MODERN ALGEBRA

MODERN ALGEBRA

By B. L. VAN DER WAERDEN, Ph.D.
PROFESSOR OF MATHEMATICS
AT THE UNIVERSITY OF AMSTERDAM

In part a development from lectures
By E. ARTIN and E. NOETHER

VOLUME II

Translated from the second revised German edition
By THEODORE J. BENAC, Ph.D.
ASSOCIATE PROFESSOR, DEPARTMENT OF MATHEMATICS
U.S. NAVAL ACADEMY

FREDERICK UNGAR PUBLISHING CO.
NEW YORK

MODERNE ALGEBRA

MODERN ALGEBRA, Volume II
(English Translation)

Printed in the United States of America

PREFACE TO THE SECOND EDITION

In this new edition, Volume II, as in the case of Volume I, has been so revised that hardly a chapter has been left untouched. In particular the last two chapters, which are concerned with hypercomplex numbers and their representations, have been considerably expanded and reorganized so as to meet the demands of the impetuous development of the modern theory of algebras. As to polynomial ideals, I have omitted those parts which belong more to algebraic geometry than to algebra.

I wish to extend my sincerest appreciation to Dr. Reichardt who assisted me in reading proofs, as well as to a number of colleagues who pointed out minor errors in the first edition.

B. L. VAN DER WAERDEN

Leipzig, February 1940

CONTENTS

CHAPTER XI

ELIMINATION THEORY

CHAPTER XII

GENERAL IDEAL THEORY OF COMMUTATIVE RINGS

CHAPTER XIII

THEORY OF POLYNOMIAL IDEALS

CHAPTER XIV

INTEGRAL ALGEBRAIC QUANTITIES

CHAPTER XV

LINEAR ALGEBRA

CHAPTER XVI

THEORY OF THE HYPERCOMPLEX QUANTITIES

CHAPTER XVII

REPRESENTATION THEORY OF GROUPS AND HYPERCOMPLEX SYSTEMS

CHAPTER XI

ELIMINATION THEORY

In elimination theory we study systems of algebraic equations in several unknowns in order to set up conditions for their solvability as well as formulas for calculating their solutions in various cases. In this chapter the corresponding theory for linear equations, i.e., the theory of determinants, is assumed as known. Furthermore, it shall also be assumed that *one* equation in a *single* unknown of degree higher than one can be solved, or more precisely, if such an equation can not be resolved in a given field, an extension field may be constructed in which it is decomposable, and in fact one in which it may be completely decomposed (Chapter 5). In the following when we refer to the "solutions of an equation" or the "zeros of a polynomial," we shall always assume that the solutions are in a suitably chosen extension field of the fixed commutative field K.

77. THE RESULTANT SYSTEM OF SEVERAL POLYNOMIALS IN A SINGLE VARIABLE

THEOREM. *Let $f_1, \ldots, f_r$ be r polynomials in a single variable of given degrees with indeterminate coefficients. Then there exists a system $D_1, \ldots, D_h$ of integral polynomials in these coefficients with the property that if these coefficients are assigned values from the field K the conditions $D_1 = 0, \ldots, D_h = 0$ are necessary and sufficient in order that either the equations $f_1 = 0, \ldots, f_r = 0$ have a solution in a suitable extension field or that the formal leading coefficients of all polynomials $f_1, \ldots, f_r$ vanish.*

The proof is based on *Kronecker's method of elimination.*

First, we transform the polynomials $f_1, \ldots, f_r$ into polynomials of the same degree by multiplying every polynomial f_i by $^{-n_i}$ and $(x-1)^{n-n_i}$ provided that n_i is smaller than n where n is the greatest (formal) degree of the given polynomials. In this way two polynomials of formal degree n arise from f_i such that for any specialization of the coefficients their common zeros and their leading coefficients are the same as those of f_i. This system of polynomials of the same degree may contain more polynomials than are in the system $f_1, \ldots, f_r$ but it has the same common zeros. We designate these polynomials by $g_1, \ldots, g_s$.

