y_m]$ with unique prime decomposition, and let $I[x_1, \dots, x_n]$ be the integral domain of the integral rational functions of n (new) indeterminates $x_1, \dots, x_n$ over I ; therefore it too is an integral domain with unique prime decomposition. Prove: In order that an element

$$a_1 x_1 + \dots + a_n x_n$$

with coefficients $a_1, \dots, a_n$ in I (a linear form in $x_1, \dots, x_n$ over I) be a prime element in $I[x_1, \dots, x_n]$, it is necessary and sufficient that the coefficients $a_1, \dots, a_n$ be relatively prime in I .

The necessity is trivial. Conversely, in a decomposition one of the factors must have the degree 0 in all the indeterminates $x_1, \dots, x_n$ simultaneously, since otherwise the normal representation of the product of both factors would contain a product $x_i x_k$ with coefficients different from zero (consider the *last* term actually appearing in both factors in order to exclude a cancellation).

29. In connection with Vol. 1, Section 17, Exer. 7, prove that the determinant $|X| \equiv |x_{ik}|$ of the matrix $X \equiv (x_{ik})$ in n^2 indeterminates over K is a prime element in $K[x_{11}, x_{12}, \dots, x_{nn}]$.

Use mathematical induction on n , expand $|X|$, say, by the first row:

$$|X| \equiv x_{11} \xi_{11} + \dots + x_{1n} \xi_{1n}$$

and apply Exer. 28. In doing so take into account that the property, ξ_{11} is a prime element in $K[x_{22}, x_{23}, \dots, x_{nn}]$, which is guaranteed by the induction assumption, carries over to $K[x_{21}, \dots, x_{n1}; x_{22}, x_{23}, \dots, x_{nn}]$

(just as in Section 1, Exer. 10), and that $\xi_{11}, \dots, \xi_{1n}$ are (normal representations) not associates in the latter integral domain.

30. In connection with Vol. 1, Section 19, Exer. 12 and Vol. 1, Section 21, Exer. 16, prove by means of the result of Exer. 29 that the determinants of the derived matrices $A^{(\nu)}$ and the complementary matrices $A^{(\nu)}$ of an arbitrary n -rowed square matrix A have the form $c_\nu |A|^{l_\nu}$ and $\gamma_\nu |A|^{l_\nu}$, with certain factors c_ν, γ_ν of K and exponents l_ν, λ_ν dependent only on ν (not on A).

Let $X \equiv (x_{ik})$ be a matrix in n^2 indeterminates over K . By the principle of substitution it is sufficient to prove the formulae

$$|X^{(\nu)}| \equiv c_\nu |X|^{l_\nu}, \quad |\Xi^{(\nu)}| \equiv \gamma_\nu |X|^{l_\nu}$$

with certain factors c_ν, γ_ν of K (units of $K[x_{11}, \dots, x_{nn}]$) and exponents l_ν, λ_ν . By Vol. 1, Section 21, Exer. 16 the prime decomposition is known for the product $|X^{(\nu)}| |\Xi^{(\nu)}|$ and the fundamental theorem can be used with the conclusion (valid, naturally, also in the general case submitted here) of Theorem 20 [187].

31. Determine the exponents l_ν, λ_ν in Exer. 30 by replacing K by $K(y)$ with a new indeterminate y and investigating the determinants of the derived and complementary matrices of the matrix (yx_{ik}) .

Take into consideration the remark after Vol. 1, Theorem 68 [141].

32. Determine the factors c_ν, γ_ν in Exer. 30.

It is sufficient to substitute the particular matrix E for A .

3. Cyclic Groups

1. Show that the proof of Theorem 36 amounts to the considerations in Section 2, Exer. 1, 2, if the isomorphism of $\mathfrak{J}$ to the additive group $\mathfrak{R}_n$ of the residue classes mod n (n the order of $\mathfrak{J}$ or $n = 0$ in case it is infinite) is taken as a basis.

Compare this highly conceptual proof also with the naive one sketched in the explanation to Vol. 1, Section 7, Exer. 1.

2. Let A be an element of a group $\mathcal{G}$. If the element has finite order n or infinite order and m is an integer, what is the order of A^m ?

Take as a basis the isomorphism of the cyclic group $\mathfrak{Z}$ generated by A to $\mathfrak{R}_n$ (as in Exer. 1) and study the linear congruence $mx \equiv 0 \pmod n$ according to Section 2, Exer. 3.

3. Let P be an n -termed cycle (Vol. 1, Section 16, Exer. 9) and m an integer. Give the decomposition of P^m into cycles (Vol. 1, Section 16, Exer. 10).

If $(m, n) = d$ and $n = dk$, then d is the number of k -termed cycles which can be explicitly written out starting from $P = (12 \dots n)$. They correspond to the composition of the d residue classes mod d from the k residue classes mod n (Section 2, Exer. 1, 2).

4. Show by a counterexample that the assumption of the commutativity of A_1 and A_2 is essential in Theorem 35.

Naturally, it must be based on a non-Abelian group. The simplest such group, the dihedral group $\mathfrak{D}_3$, will suffice (cf. Vol. 1, Section 6, Example 4; Vol. 1, Section 6, Exer. 2).

5. In connection with Theorem 35 and Vol. 1, Section 8, Exer. 5, 6, determine the order of the product $A_1 A_2$, where A_1, A_2 are two commutative elements of the prime power orders p^{μ_1}, p^{μ_2} with $\mu_1 \neq \mu_2$ of a group $\mathcal{G}$.

6. Let a finite group $\mathcal{G}$ be the composite of two cyclic subgroups $\mathfrak{Z}_1, \mathfrak{Z}_2$ which are commutative elementwise and have the intersection $\mathfrak{E}$ (*direct product* of $\mathfrak{Z}_1$ and $\mathfrak{Z}_2$; notation $\mathcal{G} = \mathfrak{Z}_1 \times \mathfrak{Z}_2$). $\mathcal{G}$ is therefore Abelian.—Prove: $\mathcal{G}$ is cyclic or not according as the orders of $\mathfrak{Z}_1$ and $\mathfrak{Z}_2$ are relatively prime or not.

Apply first of all Vol. 1, Section 7, Exer. 9 in order to determine the order of $\mathfrak{G}$, then Theorem 35 or Vol. 1, Section 8, Exer. 5.—The result is also valid for infinite groups $\mathfrak{G}$ if 0 and 0 are interpreted as *not* relatively prime.

7. Generalize Exer. 6 to the case where $\mathfrak{G}$ is the composite of an arbitrary number r of cyclic subgroups $\mathfrak{Z}_1, \dots, \mathfrak{Z}_r$, each of which is commutative elementwise with every other one and has the intersection $\mathfrak{C}$ with the composite of the remaining (*direct product* of $\mathfrak{Z}_1, \dots, \mathfrak{Z}_r$; notation, $\mathfrak{G} = \mathfrak{Z}_1 \times \dots \times \mathfrak{Z}_r$).

Apply mathematical induction (cf., in particular, Section 1, Exer. 23).

8. Conversely, prove: If $\mathfrak{G}$ is cyclic of finite order n and $n = n_1 \cdots n_r$ is a decomposition into pairwise relatively prime factors, then $\mathfrak{G}$ is the direct product of r cyclic subgroups $\mathfrak{Z}_1, \dots, \mathfrak{Z}_r$ of orders $n_1, \dots, n_r$.

The easiest way to show this is to take as a basis the isomorphism of $\mathfrak{G}$ to the additive residue class group $\mathfrak{R}_n$ and to use its representation as the direct sum of the additive residue class groups $\mathfrak{R}_{n_i}$ ($i = 1, \dots, r$) according to Section 2, Exer. 9, 12.—After this, find explicitly, in particular, primitive elements of the cyclic groups $\mathfrak{Z}_i$.

9. In general, a (finite or infinite) group $\mathfrak{G}$ is called a *direct product* of the subgroups $\mathfrak{H}_i$ ($i = 1, \dots, r$) each of which is elementwise commutative with each of the remaining, notation $\mathfrak{G} = \mathfrak{H}_1 \times \dots \times \mathfrak{H}_r$, if

(α) $\mathfrak{G}$ is composed from the $\mathfrak{H}_i$,

(β) every $\mathfrak{H}_i$ has the intersection $\mathfrak{C}$ with the composite of the $\mathfrak{H}_k$ with $k \neq i$. Prove:

(a) Any element A of $\mathfrak{G}$ has a unique representation

$$A = A_1 \dots A_r \quad (A_i \text{ in } \mathfrak{H}_i).$$

(b) For finite $\mathfrak{G}$ the order n of $\mathfrak{G}$ is the product of the orders n_i of $\mathfrak{H}_i$.

(c) $\mathfrak{S}_i$ is a normal divisor of $\mathfrak{G}$, and $\mathfrak{G}/\mathfrak{S}_i$ is isomorphic to the composite (direct product) of the $\mathfrak{S}_k$ with $k \neq i$.

(d) In the definition of direct product conditions (α) , (a) can also be used instead of conditions (α) , (β) ; for finite $\mathfrak{G}$, condition (b) instead of condition (β) .

10. Prove: If $\mathfrak{G}$ is an Abelian group of finite order n and $n = n_1 \cdots n_r$ is a decomposition of n into pairwise relatively prime factors, then $\mathfrak{G}$ can also be represented as the direct product of r subgroups of orders $n_1, \dots, n_r$.

The commutativity of $\mathfrak{G}$ implies that the solutions of the equations $X_1^{n_1} \doteq E, \dots, X_r^{n_r} \doteq E$ in $\mathfrak{G}$ form subgroups $\mathfrak{S}_1, \dots, \mathfrak{S}_r$. If $m_1 \bar{m}_1 + \cdots + m_r \bar{m}_r = 1$ is valid with $m_i = \frac{n}{n_i}$ (Section 2, Exer. 12), then for arbitrary A in $\mathfrak{G}$

$$A = A^1 = A^{m_1 \bar{m}_1} \cdots A^{m_r \bar{m}_r}$$

turns out to be the unique decomposition into components belonging to these subgroups. The statement follows from this by Exer. 9, (a), (d).

11. From the result of Exer. 10 deduce: Any finite Abelian group can be represented as the direct product of subgroups whose orders are powers of different prime numbers.

12. Let $A_1, \dots, A_n$ be the totality of elements of a finite Abelian group $\mathfrak{G}$. Consider all relations

$$A_1^{\alpha_1} \cdots A_n^{\alpha_n} = E$$

existing between $A_1, \dots, A_n$ based on the rule of combination in $\mathfrak{G}$. They yield an infinite system of n -termed vectors

$$\mathfrak{a} = (\alpha_1, \dots, \alpha_n).$$

Show: In this system a subsystem $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ can be so chosen that all vectors $\mathfrak{a}$ of the system are linear combinations with *integral* coefficients of the vectors $\mathfrak{a}_i$ of the subsystem.

This is clear (Vol. 1, Section 13, Lemma 1 [103]) for linear combinations with *rational* coefficients. For integral linear combinations bear in mind that in $\mathfrak{G}$ there exist n special relations

$$A_k^{n_k} = E \quad (k = 1, \dots, n),$$

where n_k is the order of A_k . Include the exponent vectors $n_k \epsilon_k$ in the subsystem to be chosen, and in addition the other finitely many exponent vectors which are generated from the totality $\mathfrak{a}$ by the reduction of α_k to a fixed residue system mod n_k .

13. Let $A = (\alpha_{ik})$ ($i = 1, \dots, r$; $k = 1, \dots, n$) be the integral matrix whose rows are the vectors α_i chosen in Exer. 12. According to Section 1, Exer. 39, 40, A is arithmetically equivalent to a matrix

$$B = \begin{pmatrix} e_1 & & & \\ & \ddots & & \\ & & \ddots & \\ & & & e_n \end{pmatrix},$$

where the e_k are positive integers or 0 and $e_1 | \dots | e_n$ (therefore, if there are any $e_k = 0$, they stand at the end). Let $PAQ = B$ with integral unimodular P, Q . Submit the elements A_k to the linear substitution with the matrix Q^{-1} :

$$B_k = \prod_{i=1}^n A_i^{\bar{q}_{ki}} \quad (k = 1, \dots, n), \text{ briefly } \mathfrak{B} = Q^{-1}\mathfrak{A},$$

whose converse therefore is the linear substitution

$$A_k = \prod_{i=1}^n B_i^{q_{ki}} \quad (k = 1, \dots, n), \text{ briefly } \mathfrak{A} = Q\mathfrak{B},$$

with the matrix Q , and prove: The exponent vectors $\mathfrak{b}$ of all relations existing between the generating elements B_k are integral linear combinations of the exponent vectors of the special relations

$$B_k^{e_k} = E \quad (k = 1, \dots, n).$$

Every exponent vector $\mathbf{a}$ yields an exponent vector $\mathbf{b}$ in the form $\mathbf{b} = \mathbf{a}Q$, and all $\mathbf{b}$ are generated in this way, since conversely every $\mathbf{b}$ yields an $\mathbf{a}$ in the form $\mathbf{a} = \mathbf{b}Q^{-1}$. The totality of $\mathbf{b}$, therefore, of the $\mathbf{a}Q$, is an integral linear combination of the $\mathbf{a}_iQ$, that is, of the rows of the matrix AQ , and these again are also integral linear combinations of the rows of the matrix $PAQ = B$.

14. From Exer. 13 deduce: Any finite Abelian group $\mathcal{G}$ can be represented as the direct product of cyclic groups $\mathfrak{B}_1, \dots, \mathfrak{B}_r$ such that their orders $n_1, \dots, n_r$ satisfy the condition $n_1 \mid \dots \mid n_r$. Namely, show:

(a) The periods $\mathfrak{B}_k$ of the B_k have $\mathcal{G}$ as their composite [Exer. 9, (α)].

(b) All e_k are different from zero, and $\mathfrak{B}_k$ has the order e_k .

(c) The $\mathfrak{B}_k$ have the property (β) of Exer. 9.

(a) follows from $\mathfrak{A} = Q\mathfrak{B}$. (b) and (c) follow from Exer. 13; in so doing note, in particular, that due to the finiteness of $\mathcal{G}$ every B_k has finite order—this yields $e_k \neq 0$ —and that the B_k with $e_k = 1$, possibly appearing (at the beginning), can be omitted.

15. Now prove: Any finite Abelian group $\mathcal{G}$ can be represented as the direct product of cyclic groups of prime power order (*Fundamental Theorem of Finite Abelian Groups*).

Combine Exer. 14 and Exer. 8.¹

16. Prove that the prime power orders appearing in Exer. 15 are determined uniquely by $\mathcal{G}$ (*prime power invariants* of $\mathcal{G}$).

¹ Exer. 10, 11 are not necessary for the proof of the Fundamental Theorem, laid out here, by means of the theory of elementary divisors. The Fundamental Theorem can also be proved by direct handling of the prime power factors obtained in Exer. 11. However, every such proof amounts in principle to the application of the inferences in Section 1, Exer. 38, therefore of the principal conclusion of the theory of elementary divisors.

At any rate the prime numbers p actually occurring and the product of all prime powers in a prime number p are uniquely determined [Exer. 9, (b)]. The individual prime powers can be characterized invariantly by the number of solutions of the equations $X^{p^k} \equiv E$ in $\mathfrak{G}$.

17. Generalize the proof of the Fundamental Theorem of Finite Abelian Groups obtained in Exer. 12 to 16 to Abelian groups with *finitely many generators*, which can be represented, therefore, as the composite of the periods of finitely many of its elements. In this case cycles of infinite order may appear in the direct product, corresponding to the $e_k = 0$ in the matrix B of Exer. 13.

Everything follows as before once Exer. 12 is generalized. Consider first of all the denominators appearing in the coefficients of the linear combination of all exponent rows α of a maximal system of exponent rows α_i linearly independent over the rational numbers. By means of Vol. 1, Theorem 75 [148], 83 [160], we see that these denominators (with respect to a suitable choice of these coefficients among *all* solutions of the nonhomogeneous system of linear equations in question) have a fixed least common denominator g , namely, a certain minor of the matrix of the α_i . Then augment the maximal system α , by those finitely many exponent rows which arise by reducing the numerators of the coefficients to a fixed residue system mod g .

18. How many types of Abelian groups are there of orders p^n (p a prime number), $n = p_1^{n_1} \cdots p_r^{n_r}$ ($p_1, \dots, p_r$ different prime numbers)?

By Exer. 15, 16 we know that two Abelian groups are isomorphic if and only if they have the same prime power invariants. Moreover, for any arbitrary list of prime power invariants there exists an Abelian group (abstract construction of the direct product by the scheme of the existence proofs in Vol. 1, Sections 3, 4).—The result for p^n is s_p , which is the number of decompositions of n into positive integral summands without regard to their arrangement; for n it is the product of the $s_{p_i^{n_i}}$.

19. What are the prime power invariants of the additive group of the residue class ring $\text{mod } f(x)$, where $f(x)$ is a polynomial of degree n over the residue class field P_p ?

Apply Theorem 27 [192]. [Concrete construction of Abelian groups of type $(p, \dots, p)$.]

20. In connection with Exer. 16 prove: An Abelian group $\mathcal{G}$ of order n is cyclic if and only if for every prime divisor p of n the equation $X^p \doteq E$ has exactly p solutions in $\mathcal{G}$.

4. Prime Integral Domains. Prime Fields. Characteristic

1. Let B be a ring with unity element e (not necessarily an integral domain—proper zero divisors may, therefore, occur). Prove: The integral multiples of e form a subring B_0 of B which is isomorphic to the residue class ring Γ_f relative to an integer $f \geq 0$ determined uniquely by B . B_0 is the smallest subring (intersection of all such) of B (f is the *characteristic* of B ; B_0 the *prime ring* of B).

The proofs of Theorems 38 to 40 immediately carry over to the case of a ring with unity element.

2. Also carry Theorem 42 over to this case.

Naturally, only subrings with unity elements are to be drawn into consideration.

3. Let I be either the integral domain $\Gamma[x_1, \dots, x_n]$ or $K[x_1, \dots, x_n]$ with unique prime factorization (Section 2, Exer. 27), and p a prime element of I . Then the residue class ring I_p of I relative to p is, at any rate, an integral domain (for $n \geq 1$ it need not be a field). What possibilities exist for the characteristic of I_p ?

For $K[x, x_1, \dots, x_n]$ the characteristic of $\mathbb{I}$, is always equal to the characteristic of K . For $\Gamma[x_1, \dots, x_n]$ the characteristic of $\mathbb{I}$ is 0. We then have to distinguish whether the prime element p already belongs to Γ (is an ordinary prime number) or not.

4. Prove the following generalization to Theorem 44: In domains of characteristic p the rule

$$\left(\sum_{k=1}^n a_k\right)^{p^\mu} = \sum_{k=1}^n a_k^{p^\mu}$$

is valid for every natural number μ .—Carry out the proof:

(a) by mathematical induction on μ ; (b) by direct demonstration of the divisibility of the binomial coefficients

$$\binom{p^\mu}{\nu} \quad (\nu = 1, \dots, p^\mu - 1) \text{ by } p.$$

For the latter proof take into consideration the formula

$$\binom{p^\mu}{\nu} = \frac{p^\mu}{\nu} \binom{p^\mu - 1}{\nu - 1}.$$

5. Similarly, prove in general the validity of the congruence

$$\binom{m}{n} \equiv 0 \pmod{p^{\max(0, \mu - \nu)}},$$

where p^μ and p^ν are the highest powers of the prime number p dividing m and n without remainder.

6. Show that in domains of characteristic p Theorem 44 yields the following formula for the p -th power of a difference $a_1 - a_2$:

$$(a_1 - a_2)^p = (a_1 + (-a_2))^p = a_1^p + (-1)^p a_2^p.$$

Show that in the case $p = 2$ this agrees with the rule

$$(a_1 - a_2)^p = a_1^p - a_2^p$$

proved in general in connection with Theorem 44.

7. Prove: If a is an element of a field K of prime characteristic p , then the equation $x^{p^\mu} = a$ has at most *one* solution in K ; if it exists, the solution can be *uniquely* designated by $\sqrt[p^\mu]{a}$.

Take the two solutions a_1, a_2 and apply Exer. 4 to their difference.

8. Prove that in the prime field P_p every element a has a p^μ -th root for any natural number μ . What is it?

Apply Theorem 29 [194].

9. Prove that in the field $P_p(x)$ the element x has no p -th root.

This follows from Section 1, Exer. 32.

10. Prove: If the p^μ -th roots of the elements $a_1, \dots, a_n$ exist in a field K of prime characteristic p , then the p^μ -th root of $\sum_{k=1}^n a_k$ also exists and

$$\sqrt[p^\mu]{\sum_{k=1}^n a_k} = \sum_{k=1}^n \sqrt[p^\mu]{a_k}$$

is valid.

This can be thought of as the generalization of the rule in Exer. 4 to negative μ . It is easily established by applying that rule to the right side of the given formula.

11. In addition to the generally valid proof, a second proof for Vol. 1, Theorem 70 [141] by means of the Laplace Expansion Theorem was given which applies only to fields with characteristic different from 2. However, the idea of this proof can also be used, according to *Rychlik*, for fields K of characteristic 2 if we take the following roundabout course: Consider an n -rowed square matrix $X = (x_{ik})$ of $n^2 - n$ indeterminates x_{ik} over Γ in which two rows are set with

the same indeterminates ($x_{i,k} = x_{i,k}$ for $k = 1, \dots, n$); go from the integral domain $\Gamma[x_{11}, \dots, x_{nn}]$ to the integral domain $P_2[x_{11}, \dots, x_{nn}]$ of residue classes relative to the prime element 2 (cf. the explanation to Section 2, Exer. 23); interpret this as a subdomain of the integral domain $K[x_{11}, \dots, x_{nn}]$ and in the latter go over by the principle of substitution to a matrix A over K .—(Carry out the details of this train of thought.

The salient point is the validity of the statement in the integral domain $\Gamma[x_{11}, \dots, x_{nn}]$ of characteristic 0, and the fact that $P_2[x_{11}, \dots, x_{nn}]$ can be represented from this point of view as an integral domain of residue classes, where naturally to the zero of $\Gamma[x_{11}, \dots, x_{nn}]$ there corresponds the null residue class, therefore the zero of $P_2[x_{11}, \dots, x_{nn}]$.

12. In connection with Vol. 1, Section 19, Exer. 5, prove by the same scheme: If A is a skew-symmetric matrix with an odd number of rows n over a field K of characteristic 2 for which all main diagonal terms are $a_{ii} = 0$, then $|A| = 0$. Show by a counterexample that the assumption regarding the main diagonal terms a_{ii} is essential.

For the latter $n = 1$ is certainly sufficient.

13. In connection with Vol. 1, Section 21, Exer. 6, prove: If $X = (x_{ik})$ is a skew-symmetric matrix with an even number of rows n over a field K of characteristic 2 for which all the main diagonal terms are equal, therefore

$$x_{ii} = x, \quad x_{ik} = -x_{ki} = x_{ki} \quad (i > k),$$

then we again have $|X| = f^2$, where f is an integral rational function of the x_{ik} over K .—Show by a counterexample that the assumption regarding the main diagonal terms x_{ii} is essential.

Apply Vol. 1, Section 19, Exer. 6 to the decomposition $X = xE_n + X_0$ and for the principal minors of X_0 take into account Vol. 1, Section 19,

Exer. 5, and Vol. 1, Section 21, Exer. 6. The statement then follows from Theorem 44. For a counterexample it is certainly enough to take $n = 2$.

14. Let e be the unity element of the prime field P_p , so that it consists of the p elements ke ($k = 0, 1, \dots, p-1$). Then a permutation $Q = \begin{pmatrix} k \\ q_k \end{pmatrix}$ of the p numerals k can also be interpreted as a permutation of the p elements ke of P_p and can accordingly be represented in the form $Q = \begin{pmatrix} ke \\ q_{ke} \end{pmatrix}$. In particular, the p -termed cycle $P = (0 \ 1 \ \dots \ p-1) = \begin{pmatrix} 0 & 1 & \dots & p-1 \\ 1 & 2 & \dots & 0 \end{pmatrix}$ has thus the simple representation $P = \begin{pmatrix} ke \\ (k+1)e \end{pmatrix}$.—Prove the statements:

(a) P commutes with Q if and only if $Q = P^\nu$ is a power of P .

(b) If P does *not* commute with Q , then the p permutations $P^{-\nu}QP^\nu$ ($\nu = 0, 1, \dots, p-1$) are all different from one another.

For (a). Compute $P^{-1}QP$ and interpret the condition $P^{-1}QP = Q$ by applying the representation forms specified for P and Q .

For (b). The elements of the period $\mathfrak{P}$ of P commuting with Q form a subgroup of the group $\mathfrak{P}$, and $\mathfrak{P}$ has the prime order p .

15. Starting from the defining formula (Vol. 1, Def. 38 [127]), evaluate the determinant of the matrix

$$A = \begin{pmatrix} a_0 & a_1 & \dots & a_{p-1} \\ a_{p-1} & a_0 & \dots & a_1 \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_{p-1} & \dots & a_0 \end{pmatrix}$$

or by applying the 'indexing mod p ' introduced in Exer. 14, briefly

$$A = (a_{(k-i)e}) \quad (i, k = 0, 1, \dots, p-1)$$

(p -rowed *circulant*), where the a_i are elements of a field K of prime characteristic p .¹

The cited formula for defining determinants yields:

$$|A| = \sum_Q \text{sgn } Q a_{(a_0-0)e} \cdots a_{(a_{p-1}-(p-1))e}$$

extending over all p -termed permutations

$$Q = \begin{pmatrix} ke \\ q_k e \end{pmatrix} \quad (k = 0, 1, \dots, p-1).$$

In this, always collect all terms whose Q are connected through transformation with powers of the cycle $P = \begin{pmatrix} ke \\ (k+1)e \end{pmatrix}$, and apply Theorem 14 as well as afterwards Theorem 44.