Next from $g_1, \ldots, g_s$ we form the linear combinations

$$g_u = u_1 g_1 + \cdots + u_s g_s;\ g_v = v_1 g_1 + \cdots + v_s g_s,$$

where u,v are indeterminates which are adjoined to the field K. If g_u and g_v have a common factor for any specialization of the coefficients of $g_1, \ldots, g_s$, this factor is expressible rationally in terms of u and v (Section 18). However a factor which is rationally dependent explicitly on the v cannot occur as a factor in a decomposition of g_u since g_u is independent of the v. Hence every factor common to g_u and g_v must be independent of the v and similarly of the u, and therefore must divide $g_1, g_2, \ldots, g_s$. Conversely, if $g_1, \ldots, g_s$ have a common factor, it also divides g_u and g_v.

Finally, let R be the resultant of g_u and g_v. Then the necessary and sufficient condition that g_u and g_v have either a common factor or leading coefficients which vanish is that

(1) $\qquad R = 0$ identically in the u and v.

If we arrange R according to the power products of the u and v, and denote the coefficients by $D_1, \ldots, D_h$, (1) is equivalent to

$$D_1 = 0,\ D_2 = 0, \ldots, D_h = 0.$$

We note that the D_i are integral polynomials in the indeterminate coefficients of $f_1, f_2, \ldots, f_r$. Hence the proof of the theorem is completed.

The system $D_1, \ldots, D_h$ is called the *resultant system* of the polynomials $f_1, \ldots, f_r$.

By Section 27 it follows that

$$\begin{aligned} R &\equiv 0(g_u, g_v) \\ &\equiv 0(g_1, \ldots, g_s) \\ &\equiv 0(f_1, f_2, \ldots, f_r), \end{aligned}$$

and, on arranging both sides according to power products in the u and v, we obtain

(2) $\qquad (D_1, \ldots, D_h) \equiv 0(f_1, \ldots, f_r).$

REMARKS. 1. If it is known beforehand that the formal leading coefficient of one of the polynomials f_ν, say f_1, does not vanish, we may omit the entire preliminary operation whereby the polynomials f_ν are transformed into polynomials of the same degree. Moreover the calculations may then be simplified by forming the resultant of f_1 and $v_2 f_2 + \cdots + v_r f_r$ rather than that of g_u and g_v.

2. As in Section 27 the exceptional case of the vanishing of all formal leading coefficients can be avoided by passing over to homogeneous forms in x_1 and x_2. The g_i are then formed from f_i through multiplication by $x_1^{n-n_i}$ and $x_2^{n-n_i}$ (instead of x^{n-n_i} and $(x-1)^{n-n_i}$).

3. In the case of a single polynomial the application of the process described above gives rise to a resultant system which consists only of zero.

78. GENERAL ELIMINATION THEORY

In the following $\{\xi_1, \ldots, \xi_n\}$ always indicates an ordered sequence of n elements belonging to a suitably chosen extension field of the fixed ground field K. If a polynomial f has the property $f(\xi_1, \ldots, \xi_n) = 0$, the sequence $\{\xi_1, \ldots, \xi_n\}$, or briefly ξ, is called a *zero* of f. In the general theory of elimination we are concerned with the problem of determining, at least theoretically, all solutions of a system of arbitrary algebraic equations

$$f_1(\xi) = 0, \ f_2(\xi) = 0, \ \ldots, \ f_r(\xi) = 0,$$

i.e., all zeros common to the polynomials $f_1, \ldots, f_r$ in $\mathsf{K}[x_1, \ldots, x_n]$.[1]

The method to be used is the "successive elimination" of all unknowns by means of the resultant system described in the previous section. For this purpose it is convenient to assume that the system $f_1, \ldots, f_r$ contains a polynomial of degree α in which the coefficient of x_1^α is a non-zero constant. This condition may be satisfied from the start. If not, it may be brought about as follows. We first note that all polynomials $f_1, \ldots, f_r$ may vanish identically. In this case since all sequences $(\xi_1, \ldots, \xi_n)$ are solutions, it need not interest us further. Hence we may assume that there is an f_i, say f_1, which does not vanish identically. Under this hypothesis we introduce new variables $x_1', \ldots, x_n'$ by the substitution

$$(1) \qquad \begin{cases} x_1 = u_1 x_1', \\ x_2 = x_2' + u_2 x_1', \\ \cdots\cdots \ \cdots \ \cdots \\ x_n = x_n' + u_n x_1', \end{cases}$$

where $u_1, \ldots, u_n$ are indeterminates which are adjoined to the field K. If we substitute (1) in $f_1, \ldots, f_r$, new polynomials $f_1', \ldots, f_r'$ in $x_1', \ldots, x_n'$ are obtained in which the coefficient of the highest power of x_1' is now a non-vanishing polynomial in $u_1, \ldots, u_n$. If α denotes the degree of the polynomial f_1, then

$$f_1' = f_1(u_1 x_1', \ x_2' + u_2 x_1', \ \ldots, \ x_n' + u_n x_1'),$$

and the coefficient of $x_1'^\alpha$ in this expression is $f_1^*(u_1, \ldots, u_n)$, where f_1^* is the set of terms in f_1 of highest (α-th) degree.[2]

Now we may eliminate x_1' and find a resultant system

$$d_1, \ldots, d_l,$$

which depends only on $x_2', \ldots, x_n'$. Every zero $\{\xi_2', \ldots, \xi_n'\}$ of this resultant system (since we have imposed the condition that there is a leading coefficient which

---

[1] In practice the required calculations are very often too complicated to be carried out effectively.

[2] REMARK. Instead of indeterminates u_ν we may also use particular values of the u_ν in the ground field or (in case this should be finite) in a suitably chosen extension field provided that for these values $f_1^*(u_1, \ldots, u_n)$ does not vanish.

does not vanish) leads to at least one zero $\{\xi_1', \ldots, \xi_n'\}$ of the polynomials $f_1', \ldots, f_n'$. In fact all zeros of $f_1', \ldots, f_n'$ may be obtained from this resultant system. We note that the omitted unknown ξ_1' is determined by a system of equations whose greatest common divisor is not a constant, i.e., ξ_1' satisfies an algebraic equation of the first degree at least. Next, if $d_1, \ldots, d_l$ does not vanish identically, we may continue the transformation (introducing $x_2'', \ldots, x_n''$ instead of $x_2', \ldots, x_n'$) and elimination described above, and so on. The process stops at the s-th step if, after $x_1', x_2'', \ldots, x_s^{(s)}$ have been eliminated, a system of polynomials in $x_{s+1}^{(s)}, \ldots, x_n^{(s)}$ is obtained which vanishes identically. If this does not happen, the process is continued until all indeterminates are eliminated. If the (constant) resultant thereby obtained does not vanish, the proposed system of equations obviously *cannot be solved.* However, in the case where the resultant becomes zero after s steps, we may replace $x_{s+1}^{(s)}, \ldots, x_n^{(s)}$ by arbitrary values $\xi_{s+1}^{(s)}, \ldots, \xi_n^{(s)}$ and then determine successively $\xi_1', \xi_2'', \ldots, \xi_s^{(s)}$ (in the reverse order). In fact for every specialized sequence $\{\xi_{s+1}^{(s)}, \ldots, \xi_n^{(s)}\}$ a finite number of specialized sequences $\{\xi_1', \xi_2'', \ldots, \xi_s^{(s)}\}$ is obtained. Furthermore by substitution (1) each of these leads to a solution $\{\xi_1, \xi_2, \ldots, \xi_n\}$ of the original system of equations.