16. Without this effort, prove at any rate the partial result following from this: The determinant of a p -rowed circulant in p indeterminates x_i over a field of prime characteristic p is divisible by $x_0 + \cdots + x_{p-1}$.

Apply Vol. 1, Theorem 71, Corollary [143].—This proof, and consequently the given statement, is independent of the assumption regarding the characteristic of K as well as, generally, of the prime property of the number of rows p .

¹ For characteristic different from p and for an arbitrary number of rows n , see Exer. 19, 20 to Section 10, given later, as well as Exer. 16 to Section 20.

Vol. 2. Chapter II. The Roots of Algebraic Equations

5. Roots and Linear Factors

1. Prove that the polynomial $x^p - x$ can be decomposed into p linear factors in any field of characteristic p . What is the factorization?

Apply Theorem 48 and Theorem 29 [194].

2. Prove the congruence $(p-1)! \equiv -1 \pmod{p}$ for any prime number p (*Wilson's Theorem*).

Apply Exer. 1.

3. Let p be a prime number and d a divisor of $p-1$. How many roots does the polynomial $x^d - e$ have in a field of characteristic p ?

Note that $x^d - e \mid x^{p-1} - e$ and apply Exer. 1, the uniqueness of the prime factorization and Theorem 51.

4. At most how many of these roots—considered as elements of the multiplicative group of the prime field $\mathbb{P}_p$ —have exactly the order d ?

Distinguish the two cases (a) in which there are none at all, (b) in which there is at least one such element. For the latter apply Theorem 37 [200].

5. Deduce from this by means of Section 2, Exer. 19, that the possibility (a) holds for *none* of the divisors d of $p-1$.

For this purpose enumerate, just as in Section 2, Exer. 19, all $p-1$ non-zero elements of $\mathbb{P}_p$ after they have been arranged according to their orders in the multiplicative group.

6. What does this imply regarding the type of the multiplicative group of $\mathbb{P}_p$, namely, of the group $\mathbb{P}_p$ of the prime residue classes mod p ?¹

In Exer. 5 take the special value $d = p - 1$.

7. A shorter derivation of this result can be obtained directly from Exer. 3 by using Section 3, Exer. 20.

8. By a counterexample show that Theorem 48 is no longer universally valid if rings are taken as a basis instead of fields.

It is enough to take a ring $\mathbf{B}$ which has proper zero divisors, say, the residue class ring Γ_f relative to a natural number f different from 0, 1 and prime numbers (Theorem 28 [193]). If a and b are two different complementary proper zero divisors of $\mathbf{B}$, then a polynomial of degree 2 is easily found with the three distinct roots $a, b, 0$ in $\mathbf{B}$.—What is the only natural number f with the specified properties for which this is not possible?

9. Let $\mathbf{M}$ be the non-commutative ring of all n -rowed square matrices over $\mathbf{K}$ (Vol. 1, Section 10, Exer. 4, 5). This ring contains a subfield isomorphic to $\mathbf{K}$ consisting of the diagonal matrices aE . Let $\mathbf{M}[x]$ be the non-commutative ring of all n -rowed square matrices over $\mathbf{K}[x]$. This ring contains an integral subdomain isomorphic to $\mathbf{K}[x]$ consisting of the diagonal matrices $f(x)E$. Prove that the characteristic polynomial $f(x) \equiv |xE - A|$ of A , or rather the polynomial $f(x)E$ in $\mathbf{M}[x]$ associated isomorphically to it, has the characteristic matrix $x E - A$ of A as a linear factor.

Apply Vol. 1, Section 19, Exer. 12 with $\nu = 1$ to the characteristic matrix of A .

¹ Also compare this elementary proof with the one obtained later in the proof to Theorem 122 [307] in the abstract theory of fields, as well as with that obtained in Exer. 7 based on the Fundamental Theorem for finite Abelian groups.

10. We have just obtained a relation of the form $f(x)E \equiv (xE - A)F(x)$, where $F(x)$ is a matrix in $M[x]$. Starting with this, prove that the characteristic polynomial $f(x) \equiv |xE - A|$ of A , or rather the polynomial $f(x)E$ in $M[x]$, associated isomorphically to it, has the matrix A as a root. Namely, prove that $f(A) = 0$, if we agree to substitute $x^0 = A^0 = E$ formally in the term without x when carrying out the substitution $x = A$ in $f(x)$.

Since we are dealing with a non-commutative ring, the substitution $x = A$ cannot be made *haphazardly*. On the contrary, this substitution must be *justified*. For this purpose apply Section 1, Exer. 44.

11. Sharpen Theorem 49 by showing that the property in question is possessed by even infinitely many systems of elements in the set, no two of which having an element in common.

Apply Theorem 49 to the set M which is generated by the omission of $a_1, \dots, a_n$ from M , etc. This set is also infinite.

12. Let A and B be two n -rowed square matrices over an infinite field K and assume that these matrices are similar in an extension field Λ of K (Vol. 1, Section 21, Exer. 18). This means that there exists an n -rowed square regular matrix Π in Λ such that $\Pi^{-1}A\Pi = B$. Prove that A and B are also similar in K .—For this purpose the similarity transformation between A and B in the form $A\Pi - \Pi B = 0$ can be interpreted as a linear homogeneous system of equations for the coefficients of Π , which satisfies the additional condition $|\Pi| \neq 0$. From this point of view the statement will follow by proving that there also exists a solution P in K which satisfies the additional condition $|P| \neq 0$.

The proof rests, on the one hand, on Vol. 1, Theorem 84 [241], on the other hand—in order to be able to handle the additional condition—on Theorem 49. Take as the indeterminates playing a part in

Theorem 49 the freely disposable elements in the general solution of the system of linear equations.

13. Let the polynomial $f(x) \equiv x^n + a_1 x^{n-1} + \dots + a_n$ over K resolve into linear factors in the extension field Λ of K :

$$f(x) \equiv (x - \alpha_1) \dots (x - \alpha_n).$$

Find formulae expressing the coefficients $a_1, \dots, a_n$ in terms of the roots $\alpha_1, \dots, \alpha_n$ (*Vieta's formulae*).

14. For a polynomial $f(x)$ of degree n what is the degree of the polynomial which is the associate of $(c + dx)^n f\left(\frac{a + bx}{c + dx}\right)$ ($ad - bc \neq 0$), and what are its roots under the assumption of Exer. 13?

Do not miss a point of the Exercise by assuming without justification that the literal expressions which may occur are different from zero.

15. Find a linear fractional substitution¹

$$x \rightarrow \frac{a + bx}{c + dx} \quad (ad - bc \neq 0)$$

in the field K which changes (in the sense of Exer. 14) $f(x)$ into a polynomial in which (a) the term with x^{n-1} is lacking (b) the term with x is lacking. Is this always possible?

The cases $a_1 = 0$ and $a_{n-1} = 0$ are very quickly settled. If the characteristic of K is a prime number not dividing n without remainder it suffices to use a substitution of the form $x \rightarrow x - a$ in the case of (a), and $x \rightarrow \frac{1}{x} - a$ in the case of (b). In the other cases it is possible if and only if there exists in K a root b of $f'(x)$ different from the roots α_i of $f(x)$. In this event use for (a) the substitution $x \rightarrow \frac{1}{x} + b$ and for (b) $x \rightarrow x + b$. In the case (b) $a_n \neq 0$ is also required.

¹The linear integral substitutions are special cases of these ($d = 0$ and then without loss of generality $c = e$).

16. Prove: If the polynomial $f(x)$ with integral rational coefficients has a rational root α , then α is even integral.

Set up α in the reduced quotient representation, remove the denominator and apply Theorem 23 [187].

17. Generalize this result to the case where the coefficients are in $\Gamma[x_1, \dots, x_n]$ and $K[x_1, \dots, x_n]$ instead of the integral domain Γ , and a root α in the quotient field.

The fundamental theorem of the unique prime factorization is also valid in this generalization (Section 2, Exer. 27), therefore so is Theorem 23 [187].

18. Prove: A polynomial with integral rational numerical coefficients in which a_n (the term free of x) is a prime number has at most three different rational roots.

Combine Exer. 13 and Exer. 16.

19. What can be said about the denominator of a rational root of a polynomial $f(x)$ with rational coefficients?

By a suitable linear substitution $x \rightarrow ax$ take $f(x)$ into a polynomial with integral coefficients.

20. What are the rational roots of the polynomial

$$x^6 + \frac{49}{30}x^5 + \frac{17}{15}x^4 + \frac{1}{30}x^3 - \frac{17}{30}x^2 - \frac{1}{15}x + \frac{1}{30}?$$

6. Multiple Roots, Derivative

1. Prove the validity of the so-called *chain rule* of analysis:

$$f(g(x))' \equiv f'(g(x))g'(x)$$

for integral rational functions over a field K .

The proof follows formally from (1) and (2) by taking the representation

$$f(g(x)) \equiv a_0 + a_1g(x) + \dots + a_ng(x)^n$$

as a starting point.

2. Develop the theory of the derivative also for the fractional rational function $\phi(x)$ over K , that is, in the field $K(x)$. For this purpose start from the reduced quotient representation $\phi = \frac{f}{g}$, define $\phi' = \frac{f'g - fg'}{g^2}$ and prove the rules

$$(a) \quad (\phi \pm \psi)' = \phi' \pm \psi',$$

$$(b) \quad (\phi\psi)' = \phi'\psi + \phi\psi',$$

$$(c) \quad \left(\frac{\phi}{\psi}\right)' = \frac{\phi'\psi - \phi\psi'}{\psi^2},$$

$$(d) \quad \phi(\psi(x))' \equiv \phi'(\psi(x))\psi'(x).$$

Show that Theorem 55 is also valid for the above definition of ϕ' .

As a convenient tool for these proofs, first deduce the independence of this definition of the derivative from the reduced form of the quotient representation of ϕ . Then (a) to (d) follow by easy calculations from (1), (2) and Exer. 1. In particular, for (d) multiply first the numerator and denominator of ϕ by a suitable power of the denominator of ψ .

3. Prove the rule

$$\frac{(\phi_1 \dots \phi_n)'}{\phi_1 \dots \phi_n} = \frac{\phi_1'}{\phi_1} + \dots + \frac{\phi_n'}{\phi_n}$$

for the derivative of a product of n factors (*logarithmic differentiation*).

Apply mathematical induction on n .

4. The theory of the (first) derivative $\phi'(x)$ in $K(x)$ also implies the theory of *higher derivatives* $\phi''(x) \equiv (\phi'(x))'$, ... and also the theory of *partial derivatives* in $K(x_1, \dots, x_n)$: $\phi_{x_i}(x_1, \dots, x_n)$ is generated by forming the derivative of $\phi(x_1, \dots, x_n)$ as an element of $K_i(x_i)$, where $K_i = K(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$;

$\phi_{x_i x_k}(x_1, \dots, x_n) \equiv \phi_{x_k x_i}(x_1, \dots, x_n)$.—Prove the additional rule that the order of differentiation is interchangeable:

$$\phi_{x_i x_k} = \phi_{x_k x_i}.$$

Reduce this by means of the formal differentiation rules at our disposal to the simple cases $\phi(x_1, \dots, x_n) \equiv a$ or $\equiv x_i$.

5. For an integral rational function $f(x)$ of degree n over a field of characteristic 0 (or also of prime characteristic $> n$) prove the *Taylor Formula*:

$$f(x) \equiv f(\alpha) + \frac{f'(\alpha)}{1!} (x - \alpha) + \dots + \frac{f^{(n)}(\alpha)}{n!} (x - \alpha)^n.$$

By means of rule (1) reduce this to the simple case $f(x) \equiv x^k$. Here it is to be seen from the well-known expansion of $x^k \equiv (\alpha + (x - \alpha))^k$ according to the binomial theorem.

6. Under the same assumptions, prove: If α is a ν -fold root of $f(x)$, then

$$f(\alpha) = \dots = f^{(\nu-1)}(\alpha) = 0, \quad f^{(\nu)}(\alpha) \neq 0$$

and conversely. In this case α is a $(\nu - \rho)$ -fold root of $f^{(\rho)}(x)$ ($0 \leq \rho \leq \nu$).

7. Prove that in a field K of prime characteristic $\leq n$ the first $\nu - 1$ derivatives of $f(x)$ are also zero for a ν -fold root α of $f(x)$.

This follows directly by differentiating the relation $f(x) \equiv (x - \alpha)^\nu \phi(x)$ $(\nu - 1)$ times.

8. How must the Taylor formula (Exer. 5) be written if it is to be valid without the restriction regarding the characteristic of K ?

Instead of the derivatives $f^{(\nu)}(x)$ of $f(x) \equiv \sum_{k=1}^n a_k x^k$ introduce the expressions

$$f_\nu(x) \equiv \sum_{k=1}^n \binom{k}{\nu} a_k x^{k-\nu}$$

identical with $\frac{1}{\nu!}f^{(\nu)}(x)$ on restricting the characteristic, and by means of the binomial theorem confirm the validity of the formula thus generated. Just as in Section 4, Exer. 11, 12 we can again go from the characteristic 0 to a prime characteristic.

9. Let f be a polynomial of n -th degree over a field K of characteristic 0 (or of prime characteristic $> n$), and let f be resolved into linear factors over the extension field Λ of K . Describe the decomposition into linear factors of the divisors

$$d_\nu = (f, f', \dots, f^{(\nu)}) \quad (\nu = 1, \dots, n-1)$$

of f . Show that the same simple result is not yet valid for $d_\nu = (f, f^{(\nu)})$ ($\nu \geq 2$).

Exer. 6 can be used to specify the power to which any linear factor $x - \alpha$ of f occurs in d_ν . For this purpose consider, in particular, Theorem 24 [188]. In order to establish the last statement study the function $f(x) \equiv x^3 - x$ over P and note what happens to the three linear factors in f, f' and f'' .

10. Under the same assumptions, let ϕ_ν be the product of the different linear factors among the (exactly) ν -fold linear factors of f [$\phi_\nu = e$ in case no ν -fold linear factors exist]. We then have

$$f = \phi_1 \phi_2^2 \cdots \phi_n^n.$$

The ϕ_ν are, at any rate, polynomials over Λ . Prove that they are actually polynomials over K .

They can be represented simply by the d_ν of Exer. 9.

11. Under the same assumptions prove that the product ϕ of the different linear factors among the totality of linear factors of f is a polynomial over K .

ϕ can be represented simply by the ϕ_ν of Exer. 10 and consequently also by the d_ν of Exer. 9. Find especially the latter representation.

12. What is the product of the different linear factors of the polynomials

$$\begin{aligned} & x^7 - 4x^5 + 3x^4 + 4x^3 - 12x^2 + 12 \text{ in } \mathbf{P}, \\ & x^{11} + 11x^{10} + 2x^9 + 10x^8 + 2x^7 + 2x^4 + 10x^3 \\ & + 2x^2 + 11x + 1 \text{ in } \mathbf{P}_{13}, \end{aligned}$$

and what is the factorization according to Exer. 10?

13. Let $f(x) \equiv x^n + a_1 x^{n-1} + \cdots + a_n$ be a polynomial of n -th degree over an *arbitrary* field $\mathbf{K}$. If this polynomial resolves into linear factors in an extension field Λ of $\mathbf{K}$:

$$f(x) \equiv (x - \alpha_1) \cdots (x - \alpha_n),$$

prove the formula
$$\sum_{i=1}^n \frac{f'(x)}{x - \alpha_i} \equiv f'(x).$$

Apply logarithmic differentiation (Exer. 3).

14. According to Theorem 47 [207] $x - \alpha \mid f(x) - f(\alpha)$ is always valid. Find the normal representation of this quotient

- (a) as an integral rational function of $x - \alpha$,
- (b) as an integral rational function of x .

For (a) apply Exer. 5 or 8; for (b) introduce the functions

$$g_\nu(x) \equiv x^\nu + a_1 x^{\nu-1} + \cdots + a_\nu \quad (\nu = 0, \dots, n-1).$$

15. Under the assumptions of Exer. 13, compute $f'(x)$ in another way by means of the formula found in Exer. 13, 14 (b), namely,

$$f'(x) \equiv \sum_{i=1}^n (x^{n-1} + g_1(\alpha_i) x^{n-2} + \cdots + g_{n-1}(\alpha_i)),$$

and derive from this a system of $n-1$ formulas for the so-called *power sums*

$$s_\nu = \sum_{i=1}^n \alpha_i^\nu \quad (\nu = 1, \dots, n-1)$$

of the roots α_i of $f(x)$ (*Newton's formulas*).

16. Newton's formulas enable us, by recursively solving for the s_v , to represent these power sums as integral rational functions of the coefficients a_v with integral coefficients (or more correctly with coefficients in the prime integral domain Γ or P_p of K). Besides $s_0 = n, s_1, \dots, s_{n-1}$ we now also have the power sums $s_n, s_{n+1}, \dots$, and in case $a_n \neq 0$, that is, all $\alpha_i \neq 0$, also the power sums $s_{-1}, s_{-2}, \dots$. The system of Newton's formulas can be extended on both sides to a system of formulas making it possible to express *all* s_v (recursively) in terms of the a_v with integral coefficients.

Take into consideration the relations $\alpha_i^v f(\alpha_i) = 0$ for arbitrary $v \geq 0$, and in case $\alpha_i \neq 0$, even for arbitrary integers v .

17. Find the power sums for the polynomials

(a) $x^2 - a$,

(b) $x^{n-1} + x^{n-2} + \dots + x + e$

over an arbitrary ground field K .¹

In the case (a) we have to distinguish whether K has characteristic 2 or not; in the case (b) whether the characteristic of K divides n without remainder or not. In the case (b) we can proceed either directly or—more simply—by using the fact that the power sums of $x^n - e \equiv (x - e)(x^{n-1} + x^{n-2} + \dots + x + e)$ are generated by the addition of e to the desired power sums.

18. Let the polynomial $f(x)$ over K resolve into linear factors in an extension field Λ of K :

$$f(x) \equiv (x - \alpha_1) \cdots (x - \alpha_n).$$

How can the difference product

$$d = \prod_{i < k} (\alpha_i - \alpha_k)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq k} (\alpha_i - \alpha_k)$$

¹ Regarding the assumption that the polynomials can be resolved into linear factors in an extension field Λ of K , see Theorem 87 [242], given later.

of the roots of $f(x)$ [*discriminant of $f(x)$*] be represented (a) by a determinant, (b) by the derivative $f'(x)$?

For (a) take note of Vol. 1, Section 19, Exer. 4; for (b), Exer. 13.

19. From the representation of the discriminant d of $f(x)$ as the square of a determinant [Exer. 18, (a)] derive a representation in terms of power sums of the roots of $f(x)$. Consequently, to which field does d belong? Explicitly use this to compute the discriminants of the polynomials $x^2 + a_1x + a_2$ and $x^3 + px + q$ over P .

Apply the formula for multiplying determinants (Vol. 1, Section 19, Exer. 7, 8) in a suitable way, and then Newton's formulas (Exer. 15, 16).

20. Let n different elements $a_1, \dots, a_n$ and n further elements $b_1, \dots, b_n$ be given in K . Prove: There is one and only one integral rational function $g(x)$ of the $(n-1)$ -th degree at most over K , for which $g(a_i) = b_i$ ($i = 1, \dots, n$) (*interpolation of $g(x)$ from the values b_i at the points a_i*).

The conditions imply a system of n linear nonhomogeneous equations for the unknown coefficients of $g(x)$ whose determinant is known by Vol. 1, Section 19, Exer. 4.

21. Generalize the formula of Exer. 13 by proving the formula

$$g(x) \equiv \sum_{i=1}^n \frac{g(\alpha_i)}{f'(\alpha_i)} \frac{f(x)}{x - \alpha_i}$$

(*Lagrange interpolation formula*) under the assumptions: $f(x)$ is a polynomial of n -th degree over K which resolves in an extension field Λ of K into n different linear factors $x - \alpha_i$, and $g(x)$ is an integral rational function of the $(n-1)$ -th degree at most over K .

By means of Exer. 13 establish that the right side of the given formula can be interpreted as the solution of an interpolation problem of the type considered in Exer. 20.

22. Find an integral rational function over $\mathbf{P}$ of third degree at most which has at the points 1, 2, 3, 4 the values -3, 7, 35, 125 (a) by the methods of Exer. 20, (b) by the methods of Exer. 22.

23. For the matrix $X \equiv (x_{ik})$ of n^2 indeterminates x_{ik} over $\mathbf{K}$ prove the partial differentiation formulas

$$|X|_{x_{ik}} \equiv \xi_{ik} \text{ (cofactor of } x_{ik} \text{ in } X).$$

This follows from the Laplace Expansion of $|X|$ by the i -th row or k -th column.

24. Generalize these formulas to

$$|X|_{x_{i_1 k_1} \dots x_{i_\nu k_\nu}} \equiv \operatorname{sgn} \{i_1, \dots, i_\nu\} \operatorname{sgn} \{k_1, \dots, k_\nu\} \cdot \xi_{\{i_1, \dots, i_\nu\}, \{k_1, \dots, k_\nu\}}$$

for any two combinations $\{i_1, \dots, i_\nu\}$ and $\{k_1, \dots, k_\nu\}$, which are not necessarily arranged in natural order.

This follows, as above, from the Laplace Expansion of $|X|$ by the row combination $\{i_1, \dots, i_\nu\}$ or the column combination $\{k_1, \dots, k_\nu\}$.

25. The proof of Theorem 44 [204] makes use of the binomial theorem and the explicit formula for the binomial coefficients. In domains of characteristic p prove the rule $(a+b)^p = a^p + b^p$ on the basis of Theorem 57 by considering the integral rational function $f(x) \equiv (a+bx)^p - a^p - b^p x^p$.

The $f_0(x)$ belonging to $f(x)$ in the sense of Theorem 57 with $f(x) \equiv f_0(x^p)$ must have the degree 0. Therefore, the substitution $x=0$ determines it completely, and the substitution $x=e$ yields the formula to be proved.

26. Prove: Over a perfect field $\mathbf{K}$ the integral rational functions f with $f' = 0$ are identical with the p -th powers of the integral rational functions over $\mathbf{K}$.

This immediately follows from Theorem 57 and Theorem 44 [204].

27. Prove: In a perfect field every irreducible polynomial is separable.

Note that f_0^p is not irreducible [and apply Theorem 57 and Def. 17].

28. What are the integral rational functions f over a field K of prime characteristic p for which $f'' = 0$?

On the basis of Theorem 57 it is necessary and sufficient that $f(x)$ have the form $f_0(x^p) + xg_0(x^p)$.

29. What are the rational functions ϕ over a field K of prime characteristic p for which $\phi' = 0$?

Start with the reduced quotient representation $\phi = \frac{f}{g}$ and note that $g \mid g'$ takes place only for $g' = 0$.

30. What are the integral rational functions $f(x_1, \dots, x_n)$ over a field K of prime characteristic p for which $f_{x_1} = 0, \dots, f_{x_n} = 0$ simultaneously?

This immediately follows from Theorem 57.

31. Let A be an n -rowed square matrix over K . Prove: If A has the rank ρ , then the characteristic polynomial $f(x) \equiv |xE - A|$ of A has 0 as a $(n - \rho)$ -fold root at least; in particular, for $\rho = n$ its multiplicity is exactly $n - \rho = 0$.

Apply Vol. 1, Section 19, Exer. 6.

32. Give examples to show that the multiplicity ν of the root 0 in Exer. 31 can have any of the values $n - \rho, \dots, n$ for $0 \leq \rho \leq n - 1$.

It is sufficient to construct for any $\nu = 1, \dots, n$ and any $\rho = n - \nu, \dots, n - 1$ a matrix A of rank ρ with

$$f(x) \equiv |xE - A| \equiv x^\nu(x - c)^{n-\nu}.$$

Assume that such a matrix has the form $A = \begin{pmatrix} A_\nu & 0 \\ 0 & E_{n-\nu} \end{pmatrix}$. The specified form of $f(x)$ is attained through zeros on and beneath the main

diagonal of A_ν ; the rank ρ of A [therefore $\rho = (n - \nu)$ for A_ν], by suitably distributing ones above the main diagonal of A_ν .¹

33. The multiplicity with which 0 is a root of the characteristic polynomial $f(x)$ of A is the highest exponent to which the prime function x divides $f(x)$ without remainder. Describe this multiplicity in terms of the corresponding multiplicities for the determinantal divisors $d_\nu(x)$ and elementary divisors $e_\nu(x)$ of the characteristic matrix $xE - A$ of A (Section 1, Exer. 37). What limits exist for these multiplicities?

For this purpose note (a) that $f = d_n = e_1 \cdots e_n$, (b) that d_ν has the degree ν at most, and (c) that $e_1 \mid \cdots \mid e_n$.

34. Use this to obtain another proof for the theorem in Exer. 31.

Note that the determinantal divisors $d_\nu(x)$ with $\nu > \rho$ have the root 0 if A has rank ρ .

¹ For this purpose see also Exer. 8, 9 to Section 10, given later.