We may also replace $\xi_{s+1}^{(s)}, \ldots, \xi_n^{(s)}$ by indeterminates and then determine $\xi_1', \ldots, \xi_s^{(s)}$ formally in terms of one or more systems of algebraic functions in these indeterminates. However, it should be noted that for particular values of $\xi_{s+1}^{(s)}, \ldots, \xi_n^{(s)}$ there may exist solutions which cannot be obtained by specializing the solutions in terms of the indeterminates $\{\xi_{s+1}^{(s)}, \ldots, \xi_n^{(s)}\}$. This will be illustrated in the following example.

Let
$$f_1 = x_1^2 + x_1 x_2,$$
$$f_2 = x_1 x_2 + x_2^2 + x_1 + x_2.$$

The preliminary transformation (1) is not necessary in this case since the term x_1^2 already occurs in f_1. The resultant, after x_1 is eliminated, vanishes identically since for every value of x_2 the polynomials f_1 and f_2 have the common factor $x_1 + x_2$. Hence in terms of the indeterminate ξ_2 we have $\xi_1 = -\xi_2$. However, if we assign to ξ_2 the value -1, the polynomial f_2 vanishes and ξ_1 may take on the value 0 as well as the value $+1$. It is obvious that the zero $\{0, -1\}$ cannot be obtained by specializing the general solution $\xi_1 = -\xi_2$.

As in this example the "algebraic manifold" of the zeros common to $f_1, \ldots, f_r$ may also be decomposed in the general case into distinct "irreducible manifolds" of distinct dimensions which admit a "parametric representation" by algebraic functions. In regard to the proof (independent of the theory of elimination), see Chapter 13. These manifolds and their parametric representations can be explicitly calculated by means of the theory of elimination. However we will go no further into this matter.[3]

[3] See F. S. Macaulay: *Algebraic Theory of Modular Systems,* Cambridge Tracts No. 19, Cambridge 1916, or the author's *Einführung in die algebraische Geometrie,* Berlin 1939.

From the congruence (2) of the previous section we obtain the following congruence

$$(2) \qquad (d_1, \ldots, d_l) \equiv 0(f_1', \ldots, f_r')$$

in the polynomial domain $\mathsf{K}(u)[x_1', \ldots, x_n']$.

On applying (2) to the case whereby the elimination finally produces a non-vanishing constant as a resultant, the interesting congruence

$$1 \equiv 0(f_1, \ldots, f_r)$$

is obtained. In other words, if the polynomials $f_1, \ldots, f_r$ in $\mathsf{K}[x_1, \ldots, x_n]$ have common zeros in no algebraic field over K, a relation

$$1 = A_1 f_1 + \cdots + A_r f_r$$

is valid in $\mathsf{K}[x_1, \ldots, x_n]$.

The proof is by the method of complete induction on the number of variables. The statement is valid for constants f_i as well as polynomials in a single variable. Hence we will assume that it is also valid for polynomials in $n-1$ variables. In the case of n variables the resultants $d_1, \ldots, d_l$, which first appear are polynomials in $n-1$ variables. Since these polynomials do not have a common zero a relation

$$1 = B_1 d_1 + \cdots + B_l d_l.$$

is valid in $\mathsf{K}(u)[x_2', \ldots, x_n']$. By (2) this becomes

$$1 = A_1' f_1' + \cdots + A_r' f_r'.$$

Now replace x_i' by its value given in (1). Then f_i' goes over into f_i. Furthermore, as the terms on the right are rational in the u, on multiplying through by the denominator $g(u)$ we obtain

$$g(u) = A_1(u) \cdot f_1 + \cdots + A_r(u) \cdot f_r.$$

On equating the coefficients of like power products of the u whose coefficients on the left do not vanish, the relation

$$1 = A_1 f_1 + \cdots + A_r f_r$$

follows.

EXERCISE. The degrees of the polynomials $A_1, \ldots, A_r$ are bounded as soon as the degrees of the f_i are bounded.

79. HILBERT'S NULLSTELLENSATZ

A generalization of the theorem proved at the end of the previous section is given by Hilbert's Nullstellensatz.

If f is a polynomial in $\mathsf{K}[x_1, \ldots, x_n]$, which vanishes at all zeros common to the polynomials $f_1, \ldots, f_r$, then a congruence

$$f^e \equiv 0(f_1, \ldots, f_r)$$

is valid for an integer ϱ *(and conversely).*

PROOF.[4] For $f = 0$, the result is clearly valid. To consider the case $f \neq 0$ we introduce a new variable z. The polynomials

$$f_1, \ldots, f_r, 1 - zf$$

in $K[x_1, \ldots, x_n, z]$ have no common zeros since every common zero of $f_1, \ldots, f_r$ is a zero of f and so not of $1 - zf$. Therefore, by the theorem proved in the previous section, we have

$$1 = A_1 f_1 + \cdots + A_r f_r + A(1 - zf).$$

In this identity let us make the substitution $z = \frac{1}{f}$. The fractions that are thereby introduced may be removed by multiplying by a power f^ϱ. Hence

$$f^\varrho = B_1 f_1 + \cdots + B_r f_r, \qquad \text{Q.E.D.}$$

The converse is trivial.

From this proof and the exercise of Section 78 it follows that a bound may be obtained for the exponent ϱ as soon as the degrees of $f_1, \ldots, f_r$ and f are known. In fact there is a bound for ϱ which depends *only* on $f_1, \ldots, f_r$, as will be seen in Section 95.

EXTENSION OF THE NULLSTELLENSATZ. *If the polynomials* $h_1, \ldots, h_k$ *take on the value 0 for all zeros common to* $f_1, \ldots, f_r$, *a congruence*

$$(h_1, \ldots, h_k)^\sigma \equiv 0 \ (f_1, \ldots, f_r)$$

is valid. In other words, every power product of the h_i *such that the sum of the exponents is* σ *belongs to the ideal* $(f_1, \ldots, f_r)$ *(and conversely).*

PROOF. The congruence

$$h_i^{\varrho_i} \equiv 0 \ (f_1, \ldots, f_r)$$

is valid. Let

$$\sigma = (\varrho_1 - 1) + (\varrho_2 - 1) + \cdots + (\varrho_k - 1) + 1.$$

Every power product $h_1^{l_1} \ldots h_k^{l_k}$ with $l_1 + \cdots + l_k = \sigma$ contains at least one factor $h_i^{\varrho_i}$ since otherwise $l_1 + \cdots + l_k$ would be at most equal to $(\varrho_1 - 1) + \cdots + (\varrho_k - 1) = \sigma - 1$. The theorem follows immediately.

The converse is trivial.

80. CRITERIA FOR THE SOLVABILITY OF A SYSTEM OF HOMOGENEOUS EQUATIONS

In Section 78 we gave a procedure that could be used to determine whether or not a system of algebraic equations possessed solutions. However we did not develop an "algebraic criterion" for solvability, that is, a system of integral rational functions of the coefficients whose vanishing is necessary and sufficient for the existence of solutions (as the resultant system of Section 77 in the case of a single unknown

[4] See A. Rabinowitsch: *Math. Ann.*, Bd. 102 (1929), p. 518.

or the determinant of a system of linear *homogeneous* equations). In general such a criterion cannot be developed,[5] though it does exist in the special case of homogeneous equations which we will now consider.

If $f_1, \ldots, f_r$ are homogeneous non-constant polynomials in $x_1, \ldots, x_n (n > 1)$, they always have at least the "trivial" zero $\{0, \ldots, 0\}$. We shall now find a criterion for the existence of a non-trivial zero $\{\eta_1, \ldots, \eta_n\}$ and, on account of the homogeneity, a whole "*ray*" of zeros $\{\lambda\eta_1, \ldots, \lambda\eta_n\}$.[6]

The following technique is due to H. Kapferer.[7] It is based on the method of successive elimination due to Kronecker. The first step is to consider the forms $f_1, \ldots, f_r$, as polynomials in x_1 and, according to Section 77, form the resultant system $D_1, \ldots, D_h$ (however without the preliminary transformation (1) of Section 78). It will now be shown that if the polynomials $f_1, \ldots, f_r$ have a non-trivial zero in common, then $D_1, \ldots, D_h$, as polynomials in $x_2, \ldots, x_n$, also have a non-trivial zero in common and conversely.