Vol. 2. Chapter III. The Fields of the Roots of Algebraic Equations

7. General Theory of Extensions (1). Basic Concepts and Facts

1. Show that the domains $\Gamma[\sqrt{a}]$ and $P(\sqrt{a})$ considered in Vol. 1, Section 2, Exer. 5, and the domains $\mathbb{I}[f_0(x)]$ and $K(\phi_0(x))$ considered in Vol. 1, Section 4, Exer. 2, 4 are generated by adjunction in the sense of Def. 18. In this, what integral domain or field plays the role of the auxiliary domain Λ of Def. 18?

Each of the first cases involves an integral domain adjunction starting from an *integral domain*, which is a more general process than in Def. 18.

2. What simultaneous adjunction will generate the composite of $P(\sqrt{a})$ and $P(\sqrt{a'})$ considered in Vol. 1, Section 2, Exer. 8?

Note the remark after Theorem 62.

3. Prove in general: $K(M)$ is the composite of the totality of fields $K(\alpha)$, where α runs through all elements of M .

4. Let K_0 be an arbitrary field, $f_0(x_0)$ an integral rational function of x_0 over K_0 , $K = K_0(f_0(x_0))$ (Vol. 1, Section 4, Exer. 4) and $\Lambda = K_0(x_0)$. Is the element x_0 of Λ algebraic or transcendental over K ?

We must distinguish whether $f_0(x_0)$ has degree 0 or a positive degree. In the latter case x_0 is a root of $f_0(x) - f_0(x_0)$.

5. Similarly, let $K = K_0(\phi_0(x_0))$, where $\phi_0(x_0)$ is an arbitrary rational function of x_0 over K_0 and again $\Lambda = K_0(x_0)$. Is the element x_0 of Λ algebraic or transcendental over K ?

We must again distinguish whether $\phi_0(x_0)$ has degree 0 or a positive degree (Section 1, Exer. 29).

6. Let a be a rational number $\neq 0$ and $\sqrt[3]{a}$ one of the three cube roots of a . This cube root belongs to the field of all complex numbers and may be (a) real, (b) one of two complex roots. What is the irreducible polynomial in P belonging to $\sqrt[3]{a}$?

If a is a third power of a rational number, we must distinguish between the cases (a) and (b). Then take into consideration the irreducibility of $x^3 + x + 1$ in P (Section 1, Exer. 11).

7. Let P_4 be the field of four elements (Vol. 1, Section 1, Exer. 8). Prove: P_4 is simple algebraic over the prime field P_2 and is generated from P_2 by adjunction of an algebraic element of degree 2.—Can P_4 be represented in the form $P_2(\sqrt{a})$ with a in P_2 ? Is P_4 separable over P_2 ? What is the degree of P_4 over P_2 ?

Take into consideration Section 2, Exer. 21 and Section 4, Exer. 8, as well as Theorems 67, 69.

8. Prove that the field Λ of all complex numbers is simple algebraic of degree 2 over the field K of all real numbers. What are the primitive elements of Λ over K ?

First establish that $[\Lambda : K] = 2$ (Def. 25), and then again apply Theorems 67, 69.

9. Let a be a rational number which is not the square of a rational number. What is the degree of the field $P(\sqrt{a})$ over P ? What numbers of $P(\sqrt{a})$ are primitive elements of

$P(\sqrt{a})$? Which of these are roots of *pure* equations of second degree (without term in x)? Therefore, for which rational numbers a' alone is $P(\sqrt{a'}) = P(\sqrt{a})$? Are there always integers among these?

Use the representation of the numbers of $P(\sqrt{a})$ obtained in Vol. 1, Section 2, Exer. 5, and show its uniqueness. Then everything easily follows.

10. Let a and a' be rational numbers which are neither rational squares themselves nor differ by a rational square factor. What is the degree of the field $P(\sqrt{a}, \sqrt{a'})$ over P ?

An upper estimate, at least, to the desired degree can be obtained by using the representation of the numbers of $P(\sqrt{a}, \sqrt{a'})$ derived in Vol. 1, Section 2, Exer. 8. The exact degree (and consequently the uniqueness of this representation) follows already from Theorems 71, 72, 60, and the result of Exer. 9.

11. Carry Exer. 9, 10 over to the case of an arbitrary ground field K instead of P .

12. In particular, what is the meaning of this result if K is a perfect field of characteristic 2? Moreover, what are the irreducible polynomials of second degree in K whose roots through adjunction generate extensions Λ of degree 2 of such a field K ?

In order to answer the last question note that the basis of Λ over K can be assumed to be e, α , where α is an arbitrary element of Λ not belonging to K . By a linear integral substitution (Section 5, Exer. 15) the irreducible polynomial of second degree over K belonging to α can then be reduced to the type $x^2 + x + a$.

13. Give a necessary and sufficient condition that the polynomial $x^2 + x + a$ over a field K of characteristic 2 (not necessarily perfect) be irreducible?

Set up a decomposition into two linear factors and show that $a = u^2 + u$ with u in K is necessary and sufficient for the reducibility.

14. Let K be a field of characteristic 2 and $\Lambda = K(\alpha)$, $\Lambda' = K(\alpha')$ be two extensions of degree 2, where α, α' are roots of the polynomials $x^2 + x + a, x^2 + x + a'$ irreducible in K . Give a necessary and sufficient condition that $\Lambda' = \Lambda$.

Set $\alpha' = u + v\alpha$ with u, v in K , and from the two equations for α and α' show that the condition $\alpha' = a + u^2 + u$ with u in K is necessary and sufficient.

15. For the complex numbers $a + bi$ (a, b real numbers) justify the designation: ' $a - bi$ is conjugate to $a + bi$ ' by showing that it is in agreement with Def. 26.

If K is the field of all real numbers, then $\Lambda = K(i)$ is the field of all complex numbers (Exer. 8), and the correspondence $i \longleftrightarrow -i$ [which maps every element of K onto itself] generates an isomorphism of Λ relative to K .¹

16. What is the degree over $K = K_0(f_0(x_0))$ of the field $\Lambda = K(x_0)$ in Exer. 4 if $f_0(x_0)$ has a degree $n > 0$?

First establish that every element $g(x_0)$ of Λ can be represented uniquely in the form

$$g(x_0) \equiv \sum_{\mu=0}^m r_{\mu}(x_0) f_0(x_0)^{\mu}$$

with integral rational functions $r_{\mu}(x_0)$ of degrees lower than n and an m sufficiently high. For this purpose, using the Euclidean algorithm (Section 1, E) as a guide, carry out an algorithm by which the successively appearing *quotients* (not remainders) are always again divisible by $f_0(x_0)$ with remainder. This yields, by another grouping of the terms, a unique representation of $g(x_0)$ in terms of a basis of the form x_0^{μ} with K as coefficient domain. By Def. 25 the degree $[\Lambda : K]$ can be derived from this representation.

¹ Therefore an *automorphism* relative to K ; see Def. 33 [266], given later.

17. Let K be a finite field and P_p its prime field, so that p is the characteristic of K . Prove that the number of elements of K is a power p^n of p . What is the meaning here of n ?¹

Note that K is trivially of finite degree n over P_p , and accordingly set up a basis representation.

8. Stem Fields

1. In Section 2, Exer. 20 a construction was given for finite fields of p^n elements. Subsume this construction under the general scheme of the proof of Theorem 76.

For this purpose see the special case $p^n = 2^2$ already considered in Section 7, Exer. 7.

2. Starting from the field of all real numbers carry through the construction of the field of all complex numbers by proceeding in accordance with the scheme of the proof to Theorem 76. Also, compare this construction with that used in analysis where pairs of real numbers are used with definite conventions regarding equality and combination.

For this purpose see Section 7, Exer. 8 as well as the remark made later at the end of Section 11 [249].—The construction used in analysis turns out to be formally identical with the construction according to the scheme of Section 8 if in the former the integral rational functions are again properly interpreted from the algebraic standpoint, namely, as systems of elements of the ground field with definite conventions regarding equality and combination, as was developed in Vol. 1, Section 4.

3. Let K be an imperfect field of characteristic p , and a an element of K . If there is no p -th root of a in K , prove:

(a) The polynomial $x^p - a$ is irreducible in K .

(b) $x^p - a$ has a p -fold root in a stem field Σ of $x^p - a$.

¹ In this regard see also the general theory given later in Section 20.

Show that this is a counterexample against the possibility of applying Section 6, Exer. 27 to imperfect fields.

Form a stem field and, while doing this, a root α of an irreducible factor $g(x)$ of $x^p - a$ in K . Then for (b) simply take Theorem 44 [204] into consideration; for (a), that according to this the term of $g(x)$ free from x is a power of α and that by assumption α^p , but not α , belongs to K .

4. Prove in general: If K is an imperfect field of characteristic p , then for every irreducible polynomial $f(x)$ of the form $f_0(x^p)$ (therefore every inseparable irreducible polynomial) over K the root α obtained by constructing a stem field Σ to $f(x)$ is at least p -fold.

Note that if $f(x)$ has a root α , then $f_0(x)$ has the root α^p , therefore the corresponding linear factor in Σ .

5. Prove: An extension field Λ of K can be chosen in which the system of equations

$$\sum_{k=1}^n a_{ik} x_k = \xi x_i \quad (i = 1, \dots, n),$$

where $x = (x_i)$ and ξ are unknowns, and $A = (a_{ik})$ is an arbitrary matrix over K , cannot be solved identically (that is, with $x \neq 0$).

It is sufficient to take Λ to be a stem field Σ of an irreducible factor in K of the characteristic polynomial of A and ξ to be a root of this factor in Σ .

9. General Theory of Extensions (2).

Simple and Finite Algebraic Extensions

1. Let Λ be (a) simple algebraic, (b) finite algebraic, (c) of finite degree over K . Characterize $\Lambda(x)$ over $K(x)$.

First answer (c) by showing that a basis of Λ relative to K is also a basis of $\Lambda(x)$ relative to $K(x)$. In doing so, the essential point is the

transfer of the linear independence of the basis from K to $K(x)$. For this purpose we can assume without loss of generality that the coefficients are in $K[x]$. Then apply the uniqueness of the normal representation of the elements of $\Lambda[x]$. From the above answer to (c) we can immediately answer (b) by Theorem 84; (a), by Theorem 76.

2. Give a direct proof of Theorem 82 according to the scheme sketched below.

If $f(x)$ is irreducible, $f(\alpha) = 0$ and $\phi(\alpha) = \frac{h(\alpha)}{g(\alpha)}$ with $(g, f) = e$, then we can remove the denominator $g(\alpha)$ by means of a relation $f\bar{f} + g\bar{g} = e$.

3. Show that this process is formally identical with the ordinary process for rationalizing denominators in expressions of the form $\frac{a+b\sqrt{u}}{c+d\sqrt{u}}$, where u is a non-square element of K .

4. Carry through the process of Exer. 2 for the number $\frac{1}{\alpha^2 + \alpha + 1}$, where α is a root of the polynomial $x^3 + x + 3$ over P . First show the irreducibility of this polynomial.

This follows by means of the results of Section 5, Exer. 16, 18.

5. Give the basis representation of $\frac{e}{\alpha}$ in the sense of Theorem 74 (III) [231], where α is an algebraic element over K .

Note that $f(0) \neq 0$ because in Theorem 74 $f(x)$ was assumed to be irreducible.

6. Is the polynomial $x^2 - 2$ (irreducible in P) also irreducible in the field $P(\alpha)$, where α has the meaning described in Exer. 4?

Apply Theorem 81.

7. Represent the number $\frac{1}{\alpha + \sqrt{2}}$ as an integral rational function of α and $\sqrt{2}$ over P , where α has again the meaning described in Exer. 4.

First remove $\sqrt{2}$ from the denominator, then α ; in each case this can be done by the process of Exer. 2.

8. Let $f(x)$ be an irreducible polynomial of degree n with integral rational coefficients (prime polynomial of $\Gamma[x]$) and $g(x)$ an integral rational function with integral rational coefficients (elements of $\Gamma[x]$). If α is a root of $f(x)$, let $g(\alpha) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$ be the unique basis representation in the sense of Theorem 74 (III) [231]. Prove that the rational numbers $c_0, \dots, c_{n-1}$ are integers.

The division of $g(x)$ by $f(x)$ yields a remainder $h(x)$ with integral coefficients.

9. The scheme for determining the degree in Section 7, Exer. 16 can also be used on the basis of Theorem 77 to determine the degree of the element x_0 of $\Lambda = K_0(x_0)$ over the field $K = K_0(f_0(x_0))$. According to Section 7, Exer. 16 this amounts to the demonstration of the irreducibility of $f_0(x) - f_0(x_0)$ in K . Prove this on the basis of Gauss' Theorem (Section 2, Exer. 24) and the isomorphism established in Vol. 1, Section 4, Exer. 2, 4.

According to the result last cited $t = f_0(x_0)$ is transcendental over K_0 (Def. 21 [223]). The polynomial in $K = K_0(t)$ to be proved irreducible is $f_0(x) - t$. Apply Gauss' Theorem to a hypothetical decomposition in the integral domain $K_0[t, x]$.

10. Analogously, for an arbitrary rational function $\phi_0(x_0)$ over K_0 of positive degree determine, in connection with Section 7, Exer. 5, the degree of the element x_0 of $\Lambda = K_0(x_0)$ over the field $K = K_0(\phi_0(x_0))$.

If $t = \phi_0(x_0)$ and $\phi_0 = \frac{f_0}{g_0}$ is the reduced quotient representation of ϕ_0 , then this amounts to the proof of the irreducibility of $f_0(x) - tg_0(x)$ in $K_0(t)$. Again apply the Gaussian Theorem in $K_0[t, x]$.

11. Along with Theorem 78 form an example of a separable element α over K and of an inseparable element over K , and confirm the relations $K(\alpha^n) = K(\alpha)$ and $K(\alpha^n) < K(\alpha)$, respectively.

Naturally, we must start with an imperfect field K . For this take $K = P_2(z)$ with z transcendental over P_2 (cf. Section 6 [217]). According to Def. 17 [214] it is then easy to find a separable and also an inseparable irreducible polynomial of degree 2 over K . Why can P_2 not be used as a ground field for this purpose? (Cf. again Section 6 [217]).

10. Root Fields

1. Let a be a rational number which is not a third power of a rational number. What is the degree of the root field W of the polynomial $x^3 - a$ over P ?

$x^3 - a$ splits off the linear factor $x - \alpha$ in the stem field $\Sigma = P(\alpha)$ of a root $\alpha = \sqrt[3]{a}$. To prove the irreducibility in Σ of the remaining quadratic factor proceed as in Section 9, Exer. 6 (cf. also Section 7, Exer. 6, already given).

2. Under the data of Exer. 1 decide whether the three stem fields $\Sigma_1 = P(\alpha_1), \Sigma_2 = P(\alpha_2), \Sigma_3 = P(\alpha_3)$, contained in the root field W , corresponding to the roots $\alpha_1, \alpha_2, \alpha_3$ of $x^3 - a$, are equal or distinct.

Note (a) that W is the composite of any two of the three stem fields, and (b) that an equality between them will affect the degree of W .

3. Prove the distinctness of the three stem fields $\Sigma_1, \Sigma_2, \Sigma_3$ in Exer. 2 by representing the root field W in the field of all complex numbers.

Note that in this representation of W one of the three stem fields, let us say, Σ_1 , is already contained in the field of all real numbers, while the two others Σ_2, Σ_3 are not. In order to exclude $\Sigma_2 = \Sigma_3$,

consider the quotients $\frac{\alpha_2}{\alpha_3}$ and again take the degree into consideration as in Exer. 1.

4. Give a representation for the root field of the polynomial $x^4 - 10x^2 + 1$ over P .

It is better here to deviate somewhat from the general scheme of the proof to Theorem 87. Thus, corresponding to the structure of the given polynomial, first decompose the polynomial into two quadratic factors through the transition to an easily found quadratic field Λ , and then form the root fields W, W' of these two quadratic factors. We thereby establish that $W' = W$ (Section 7, Exer. 9, 11).

5. Prove that in Exer. 4

$$W = \Lambda(\sqrt{2}) = \Lambda(\sqrt{3}), \quad W = P(\sqrt{2}, \sqrt{3})$$

is also valid.

Apply again Section 7, Exer. 9, 11.

6. Let A be an n -rowed square matrix over K and

$$f(x) \equiv (x - \alpha_1)^{r_1} \cdots (x - \alpha_r)^{r_r} \quad (v_1 + \cdots + v_r = n)$$

the decomposition of its characteristic polynomial

$$f(x) \equiv |xE - A|$$

in its root field W into powers of different linear factors. $\alpha_1, \dots, \alpha_r$ are called the *characteristic roots* of A with the *multiplicities* $v_1, \dots, v_r$. The determinantal divisors $d_\nu(x)$ and the elementary divisors $e_\nu(x)$ ($\nu = 1, \dots, n$) of the characteristic matrix $xE - A$ of A are also, briefly, called the *determinantal divisors* and *elementary divisors* of A .—Describe the decomposition of the determinantal divisors and elementary divisors of A into powers of different linear factors. What relations and bounds exist for the multiplicities $\delta_{i\nu}$ and $\epsilon_{i\nu}$ of the roots α_i in $d_\nu(x)$ and $e_\nu(x)$?

See the explanation to Section 6, Exer. 33.

7. Of the n exponents $\epsilon_{i1} \leq \dots \leq \epsilon_{in}$ let the last μ_i be simultaneously > 0 . Let $\bar{\alpha}_1, \dots, \bar{\alpha}_s$ designate the above $\alpha_1, \dots, \alpha_r$ with the multiplicities $\mu_1, \dots, \mu_r$ ($s = \mu_1 + \dots + \mu_r$); that is, the elements obtained by counting each α_i μ_i times. Let the s powers $(x - \alpha_i)^{\epsilon_{iv}}$ with $\epsilon_{iv} > 0$ be correspondingly designated by $(x - \bar{\alpha}_i)^{\epsilon_i}$ ($i = 1, \dots, s$) without regard to the ordering of the $\bar{\alpha}_i$. The $(x - \bar{\alpha}_i)^{\epsilon_i}$ are called the *simple elementary divisors* of A .— Show that the compound elementary divisors $e_\nu(x)$ ($\nu = 1, \dots, n$) of A are determined uniquely by giving these simple elementary divisors (in any order) backwards. What (single) restriction exists on the exponents ϵ_i (besides $\epsilon_i > 0$ due to the definition)?

8. Determine the simple elementary divisors of the ϵ -rowed square matrix

$$E_\epsilon(\alpha) = \begin{pmatrix} \alpha & e & & \\ & \ddots & \ddots & \\ & & e & \\ & & & \alpha \end{pmatrix}$$

(where the places not marked are occupied by zeros and $E_1(\alpha) = \alpha$ is understood).

Note that $d_{\epsilon-1}(x) \equiv e$ is also true due to the minor of $(\epsilon-1)$ -st degree in the right upper corner.

9. Determine in general the simple elementary divisors of the matrix

$$E_{\epsilon_1, \dots, \epsilon_s}(\bar{\alpha}_1, \dots, \bar{\alpha}_s) = \begin{pmatrix} E_{\epsilon_1}(\bar{\alpha}_1) & & \\ & \ddots & \\ & & E_{\epsilon_s}(\bar{\alpha}_s) \end{pmatrix}$$

[diagonal ordering of the $E_{\epsilon_i}(\bar{\alpha}_i)$].

The direct calculation of the determinantal divisors, as in Exer. 8, is very complicated. Rather than doing this note that by the result of Exer.

8 the characteristic matrix $xE - E_\epsilon(\alpha)$ is arithmetically equivalent to

$$\begin{pmatrix} e & & \\ & e & \\ & & (x - \alpha)^e \end{pmatrix}. \text{ Through composition this yields a similarly con-}$$

structed matrix which is arithmetically equivalent to the characteristic matrix $xE - E_{\epsilon_1 \dots \epsilon_s}(\bar{\alpha}_1, \dots, \bar{\alpha}_s)$ (in which, in addition, the powers of linear factors can be brought to the bottom by permuting the rows). The determinantal divisors can be easily read off from this by returning again to the original designation $(x - \alpha)^{\epsilon_i \nu}$ for the powers of linear factors (Exer. 7).

10. To summarize, now deduce: Every n -rowed square matrix A is similar in the root field $\mathbf{W}$ of its characteristic polynomial $f(x)$ to a matrix of the type in Exer. 9 with uniquely determined $\epsilon_i > 0$ and $\sum_{i=1}^s \epsilon_i = n$.

Apply the similarity criterion of Section 1, Exer. 47.—Regarding the similarity in the root field $\mathbf{W}$ take Section 5, Exer. 12 into consideration. For the rest confirm, by tracing back the chain of ideas to Section 1, Exer. 38, that the similarity is already proved by the conclusions drawn in the field $\mathbf{W}$.

11. Show that in Exer. 9 we have also solved the problem of constructing—of course, not in the ground field $\mathbf{K}$ —a matrix with given elementary divisors $e_1(x), \dots, e_n(x)$ satisfying the necessary restrictions $e_1(x) \mid \dots \mid e_n(x)$ and $e_1(x) \cdots e_n(x)$ of degree n .

That $e_1(x) \cdots e_n(x)$, in addition, has the degree ν at most is already formally implied in the two cited restrictions.

12. Give a necessary and sufficient condition that A be

similar to a diagonal matrix $\begin{pmatrix} \bar{\alpha}_1 & & \\ & \ddots & \\ & & \bar{\alpha}_n \end{pmatrix}.$

Apply the uniqueness in Exer. 10 and the elementary divisor determination in Exer. 9. The result can be expressed either as a condition on the simple elementary divisors or as a condition on the last elementary divisor $e_n(x)$.

13. What are the characteristic polynomials of the matrices

$$A = \begin{pmatrix} 0 & e & & & \\ & 0 & e & & \\ & & \ddots & \ddots & \\ & & & 0 & e \\ -a_n & \dots & -a_2 & -a_1 & \end{pmatrix}, \quad A(\alpha) = \begin{pmatrix} \alpha & e & & & \\ & \alpha & e & & \\ & & \ddots & \ddots & \\ & & & \alpha & e \\ -a_n & \dots & -a_2 & \alpha - a_1 & \end{pmatrix}?$$

In order to calculate the determinants, expand by the first column and use mathematical induction. The formulation for this can be obtained from the easily computable cases $n = 1$ and $n = 2$.

14. Also determine the elementary divisors of the matrices in Exer. 13, and from this illustrate the meaning of the matrices $E_e(\alpha)$ in Exer. 8 to 10.

Proceed as in Exer. 8.

15. For the class of matrices similar to A construct a unique normal form belonging to the ground field K .

Proceed as in Exer. 9, 10. Namely, order diagonally the elementary divisors $e_v(x)$ of the corresponding matrices of the first type considered in Exer. 13 and make full use of the arithmetical equivalence to the normal form of Section 1, Exer. 39, 40.

16. Let the n -rowed square matrix A over K have the characteristic roots $\alpha_1, \dots, \alpha_n$ (not collected according to multiplicities), and let $g(x)$ be an arbitrary integral rational function of x over K . What are the characteristic roots of the matrix $g(A)$ (cf. Section 5, Exer. 9).

Transform A by a similarity transformation $P^{-1}AP$ to the normal form of Exer. 9, 10 and make use of the invariance of the characteristic polynomial (Vol. 1, Section 21, Exer. 19) as well as the fact

$g(P^{-1}AP) = P^{-1}g(A)P$. Then the characteristic roots of $g(A)$ can be immediately read off from the main diagonal.

17. Prove: If

$$h(x) \equiv b(x - \beta_1) \cdots (x - \beta_m)$$

is the decomposition of an arbitrary integral rational function of x over K into linear factors (in its root field), then for any n -rowed square matrix A over K we have

$$h(A) \equiv b(A - \beta_1 E) \cdots (A - \beta_m E).$$

Due to the fact that A and its powers commute with the diagonal matrices $\beta_i E$ we can expand the right side in the usual way. Then apply Vieta's formulae (Section 5, Exer. 13).

18. Give another proof that $g(A)$ has the characteristic roots $g(\alpha_k)$, if A has the characteristic roots α_k (Exer. 16). For this purpose, introduce a new indeterminate y , decompose the integral rational function $h(x) \equiv y - g(x)$ of x over $K(y)$ into linear factors in its root field, and apply Exer. 17 to calculate the characteristic polynomial

$$f(y) \equiv |yE - g(A)| \equiv |h(A)|.$$

Decompose all factors $|A - \beta_i E| = (-1)^n f(\beta_i)$ as they occur according to the linear factorization of $f(x)$ into a product and then form a simple product by collecting the factors of the generated double products in another way.

19. Represent the matrix

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & \vdots & \cdots & a_0 \end{pmatrix}$$

(n -rowed circulant; cf. Section 4, Exer. 15, already given) as an integral rational function of a matrix N such that the

function has degree $(n-1)$ at most. From this calculate its determinant.

Use the linear homogeneous representation of A in terms of n matrices $N_0, \dots, N_{n-1}$, each of which has only ones running along parallels to the main diagonal in a cyclic fashion, and derive all these N_ν from $N_1 = N$. To evaluate the determinant, note that according to Exer. 9, 10 (or even by setting $x = 0$ in the characteristic polynomial) the determinant is the product of the characteristic roots, and apply Exer. 16, 18.¹

20. Subsume Section 4, Exer. 15 under this result.

If the basic field K has characteristic p , then for $n = p$ the characteristic polynomial of $N = P = \begin{pmatrix} 0 & e & & \\ & & \ddots & \\ & & & e \\ e & & & 0 \end{pmatrix}$ has the p -fold root e according to Exer. 13 and Theorem 44 [204].

21. Express the characteristic roots of the ν -th derived matrix $A^{(\nu)}$ of a matrix A in terms of the characteristic roots α_i of A .

Proceed as in the case of Exer. 16.

22. Accordingly, prove: If $\alpha_1, \dots, \alpha_n$ are the roots of a polynomial $f(x)$ over K , then the products $\alpha_{i_1} \dots \alpha_{i_\nu}$, where $\{i_1, \dots, i_\nu\}$ runs through all $\binom{n}{\nu}$ combinations of the numerals $1, \dots, n$, are the roots of a polynomial $g_\nu(x)$ over K .²

Represent $f(x)$ according to Exer. 13 as the characteristic polynomial of a matrix A over K and apply Exer. 21.

23. Similarly, prove: If $f(x), g(x)$ are polynomials over K and α_i, β_k ($i = 1, \dots, m; k = 1, \dots, n$) are their roots, then the

¹ For the representation of the result see also Theorem 120 [304], given later, as well as Exer. 16 to Section 20, given later.

² This will computationally prove a statement involved in the *Theorem on Symmetric Functions* (Theorem 131 [329]), given later.

difference product $\prod_{i=1}^m \prod_{k=1}^n (\alpha_i - \beta_k)$

is an element of K (*resultant* of f and g).¹

Again, represent $f(x)$ according to Exer. 13 as a characteristic polynomial of a matrix A over K and apply Exer. 18.

24. What criterion in terms of determinants is obtained from this for the validity of the relation $(f, g) = e$?

$|g(A)| \neq 0$, where A is the matrix of Exer. 13 to

$$f(x) \equiv x^n + a_1 x^{n-1} + \cdots + a_n.$$

25. Let $x^2 + ax + b$ and $x^2 + cx + d$ be two polynomials of second degree. Use the above criterion to form an expression (their resultant) from their coefficients a, b, c, d which can be used to decide whether these polynomials are relatively prime or not. By suitable bordering and application of the Corollary to Vol. 1, Theorem 71 [142], bring the resulting two-rowed determinant to the form

$$\begin{vmatrix} e & a & b & 0 \\ 0 & e & a & b \\ e & c & d & 0 \\ 0 & e & c & d \end{vmatrix}$$

and interpret the result in the sense of Vol. 1, Theorem 73 [145] with $\mathfrak{x} = (x^3, x^2, x, e)$.

11. The So-called Fundamental Theorem of Algebra

1. Prove (with the help of analysis): In the field K of all real numbers any polynomial $f(x)$ of odd degree n has (at least) one root in K .²

¹ See footnote 4 on p. 153.

² For a proof of the so-called Fundamental Theorem of Algebra based on this theorem and using in addition only purely algebraic conclusions, see Exer. 7 to 9 to Section 17, given later.

Use the theorem: If a function $f(x)$ is real and continuous in an interval $a \leq x \leq b$ and $f(a) < 0, f(b) > 0$, then there exists a c in this interval with $f(c) = 0$. In addition, note that $\lim_{x \rightarrow \pm \infty} \frac{f(x)}{x^n} = 1$.

2. A field A is called *algebraically closed* if it has no proper algebraic extensions. Therefore, the so-called Fundamental Theorem of Algebra establishes that the field of all complex numbers is algebraically closed.—Prove: If an algebraic extension A of K has the property that any polynomial over K resolves into linear factors in A , then A is algebraically closed.

Apply Theorem 86 [242].

3. Give (on the basis of the so-called Fundamental Theorem of Algebra) the prime functions of the integral domain $K[x]$, if K is (a) the field of all complex numbers, (b) the field of all real numbers.

In the case (b) note that $[K(i) : K] = 2$ (Section 7, Exer. 8). Consequently, we only have to determine whether the quadratic polynomial $x^2 + ax + b$ over K is irreducible or not (for this purpose, see Section 1, Exer. 11).

4. For a polynomial with real coefficients, how is the decomposition into irreducible polynomials over the field of all real numbers connected with its decomposition into irreducible polynomials over the field of all complex numbers?

Apply Theorem 25 [189].

5. Let A be a symmetric matrix (Vol. 1, Section 19, Exer. 5) in the field of all real numbers. Prove that the characteristic roots α of A are real by investigating the meaning of the fact that the determinant of the linear homogeneous system of equations $(A - \alpha E)x = 0$ is zero.

Let $\bar{\xi}'$ stand for the one-rowed matrix generated from the one-columned solution matrix (vector ξ) by transposition and transition to the conjugate complex. Then subject the relation $\bar{\xi}'A\xi = \alpha\bar{\xi}'\xi$ to just these two operations and use the transposition rule of Vol. 1, Section 10, Exer. 13.

6. What sharper assumption must be imposed on the matrix A in order to enable us to conclude that the characteristic roots α are positive?

The quadratic form $\bar{\xi}'A\xi = \sum_{i,k=1}^n a_{i,k}x_i\bar{x}_k$ constructed with the matrix A must be positive for all real $\xi \neq 0$ (*positive definite quadratic form*).

7. To which more general matrices A over the field of all complex numbers can the results of Exer. 5, 6 be carried over?

Exer. 5 carries over to the matrices which satisfy the transposition condition $\bar{A}' = A$ (*Hermitian matrices*); Exer. 6 to those which have in addition positive $\bar{\xi}'A\xi = \sum_{i,k=1}^n a_{i,k}\bar{x}_i x_k$ throughout for complex $\xi \neq 0$ (*positive definite Hermitian form*).

Vol. 2. Chapter IV. The Structure of the Root Fields of Algebraic Equations

12. Simplicity and Separability of the Root Fields of Separable Polynomials, More Generally, of Finite Algebraic Extensions with Separable Primitive System of Elements

1. Carry through the proof of Theorem 90 in the case $\Lambda = \mathbb{P}(\sqrt{2}, \sqrt{3})$. In doing so, a primitive element of Λ will show up. Use this primitive element to obtain representations of $\sqrt{2}$ and $\sqrt{3}$. (For this purpose cf. also Section 10, Exer. 4, 5.)

$\theta = \sqrt{2} + \sqrt{3}$ can be used for this. In order to determine the greatest common divisor of $\phi(x)$ and $f_2(x)$, apply the Euclidean algorithm.

2. Let $\Lambda_1 = \mathbb{K}(\sqrt{a_1})$, $\Lambda_2 = \mathbb{K}(\sqrt{a_2})$ be two different extensions of degree 2 over $\mathbb{K}$. In general, what is the representation of the extension $\Lambda = \mathbb{K}(\sqrt{a_1}, \sqrt{a_2})$ as a simple algebraic extension of $\mathbb{K}$ if the characteristic of $\mathbb{K}$ is not 2? Such a representation will again involve a primitive element of Λ . Use this primitive element to obtain representations of $\sqrt{a_1}$ and $\sqrt{a_2}$.

3. By a counterexample show that Theorem 90 is in general no longer valid for algebraic extensions Λ with inseparable primitive system of elements. For this purpose take, for instance, $\mathbb{K}$ in Exer. 2 to be an (imperfect) field of characteristic 2.

Note that in this case $e, \sqrt{a_1}, \sqrt{a_2}, \sqrt{a_1}\sqrt{a_2}$ is a basis of Λ relative to $\mathbb{K}$ (proof to Theorem 71 [228]), and accordingly determine the degree of the generic element of Λ over $\mathbb{K}$ by Theorem 44 [204].

4. Prove: If K is perfect, then every algebraic extension of finite degree Λ of K is also perfect.

For this purpose note that perfect fields are characterized by the fact that there are no inseparable simple algebraic extensions over them (Section 6, Exer. 27; Section 8, Exer. 3), and apply Theorem 91 as well as Theorems 86 [242], 66 [224].

5. In the field of all complex numbers select the subfield Λ of all rational functions over P of the square roots of finitely many arbitrary rational numbers at a time. It is, incidentally, sufficient to use only the square roots of $p_0 = -1$ and of all prime numbers $p_1, p_2, \dots$ for the formation of Λ (Theorem 12 [178]). Show that Λ is an algebraic extension of P containing elements of *any* degree whatsoever. (Theorem 91, Corollary.)

We have to show the irreducibility of $x^2 - p_r$ in

$$\Lambda_{r-1} = P(\sqrt{p_0}, \dots, \sqrt{p_{r-1}}).$$

Use mathematical induction and show that of the elements in the field Λ_{r-1} , which has the basis $\sqrt{p_0}^{v_0} \cdots \sqrt{p_{r-1}}^{v_{r-1}}$ ($v_0, \dots, v_{r-1} = 0, 1$) by the induction assumption, only the multiples $\alpha \sqrt{p_0}^{v_0} \cdots \sqrt{p_{r-1}}^{v_{r-1}}$ of the basis elements (α arbitrary in P) have rational squares (are roots of pure equations over P). Then, the irreducibility of $x^2 - p_r$ follows from the fundamental theorem of the unique decomposability into prime numbers.

13. Normality of Root Fields and Their Primitive Elements. Galois Resolvents

1. Let a be a rational number which is not a third power of a rational number. Is any $\sqrt[3]{a}$ normal over P ?

Section 10, Exer. 2 answers the question simply according to Def. 29, 30.

2. Construct a Galois resolvent for the polynomial $x^3 - a$ (a as in Exer. 1) over P .

The simple sum of two roots can obviously not be used here as θ in the sense of the proof of Theorem 90 [251]; on the other hand, for the a appearing there any rational number different from 0, ± 1 can be chosen. The result is especially simple for $a = 2$. Incidentally, we could also choose $a = -1$ (the condition in the proof to Theorem 90 [251] is only sufficient, not necessary), but not $a = 0, 1$.

3. Between two different roots α, α' of an irreducible polynomial $f(x) \equiv x^3 + a_1x^2 + a_2x + a_3$ over K can there exist a relation $\alpha' = c_0 + c_1\alpha$ with c_0, c_1 in K ?

First note that, at any rate, $c_1 \neq 0$ would have to be valid. Then apply Theorem 53 [210] to $f(c_0 + c_1x)$. In doing so, we must distinguish whether K has characteristic 3 or not. In the latter case we can assume $a_1 = 0$ without loss of generality (Section 5, Exer. 15); then we easily obtain that $c_0 = 0$ and, since $a_3 \neq 0$, that $c_1^3 = e$. Now, if $a_2 \neq 0$, then $c_1 = e$, contradicting $\alpha' \neq \alpha$. However, if $a_2 = 0$, namely, if $f(x)$ is a pure polynomial (cf. Def. 38 [302]), then besides $c_1 = e$ there is still the possibility $c_1^2 + c_1 + e = 0$. For certain fields $x^3 + x + e$ is reducible, for instance in P_7 ; for such fields $c_1 = 2e$ and $c_1 = 4e$ are also possible besides $c_1 = e$ (cf. Theorem 123 [312], given later). In the former case it likewise follows that $c_0 = 0, c_1 = e$ unless $a_1 = 0$ is valid. However, if $a_1 = 0$, then, for instance, $\alpha' = c_0 + \alpha$ is possible for suitable a_2, c_0 . The polynomial $x^3 - x - e$ irreducible in P_3 is an example of this.

4. Prove in general: Every irreducible polynomial of the form $x^p - x - a$ is normal in a field K of characteristic p .

Note that if α is a root so also is $\alpha + ne$ for arbitrary ne in the prime field P_p of K .

5. In connection with Section 7, Exer. 13, derive the necessary and sufficient condition for the irreducibility of a polynomial of the form $x^p - x - a$ in a field K of characteristic p .

The assumption that $g(x)$ is an irreducible divisor of $f(x)$ in K which, besides a root α , has still another root $\alpha + ne$ ($n = 1, \dots, p-1$) of $f(x)$, implies $g(x - ne) \equiv g(x)$ (Theorem 53 [210]), and the consideration

of the coefficient of the term of $g(x)$ of second highest degree in x yields a contradiction. Therefore, the irreducibility criterion is obtained simply by excluding a root α in K .

6. In connection with Section 7, Exer. 14, derive the necessary and sufficient condition for the equality of the root fields W, W' of two irreducible polynomials $x^p - x - a, x^p - x - a'$ over a field K of characteristic p .

The setup $\alpha' = c_0 + c_1\alpha + \cdots + c_{p-1}\alpha^{p-1}$ yields relations between the $c_0, \dots, c_{p-1}$. If we take into consideration that $x^p - x$ has *only* the elements ne of P_p as roots in K , and that $x^p - x - a$ has by assumption *no* root in K , then these relations yield successively

$$c_{p-1} = 0, \dots, c_2 = 0, c_1 = ne \neq 0, a' = na + c_0^p - c_0.$$

We can easily prove that the latter condition, which is necessary according to this, is also sufficient.

7. In connection with Theorem 93, construct an example in which $N \supseteq \bar{K} \supseteq K$ and N is normal over K but $\bar{K}$ is not normal over K .

It is sufficient to take the root field of $x^3 - a$ (Exer. 1) as N and one of the three stem fields as $\bar{K}$ over $K = P$.

8. Draw the following conclusion from Theorem 103: If $\Lambda = K(\alpha)$ is a separable simple algebraic extension of K of degree n , then an element $\beta = h(\alpha)$ of Λ is a primitive element of Λ if and only if the conjugates $\beta_1, \dots, \beta_n$ are different from one another (Theorem 95).

Make full use of the remark after Theorem 103 and apply Theorem 81 [240].

9. *Steinitz* gave a definition of normality differing from Def. 29, namely: An extension N of K is called normal over K if every polynomial $f(x)$ over K which has a root in N also resolves into linear factors in N . Prove that this definition is the same as Def. 29 in the case of separable extensions N of finite degree.

That the Steinitz definition in the case of separable N of finite degree implies the property underlying Def. 29 can be seen by representing N as a stem field of an irreducible polynomial over K (Theorems 91 [254], 99). The converse follows by Exer. 8 (see also the remark following Theorem 97).— Both definitions also coincide in the case of *arbitrary* algebraic extensions N ; however, the proof of this fact would take up too much of our space.

10. Show that the Steinitz definition of normality differs from Def. 29 in the case of simple transcendental extensions.

In the sense of Steinitz $K(x)$ would have to be called normal over K (main point in Vol. 1, Section 4, Exer. 4); in the sense of Def. 29 it would not, since $K(x) \neq K(x')$ within $K(x, x')$, or also in view of Section 1, Exer. 30 and Vol. 1, Section 4, Exer. 5.

11. Under the same assumptions as in Exer. 8, let $\gamma_1, \dots, \gamma_n$ be any system of n elements of Λ and $\gamma_{1k}, \dots, \gamma_{nk}$ ($k = 1, \dots, n$) the n conjugate systems in the sense of Theorem 95 (and Theorem 103). Let

$$\gamma_i = \sum_{\nu=1}^n a_{i\nu} \alpha^{\nu-1} \quad (i = 1, \dots, n)$$

be representations of the γ_i in terms of the basis $e, \alpha, \dots, \alpha^{n-1}$ of Λ . From this derive a matrix relation by going over to the conjugate base $e, \alpha_k, \dots, \alpha_k^{n-1}$.

Due to the isomorphisms relative to K between the n stem fields $\Lambda_k = K(\alpha_k)$ we are permitted to adjoin the 'conjugate indices' $k = 1, \dots, n$ successively to α and the γ_i throughout the given system of formulae without altering the coefficients $a_{i\nu}$. A matrix product relation can then be obtained.

12. From this derive a necessary and sufficient condition that $\gamma_1, \dots, \gamma_n$ be a basis of Λ .

At any rate, it is necessary that the matrix $A = (a_{ik})$ be regular over K , that is, that $|A| \neq 0$, since otherwise the γ_i would be linearly dependent (over K) (Vol. 1, Theorem 77 [236]). By means of Vol. 1,

Theorem 74 [231] show that this is also sufficient, that is, that the α^{p-1} are then linear combinations of the γ_i over K .

13. The square of the determinant of the matrix (γ_{ik}) obtained in Exer. 11 whose columns consist of systems conjugate to the system γ_i is called the *discriminant* of the system $\gamma_1, \dots, \gamma_n$; notation $d(\gamma_1, \dots, \gamma_n) = |\gamma_{ik}|^2$.—Prove: $d(\gamma_1, \dots, \gamma_n)$ is an element of the ground field K .

Apply Exer. 11 and Section 6, Exer. 19.

14. How can the basis property of a system $\gamma_1, \dots, \gamma_n$ be characterized through its discriminant $d(\gamma_1, \dots, \gamma_n)$?

Again apply Exer. 11 and take note of $|\alpha_k^{p-1}| \neq 0$ (Vol. 1, Section 19, Exer. 4).

15. What can be said about the sign of the basis discriminant $d(\gamma_1, \dots, \gamma_n)$ if the rational field K is used as the ground field P ?

Section 11, Exer. 4 implies that $|\alpha_k^{p-1}|$ retains or changes its sign in the transition to the conjugate complex according to the evenness or oddness of the number of irreducible factors of second degree of $f(x)$ in the field of all real numbers [the number of pairs of conjugate complex roots of $f(x)$].

16. Accordingly, what is the sign of the basis discriminants $d(\gamma_1, \gamma_2, \gamma_3)$ of a field $P(\sqrt[3]{a})$ in Exer. 1?

14. The Automorphism Group of an Extension Domain

1. Let K be a perfect field of characteristic p . Show that the correspondences $a \rightarrow a^p$ for arbitrary a in K yield an automorphism A of K .

Regarding the conditions in Vol. 1, Section 2, (II): $(\delta), (\epsilon)$ are trivially satisfied; (δ') , because K is perfect; (ϵ') , according to Section 4, Exer. 7. Regarding the conditions in Def. 32, (1) is satisfied by Theorem 44 [204]; (2), trivially.

2. The automorphism A of Exer. 1 generates a cyclic subgroup $\mathfrak{A}$ of the entire automorphism group of K . Give a representation for this subgroup.

For positive n , A^n is given by $a \rightarrow a^{p^n}$; for negative $n = -n'$, by $a \rightarrow \sqrt[n']{a^{p^n}}$.

3. Prove that the cyclic automorphism group $\mathfrak{A}$ of Exer. 2 is finite if and only if K is a finite field (of characteristic p).

Note (a) that for finite K there exist only finitely many permutations of the elements of K , (b) that for infinite K the equation $x^{p^n} - x = 0$ cannot be satisfied for all elements of K (Theorem 48 [208]).

4. To be more exact, prove: If K is a finite field of p^n elements (cf. Section 7, Exer. 17), then $\mathfrak{A}$ is cyclic of order n .¹

First apply Fermat's Theorem to the multiplicative group of K (analogously to Theorem 29 [194]; see also Section 2, Exer. 15) and then proceed analogously to Exer. 3, (b).

5. For which prime fields P_q different from P_p do the correspondences $a \rightarrow a^p$ yield an automorphism of P_q ?

This automorphism must, at any rate, be the identity (see the remark after Theorem 104). By considering the behavior of the multiplicative group of P_q and taking note of Section 5, Exer. 6, we find that $q - 1 \mid p - 1$ is a necessary and sufficient condition.

6. Prove that the entire automorphism group of a domain B coincides with the automorphism group relative to its prime domain.

See again the remark after Theorem 104.

7. Show that the substitution $\sqrt{-e} \rightarrow -\sqrt{-e}$ generates an automorphism of $P_3(\sqrt{-e})$; what's more, it is just the automorphism A of Exer. 1. Is the corresponding fact also valid for $P_5(\sqrt{-e})$?

¹ In this regard see also the general theory given later in Section 20.

$\sqrt{-e}$ is a root of the polynomial $x^2 + e$ irreducible in P_3 . Therefore, apply Theorem 95 [257] and establish, besides, $\sqrt{-e^3} = -\sqrt{-e}$. For P_5 , $x^2 + e$ is reducible and $\sqrt{-e} \rightarrow -\sqrt{-e}$ does not generate an automorphism at all (Theorem 73 [230]).

8. For which prime fields P_p is $x^2 + e$ irreducible? reducible?

Take into consideration the cyclic nature of the multiplicative group of P_p (Section 5, Exer. 6). According to this the square root of $-e$ can be taken in P_p if and only if the exponent in the representation of $-e$ through a basis element is even. On the other hand, this exponent, except for the trivial case $p = 2$, is $\frac{p-1}{2}$, since $(-e)^2 = e$, $-e \neq e$.

9. Give the automorphism group of $K(x)$ relative to K . Show by direct methods, too, that the resulting set of substitutions has the group property.

Every automorphism is generated, at any rate, by the substitution $x \rightarrow \phi_0(x)$ for x . The necessary and sufficient condition that such a substitution yields an automorphism of $K(x)$ relative to K was derived in Section 1, Exer. 30 and Vol. 1, Section 4, Exer. 5.

15. The Galois Group of a Separable Normal Extension of Finite Degree

1. What is the type of the Galois group of a separable normal extension N of prime degree over K ?

There is only one group type for a given prime order (Vol. 1, Section 8, Exer. 7).

2. A separable normal extension N of degree 2 over K is the root field of a polynomial of the form $x^2 - a$ or $x^2 - x - a$ over K (Section 7, Exer. 12; Section 13, Exer. 4) according as K has a characteristic different from 2 or equal to 2. For all elements of N give the correspondences yielding the non-identical automorphisms of N over K .

3. Give the Galois group of the (non-separable) normal extension $N = K(\sqrt[p]{a})$ of degree p over an (imperfect) field K of characteristic p . Accordingly, is Theorem 105 also valid here?

Note that there exist no conjugates of $\sqrt[p]{a}$ different from $\sqrt[p]{a}$ (Section 4, Exer. 7).

4. If α is a root of an irreducible polynomial of the form $x^p - x - a$ over a field K of characteristic p , then $N = K(\alpha)$ is normal (Section 13, Exer. 4) and naturally separable. The Galois group is cyclic (Exer. 1). Represent its automorphisms explicitly.

This likewise follows immediately from Section 13, Exer. 4 (see also Exer. 2, above).

5. It is easily established that the two polynomials

$$(a) f(x) \equiv x^3 - 3x + 1,$$

$$(b) f(x) \equiv x^3 + x^2 - 2x - 1$$

over $\mathbb{P}$ have the property $f(x) \mid f(x^2 - 2)$.¹ What consequences follow from this regarding the associated stem fields and the Galois groups of their root fields? Represent these Galois groups explicitly in the sense of Theorem 106.

First prove the irreducibility (Section 5, Exer. 18) and the normality (Theorem 99 (III) [259]) of these polynomials and then take Exer. 1 into consideration.

6. In Section 10, Exer. 4, 5 we considered the root field of $x^4 - 10x^2 + 1$ over $\mathbb{P}$. What is the type of the Galois group of this root field?

First, the proof of the irreducibility immediately follows from the decomposition into two quadratic factors used in Section 10, Exer. 4,

¹ How we arrived at this cannot be discussed here. For this purpose cf. Exer. 16, 17 to Section 21, given later.

and from the non-existence of a rational root. The normality follows from the relation $W' = W$ already established. Therefore, the Galois group has the order 4. Its automorphisms arise from the structure obtained in Section 10, Exer. 5 for the root field.

7. In general, what is the type of the Galois group in the case of a biquadratic field of the form $N = K(\sqrt{a}, \sqrt{a'})$ over a field K with characteristic different from 2, provided that $\frac{a}{a'}$ is not the square of an element in K (cf. Section 7, Exer. 10, 11)?

The normality of N follows from Theorem 94 [256]; the automorphisms are generated just as in the special case of Exer. 6.

16. The Galois Group of a Separable Polynomial

1. Let $f(x)$ be an irreducible separable polynomial in K . Prove the transitivity of the representation of the Galois group of $f(x)$ as a permutation group of the roots of $f(x)$ (Vol. 1, Section 16, Exer. 4). The existence of this representation follows from Theorem 107.

Note that for irreducible $f(x)$ Theorem 95 [257] yields a statement about the existence of automorphisms for the required kind of root fields.

2. As a converse and generalization of this prove that for reducible separable $f(x)$ the above representation of the Galois group of $f(x)$ by permutations is intransitive. Namely, show that its transitive components correspond exactly to the systems of roots of those irreducible factors $f_i(x)$ of $f(x)$ which are different.

The root field W of $f(x)$ is the composite of the root fields W_i of the different $f_i(x)$. Use Theorem 89 [246] to apply this result to the Galois group of W . In addition, take note of the fact following from Theorem 113 [284]—applied to the Galois resolvent of $f(x)$ —that the

roots of an $f_1(x)$, counted to certain multiplicities, represent a complete system of conjugate elements of W .

3. What types are possible for the Galois group in the case of an irreducible separable polynomial $f(x)$ of degree 3 (over an arbitrary ground field K)?

All transitive permutation groups of 3 elements have to be determined. There are only two such groups, one cyclic and one non-Abelian.

4. Answer the same question regarding the degree 4.

Either, the transitive permutation groups of 4 elements are set up directly on the basis of the decomposition of the 24 permutations of $\mathfrak{S}$ into cycles. Or, these groups are set up on the basis of the representation of $\mathfrak{S}_4$ as the octahedral group $\mathfrak{O}$ proved in Vol. 1, Section 16, Exer. 27—in this, to the 4 elements there correspond the 4 axes through the center of faces and the subgroups of $\mathfrak{O}$ in question are found geometrically (see the Exer. to Vol. 1, Sections 7, 9, where, however, we did not have to determine *all* subgroups of $\mathfrak{O}$).