In the proof we need to consider only two cases.

CASE 1. The coefficients of the terms in $f_1, \ldots, f_r$ consisting only of powers of x_1 do not all vanish. In this case on applying the properties of resultant systems we have that every non-trivial zero $\{\xi_2, \ldots, \xi_n\}$ of $D_1, \ldots, D_h$ gives rise to at least one zero $\{\xi_1, \xi_2, \ldots, \xi_n\}$ of $f_1, \ldots, f_r$ which of course cannot be trivial. Conversely, every zero $\{\xi_1, \ldots, \xi_n\}$ of the f_ν gives rise to a zero $\{\xi_2, \ldots, \xi_n\}$ of the D_ν, which also cannot be trivial because the vanishing of $\xi_2, \ldots, \xi_n$ would lead immediately to the vanishing of ξ_1 since $f_\lambda = c\xi_1^m + \cdots = 0$.

CASE 2. The coefficients of the terms in $f_1, \ldots, f_r$ consisting only of powers of x_1 all vanish. By Section 77 $D_1, \ldots, D_h$ vanish identically in this case. Hence the system $D_1, \ldots, D_h$ has a non-trivial zero, say $\{1, 1, \ldots, 1\}$. Furthermore, in this case, the polynomials $f_1, \ldots, f_r$ have a non-trivial zero, namely, $\{1, 0, \ldots, 0\}$, since the terms with the highest power of x_1 are all omitted.

---

[5] This is illustrated by the following example: the equations

$$\left.\begin{aligned} a_1x_1 + a_2x_2 + a_3 = 0, \\ b_1x_1 + b_2x_2 + b_3 = 0 \end{aligned}\right\}$$

have "in general" a solution, i.e., for $a_1b_2 - a_2b_1 \neq 0$. Hence, if

$$D_1(a, b) = 0, \quad \ldots, \quad D_h(a, b) = 0$$

were necessary and sufficient for solvability, the D must vanish for the indeterminates a, b, and so must vanish identically. Accordingly the equations would always have a solution, which is not true. (Also the inequality $a_1b_2 - a_2b_1 \neq 0$ is not necessary and sufficient.)

[6] The zeros $\{\lambda\eta_1, \ldots, \lambda\eta_n\}$ for fixed η and variable λ form a line of the space R_n which goes through the origin $\{0, \ldots, 0\}$ and on this account is called a "ray." The rays will also be thought of as "points" of the "projective space" P_{n-1} whose "homogeneous coordinates" are the η, cf. Section 91.

[7] Kapferer, H.: "Über Resultanten und Resultantensysteme." *Sitzungsber. Bayer. Akad. München 1929, pp. 179-200.*

This proves the statement made above. Now $D_1, \ldots, D_h$ are homogeneous in $x_2, \ldots, x_n$. Hence the elimination may be continued. On eliminating x_2, etc., a system of forms in x_n

$$b_1 x_n^{s_1},\ b_2 x_n^{s_2},\ \ldots,\ b_k x_n^{s_k}$$

is finally obtained. These forms possess a non-trivial zero if and only if all coefficients $b_1, \ldots, b_k$ vanish.

The quantities $b_1, \ldots, b_k$ are obtained by fixed, namely dependent only on the degrees of the original forms, integral rational processes on the coefficients of these forms. Hence they are integral polynomials of the coefficients of $f_1, \ldots, f_r$.

The system of polynomials $b_1, \ldots, b_k$ (or any other system whose vanishing implies the existence of a zero) is also called a *resultant system* of the forms $f_1, \ldots, f_r$.