We obtain five possible types, namely, $\mathfrak{O}$, $\mathfrak{I}$, $\mathfrak{D}_4$, $\mathfrak{D}_2$, $\mathfrak{B}_4$ in the notation used previously.

5. To which of the two possible types does the Galois group of a polynomial $x^3 - a$ over K belong, inasmuch as it is irreducible and separable (a not a third power in K and K not of characteristic 3)?

This depends on whether $x^3 + x + e$ is reducible or irreducible in K ; namely, whether, in case the characteristic is different from 2, $\sqrt{-3e}$ belongs to K or not, or else, if the characteristic is 2, whether there is a u in K with $u^3 + u = e$ or not (Section 1, Exer. 11) (see the special case in Section 10, Exer. 1).

6. To which of the five possible types does the Galois group of a polynomial $x^4 - a$ over K belong inasmuch as it is irreducible and separable and K does not have characteristic 2? Prove that for the irreducibility it is necessary and sufficient that neither $a = a_0^2$ nor $a = -\frac{a_0^4}{4}$ be valid in K .

The decomposition into linear factors can be written down by means of a root α of $x^4 - a$ and a root i of $x^2 + e$. There are essentially two possibilities whereby $x^4 - a$ has a quadratic factor in K . One of these yields immediately $\alpha^2 = a_0$ in K , that is, $a = a_0^2$ in K . The other leads, at first, only to $i\alpha^2 = b_0$ in K , that is, $a = -b_0^2$ in K , but at the same time $(e + i)\alpha$ in K . These two restrictions yield the sharper condition $a = -\frac{a_0^4}{4}$ in K . After splitting off $(x - \alpha)(x + \alpha)$ in $K(\sqrt[4]{a})$ it depends on whether $i = \sqrt{-e}$ belongs to $K(\sqrt[4]{a})$ or not. This is answered by Section 7, Exer. 9, 11. We find then that only the two types $\mathfrak{B}_4, \mathfrak{D}_4$ of Exer. 4 can occur; which of these two types actually occurs depends on whether $-a$ is a square in K or not, without, however, $-a = \frac{a_0^4}{4}$.

7. Furthermore, to which of the five possible types does the Galois group belong in the case of an irreducible polynomial $f(x) \equiv x^4 + ax^2 + b$ over a K with characteristic different from 2?

The roots can easily be represented in the form

$$\alpha_1 = \sqrt{-\frac{a}{2} + \sqrt{\frac{a^2}{4} - b}}, \quad \alpha_2 = \sqrt{-\frac{a}{2} - \sqrt{\frac{a^2}{4} - b}},$$

$\alpha_3 = -\alpha_1, \alpha_4 = -\alpha_2$. Accordingly, $W = K(\alpha_1, \alpha_2)$. A primitive element in the sense of Theorems 90 [251], 101 [261] can be set up in the form $\vartheta = \alpha_1 + 2\alpha_2$ (why will $\vartheta = \alpha_1 \pm \alpha_2$ not suffice?), and $f(x)$ has in general a polynomial of degree 8 as its Galois resolvent, therefore $[W : K] = 8$. Now apply Theorem 105 [267]. However, if $\sqrt{b}$ or $\sqrt{b(a^2 - 4b)}$ should belong to K (both cannot belong to K at the same time, since otherwise $f(x)$ would be reducible according to Section 1, Exer. 11), then $[W : K] = 4$. In order to decide which of the two cases $\mathfrak{D}_2$ or $\mathfrak{B}_4$ applies each time, take $\sqrt{b} = \alpha_1\alpha_2$ and $\sqrt{b(a^2 - 4b)} = \alpha_1\alpha_2(\alpha_1^2 - \alpha_2^2)$ into consideration, and apply Theorem 107. For each of the last two cases prove the relation $W = K(a_1)$, which excludes $\mathfrak{G} = \mathfrak{D}_4$.

8. A permutation group of p elements (p a prime number) is called *linear* if its permutations $R = \binom{k}{r_k}$ ($k = 0, 1, \dots, p-1$)

can be expressed in terms of integral linear functions $ax + b (a \neq 0)$ over the prime field P_p in the form

$$r_k e = a \cdot ke + b = ka + b \quad (k = 0, 1, \dots, p-1)$$

(cf. also Section 4, Exer. 14).—Prove that the set of all $p(p-1)$ linear functions over P_p gives rise to a transitive permutation group $\mathfrak{L}_p$ in which the p permutations $r_k e = ke + b$ form a cyclic normal divisor $\mathfrak{Z}_p$ with cyclic factor group $\mathfrak{L}_p/\mathfrak{Z}_p$, and the $p-1$ permutations $r_k e = ka$ form a cyclic subgroup $\mathfrak{Z}_{p-1}$ with $p-1$ conjugates different from this and from one another.

The group property and transitivity are obvious. Let re be a basis element of the cyclic multiplicative group of P_p (Section 5, Exer. 6), and let A and B stand for the permutations $r_k = ke + e = (k+1)e$ and $r_k = kre$. Then it is easy to confirm that the relations

$$A^p = E, \quad B^{p-1} = E, \quad B^{-1}AB = A^r$$

are valid, and that $p, p-1$ are also the exact orders of A, B . This summarizes all relations between the group elements and enables us to represent the group elements in the form $A^\mu B^\nu$ ($\mu = 0, 1, \dots, p-1$; $\nu = 0, 1, \dots, p-2$).

9. Prove that the Galois group of an irreducible separable polynomial of degree 3 (Exer. 3) is always linear.

The alternating and the symmetric permutation groups of $p = 3$ elements correspond in Exer. 7 to the normal divisors $\mathfrak{Z}_p$ and to the full linear groups $\mathfrak{L}_p$ (cf. also Vol. 1, Sections 6, 7, Example 4).

10. Prove in general that the dihedral group $\mathfrak{D}_p$ ($p \neq 2$) can be represented isomorphically as a linear transitive permutation group for the prime number p .

$\mathfrak{D}_p$ is isomorphic to the normal divisor of $\mathfrak{L}_p$ generated by A and $B^{\frac{p-1}{2}}$. For this purpose use the fact that $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ (Section 14, Exer. 8), so that the generators are the cyclic permutation $r_k e = (k+1)e$ and the permutation $r_k e = -ke$.

11. Prove: If the Galois group $\mathfrak{G}$ of an irreducible separable polynomial $f(x)$ of prime degree p is linear, then $\mathfrak{G}$ is a subgroup of $\mathfrak{L}_p$ which contains the normal divisor $\mathfrak{Z}_p$.—Furthermore, prove that for any divisor d of $p-1$ there is exactly one such group $\mathfrak{G}$ (notation $\mathfrak{L}_p^{(d)}$) and that $\mathfrak{L}_p^{(d)}$ is a normal divisor of $\mathfrak{L}_p = \mathfrak{L}_p^{(p-1)}$.

On the basis of Exer. 1 and Vol. 1, Section 16, Exer. 7, we find that $\mathfrak{G}$ must contain a power $A^\mu \neq E$.

17. The Fundamental Theorem of the Galois Theory

1. The graphic representation given in Fig. 1 (to Theorem 109) of the structural relations in the Fundamental Theorem of the Galois Theory can be extended in the following manner:

To each finite group $\mathfrak{G}$ associate a *graph* in which every subgroup $\mathfrak{H}$ is represented by a point, every relation $\mathfrak{H} \leq \mathfrak{H}'$ between two subgroups by an arrow directed from $\mathfrak{H}'$ to $\mathfrak{H}$. For

$$\mathfrak{H} \leq \mathfrak{H}' \leq \mathfrak{H}''$$

three arrows are to be drawn corresponding to

$$\mathfrak{H} \leq \mathfrak{H}', \mathfrak{H}' \leq \mathfrak{H}'', \mathfrak{H} \leq \mathfrak{H}''.$$

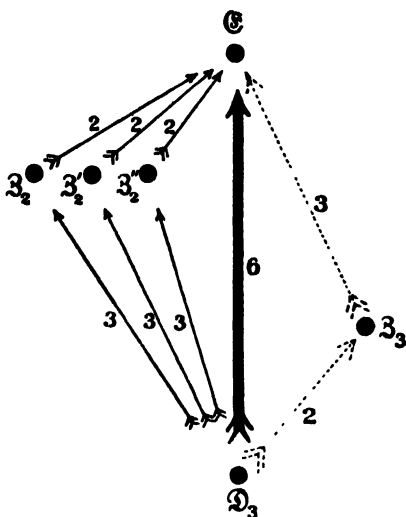
These arrows may either be placed side by side close together or characterized by curvilinear design. If $\mathfrak{H}$ and $\bar{\mathfrak{H}}$ are conjugate subgroups of $\mathfrak{H}'$, draw the two associated arrows in the same color; otherwise, not. Therefore, subgroups contained as normal divisors correspond to arrows from whose starting point originate no two arrows of the same color. Finally, to each arrow attach a number which indicates the index of the subgroup $\mathfrak{H}$ in $\mathfrak{H}'$.

Similarly, to every separable normal extension N of finite degree of a field K associate a graph which represents all intermediate fields Λ by points, all subfield relations $\Lambda' \leq \Lambda$

by arrows directed from Λ' to Λ , conjugateness by arrows in the same color and the degree $[\Lambda : \Lambda']$ by a number on the associated arrow.

The Fundamental Theorem of the Galois Theory then says that the graph of N over K coincides with the graph of the associated Galois group $\mathfrak{G}$ in all determinative parts underlying the construction of the graphs.

As an example of a graph, we give the one shown (right) for the dihedral group $\mathfrak{D}_3$, or, therefore, for the symmetric group $\mathfrak{S}_3$ of three elements ¹



Set up the graphs for the groups $\mathfrak{S}_p, \mathfrak{S}_{2p}, \mathfrak{D}_p, \mathfrak{D}_{2p}$ (p a prime number), $\mathfrak{I} \cong \mathfrak{A}_4, \mathfrak{Q} \cong \mathfrak{S}_4, \mathfrak{J} \cong \mathfrak{A}_5, \mathfrak{Q}_5$ and thereby show the structure of separable normal extensions with these Galois groups.

Regarding the specified groups use the information obtained in the exercises to Vol. 1, Sections 6 to 9, as well as in Section 16, Exer. 8 to 10. For $\mathfrak{S}_{2p}, \mathfrak{D}_p, \mathfrak{D}_{2p}$ distinguish whether $p = 2$ or $p \neq 2$.

2. Set up the graph of the group $\mathfrak{Q}$ of order 8 which is generated from the elements A, B, V with the relations

$$A^2 = V, B^2 = V, V^2 = E,$$

$$AV = VA, BV = VB, BA = VAB$$

(quaternion group). How many series containing more than one conjugate subgroup are there in $\mathfrak{Q}$?

¹ For typographical reasons the different colors are represented by drawing different kinds of lines.

Due to $A^2 = B^2, A^4 = E$ the 8 elements of Ω can be uniquely represented in the form $A^\mu B^\nu (\mu \bmod 4, 0 \leq \nu < 2)$. A, B, AB each generate a subgroup of type $\mathfrak{B}_4$; these are different and normal divisors. V generates a normal divisor of type $\mathfrak{B}_2$. There are no further proper subgroups.

3. Prove the distinctness of the five types of groups of order 8 which arise from the previously given groups, namely, $\mathfrak{B}_8, \mathfrak{B}_4 \times \mathfrak{B}_2, \mathfrak{B}_2 \times \mathfrak{B}_2 \times \mathfrak{B}_2, \mathfrak{D}_4, \Omega$. Furthermore, show that there are no further group types of order 8.

The distinctness can be seen from the distinctness of the graphs. However, we do not have to make full use of these graphs. For example, the first three types are surely different from the last two (Abelian versus non-Abelian); furthermore, the first three are different from one another (Section 3, Exer. 16); finally, so also are the last two (property in Exer. 2).—That the indicated system of Abelian type is complete follows from Section 3, Exer. 15. A non-Abelian group $\mathfrak{G}$ of order 8 may contain an element A of order 4. Such an element must generate a normal divisor $\mathfrak{R}$. Furthermore, if $\mathfrak{G} = \mathfrak{R} + \mathfrak{R}B$, then we must have $B^{-1}AB = A^{-1}$ and B^2 in $\mathfrak{R}$, and this leads to $\mathfrak{D}_4$ or Ω according as $B^2 = E$ or not. Therefore, all that we still have to do is to exclude the case of a non-Abelian group in which all elements $\neq E$ have the order 2. This is easily done by showing that $A^2 = E, B^2 = E, (AB)^2 = E$ implies the commutativity of A and B .

4. Under the assumptions of Theorem 109 for an infinite ground field K construct an element β of N belonging to a given subgroup $\mathfrak{F}$ of $\mathfrak{G}$ (Def. 36). For this purpose start from a primitive element ϑ of N .

Take as a basis the characterization of such an element β given in Theorem 112 and set β in the form

$$\beta = (a - \vartheta_{A_1}) \cdots (a - \vartheta_{A_m}),$$

where $A_1, \dots, A_m$ are the elements of $\mathfrak{F}$, and a a suitable element of K to be determined. For this determination use Theorem 49 [208].

5. Apply Theorem 114 to $K = P$, the root field of the polynomial

$$x^3 - 2 \equiv (x - \sqrt[3]{2})(x - \rho\sqrt[3]{2})(x - \rho^2\sqrt[3]{2}) \quad \left(\text{where } \rho = \frac{-1 + \sqrt{-3}}{2} \right)$$

as N and $\vartheta = \sqrt[3]{2} + a\rho\sqrt[3]{2}$ ($a \neq 0, \pm 1$ in P ; see Section 13, Exer. 2) and determine the decompositions (1) to (4), given there, for the two different subfield types $\Lambda = P(\sqrt[3]{2})$ and $\Lambda = P(\sqrt{-3})$.

(ϑ is the dihedral group $\mathfrak{D}_3$ (Section 16, Exer. 5), therefore given by $A^3 = E, B^3 = E, AB = BA^{-1}$. By choosing A and B suitably among equally qualified elements (conjugates) we have

$$\vartheta_A = \rho\sqrt[3]{2} + a\rho^2\sqrt[3]{2} = \rho\vartheta, \vartheta_B = \sqrt[3]{2} + a\rho^2\sqrt[3]{2}.$$

Everything easily follows from this.

6. Show that the element $\vartheta = \alpha_1 + a\alpha_2$ constructed in the proof to Theorem 90 [251] is a root of a polynomial over K of degree $n_1 n_2$.

In order to prove that the polynomial

$$g(x) \equiv \prod_{\nu_1=1}^{n_1} \prod_{\nu_2=1}^{n_2} (x - \vartheta_{\nu_1 \nu_2}) \equiv \prod_{\nu_1=1}^{n_1} \prod_{\nu_2=1}^{n_2} (x - \alpha_{1\nu_1} - a\alpha_{2\nu_2})$$

belongs to K , first show that

$$\phi(x, x') \equiv \prod_{\nu_2=1}^{n_2} (x - x' - a\alpha_{2\nu_2})$$

has coefficients in K and then that

$$g(x) \equiv \prod_{\nu_1=1}^{n_1} \phi(x, \alpha_{1\nu_1})$$

has coefficients in K . In both cases do so by applying Theorem 107 [271] and Theorem 112 to the coefficients as elements of the root fields of $f_1(x)$ and $f_2(x)$.

7. Let $f(x) \equiv (x - \alpha_1) \cdots (x - \alpha_n)$ be an irreducible separable polynomial over K resolved into linear factors in the root field W . Prove that the elements $\alpha_1 + \alpha_2, \alpha_1 \alpha_2$, and in general

$\vartheta = (\alpha_1 + \alpha_2) + a\alpha_1\alpha_2$ with arbitrary a in K , are roots of polynomials over K of degree $\binom{n}{2} = \frac{n(n-1)}{2}$.

This can be deduced just as in Exer. 6, except that in this case only one step is needed, by considering the polynomial

$$g(x) \equiv \prod_{\{i, k\}} (x - \vartheta_{ik}),$$

where $\vartheta_{ik} = (\alpha_i + \alpha_k) + a\alpha_i\alpha_k$, and $\{i, k\}$ runs through the $\binom{n}{2}$ combinations of second order of the numbers $1, \dots, n$. For this purpose take Vol. 1, Theorem 59 [121] into consideration.

8. In Exer. 7 assume in addition that K is infinite, and let a be determined as in the proof to Theorem 90 [251] so that the ϑ_{ik} are all different from one another. Prove that in this case $\alpha_1 + \alpha_2$ and $\alpha_1\alpha_2$ belong to the subfield $K(\vartheta)$ of W .

Represent the automorphisms of the Galois group of W as permutations of the α_i . In this form they map ϑ into a certain subset of the $\vartheta_{i,k}$ and $\alpha_1 + \alpha_2, \alpha_1\alpha_2$ into the corresponding subset of the $\alpha_i + \alpha_k, \alpha_i\alpha_k$. According to the choice of ϑ the subgroup belonging to $K(\vartheta)$, with respect to its representation by permutations of the α_i , leaves the combination $\{1, 2\}$ invariant, and consequently also $\alpha_1 + \alpha_2$ and $\alpha_1\alpha_2$. The statement then follows from Theorem 109, (1b).

9. On the basis of Exer. 7, 8, and in connection with Section 11, Exer. 1, prove by mathematical induction on the power of 2 involved in the degree n that every irreducible polynomial $f(x)$ over the field K of all real numbers has a root in the field Λ of all complex numbers (so-called *Fundamental Theorem of Algebra*).

Note that if n is even, the exponent of 2 in $\binom{n}{2}$ is one less than that in n . Furthermore, note that α_1 and α_2 are the roots of the quadratic polynomial $x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2$ over $K(\alpha_1 + \alpha_2, \alpha_1\alpha_2)$, and that every quadratic polynomial is reducible in $\Lambda = K(i)$:

$$\sqrt{a} + bi = \pm \left(\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + \operatorname{sgn} b \sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}} i \right) \quad (a, b \text{ real}).$$

10. Let the Galois group $\mathcal{G}$ of a separable normal extension N of finite degree over K be the direct product of the subgroups $\mathfrak{H}_1, \dots, \mathfrak{H}_r$ (Section 3, Exer. 9). Introduce the subfields N_i which are associated to the composites $\mathcal{G}_i$ of $\mathfrak{H}_k$ ($k \neq i$) according to the Fundamental Theorem of the Galois Theory, and describe the structure of N through these subfields N_i .

According to Theorems 109, 110, Corollary we find: N is the composite of the N_i , and the intersection of N_i with the composite of the N_k ($k \neq i$) is K . The Galois group of N_i is isomorphic to $\mathfrak{H}_i$.

11. N is called the *direct composite* of the normal subfields N_i if N is the composite of the N_i and every N_i has the intersection K with the composite of the N_k ($k \neq i$).—As a converse to Exer. 10, prove that in this case $\mathcal{G}$ is the direct product of subgroups $\mathfrak{H}_i$ which are isomorphic to the Galois groups of the N_i .

This follows as above from Theorems 109, 110, Corollary.

12. Use this to reduce the structure of separable Abelian extensions to the structure of separable cyclic extensions.

Apply the Fundamental Theorem of finite Abelian groups (Section 3, Exer. 15).

13. As in Section 16, Exer. 11, let $f(x)$ be an irreducible separable polynomial over K of prime degree p with linear Galois group $\mathcal{G}$. Furthermore, let α_1, α_2 be any two different roots of $f(x)$. Prove that $K(\alpha_1, \alpha_2)$ is already identical with the root field W of $f(x)$.

$\mathcal{G}$ can be represented as a linear permutation group $\mathfrak{L}_p^{(d)}$ (Section 16, Exer. 8, 11) of the indices of the suitably arranged roots $\alpha, \alpha', \dots, \alpha^{(p-1)}$ of $f(x)$. This arrangement $\alpha^{(k)}$ can be subjected at the beginning to a fixed linear permutation of the form $ka \rightarrow ka_0 + b_0(a_0 \neq 0, b_0$ in P_p), and this linear permutation can be (uniquely) normalized so that α, α' are precisely the two given roots α_1, α_2 . As subfields of W , $K(\alpha)$ and $K(\alpha')$ then belong to those subgroups of $\mathfrak{L}_p^{(d)}$ which

leave the elements 0 and e , respectively, of P , fixed. In the symbolism of Section 16, Exer. 8, 11, these are the cyclic subgroups generated by $B_0 = B^{\frac{p-1}{d}}$ and by $A^{-1}B_0A$. According to Theorem 110 we have to show that the intersection of these two subgroups is the identity subgroup.

14. In the special case $K = P, p \neq 2$, what conclusion can be drawn from this result regarding the realness of the roots of $f(x)$ in the field of all complex numbers? To which of the two types does the cyclic $f(x)$ belong?

Take Section 11, Exer. 1 into consideration.

15. Under the assumptions of Exer. 13 resolve $f(x)$ into irreducible factors in the stem field $\Sigma = K(\alpha)$ of a root α of $f(x)$.

Σ is a subfield of W . Hence according to the explanation to Exer. 13, Σ belongs to the cyclic subgroup generated by B_0 . Therefore, W is cyclic of degree d over Σ ; furthermore, by Exer. 13, $W = \Sigma(\alpha') = \dots = \Sigma(\alpha^{(p-1)})$. This easily yields that $\frac{f(x)}{x-\alpha}$ resolves in Σ into $\frac{p-1}{d}$ irreducible factors of degree d whose roots in each case are the sets $\alpha^{(k)}$ with k congruent mod $\frac{p-1}{d}$.

16. Let $f(x)$ be an irreducible separable polynomial in K and W its root field. Describe the decomposition of $f(x)$ into irreducible factors in a subfield Λ of W over K , starting from the representation of the Galois group of W by permutations of the roots of $f(x)$. In particular, subsume Exer. 15 in this general situation.

Apply Section 16, Exer. 2, combined with Theorem 109.

18. Dependence on the Ground Field

1. By means of a counterexample show that the degree relations in Theorem 119 (I) are not valid unless N is normal.

In order to avoid difficulties with the free composition, start from a suitable field $\bar{N}$ over K and choose N and also $\bar{A}$ as subfields *not* normal over K with the composite $\bar{N}$. It is enough to take $\bar{N}$ as a normal separable field with the Galois group $\mathfrak{D}_3 \cong \mathfrak{S}_3$ (see Section 17, Exer. 1), or we can also take Section 17, Exer. 13 as a more general starting point.

2. In Theorem 119 let $\bar{A} = K(x)$. Prove that in this case the intersection is $A = K$. Use this to illustrate the meaning of the remaining statements of Theorem 119 for this case.

At any rate, A is separable of finite degree, therefore simple algebraic over K . Hence it amounts to showing that $K(x)$ has no simple algebraic subfields over K except for K itself. Apply Section 7, Exer. 5, as well as Theorem 71 [228], or also simply Vol. 1, Section 4, Exer. 4.

3. Let N_1, N_2 be separable normal extensions of finite degree over K . Prove that in this case their free composite $N = \{N_1, N_2\}$ and their intersection $N_0 = [N_1, N_2]$ are also separable normal over K .

The normality of the composite of N over K follows immediately from the Def. 29 [255] of normality by noting that the free composite within any extension A containing it is the ordinary composite. The separability of N over K follows likewise according to Theorem 90 [251]. For the intersection N_0 see Theorem 119 (III).

4. In connection with Exer. 3, let $\mathfrak{G}_1, \mathfrak{G}_2, \mathfrak{G}$ be the Galois groups of N_1, N_2, N over K and $\mathfrak{G}_{01}, \mathfrak{G}_{02}$ the normal divisors of $\mathfrak{G}_1, \mathfrak{G}_2$ associated to the normal subfield N_0 of N_1, N_2 . Then $\mathfrak{G}_1/\mathfrak{G}_{01} \cong \mathfrak{G}_2/\mathfrak{G}_{02}$ (Galois group of N_0). Show that the type of $\mathfrak{G}$ is uniquely determined by the types of $\mathfrak{G}_1$ and $\mathfrak{G}_2$ as well as by giving the isomorphism between $\mathfrak{G}_1/\mathfrak{G}_{01}$ and $\mathfrak{G}_2/\mathfrak{G}_{02}$. In other words, show that $\mathfrak{G}$ is isomorphic to that subgroup $\bar{\mathfrak{G}}$ of the direct product $\mathfrak{G}_1 \times \mathfrak{G}_2$ which consists of elements

whose uniquely determined components S_1 of $\mathfrak{G}_1$, S_2 of $\mathfrak{G}_2$ belong to the associated residue classes relative to $\mathfrak{G}_{01}, \mathfrak{G}_{02}$ with respect to that isomorphism.

Any automorphism S of $\mathbf{N}$ is uniquely characterized by the two automorphisms S_1, S_2 of $\mathbf{N}_1, \mathbf{N}_2$ induced by it, and to the multiplication of S thereby corresponds the elementwise multiplication of the associated pair (S_1, S_2) . Therefore, $\mathfrak{G}$ is isomorphic to a subgroup $\bar{\mathfrak{G}}$ of the group of all those pairs with respect to elementwise multiplication, that is, of the direct product $\mathfrak{G}_1 \times \mathfrak{G}_2$. From the behavior of the elements of $\mathbf{N}_0$ we immediately establish that $\bar{\mathfrak{G}}$ is, at any rate, a subgroup of the subgroup $\bar{\mathfrak{G}}$ of $\mathfrak{G}_1 \times \mathfrak{G}_2$ specified in the statement. It suffices, therefore, to prove in addition that $\mathfrak{G}$ and $\bar{\mathfrak{G}}$ have the same order. The order of $\mathfrak{G}$ is known by Theorem 119; the order of $\bar{\mathfrak{G}}$ is easily determined directly from the definition.—Be sure not to write the elements (S_1, S_2) of $\mathfrak{G}_1 \times \mathfrak{G}_2$ simply as products $S_1 S_2$; for S_1 and S_2 cannot actually be multiplied in the sense of Theorem 104 [265], since they are automorphisms of two different fields $\mathbf{N}_1, \mathbf{N}_2$. Rather, the only meaningful expression of this as a product is

$$(S_1, S_2) = (S_1, E_2) (E_1, S_2) \quad (E_1, E_2 \text{ the unity elements of } \mathfrak{G}_1, \mathfrak{G}_2).$$

Here the factors $\bar{S}_1 = (S_1, E_2), \bar{S}_2 = (E_1, S_2)$ run through groups $\bar{\mathfrak{G}}_1, \bar{\mathfrak{G}}_2$ isomorphic to $\mathfrak{G}_1, \mathfrak{G}_2$. $\bar{\mathfrak{G}}_1 \times \bar{\mathfrak{G}}_2$ then turns out to be the realization of the type $\mathfrak{G}_1 \times \mathfrak{G}_2$ taken here as a basis.

5. Let $f(x), g(x)$ be two irreducible separable polynomials on $\mathbf{K}$ of degree m, n ; furthermore, let α, β be roots of $f(x), g(x)$ respectively and

$$f(x) \equiv \phi_1(x) \dots \phi_r(x)$$

$$g(x) \equiv \psi_1(x) \dots \psi_s(x)$$

be the decompositions of $f(x), g(x)$ in $\mathbf{K}(\beta), \mathbf{K}(\alpha)$ into irreducible factors. Prove that $r = s$ and that the degrees m_i, n_i of the $\phi_i(x), \psi_i(x)$ (with respect to a suitable ordering) satisfy

the relation $\frac{m_i}{n_i} = \frac{m}{n}$ (Kronecker's Theorem).

Represent the Galois group $\mathfrak{G}$ of the root field W of $f(x)g(x)$ as a permutation group of the roots α_i, β_k of $f(x), g(x)$. The structure of $\mathfrak{G}$ in Exer. 4 corresponds then to the decomposition of these permutations according to the two systems of elements connected transitively by $\mathfrak{G}$; namely, on the one hand, to the system of the α_i and, on the other hand, to the system of the β_k (Section 16, Exer. 2). If $\mathfrak{H}_\beta$ is the subgroup of $\mathfrak{G}$ belonging to $K(\beta)$, then the decomposition of $f(x)$ in $K(\beta)$ corresponds to the different systems of $\mathfrak{H}_\beta$ connected transitively with respect to α_i (somewhat more general than in Section 17, Exer. 16), and the comparison of degrees in $K(\alpha_i, \beta)$ yields $m, n = m\bar{n}_i$, where $\bar{n}_i$ is the degree of the irreducible factor $\bar{\psi}_i(x)$ of $g(x)$ in $K(\alpha_i)$ belonging to β . It must now be shown on the basis of the structure of $\mathfrak{G}$ obtained in Exer. 4 that the r polynomials $\bar{\psi}_i(x)$, where α_i runs through just one root from each $\phi_i(x)$, are biuniquely associated to the irreducible factors $\psi_i(x)$ of $g(x)$ in $K(\alpha)$. For this purpose apply to $\bar{\psi}_i(x)$ in each case an automorphism S_i of $\mathfrak{G}$ which will map α_i on α . For reasons of symmetry it is enough merely to show that the correspondence is unique in one direction, say, that the polynomials $\psi_i(x) \equiv \bar{\psi}_{i,s_i}(x)$ generated by the S_i are all different from one another. This would mean that $s \geq r$.

6. Carry out the decompositions of Exer. 5 in the simple special case of the two irreducible polynomials $x^6 - 2, x^9 - 2$ over P .

7. Carry out the proof of the theorems of Section 17, Exer. 14 by extending P to the field of all real numbers $\bar{P}$ and applying Theorem 119.

If $f(x)$ has at least one non-real root, then the transition to the conjugate complex is an automorphism of order 2 for the root field, therefore the power $B_0 = B^{\frac{p-1}{2}}$ by suitably normalizing the B in Section 16, Exer. 8. By the extension to $\bar{P}$ the Galois group $\mathfrak{G}^{(d)}$ must reduce to a subgroup of order 2, which is determined by B_0 belonging to it. Then apply Section 16, Exer. 2.

Vol. 2. Chapter V. Solvability of Algebraic Equations by Radicals

19. Definition of Solvability by Radicals

1. Give an example of an element α algebraic over a field K such that α is the root of a pure polynomial (of degree higher than the first) over a proper extension $\bar{K}$ of K , but not a root of a pure polynomial over K (cf. footnote 2).

Take, for instance, $K = \mathbb{P}, \bar{K} = \mathbb{P}(\sqrt{2})$. Then numbers $\alpha_0 = a + b\sqrt{2}$ can easily be found in $\mathbb{P}(\sqrt{2})$ which are not squares in $\mathbb{P}(\sqrt{2})$ and all of whose powers (different from 1) do not lie in $\mathbb{P}$. For the former use the fact that if $\alpha_0 = a + b\sqrt{2}$ is a square in $\mathbb{P}(\sqrt{2})$, then $\bar{\alpha}_0 = a - b\sqrt{2}$ is also, so that $\alpha_0\bar{\alpha}_0 = a^2 - 2b^2$ must be a square in $\mathbb{P}$. Then, a root α of $x^2 - \alpha_0$ satisfies the stated conditions.

2. Show that a polynomial of the form $f(x) \equiv x^4 + ax^2 + b$ over a field with characteristic different from 2 can always be solved by radicals.

It is easy to find the pure equations which can be used to construct the roots of $f(x)$. Regarding the irreducibility of these equations note that the four roots of $f(x)$ must have the form $\pm\alpha, \pm\beta$. This implies that $f(x)$ is irreducible only if $f_0(x_0) \equiv x_0^2 + ax_0 + b$ is irreducible, that is, only if $a^2 - 4b$ is not a square in the ground field. In this case the first of the two pure equations under consideration is irreducible, though the second need not be. (Give a counterexample.) In order that the latter also be irreducible it is necessary and sufficient, if $b = b_0^2$ is in the ground field, that neither $-a + 2b_0$ nor $-a - 2b_0$ be squares in the ground field. This additional condition together with the irreducibility of $f_0(x_0)$ turns out to be sufficient for the irreducibility of $f(x) \equiv f_0(x^2)$.

3. Show that a polynomial $f(x)$ of degree 6 over a field with characteristic different from 2 which has the properties $x^6 f\left(\frac{e}{x}\right) \equiv -f(x), f(-x) \equiv f(x)$ can always be solved by radicals.

On splitting off the linear factor $x^2 - e$ we come to the case of Exer. 2.

20. Cyclotomic Fields. Finite Fields

1. Compute the discriminant (Section 6, Exer. 18) of the polynomial $x^n - e$.

The simplest thing to do is to use Section 6, Exer. 18 (b) and the last of Vieta's formulas (Section 5, Exer. 13). We can also combine Section 6, Exer. 17, 19.

2. In order to prove that there exists at least one primitive n -th root of unity, and even that there are exactly $\phi(n)$ such roots (Theorem 120 and Corollary) we can also proceed as follows: First, show that the roots of $x^n - e$ are distinct (under the restriction regarding the characteristic). Then, through multiplication and division construct a polynomial $g_n(x)$ from the polynomials $x^t - e$, where t runs through suitable divisors of n , in which just those linear factors of $x^n - e$ occur, and only once, which do not appear in $x^d - e$ for any proper divisor d of n . In doing this, we obtain at the same time an explicit construction for the polynomial $g_n(x)$ of Theorem 121. Write this formula for $g_n(x)$ by means of the following number-theoretic function: $\mu(n) = 0$, in case n contains the square of a prime number, $\mu(n) = (-1)^r$ in case n is composed of r different prime numbers, in particular $\mu(1) = 1$ for $r = 0$ (*Möbius function*).

If $p, p', p'', \dots$ are the different prime factors of n , then as a basis for t it is enough to take divisors of the types $n; n_1 = \frac{n}{p}, \frac{n}{p'}, \frac{n}{p''}, \dots;$

$n_2 = \frac{n}{pp'}, \frac{n}{pp''}, \frac{n}{p'p''}, \dots; \dots$ Let $P_0 = x^n - e$ and $P_1 = \prod_{n_1} (x^{n_1} - e)$.

Then $\frac{P_0}{P_1}$ has just the desired linear factors in the numerator, but in general also some of these factors in the denominator. In $\frac{P_0 P_2}{P_1}$ the latter are missing, with some undesirable linear factors, however, generally appearing in the numerator, etc. Let $g_n(x)$ be the polynomial finally generated. Compute its degree according to the explicit formula for $\phi(n)$ (see Section 2, Exer. 14).

3. Prove in general (without the restriction regarding the characteristic): If $n \mid m$, then $T_n \leq T_m$. If $n = n_1 n_2$ with $(n_1, n_2) = 1$, then $T_n = \{T_{n_1}, T_{n_2}\}$.

For the latter apply Section 3, Exer. 10 to the group of the n -th roots of unity.

4. Prove (at first, again with the restriction regarding the characteristic): If $n = n_1 \cdots n_r$ is a decomposition into pairwise relatively prime factors, then T_n is the direct composite (Section 17, Exer. 11) of $T_{n_1}, \dots, T_{n_r}$.

Apply Theorem 121, Section 17, Exer. 10, as well as Section 2, Exer. 12.

5. How are the results in Theorems 120, 121 and in Exer. 2, 4 to be modified if the restriction regarding the characteristic of K is dropped?

If K has the characteristic p and $n = p^r n_0$ with $(n_0, p) = 1$, then $T_{p^r} = K$ (Theorem 122, Corollary), therefore $T_n = T_{n_0}$ by Exer. 3.

6. The *Eisenstein-Schönemann Theorem* says: If

$$f(x) \equiv x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

is a polynomial in $\Gamma[x]$ which has the properties $p \mid a_1, \dots, p \mid a_n$ and $p^2 \nmid a_n$ for a prime number p , then $f(x)$ is irreducible in P .— Prove this by assuming that there is a proper decomposition $f = gh$ in the residue class ring $\Gamma[x]_p$ of $\Gamma[x]$ relative to the

prime element p . Such an assumption is permissible according to Gauss's Theorem (Section 2, Exer. 24).

$\Gamma[x]_p$ is isomorphic to $\Gamma_p[x] = \mathbb{P}_p[x]$ (explanation to Section 2, Exer. 23). We have $f \equiv x^n \pmod{p}$ and x^n has in $\mathbb{P}_p[x]$ only the trivial decompositions $x^n = x^\mu x^\nu$ ($\mu + \nu = n$). This means that

$$g \equiv x^\mu, h \equiv x^\nu \pmod{p}$$

would be true which contradicts $a_n \not\equiv 0 \pmod{p^2}$ on substituting $x = 0$.

7. From this deduce the irreducibility of

$$g_p(x) \equiv \frac{x^p - 1}{x - 1} \equiv x^{p-1} + x^{p-2} + \cdots + x + 1 \text{ in } \mathbb{P}.$$

The Eisenstein-Schönemann Theorem can be applied to $g_p(x+1)$ (see proof to Theorem 44 [204]).

8. In order to prove that $g_n(x)$ is also irreducible in $\mathbb{P}$ if n is a composite number, consider the irreducible polynomial $f(x)$ in $\mathbb{P}$ belonging to a primitive n -th root of unity ζ and successively prove:

(a) The coefficients of the representation of $f(\zeta^k)$ through the basis $1, \zeta, \dots, \zeta^{r-1}$ (r the degree of f) of T_n are integral rational numbers. They depend only on the residue classes of $k \pmod{n}$.

(b) For prime numbers $k = p$ these coefficients are all divisible by p . For sufficiently large prime numbers p they are actually all equal to 0.

(c) $f(\zeta^m) = 0$ for every m prime to n .

(d) $g_n(x) = f(x)$, therefore $g_n(x)$ is irreducible in $\mathbb{P}$.

(Proof developed on 8 lines by Landau, *Mathematische Zeitschrift* (Journal of Mathematics), 29 [1929].)

For (a) apply Section 9, Exer. 8 and again take the Gaussian Theorem into consideration (Section 2, Exer. 24). For (b) make use of the congruence $f(x^p) - f(x)^p \equiv 0 \pmod{p}$ (Theorem 44 [204]) which is valid in $\Gamma[x]$ and note, furthermore, that a multiple a of p with

$|a| < p$ must be equal to 0. For (c) prove the existence of an $m' \equiv m \pmod{n}$ which is not divisible by finitely many given prime numbers $p_1, \dots, p_s$ (say on the basis of Section 2, Exer. 12). For (d) apply Theorem 53 [210].

9. According to Theorems 121, 122, and Exer. 7, the cyclotomic field T_p over P is cyclic of degree $p-1$ and its Galois group $\mathfrak{G}_p$ is isomorphic to the group $\mathfrak{P}_p$ of the prime residue classes $\pmod{p}$. Let $\mathfrak{F}$ be any subgroup of $\mathfrak{G}_p$ of index j and $\mathfrak{Q}$ the associated subgroup of $\mathfrak{P}_p$. Prove that $\eta = \sum_q \zeta^q$, where q runs through a complete system of representatives of the residue classes of $\mathfrak{Q}$, is then an element of T_p belonging to $\mathfrak{F}$, that is, generates the subfield H of T_p belonging to $\mathfrak{F}$, therefore $H = P(\eta)$.— $\mathfrak{Q}$ is completely determined by j (Theorem 36 [199]). Represent q in terms of a primitive root $r \pmod{p}$ and j . Use this to represent η and its conjugates (the *m-termed cyclotomic periods*, where $mj = p-1$).

According to Theorems 111, 112 [283] it is sufficient to prove the distinctness of the j conjugates to η which correspond to the j residue classes of $\mathfrak{G}_p$ relative to $\mathfrak{F}$. If representatives of the residue classes of the reduced residue system $\pmod{p}$ are used in the ζ -exponents, an equality between two of these conjugates leads easily to a contradiction of the irreducibility of $g_p(x)$ in P , namely, to the fact that $g_p(x)$ is the polynomial of lowest degree in P which has ζ as a root.

10. Give a representation for the automorphism of the cyclotomic field T_p (p a prime number) over P induced by the non-identity automorphism $\alpha \rightarrow \bar{\alpha}$ of the field of all complex numbers including T_p , namely, by the automorphism determined by transition to the conjugate complex. How do the two-termed cyclotomic periods behave with respect to this automorphism?

$\bar{\zeta}$ is determined by the fact that $\zeta\bar{\zeta}$ is, on the one hand, positive real, on the other hand, a p -th root of unity. For the question note the discussion to Section 14, Exer. 8.

11. What is the discriminant of that irreducible quadratic polynomial in P whose roots are the $\frac{p-1}{2}$ -termed cyclotomic periods η, η' to p , therefore the square of

$$\tau = \eta - \eta' = \sum_{\mu \bmod p-1} (-1)^\mu \zeta^{r^\mu}$$

(quadratic *Gaussian sum* to p)? For this purpose first calculate the product $\tau\bar{\tau}$. Accordingly, how are η, η' represented in terms of square roots?

$\tau\bar{\tau}$ is a double sum. In this sum replace the summation letters μ, ν by $\mu' \equiv \mu - \nu, \nu' \equiv \nu \bmod p-1$ and then carry out first the summation over ν' . For the second question also calculate, in addition, $\eta + \eta'$. This is easily done.

12. Represent the 5-th roots of unity over P by square roots.

Exer. 11 yielded representations of the two-termed periods $\eta = \zeta + \zeta^4, \eta' = \zeta^2 + \zeta^3$. In virtue of the further relations

$$\zeta\zeta^4 = 1, \zeta^2\zeta^3 = 1$$

these representations immediately enable us to find for $p = 5$ the representations of the single-termed periods, therefore of the roots of unity themselves.

13. Represent the 17-th roots of unity over P by square roots, and from this develop a method for constructing with ruler and compass the regular polygon of seventeen sides.

Just as above, this objective is attained by successively forming the sum and product of two matching 8-termed, 4-termed, 2-termed, 1-termed periods. Base the geometric construction on the Pythagorean Theorem and, in addition, note the reduction given in the discussion

to Section 17, Exer. 9, whereby a square root of a complex number is reduced to square roots of real numbers.

14. As a corollary to the result of Gauss, prove: In order that $2^{\nu} + 1$ be a prime number for $\nu \geq 1$ it is necessary that ν be a power of 2.

Note that the polynomial $x^u + 1$ in $\Gamma[x]$ has the divisor $x + 1$ if u is odd. The statement easily follows from this if the substitution $x = 2^{\rho}$ is made.

15. Prove: This necessary condition is, however, not sufficient. While $2^{2^{\mu}} + 1$ is actually a prime number for $\mu = 0, 1, 2, 3, 4$, $2^{2^5} + 1$ is divisible by 641.

Naturally, it is possible to carry out the involution and consequent division. However, there is a much more elegant way of doing this: Start with the expressions $641 = 5^4 + 2^4$ and $641 = 2^7 \cdot 5 + 1$. Write these equations as congruences mod 641, raise the second one to the 4-th power and in this substitute the value 5^4 from the first.

16. Give a new proof of the formula for the determinant of an n -rowed circulant (Section 10, Exer. 19), for the case that the characteristic of K is not a prime number dividing n without remainder. For this purpose make use of the ideas applied in Section 4, Exer. 16.

First of all, establish for indeterminates that the determinant is divisible by the product of the linear forms in question. The consideration of the degree then shows that the quotient is a unit (element of K) which is easily determined by comparing coefficients.

17. Prove that there are irreducible polynomials of any given degree m over P_p .

Apply (IV) and (VIII).

18. Prove: The polynomial $x^{p^m} - x$ over P_p is the product of all the different irreducible polynomials over P_p whose degrees are divisors of m . From this calculate the number of irreducible polynomials over P_p of degree m .

The stem field to an irreducible polynomial $f(x)$ over $\mathbb{P}_p$ of degree μ is a finite field of p^μ elements. The statement easily follows from this by (III) to (VI). To determine the number of polynomials apply a process corresponding to that in Exer. 2 and write the enumerating formula by means of the Möbius function $\mu(n)$.

19. Prove: If K is a finite skew field (Vol. 1, Section 15, Exer. 2) of q elements and K_0 a skew subfield of K of q_0 elements, then q is a power of q_0 .

In analogy to Def. 24 [225] introduce in K the concepts of linear dependence and linear independence relative to left multiplication by elements of K_0 . Then prove the existence of a left basis of K relative to K_0 , where the basis is defined in analogy to Def. 25 [225].

20. Let the class $\mathfrak{C}_a$ of conjugate elements determined by an element a ($\neq 0$) of a skew field K , as well as the normalizer N_a of a (Vol. 1, Section 9, Exer. 13) and the centrum Z of K (Vol. 1, Section 7, Exer. 8), be interpreted in the sense of the multiplicative group of the elements $\neq 0$ of K .—Prove that the elements of N_a together with 0 form a skew subfield of K , and that the elements of Z together with 0 form a subfield of K and of N_a (with 0).

21. Next, let K be a *finite* skew field and z the number of elements of Z (with 0), so that the number of elements of K is therefore a power z^n and the number of elements of N_a (with 0) is a power z^{n_a} with $n_a | n$ (Exer. 19). How many elements are there in $\mathfrak{C}_a$ in this case?

Apply Vol. 1, Section 9, Exer. 13.

22. Now, let a run through a complete system of representatives for the classes of conjugate elements of the finite skew field K and express the number of elements of K (without 0) as the sum of the number of elements of the individual

classes $\mathfrak{C}_a$. In doing this collect the contribution of the classes with one element together into a single summand.

The classes with one element are just the classes arising from the elements of $\mathbf{Z}$ (without 0).

23. Finally, prove that the integral rational number $g_n(z)$ (Theorem 121) is a divisor of the left side as well as of all contributions on the right side of the resulting formula originating from classes of many elements. From this conclude that necessarily $n = 1$, therefore $\mathbf{K} = \mathbf{Z}$. Consequently: Any finite skew field is a field (*Wedderburn's Theorem*, proved by *Witt*).

First show that the divisibility is valid if the number z is replaced by an indeterminate x . Then apply Section 2, Exer. 24. Finally, by considering the absolute values of the linear factors of $g_n(x)$ for $x = z$, establish that $g_n(z) | z - 1$ is valid only for $n = 1$ (whereby $z > 1$ is to be taken into consideration).

21. Pure and Cyclic Extensions of Prime Degree

1. Calculate the discriminant (Section 6, Exer. 18) of $x^n - a$.

2. Calculate the resultant (Section 10, Exer. 23) of $x^{n_1} - a_1$ and $x^{n_2} - a_2$.

3. Prove the statements under (b) in Theorem 123 by a process analogous to that in Section 13, Exer. 4, 5.

Instead of the transition from $g(x)$ to $g(x - ne)$ appearing there, we have to go here from $g(x)$ to $g(\zeta^{-n}x)$ ($n = 1, \dots, p - 1$).

4. Prove: If the polynomial $f(x)$ of $\Gamma[x]$ is irreducible in $\mathbf{P}_p$ on passing over to the residue class ring $\Gamma[x]_p$, then it is also irreducible in $\mathbf{P}$.—Can the proof of Theorem 123, (b) be carried through in this way for a in Γ if $\mathbf{K} = \mathbf{P}$?

Make use of Section 2, Exer. 24 as well as Section 4, Exer. 8.

5. Assume that K is a field with characteristic different from p and that a is an element of K which is not a p -th power in K . Prove that the Galois group $\mathcal{G}$ of $x^p - a$ is linear (Section 16, Exer. 8). How is the d of Section 16, Exer. 11 determined? Also, verify Section 17, Exer. 14 by direct methods.

According to Theorems 123, 124 and Theorems 121, 123 [305, 312], $\mathcal{G}$ contains a cyclic normal divisor β of order p with cyclic factor group of order $d \mid p-1$. A generator A of β is obtained by $(\alpha \rightarrow \zeta\alpha)$, where α is a root of $x^p - a$ and ζ a primitive p -th root of unity. $\mathcal{G}$ can then be decomposed in the form $\sum_{r=0}^{d-1} B^r \beta$ relative to β , and B can be normalized so that $\alpha \rightarrow \alpha$ and according to Theorem 109, (V) [274], $\zeta \rightarrow \zeta^r$ is valid, where r is a primitive root mod p and $dn = p-1$. Then determine $B^{-1}AB$ and B^d .

6. Generalize the statements in Theorem 123 to a pure polynomial $x^n - a$ of composite degree n under the assumption that K contains the n -th roots of unity over K and the characteristic of K is not a prime number dividing n without remainder. What is the decomposition of $x^n - a$ into irreducible factors over K ? What is the representation of the Galois group of the root field W of $x^n - a$ over K ? of the subfield of W over K ?

It depends on the smallest exponent n_0 for which a^{n_0} is an n -th power in K and on its complementary divisors d in n . The power a^{n_0} ($n_0 = mj$) of a root of $x^n - a$ can be taken as a primitive element of the (uniquely determined) subfield of degree j .

7. Under the same assumptions regarding K let two arbitrary (not necessarily irreducible) pure polynomials $x^n - a_1$ and $x^n - a_2$ of degree n in K be given. Determine the Galois group $\mathcal{G}$ of the composite of their root fields W_1 and W_2 , and give a property which characterizes the degree d of

the intersection $[W_1, W_2]$. In particular, what relation between a_1 and a_2 is therefore necessary and sufficient for $W_1 \leq W_2$? for $W_1 = W_2$? (For $n = 2$, cf. Section 7, Exer. 9 to 11, already given.)

Apply the theory developed in Section 18, Exer. 4. Let α_1, α_2 each be one root. Then $\mathfrak{G}$ is represented by pairs of substitutions $(\alpha_1 \rightarrow \zeta^{v_1} \alpha_1, \alpha_2 \rightarrow \zeta^{v_2} \alpha_2)$, where the exponents v_1, v_2 are divisible by the analogues d_1, d_2 of the d in Exer. 6 and are tied to one another by a congruence condition which arises from the group isomorphism considered in Section 18, Exer. 4. For this purpose make use of the result of Theorem 37 [200] which enables us to survey all isomorphisms between two cyclic groups of the same order. The coefficients in the congruence condition between v_1, v_2 are not yet determined. In order to characterize them through the given a_1, a_2 so as to be able to answer the other questions, too, using only the given a_1, a_2 , it is advisable to calculate in the factor group $\mathfrak{K} = K^*/K^{*n}$, where K^* stands for the multiplicative group of K (Vol. 1, Section 6, Example 1 [61]). According to Vol. 1, Theorems 34, 35 [75], the elements of $\mathfrak{K}$ are the residue classes relative to a congruence relation $\equiv$ in K . If n_1, n_2 bear the same relation to W_1, W_2 that n_0 does to W in Exer. 6, then $a_1^{n_1} \equiv 1, a_2^{n_2} \equiv 1$ is valid, and a_1, a_2 generate cyclic subgroups $\mathfrak{A}_1, \mathfrak{A}_2$ of orders n_1, n_2 in $\mathfrak{K}$ which are isomorphic to the Galois groups $\mathfrak{G}_1, \mathfrak{G}_2$ of W_1, W_2 . Consider now all relations of the form $a_1^{v_1} a_2^{v_2} \equiv 1$ between the generators a_1, a_2 and show that they are all formal consequences of the two specified relations and of a single further one, where the latter involves the degree d and the previously given coefficients of v_1, v_2 . To do this study the behavior of the power products $a_1^{v_1} a_2^{v_2}$ in $\mathfrak{G}$. The resulting statement describes $\mathfrak{G}$ explicitly and characterizes d . Moreover, it is easily established that the Galois groups $\mathfrak{G}$ and $\mathfrak{G}_0$ of the composite and intersection of W_1, W_2 are isomorphic to the composite and intersection, respectively, of the subgroups $\mathfrak{A}_1, \mathfrak{A}_2$ of $\mathfrak{K}$.

8. In Exer. 7 we found a condition for $W_1 \leq W_2$. Derive this condition in still another way by representing α_1 through

the basis $e, \alpha_2, \dots, \alpha_2^{n_1-1}$ of W_2 and applying to this the automorphisms of W_2 .

Under the assumption $W_1 \leq W_2$ note that α_1 goes over to a conjugate whose basis representation can also be directly found, and make use of the uniqueness of the basis representation.

9. The analogue to Theorem 124 for fields of characteristic p is given by Section 13, Exer. 4 (cf. also Section 15, Exer. 4). As a converse to this, now prove the analogue to Theorem 125 for fields of characteristic p , namely, the theorem: Over such a field K any separable normal extension of degree p is a root field of a polynomial of the form $x^p - x - a$.

The proof can be carried out in close analogy to the proof of Theorem 125. Instead of the summands $\zeta^{-\mu\nu} \partial_{A\mu}$ take here the expressions $\frac{-\mu \partial_{A\mu}}{s_\nu}$ as summands, where $s_\nu = \sum_{\mu=0}^{p-1} \partial_{A\mu}^\nu$. Corresponding to the second part of the proof, show that ν can be chosen so that the element $s_\nu \neq 0$ (belonging to K) (this conclusion can be drawn from the determinant $|\partial_{A\mu}^\nu|$, separability). For the first part of the proof use

$$x^p - x \equiv x(x-e) \cdots (x-(p-1)e)$$

(Section 5, Exer. 1) and the formula arising from this by the replacement of x by $x - \alpha$.

10. Under the same assumptions regarding K as in Exer. 6, 7, prove the generalization of Theorem 125: Every cyclic extension of n -th degree is pure over such a K .

The extension is automatically separable due to the restriction on the characteristic (Def. 17 [214] and Theorem 79 [237]). The first part of the proof of Theorem 125 makes use of the primeness of p only insofar as the normality implies the cyclicity. Modify the second part (in analogy to Exer. 9) in such a way that the primitive n -th root of unity ζ is retained but ∂ is replaced by the powers $\partial, \partial^2, \dots, \partial^{n-1}$.

11. Prove that in order to form the Lagrange resolvents (in the sense of Exer. 10) of η , where η is an m -termed

cyclotomic period to p (Section 20, Exer. 9), we can get along with the first power of η . This means that the *Gaussian sums* of n -th degree to p :

$$\tau(\epsilon) = \sum_{\nu=0}^{n-1} \epsilon^{-\nu} \eta^{(\nu)}, \quad \text{where} \quad \eta^{(\nu)} = \sum_{\mu \bmod m} \zeta_{r^{\nu+\mu n}}$$

(ζ primitive p -th, ϵ primitive n -th root of unity over $\mathbb{P}$;
 r primitive root mod p ; $p-1 = mn$)

are different from zero. Furthermore, to generalize Section 20, Exer. 11, calculate $\tau(\epsilon) \cdot \overline{\tau(\epsilon)}$ and reduce $\tau(\bar{\epsilon})$ also to $\overline{\tau(\epsilon)}$, in analogy to Section 20, Exer. 10.

As in Section 20, Exer. 9, $\tau(\epsilon) = 0$ yields a contradiction to the irreducibility of $g_p(x)$, in $\mathbb{T}_n$ now (Section 20, Exer. 4). For the rest proceed analogously to the special case $n = 2$.

12. Give a necessary and sufficient condition that $\tau(\epsilon)^n$ be a rational number.

By applying the automorphisms of $\mathbb{T}_n$ to $\tau(\epsilon)^n$ obtain relations of the form $\tau(\epsilon^s) = \epsilon^{as} \tau(\epsilon)$ for any s prime to n ; from this (analogously to Exer. 11) it is easy to show that $s \equiv 1 \pmod{n}$ only for $n = 2$, except for the trivial case $n = 1$.

13. Find the cubic polynomial in $\mathbb{P}$ whose roots are the two-termed cyclotomic periods η, η', η'' for the prime number 7, as well as the third powers of the two associated cubic Gaussian sums $\tau, \bar{\tau}$. For the latter use the rational representation of the sums by $\sqrt{-3}$.

Find the relations $\eta + \eta' + \eta'' = -1$ and $\eta\eta' = \eta + \eta''$. Through these the desired cubic polynomial is easily obtained on the basis of Vieta's formulas (Section 5, Exer. 13). In order to compute $\tau^3, \bar{\tau}^3$ take the relations $\tau\bar{\tau} = 7$ (Exer. 11) and $\tau + \bar{\tau} = 3\eta + 1$ into consideration, and then compute $\tau^3 + \bar{\tau}^3$ by having recourse to the cubic equation for η .

14. Represent the 7-th roots of unity over $\mathbb{P}$ by radicals.

The result of Exer. 13 enables us to obtain rational representations of the two-termed periods η, η', η'' through cube roots of numbers from $T_3 = P(\sqrt{-3})$ by solving a system of linear equations. The 7-th roots of unity themselves can then be obtained by using the pair of relations $\zeta + \zeta^6 = \eta, \zeta\zeta^6 = 1; \dots$

15. Show that the representation of the 7-th roots of unity over P by radicals can also be obtained by using as intermediate steps the three-termed periods ϑ, ϑ' , which have already been represented rationally through $\sqrt{-7}$ in Section 20, Exer. 11.

For this purpose extend the ground field P to $T_3 = P(\sqrt{-3})$. Next, represent the third powers of the Lagrange resolvents $\lambda, \hat{\lambda}; \lambda', \hat{\lambda}'$ rationally in terms of $\sqrt{-3}$ and $\sqrt{-7}$, where the resolvents belong to the extended cyclotomic field $\{T_7, T_3\} = T_{21}$. Then the 7-th roots of unity themselves are again obtained by solving a system of linear equations.

16. The significance of the cubic polynomial $f(x)$ of Section 15, Exer. 5 (b) was shown in Exer. 13. Now use the representation $\eta = \zeta + \zeta^6 = \zeta + \zeta^{-1}$ of a root of $f(x)$ to illustrate the meaning of the property given there.

17. Use this knowledge to characterize the root field of the cubic polynomials in Section 15, Exer. 5 (a).

Go over to $g(y) \equiv y^3 f(y + y^{-1})$.

18. Prove in general: For prime numbers $p \neq 2$, T_{p^v} is cyclic over P , and also the direct composite of T_p and a cyclic field of degree p^{v-1} over P .

Note that the prime residue class group $\mathfrak{P}_{p^v}$ contains the element $1+p$ of order p^{v-1} and surely an element r of order $p-1$ at least, and apply Section 3, Exer. 10. Accordingly, how is it always possible to normalize a primitive root $r \bmod p$ for the study of $\mathfrak{P}_{p^v}$?

19. Prove analogously: In the sense of Section 3, Exer. 16, $\mathfrak{P}_{2^v}$ has the prime power invariants $2, 2^{v-2}$. Therefore, what

is the structure of T_{2^v} over P ? What are the subfields that belong to the (single) cyclic subgroup of order 2^{v-2} ?

The element 5 is mod 2^v of order 2^{v-2} and is independent of -1 . In order that a 2^v -th root of unity ζ be invariant with respect to the automorphisms corresponding to the residue class of 5, $\zeta^4 = 1$ must be valid.

20. Assuming the representation of the p -th roots of unity as known, represent the p^v -th roots of unity over P by radicals. Then represent the n -th roots of unity for arbitrary n . Accordingly, for which n alone can the regular n -gon be constructed by ruler and compass?

The polynomials $x^{p^v-1} - \zeta$ (ζ primitive p -th root of unity, $p \neq 2$) and $x^{2^v-1} - i$ are irreducible in T_p and T_4 , respectively. Furthermore, the former remains irreducible also in the extension of T_p by those roots of unity which are required according to Theorem 126 for the solution of T_{p^v} . This is easily confirmed on the basis of the determination of the degree in Theorem 121 [305] and by Section 20, Exer. 8. For composite n , see the discussion to Section 20, Exer. 4. The constructibility follows by a trivial reduction to prime powers p^v in analogy to the special case $v = 1$ (Result of Gauss [308]).

21. Represent the 257-th and 65,537-th roots of unity by reducible radicals (radicals of reducible pure polynomials).

$x^{257} - 1$ and $x^{65537} - 1$ are reducible pure polynomials.—Accordingly, show that nothing is gained by allowing reducible radicals to be used for investigating the algebraic structure of cyclotomic fields (cf. footnote 1 before Def. 39 [303]).

22. Find a primitive element of the cyclic field H which is of degree p over P and is contained in the cyclotomic field T_{p^2} ($p \neq 2$) over P .

If ζ is a primitive p^2 -th root of unity over P , then set up the $p-1$ conjugates to ζ relative to H with the help of a primitive root $r \bmod p$ normalized according to the explanation to Exer. 18. In

analogy to Exer. 11 it is again sufficient to show that for this sum η the p conjugates $\eta, \eta', \dots, \eta^{(p-1)}$ relative to P are different from one another. Instead of this, however, we can proceed as follows: First note that due to the normality these conjugates all belong to H , and secondly that by Theorem 111 [283] they are either all different and consequently primitive elements of H , or are all equal and consequently already in P . Now these conjugates are connected with the p -termed system consisting of 0 and the $p-1$ conjugates ζ^{ν} ($\nu = 0, \dots, p-2$) of ζ relative to H by a system of linear equations over T_p with regular matrix. This follows by using in the representations

$$\eta^{(\mu)} = \sum_{\nu=0}^{p-2} \zeta^{\nu(1+p)^{\mu}} \quad (\mu = 0, \dots, p-1)$$

that $(1+p)^{\mu} \equiv 1 + \mu p \pmod{p^2}$, and correspondingly introducing the primitive p -th root of unity $\zeta^p = \zeta_0$ of T_p . On the basis of this system of equations $\eta, \eta', \dots, \eta^{(p-1)}$ is at any rate a primitive system of elements for T_p relative to T_p , and consequently $\eta, \eta', \dots, \eta^{(p-1)}$ cannot lie in P .

23. Under the same assumptions regarding K as in Exer. 6, 7, 10, let N be a cyclic extension of degree n over K . Furthermore, let K_0 be a subfield of K such that K is separably cyclic over K_0 . In accordance with Exer. 10, let N be a root field for the pure irreducible polynomial $x^n - a$ over K . What condition on a is necessary and sufficient in order that (a) N be normal, (b) N be Abelian, (c) N be cyclic over K_0 ?

In particular, what are these conditions if :

- (α) the n -th roots of unity in K already belong to K_0 ,
- (β) $n = p$ is a prime number and $K_0 = P, K = T_n$?

For (α). Let α be a root of $x^n - a$ in N and S_0 a generator of the Galois group $\mathcal{G}_0$ of K relative to K_0 . Then the root field to $x^n - a_{S_0}$ over K is conjugate to N relative to K_0 . Apply Def. 29 [255] and Exer. 7. Result: $a_{S_0} = a^k c^n$ with $(k, n) = 1$ and c in K .

For (β). If N is normal over K_0 with the Galois group $\mathcal{G}$, then S_0 corresponds to a residue class $\mathfrak{p}S$ of $\mathcal{G}$ relative to the normal divisor $\mathfrak{p}$.

In so doing, S can be normalized uniquely so that α_s is a given root of $x^n - a_{s_0}$. Therefore, express the roots of $x^n - a_{s_0}$ according to (a) in terms of α , normalize S suitably, and then bring forward the relation $S^{-1}AS = A$ necessary for (b), where A is a generator of the Galois group $\mathfrak{G}$ of N relative to K . Note besides that for a primitive and consequently for any n -th root of unity ζ , $\zeta_{s_0} = \zeta^s$ is valid with a definite s characterized by $s^m \equiv 1 \pmod{n}$, where $m = [K : K_0]$. Result: $k \equiv s \pmod{n}$.

For (c). Express the fact that not only (b) but also $S^m = A$ must be valid (with respect to a suitable normalization of the generator A of $\mathfrak{G}$). Result:

$$a^{\frac{s^m-1}{n}} c^{s^{m-1}} c_{s_0}^{s^{m-1}} \cdots c_{s, m-1} = \zeta.$$

24. If K_0 is a field with characteristic different from 2, let K be an extension of degree 2 over K_0 , namely, the root field of the polynomial $x^2 - d_0$ over K_0 . What condition on d_0 is necessary and sufficient that an extension N of degree 2 over K should exist which is cyclic over K_0 .

In the first place, Exer. 23, (c) yields the necessary condition that $-e$ must have the form cc' , where c is an element of K and c' is its conjugate relative to K_0 . Hence it is necessary that $-e$ be representable in the form $u_0^2 - dv_0^2$ with u_0, v_0 in K_0 . If this is the case, then we can also actually construct an a in K with the sufficient property $a' = ac^2$ by noting the behavior of $e + c^2$ in the transition to the conjugate. Of course, the case $c^2 = -e$ is an exception; in this case, however, simply take a as one of the roots of $x^2 - d_0$.

The resulting condition can be expressed in terms of d_0 except for the cited exceptional case. In the latter it is easy to see that not only K but also K_0 contains the 4-th roots of unity ($c' = c$), therefore, that d_0 can be represented trivially as the sum of two squares in K_0 .

25. In Exer. 23 let $n = p$ (prime number) and $[K : K_0] = d$ be a divisor of $p-1$. What condition on a is necessary and sufficient that N be normal over K_0 with the Galois group of the type $\mathfrak{L}_p^{(d)}$? In particular, what is this condition under the assumptions (α) or (β) ?

First of all, we have the normality criterion of Exer. 23, (a). Furthermore, instead of the basic relation appearing in (b) we must now require $S^{-1}AS = A^h$, where $h \bmod p$ has the order d ; this yields a restriction on the k appearing there. The relation $S^d = E$ required here instead of the one in (c) is then automatically satisfied, since S^d lies in $\mathfrak{S}$ and commutes with S . This can also be confirmed by means of the explicit connection between a and c due to this relation.

26. Prove: If K is separably cyclic over K_0 of degree m , S_0 a generator of the Galois group of K over K_0 and c an element of K with $cc_{S_0} \cdots c_{S_0^{m-1}} = e$, then for any u in K the element $b = u + u_{S_0^{-1}}c_{S_0^{-1}} + u_{S_0^{-2}}c_{S_0^{-1}}c_{S_0^{-2}} + \cdots + u_{S_0^{-(m-1)}}c_{S_0^{-1}}c_{S_0^{-2}} \cdots c_{S_0^{-(m-2)}}$ in K has the property $b_{S_0} = cb$, and u can be chosen so that $b \neq 0$, therefore $c = \frac{b_{S_0}}{b}$.

For the latter allow u to run through the elements of a basis of K relative to K_0 and take Section 13, Exer. 14 (and the separability) into consideration.

27. In Exer. 25 let $n = p$, $K_0 = P$, $K = T_p$. Then the property $a_{S_0} = ac^p$ with c in K and $cc_{S_0} \cdots c_{S_0^{p-1}} = 1$ is a *sufficient* (but not necessary) condition on a . Use Exer. 26 to simplify this condition.

Note that as far as this exercise is concerned a can be replaced by any element av^p with $v \neq 0$ in K .

22. Criterion for the Solvability by Radicals

1. Prove that a separable normal extension N of prime degree p over a field K of characteristic p cannot be solved by radicals.

Let us assume that it can be solved by radicals and that $\bar{\Lambda}_{r-1}$ is the last field in the chain according to Def. 40 [303] with $[N, \bar{\Lambda}_{r-1}] = K$. Then $\bar{\Lambda}_r = \{N, \bar{\Lambda}_{r-1}\}$ would be normal of prime degree p over $\bar{\Lambda}_{r-1}$ and pure as well as separable.

2. Section 13, Exer. 4; Section 15, Exer. 4; Section 21, Exer. 9 suggest the following modification of the concept of solvability in the case of ground fields of characteristic p : (a) restricting the concept to *separable* irreducible pure polynomials, therefore irreducible pure polynomials of degree prime to p ; (b) allowing the concept to apply also to the separable irreducible polynomials $x^p - x - a$ of prime degree p . In the following let the concept *solvable* always be understood in *this* sense whenever dealing with ground fields of characteristic p .—Prove that in this sense Theorem 127 is also valid for separable normal extensions N over a field K of characteristic p .

We must first show that the cyclotomic fields T_n over K are solvable in this sense. (It is sufficient to handle the case in which n is a prime number $q \neq p$, even though the proof goes through just as well for arbitrary n .) For this purpose note that T_n is separable (Theorem 121 [305]; Section 20, Exer. 5) and apply mathematical induction relative to n , just as in the proof to Theorem 126 [316], based on Theorem 125 [315] or Section 21, Exer. 9. The required proof can also be carried through in the general case just as in the case of the proof of Theorem 127.

3. Prove: Every Abelian extension is solvable.

Note that every Abelian group is metacyclic [Example 2, as well as Section 3, Exer. 9, (c), Exer. 14], and apply Theorem 127 or Exer. 2.

4. Prove: The dihedral groups $\mathfrak{D}_n$ and the linear groups $\Omega_p^{(d)}$ are metacyclic.

5. Prove: Any subgroup $\mathfrak{U}$ and any factor group $\mathfrak{G}/\mathfrak{N}$ of a metacyclic group $\mathfrak{G}$ is metacyclic. What theorems about solvable extensions follow from this?

Form the intersections $[\mathfrak{F}_i, \mathfrak{U}]$ and the composites $\{\mathfrak{F}_i, \mathfrak{U}\}$ with a chain of subgroups $\mathfrak{F}_i$ according to Def. 41 and apply Vol. 1, Section 9, Exer. 14 (with $\mathfrak{F} = \mathfrak{F}_{i+1}$, $\mathfrak{Z} = [\mathfrak{F}_i, \mathfrak{U}]$ and $\mathfrak{F} = \{\mathfrak{F}_{i+1}, \mathfrak{U}\}$, $\mathfrak{Z} = \mathfrak{F}_i$, respectively).

6. Solve for the roots $\alpha, \alpha', \alpha''$ of an irreducible cubic polynomial over a field K with characteristic different from 2 and 3. For this purpose it can be assumed without loss of generality that the polynomial has the form $x^3 + ax + b$.

In Section 16, Exer. 3 it is proved that the Galois group $\mathcal{G}$ is of the type 3_2 or $\mathfrak{D}_3$. First of all, show that (if K has characteristic different from 2) these two types are to be distinguished according to whether the discriminant d of the polynomial—express it in terms of a and b —is a square in K or not. For this purpose take note of the behavior of the difference products

$$(\alpha - \alpha')(\alpha' - \alpha'')(\alpha'' - \alpha)$$

with respect to $\mathcal{G}$. In any case, the formation of the Lagrange resolvents (Theorem 125 [315]) yields representations of the roots $\alpha, \alpha', \alpha''$ by radicals. Therefore, the third powers of these Lagrange resolvents must be represented rationally over K by cube roots of unity and (if $\mathcal{G} = \mathfrak{D}_3$) $\sqrt[3]{d}$.

7. Carry this exercise through (in the sense of Exer. 2) if K has characteristic 3. In this case the polynomial can no longer be assumed to be without a term with x^2 (Section 5, Exer. 15). Also determine an analogue to $\sqrt[3]{d}$ and use this to characterize the two group types for the case of characteristic 2.

For the case of characteristic 3 apply the method of Lagrange resolvents as modified in Section 21, Exer. 9. If the term with x^2 exists, then $\lambda = \frac{\alpha' + 2\alpha''}{\alpha + \alpha' + \alpha''}$ is such a resolvent, otherwise $\lambda = \frac{\alpha'^2 + 2\alpha''^2}{\alpha^2 + \alpha'^2 + \alpha''^2}$ in any case. Then represent $\lambda^3 - \lambda$ rationally over K in terms of $\sqrt[3]{d}$. For the case of characteristic 2 we can take as an analogue to $\sqrt[3]{d}$ any expression δ in the roots which is invariant with respect to 3_2 but not with respect to $\mathfrak{D}_3$, for instance, $\delta = \frac{\alpha}{\alpha'} + \frac{\alpha'}{\alpha''} + \frac{\alpha''}{\alpha}$.

8. Prove that the octahedral group $\mathfrak{O}$ is metacyclic. Use the structure of this group to solve for the roots α_i of an

irreducible biquadratic polynomial $x^4 + ax^2 + bx + c$ over a field K with characteristic different from 2 and 3.

The structure of $\mathfrak{D}$ was obtained in Vol. 1, Section 9, Exer. 4, 6. Furthermore, the subgroups of $\mathfrak{D}$ that are involved in the Galois group $\mathfrak{G}$ are known from Section 16, Exer. 4. By considering the difference product of the α_i and noting $\mathfrak{D} \cong \mathfrak{S}_4, \mathfrak{T} \cong \mathfrak{A}_4$ we find that $\mathfrak{G} = \mathfrak{T}$ or $\mathfrak{D}_2$, if the discriminant d of the polynomial is a square in K , otherwise $\mathfrak{G} = \mathfrak{D}$ or $\mathfrak{D}_4$ or $\mathfrak{S}_4$. In the latter case we see, in addition, that, on extending to $K(\sqrt{d})$, the group $\mathfrak{G}$ reduces to a subgroup $\mathfrak{H} = \mathfrak{T}$ or $\mathfrak{D}_2$ or $\mathfrak{S}_2$ (corresponding to the three types of $\mathfrak{G}$). $\mathfrak{H} = \mathfrak{S}_2$ is characterized by the fact that the polynomial becomes reducible in $K(\sqrt{d})$ (Section 16, Exer. 1, 2). In order to distinguish between $\mathfrak{H} = \mathfrak{T}$ and $\mathfrak{D}_2$ consider the element $\beta = (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)$ invariant with respect to $\mathfrak{D}_2$ and its two other conjugates β', β'' [obtained, for instance, through the cycle (234)]. We find that these conjugates have the sum 0 and are different from one another (K does not have characteristic 3). Therefore, they are the roots of a cubic polynomial without term with x^2 in $K(\sqrt{d})$. Express its coefficients in terms of a, b, c and $\sqrt{d}$. According as it is irreducible or reducible in $K(\sqrt{d})$, $\mathfrak{H} = \mathfrak{T}$ or $\mathfrak{D}_2$. In the first case, insert the solution for this cubic polynomial according to Exer. 6. Thereby $\mathfrak{H}$ reduces again to a subgroup $\mathfrak{K} = \mathfrak{D}_2$ or $\mathfrak{S}_2$ or $\mathfrak{E}$, according to the way in which the given polynomial reduces in the extensions leading to the solution of the cubic polynomial. The consideration of $\gamma = \alpha_1 - \alpha_2, \gamma' = \alpha_3 - \alpha_4$ now easily leads to the conclusion.

9. By enumerating the number of elements in the individual classes of conjugate elements, just as in Section 20, Exer. 21 to 23, prove that a group $\mathfrak{G}$ whose order is a prime power p^n has a centrum $\mathfrak{Z}$ different from $\mathfrak{E}$.

10. Prove: Every group $\mathfrak{G}$ of prime power order is metacyclic.

In order to pass from $\mathfrak{G}/\mathfrak{Z}$ to $\mathfrak{G}$, note that $\mathfrak{Z}$ is an Abelian normal divisor and apply the homomorphism of Vol. 1, Section 9, Exer. 9.—

It would exceed the space at our disposal to prove the theorem that any group is metacyclic whose order does not contain the square of a prime number.¹

11. Carry out in detail the proof of the remark made in connection with Theorem 127, namely, that an arbitrary (separable) extension Λ of K is solvable if and only if this is the case for the associated normal extension N over K .

See the explanation given there.

12. Prove: The normalizer of a linear permutation group $\mathfrak{L}_p^{(d)}$ in the symmetric group $\mathfrak{S}_p$ (therefore, especially the normalizer of the cyclic group $\mathfrak{Z}_p = \mathfrak{L}_p^{(1)}$) is the full linear group $\mathfrak{L}_p = \mathfrak{L}_p^{(p-1)}$.

A, B may have the meaning of Section 16, Exer. 8. For an element Q of the normalizer, $Q^{-1}AQ$ must be an element of order p in $\mathfrak{L}_p^{(d)}$, therefore a power of A (different from E). This can also be deduced from A through transformation by a suitable power B^v . Then apply Section 4, Exer. 14, (a) to QB^{-v} .

13. From this deduce the converse to Exer. 4: The Galois group $\mathfrak{G}$ of an irreducible solvable polynomial $f(x)$ of prime degree is linear.

This amounts essentially to Theorem 127, Corollary. Consider an extension chain $\bar{\Lambda}_i$ with the properties given there for the root field W of $f(x)$. Let $\bar{\Lambda}_{i+1}$ be the first field of the chain which contains a root of $f(x)$. By Theorem 119 [293] deduce from the properties of $\bar{\Lambda}_{i+1}$ over $\bar{\Lambda}_i$ that $\bar{\Lambda}_{i+1}$ already contains W . Furthermore, show that the subgroup corresponding to $\bar{\Lambda}_i$ differs from $\mathfrak{G}$ by permutations of the roots of $f(x)$ with respect to the representation of $\mathfrak{G}$ and is the cyclic group $\mathfrak{Z}_p$. Then apply Exer. 12 by going backwards from $\bar{\Lambda}_i$ along the chain.

¹ Cf., for instance, Speiser, *Theorie der Gruppen von endlicher Ordnung* (Theory of Groups of Finite Order), Theorem 121.

14. Let K be a real field (subfield of the field of all real numbers) and N a real normal extension of K solvable by radicals. Under what condition can the solution be real, that is, have a real extension chain $\bar{\Lambda}_i$ in the sense of Def. 40 [303]?

Note that only the square roots of unity are real, therefore that an irreducible pure polynomial $x^p - \alpha$ over a real field Λ has a real root field only for $p = 2$. Furthermore, note that the property $\bar{\Lambda}_r \geq N$ is preserved by any isomorphism of $\bar{\Lambda}_r$ (automorphism of the associated normal field). We can see by considerations within N that the necessary condition thereby obtained is also sufficient.

23. Existence of Algebraic Equations not Solvable by Radicals

1. Prove that the first $n - 1$ elementary symmetric functions $x_1, \dots, x_{n-1}$ of the indeterminates $\xi_1, \dots, \xi_n$ over K are prime functions in $K[\xi_1, \dots, \xi_n]$.

Use a line of reasoning as in Section 2, Exer. 29.

2. Prove that the discriminant d of the generic polynomial of n -th degree ($n > 1$) over a field K with characteristic different from 2 is a prime function in $K[x_1, \dots, x_n]$.

We know the decomposition of d into prime elements in the extension integral domain $K[\xi_1, \dots, \xi_n]$. Then apply Theorem 25 [189] (or rather its generalization according to Section 2, Exer. 27) as well as the automorphisms according to Theorem 129, and take into consideration that by Theorem 132, d does not belong to K_n .

3. Give a proof of the *Theorem on Symmetric Functions* [statements (1), (2) after Theorem 131] on the following basis (proof by Furtwängler; cf. footnote 12):

(a) If g is a symmetric function in $l[\xi_1, \dots, \xi_n]$, then the *homogeneous components* of g , that is, the terms g_m with the same sum m for the exponents of the $\xi_1, \dots, \xi_n$ (the *dimension*)

in the normal representation of $g = \sum_m g_m$, are also symmetric. Hence we can restrict ourselves to homogeneous g .

(b) Then apply, on the one hand, mathematical induction on the number n of indeterminates. For this purpose start from the congruence $g(\xi_1, \dots, \xi_n) \equiv g(\xi_1, \dots, \xi_{n-1}, 0) \pmod{\xi_n}$ relative to the prime element ξ_n of $|\xi_1, \dots, \xi_n|$ and take the congruences $x_1 \equiv x'_1, \dots, x_{n-1} \equiv x'_{n-1}, x_n \equiv 0 \pmod{\xi_n}$ into consideration, where $x'_1, \dots, x'_{n-1}$ are the elementary symmetric functions of $\xi_1, \dots, \xi_{n-1}$. We thereby obtain a reduction $g(\xi_1, \dots, \xi_n) \equiv h(x_1, \dots, x_{n-1}) + x_n g_1(\xi_1, \dots, \xi_n)$.

(c) Furthermore, in order to bring the remaining residue function g_1 under control, set up, on the other hand, a mathematical induction (with respect to a fixed n) on the dimension m .

For (a). This immediately follows from the uniqueness of the normal representation and the definition of symmetry.

For (b). In the first place, $g(\xi_1, \dots, \xi_{n-1}, 0) \equiv h(x'_1, \dots, x'_{n-1})$, therefore $g(\xi_1, \dots, \xi_n) \equiv h(x_1, \dots, x_{n-1}) \pmod{\xi_n}$. In the latter congruence note the symmetry of both sides and the distinctness of the prime elements $\xi_1, \dots, \xi_n$. That the statement is valid for $n = 1$ is trivial.

For (c). We have to show that the dimensions of the homogeneous components of g_1 are smaller than the dimension m of g . For this purpose note that $g(\xi_1, \dots, \xi_{n-1}, 0)$ is also homogeneous of dimension m (or $\equiv 0$), and conclude from this on the basis of Theorem 128 that only terms $ax'_1{}^{\mu_1} \dots x'_{n-1}{}^{\mu_{n-1}}$ with $\mu_1 + 2\mu_2 + \dots + (n-1)\mu_{n-1} = m$ appear in the normal representation of h . Then it follows that g_1 itself is homogeneous of dimension $m - n$ (or $\equiv 0$). That the statement is valid for $m = 0$ is trivial.

4. This proof yields a reduction process which can be used to represent an integral rational symmetric function through the elementary symmetric functions. Carry this through in the case of the symmetric function $\sum_{\substack{i, k=1 \\ i \neq k}}^n \xi_i^2 \xi_k$.

If f_v designates this formation for v indeterminates ($v \geq 2$), then it follows from the dimension relation obtained in (c) that the representation for f_n arises from that for f_3 by replacing the elementary symmetric functions x'_1, x'_2, x'_3 of ξ_1, ξ_2, ξ_3 by the first three elementary symmetric functions x_1, x_2, x_3 of $\xi_1, \dots, \xi_n$. The residue function g_1 appearing in the reduction of f_3 to f_2 can easily be found, since f_2 can be immediately expressed.

5. Prove Theorem 113 and Corollary [284, 285] on the basis of the Theorem on Symmetric Functions.

Begin with the proof that $\bar{g}(x)$ is a polynomial in K . Then, by considering $g(h(x))$ prove according to Theorem 53 [210] that $g(\beta_i) = 0$ for each of the roots β_i of $\bar{g}(x)$, and conclude from this, again by Theorem 53, that $g(x)$ is the single irreducible factor of $\bar{g}(x)$.

6. On the basis of the Theorem of Symmetric Functions, prove the generalization of Section 6, Exer. 20, 21: If the b_i of K appearing there are replaced by a system of conjugates $\beta_i = \phi(\alpha_i)$ corresponding to the α_i (with rational, not necessarily integral ϕ), then $g(x)$ becomes an integral rational function over K (not only, as is trivial, over Λ). Also, show that this yields another proof of Theorem 82 [240] (cf. also Section 9, Exer. 2).

According to Section 6, Exer. 21, set up the expression

$$g(x) \equiv \sum_{i=1}^n \beta_i \prod_{\substack{k=1 \\ k \neq i}}^n \frac{x - \alpha_k}{\alpha_i - \alpha_k}.$$

7. Give the proof of the Abelian Theorem (Theorem 90 [251]) on the basis of the Theorem on Symmetric Functions by constructing the elements θ_{ν_1, ν_2} as there and then considering the polynomial

$$g(x) \equiv \prod_{\nu_1, \nu_2} (x - \theta_{\nu_1, \nu_2})$$

as well as

$$h_1(x) \equiv \sum_{\nu_1, \nu_2} \alpha_{1\nu_1} \frac{g(x)}{x - \theta_{\nu_1, \nu_2}}, \quad h_2(x) \equiv \sum_{\nu_1, \nu_2} \alpha_{2\nu_1} \frac{g(x)}{x - \theta_{\nu_1, \nu_2}}.$$

Here we must apply the Theorem of Symmetric Functions in two steps: on the one hand, to the n_1 roots α_{1r} of $f_1(x)$, on the other hand, to the n_2 roots α_{2r} of $f_2(x)$. Consequently, start from a system of $n_1 + n_2$ indeterminates. (For $g(x)$ see also Section 17, Exer. 6, already given.)

8. On the basis of Section 22, Exer. 13, construct a polynomial $f(x)$ not solvable over $\mathbb{P}$ for any prime degree $p \geq 5$.

It is enough to construct $f(x)$ of degree p so that the number ρ of its real roots satisfies the inequalities $1 < \rho < p$. $\rho < p$ can be attained by assigning the value 0 to the sum of second powers of the roots (Section 6, Exer. 15); $\rho > 1$ can be attained, say, through $f(0) > 0, f(1) < 0$ (see the discussion to Section 11, Exer. 1); the irreducibility is secured on the basis of the Eisenstein-Schönemann Theorem (Section 20, Exer. 6). Also, show that the conditions of this construction are not realized for $p = 3$.

9. Prove: A transitive permutation group $\mathfrak{P}$ of p elements (p a prime number) is identical with the symmetric group $\mathfrak{S}_p$ if it contains a two-termed cycle.—For this purpose think of the occurrence of a two-termed cycle (rs) in $\mathfrak{P}$ as an equivalence relation between r and s and study the corresponding partition.

That this is actually an equivalence relation (provided that the improper cycles (rr) are interpreted as representations of the unity element) follows through transformation of a two-termed cycle by another. Furthermore, through suitable transformation the transitivity of $\mathfrak{P}$ yields that all classes contain the same number of numerals. This implies the statement.—In regard to the process to be used for transforming a cycle, see the remark in the discussion to Vol. 1, Section 16, Exer. 11.

10. Prove: If an irreducible polynomial of prime degree p over a real field K has exactly 2 non-real roots, then its Galois group is $\mathfrak{S}_p$.

Consider the reduction of the Galois group in the extension of $\mathbb{K}$ to the field of all real numbers and apply Exer. 9 and Section 16, Exer. 1.

11. For any prime degree p construct a polynomial $f(x)$ which is irreducible over $\mathbb{P}$ and whose Galois group is symmetric.

That $f(x)$ has exactly $p-2$ real roots can be inferred from the formulation $f(x) \equiv (x^2 + a)(x - a_1) \cdots (x - a_{p-2}) + b$ with rational $a > 0, a_1, \dots, a_{p-2}, b$ by taking b sufficiently small in absolute value. In order to prove the irreducibility on the basis of the Eisenstein-Schönemann Theorem choose, say, all $a, a_1, \dots, a_{p-2}$ as integral multiples of a prime number q and $b = \frac{q}{c}$ with integral c sufficiently large in absolute value, and go over to $c^p f\left(\frac{x}{c}\right)$. In doing this, $f(x)$ turns out to have integral coefficients.

12. What is the Galois group of the polynomial $x^5 - 2qx + q$ over $\mathbb{P}$, where q is an arbitrary prime number?

Make full use of the explanation to Exer. 8.

13. In order to obtain a proof for the *simplicity* of the alternating group $\mathfrak{A}_n$ in the case $n \geq 5$ (for $n = 5$ see Vol. 1, Section 9, Exer. 6, already given), first prove: If a normal divisor $\mathfrak{N}$ of $\mathfrak{A}_n$ contains a three-termed cycle, then $\mathfrak{N} = \mathfrak{A}_n$.

Apply Vol. 1, Section 16, Exer. 16, 19, as well as the formula

$$(12)(34) = (124)(134), (12)(13) = (123).$$

This enables us to handle the case $n \geq 5$. It is obvious that the theorem itself is also valid for $n = 3, 4$.

14. Now prove the simplicity of $\mathfrak{A}_n$ for $n \geq 5$ by showing: If $\mathfrak{N}$ is a normal divisor of $\mathfrak{A}_n$ and $P \neq E$ a permutation of $\mathfrak{N}$ which leaves as many numerals invariant as possible, then P is a three-termed cycle.—For this purpose investigate the commutator (likewise belonging to $\mathfrak{N}$) $K = P^{-1}Q^{-1}PQ$ of P with a suitable three-termed cycle Q . (Proof by *Bauer*.)

The decomposition of P into cycles without common numerals (Vol. 1, Section 16, Exer. 10) is either of the type (a) $P = (12)(34)\dots$ (product of only two-termed cycles, at least two), or of the type (b) $P = (123)\dots$ (at least one cycle of more than two terms). In the case (a) suppose that P were to change another numeral 5; in the case (b), another numeral 4 and (then necessarily) another numeral 5. Then show that K leaves more numerals invariant for $Q = (345)$ than P , but is at the same time $\neq E$. This commutator further shows that case (a) cannot be valid.

15. A chain of subgroups $\mathfrak{G} = \mathfrak{G}_0 \geq \mathfrak{G}_1 \geq \dots \geq \mathfrak{G}_r = \mathfrak{E}$ of a group $\mathfrak{G}$ (not necessarily finite) in which every $\mathfrak{G}_{i+1}$ is a normal divisor of $\mathfrak{G}_i$ is called a *normal chain* of $\mathfrak{G}$ and r its *length*. A normal chain H' generated by the insertion of new suitable subgroups of a normal chain $H = (\mathfrak{G}_i)$ is called a *refinement* of H . Two normal chains $H = (\mathfrak{G}_i)$ and $K = (\mathfrak{K}_i)$ of the same length from $\mathfrak{G}$ are called *isomorphic*, if their factor groups $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ and $\mathfrak{K}_i/\mathfrak{K}_{i+1}$ are the same (in the sense of isomorphism) except for the ordering.—Prove: To any two normal chains

$$H = (\mathfrak{G}_i) \quad (i = 0, 1, \dots, r) \quad \text{and} \quad K = (\mathfrak{K}_j) \quad (j = 0, 1, \dots, s)$$

there exist refinements isomorphic to one another. For example, we could take the chains H' and K' which arise by inserting the groups¹

$$\mathfrak{G}_{ij} = \mathfrak{G}_i[\mathfrak{G}_{i-1}, \mathfrak{K}_j] \quad (j = 1, \dots, s-1)$$

in H and by inserting the groups

$$\mathfrak{K}_{ij} = [\mathfrak{G}_i, \mathfrak{K}_{j-1}] \mathfrak{K}_j \quad (i = 1, \dots, r-1)$$

in K . (*Theorem of Schreier.*)

¹ The composite $\mathfrak{B} = \{u, \mathfrak{B}\}$ of two subgroups of a group $\mathfrak{G}$ of which there is at least one normal divisor of a group containing the other (therefore surely of $\mathfrak{B}$) can be written as the product $\mathfrak{B} = u\mathfrak{B} = \mathfrak{B}u$ in the sense of Vol. 1, Section 9, Def. 20 [222].

For this purpose prove, as shown by *Zassenhaus*, the generalization to Vol. 1, Section 9, Exer. 14 given by the following theorem regarding the four subgroups $u, \mathfrak{U}, v, \mathfrak{B}$ of a group $\mathfrak{G}$: If u is a normal divisor of $\mathfrak{U}$, v a normal divisor of $\mathfrak{B}$, then (a) $u[\mathfrak{U}, v]$ is a normal divisor of $u[\mathfrak{U}, \mathfrak{B}], [u, \mathfrak{B}]v$ a normal divisor of $[\mathfrak{U}, \mathfrak{B}]v$, and

$$(b) u[\mathfrak{U}, \mathfrak{B}]/u[\mathfrak{U}, v] \cong [\mathfrak{U}, \mathfrak{B}]v/[u, \mathfrak{B}]v.$$

For (a). This easily follows from the assumptions. In order to show, in particular, the invariance of $u[\mathfrak{U}, v]$ with respect to transformation by the elements u of u , note that

$$UuU^{-1} = u'(U \text{ in } \mathfrak{U}, u' \text{ in } u) \text{ implies } u^{-1}Uu = u^{-1}u'U.$$

For (b). Apply Vol. 1, Section 9, Exer. 14 to the composite

$$u[\mathfrak{U}, \mathfrak{B}] = u[\mathfrak{U}, v][\mathfrak{U}, \mathfrak{B}], [\mathfrak{U}, \mathfrak{B}]v = [\mathfrak{U}, \mathfrak{B}][u, \mathfrak{B}]v,$$

and use the fact that intersections satisfy the relation

$$[u[\mathfrak{U}, v], [\mathfrak{U}, \mathfrak{B}]] = [\mathfrak{U}, \{u, v\}, \mathfrak{B}] = [[\mathfrak{U}, \mathfrak{B}], [u, \mathfrak{B}]v],$$

which is easy to prove. Its symmetry yields the statement.

16. What property does the factor groups $\mathfrak{G}_i/\mathfrak{G}_{i+1}$ of a normal chain $H = (\mathfrak{G}_i)$ of $\mathfrak{G}$ have if it can no longer be refined? For finite groups $\mathfrak{G}$ are there always normal chains of this kind? What can be said about any two such chains? (*Jordan-Hölder Theorem*.)

17. Give all possible normal chains with simple factor groups for the groups

$$\mathfrak{D}_3 \cong \mathfrak{S}_3, \mathfrak{D}_4, \mathfrak{A} \cong \mathfrak{A}_4, \mathfrak{D} \cong \mathfrak{S}_4, \mathfrak{Q}, \Omega_p^{(d)},$$

studied earlier.

18. Let a finite group $\mathfrak{G}$ of order n be given. Construct a ground field K and a separable normal extension N of this field such that N over K has the Galois group $\mathfrak{G}$.

Note that $\mathfrak{G}$ is isomorphic to a subgroup of $\mathfrak{S}_n$ (Vol. 1, Section 16, Exer. 21, 23), and apply Theorem 129 as well as the Fundamental Theorem of the Galois Theory.—Also, show that this still does not solve the problem (at the present this problem is unsolved in general) of constructing a *polynomial* $f(x)$ over a suitable K with a given permutation group as Galois group.

19. In connection with Vol. 1, Section 19, Exer. 4, calculate the determinants

$$|\xi_i^{\eta-k}| \quad (i = 1, \dots, n; k = 0, 1, \dots, l-1, l+1, \dots, n)$$

for $l = 1, \dots, n$ by regarding the ξ_i as the roots of the generic polynomial $f_n(x)$. These determinants are needed for the complete solution of Vol. 1, Section 20, Exer. 2.

A column relation yields the divisibility by the l -th elementary symmetric function r_l . The factor still remaining in this case is again a Vandermonde determinant except for the sign.

20. In order to complete Theorem 132 regarding the ground field K of characteristic 2, find also for this case a primitive element of V_n relative to K . (For $n = 3$, see Section 22, Exer. 7, already given.)

A primitive element that can be used is obtained from the expansion of the determinant $|\xi_i^{k-1}|$ specified in Theorem 132. For this purpose carry out the expansion according to Vol. 1, Def. 38 [127] by summing only for $\text{sgn } P = +1$ in δ . However, we can also construct a new kind of calculating expression from the square array (ξ_i^{k-1}) if in the definition of determinants the operations are interchanged (addition with multiplication, subtraction with division). This expression takes on its inverse value under an odd permutation.

AUTHOR AND SUBJECT INDEX

*(The numbers outside of parentheses are page numbers;
the numbers inside parentheses are exercise numbers.)*

- Addition matrix** 40 (6)
Automorphism 29 (13, 14)
Bauer 206 (14)
Centrum 28 (8), 34 (8), 200 (9)
Chain rule 129 (1)
Characteristic matrix 100 (43), 126 (9)
 polynomial 68 (6), 127 (10), 137 (31, 32), 138 (33), 148 (6), 151 (13)
 roots 148 (6), 151 (16), 152 (18), 153 (21), 155 (5), 156 (6)
Circulant 123, 124 (15, 16), 152 (19), 186 (16)
Commutator 25 (5), 36 (18, 19)
 group 36, 37 (20, 21)
Composite of fields 17 (7, 8)
 see also **Direct composite**
Cycles 55-58 (9-18), 113 (3)
Cyclotomic periods 184, 185 (9-11)
Determinantal divisors
 98 (37), 99 (41)
 of a matrix 148 (6)
Dihedral group, *see* Group
Direct composite 175 (11), 182 (4)
 product of groups 113-115 (6, 11), 117 (14, 15)
 sum of residue class rings 104 (9)
Discriminant 73 (20), 134 (18), 135 (19), 162 (13-16), 181 (1), 188 (1), 202 (2)
Eisenstein-Schönemann Theorem 182, 183 (6, 7)
Elementary divisors 98 (37), 99 (40, 41), 100 (42), 101 (45), 102 (47)
 of a matrix 148, 149 (6, 9)
Euler's function 105 (11, 12), 106, 107 (14, 16-19)
Fermat Theorem 106 (15)
Field algebraically closed 155 (2)
 finite 14 (7), 15 (8), 18 (12), 97 (33), 140 (7), 107 (20-22), 163 (3, 4)
 imperfect 143, 144 (3, 4)
 isomorphic to subfield 21 (4-6)
 perfect 136 (26), 137 (27), 162 (1)
Full ring 19 (3), 20 (4, 5), 104 (6)
Fundamental Theorem of algebra 174 (9)
 of finite Abelian groups 117 (15)
Furtwängler 202 (3)
Gaussian prime numbers 186 (14, 15)
 sum 185 (11), 191 (11)
Gauss's Theorem 108 (23), 109 (24)
Graph 170 (1) ff.
Group
 cyclic 24 (2), 25 (1), 28 (9)
 dihedral 24 (2), 26 (2), 28 (10, 11), 29 (2), 32 (2, 3), 37 (21), 62 (27, 29), 170 (1), 208 (17)
 Group (cont.)
 icosahedral 33 (4-6), 37 (21), 62 (27-29), 170 (1)
 linear permutation 168, 170 (8-11), 170 (1)
 octahedral 33 (4-6), 37 (21), 62 (27, 29), 170 (1), 199 (8), 208 (17)
 of coincidence motions 24 (1, 2), 31 (1), 61, 62 (24-29)
 tetrahedral 24 (2), 26 (3), 29 (2), 32 (2, 3), 37 (21), 62 (27, 29), 170 (1), 208 (17)
 Groups
 linear permutation 170 (1), 201 (12, 13), 208 (17)
 of prime order 30 (7)
 Hermitian form 156 (7)
 matrices 156 (7)
 Homomorphism 34 (9)
 Icosahedral Group, *see* Group
 Identity matrix 40 (5)
 Imperfect field 143, 144 (3, 4)
 Integral domain isomorphic to sub-domain 20 (2, 3)
 with finite number of elements 15 (9)
 Interchangeability of order of differentiation 130 (4)
 Interpolation 135, 136 (20-22)
 Intersection of fields 17 (6)
 Jordan-Hölder Theorem 208 (16)

- Kronecker's Theorem** 178 (5)
- Lagrange interpolation formula** 135 (21)
- Landau** 183 (8)
- Linear permutation group, see Group**
- Linked systems** 45, 46 (1-3)
- Logarithmic differentiation** 130 (3)
- Matrices**
 arithmetically equivalent 98 (36, 38), 99 (39, 41), 100 (43)
 determinantal divisors of 98 (37), 99 (41), 148 (6)
 elementary divisors of 98 (37), 99 (40, 41), 100 (42), 101 (45), 102 (47), 148, 149 (6-9)
 equivalent 80 (9)
 product of 38-43 (3, 4, 10-14)
 similar 83 (18), 100 (43), 102 (47, 48), 150 (10 ff.)
- Matrix**
 characteristic 100 (43), 126 (9)
 idempotent 40 (5)
 identity 40 (5)
 integral 97 (34)
 inverse 41 (7-9), 50 (1-4)
 multiplication 38-43 (3, 4, 10-14)
 regular 50 (1-5)
 skew-symmetric 122 (12, 13)
- Matrix (cont.)**
 symmetric 67 (5), 155 (5)
 unimodular 97 (35)
 Möbius function 181 (2)
 Multiplication matrix 40 (6)
 of determinants 69 (7, 8)
- Newton's formulas** 133 (15)
- Normalizer** 34, 35 (11-14), 201 (12)
- Octahedral group, see Group**
- Perfect field** 136 (26), 137 (27), 162 (1)
- Permutation group** 53 (1)
- Polygon of seventeen sides, regular** 185 (13)
- Power sums** 133 (15), 134 (16, 17)
- Prime power invariants** 117 (16), 119 (19)
- Principal minor** 68 (6)
- Product of determinants** 69 (7, 8)
 matrices 38 (3)
- Quaternion group** 171 (2), 208 (17)
- Quadratic form, positive definite** 156 (6)
- Regular element** 19 (1, 2), 103 (5)
- Representation of groups by permutation** 59-62 (20-29)
- Resultant** 153, 154 (23-25), 188 (2)
- Rychlik** 121 (11)
- Schreier** 207 (15)
- Simplicity of the alternating group** 33 (6), 206 (13)
- Skew field** 51 (2), 187, 188 (19-23)
- Speiser** 200 (10)
- Steinitz** 160, 161 (9, 10)
- Symmetric functions** 202 (1, 3 ff.)
- Taylor formula** 131 (5, 8)
- Tetrahedral group, see Group**
- Transitive permutation groups** 54, 55 (4-8), 205 (9)
- Transposition** 57, 58 (14-17)
 matrix 40 (6)
- Vandermonde determinant** 67 (4), 209 (19)
- Vieta's formulae** 128 (13)
- Wedderburn's Theorem** 188 (23)
- Wilson's Theorem** 125 (2)
- Witt** 188 (23)
- Zassenhaus** 207 (15)
- Zermelo** 94 (25)
- Zero divisor** 18 (1), 103 (5)
 proper 18 (1)