Let us apply the relation

$$(D_1, \ldots, D_h) \equiv 0\,(f_1, \ldots, f_r),$$

which was proved earlier, at every step of the successive eliminations. On combining all these relations together we obtain

$$x_n^{s_\nu} b_\nu \equiv 0\,(f_1, \ldots, f_r) \qquad (\nu = 1, \ldots, k). \tag{3}$$

The construction of $b_1, \ldots, b_k$ enables us to show easily that they are homogeneous forms in the coefficients of every individual form f_i. Thus the system $D_1, \ldots, D_h$ is generated by a resultant R in which the coefficients a_ν of f_i appear only in the combinations $a_\nu u_i$ and $a_\nu v_i$. Hence every term of R has the same degree in the a_ν as in the u_i and v_i together, and if R is then arranged according to the power products in the u and v, the coefficient D_j of such a power product is homogeneous with a definite degree in the a_ν. If we apply the same line of reasoning to the second, third, etc. steps of the elimination, our result is proved.

To recapitulate we have:

r forms $f_1, \ldots, f_r$ with indeterminate coefficients possess a resultant system of integral polynomials b_ν in these coefficients such that for special values of the coefficients in an arbitrary field K *the vanishing of all resultants is necessary and sufficient in order that the equations $f_1 = 0, \ldots, f_r = 0$ have a solution distinct from the zero solution. The b_ν are homogeneous in the coefficients of every individual form f_i and satisfy a congruence (3).*

EXERCISES. 1. What can be said about the resultant system of a system of linear forms?

2. Let $\varphi_1(t_1, t_2), \ldots, \varphi_n(t_1, t_2)$ be homogeneous forms without a common factor. In the projective space consider the totality of points ξ with the property that the ratios of the coordinates of each point ξ are given by the parametric equation

$$\xi_1 : \xi_2 : \ldots : \xi_n = \varphi_1(\tau_1, \tau_2) : \varphi_2(\tau_1, \tau_2) : \ldots : \varphi_n(\tau_1, \tau_2) \tag{4}$$

for non-trivial τ-values. This totality, augumented by the sequence $\{0, \ldots, 0\}$, may also be characterized by homogeneous equations $F(\xi_1, \ldots, \xi_n) = 0$. [First express the ratios (4) as homogeneous equations in the ξ and τ .]

3. Let $f_1(x_1, \ldots, x_n) = 0, \ldots,$ be a system of homogeneous equations in which indeterminate parameters beside the x appear rationally. If the system has a solution for a particular indeterminate parameter, it has a solution for every specialization of this parameter.

4. Give an algebraic criterion for the solvability of a system of equations in several sequences of unknowns $x_1, \ldots, x_n; y_1, \ldots, y_m; \ldots,$ which are homogeneous in each one of these sequences.

In regard to the determination of the solutions of homogeneous equations, see also F. Mertens: *Sitzungsber. Wiener Akad. Wiss.* Bd. 108 (1889) p. 1174, as well as Section 83 of this volume.

81. ON INERTIA FORMS

In the previous section we obtained a resultant system for an arbitrary number of homogeneous forms. As a rule such a resultant system contains numerous forms. It will now be shown that for n forms in n variables a single resultant is sufficient, while in general for less than n forms no condition for solvability is necessary. In order to prove these results we will first establish a number of theorems concerning the so-called "inertia forms."

Let

$$\begin{aligned} f_1 &= a_1 x_1^{\lambda} + a_2 x_1^{\lambda-1} x_2 + \cdots + a_\omega x_n^{\lambda}, \\ f_2 &= b_1 x_1^{\mu} + b_2 x_1^{\mu-1} x_2 + \cdots + b_\omega x_n^{\mu}, \\ &\cdots\cdots \quad \cdots\cdots \quad \cdots\cdots \\ f_r &= e_1 x_1^{\nu} + c_2 x_1^{\nu-1} x_2 + \cdots + e_\omega x_n^{\nu} \end{aligned}$$

be r forms of degrees $l_1 = \alpha, l_2 = \beta, \ldots, l_r = \varepsilon$ such that all coefficients are indeterminates. It is to be noted that the last coefficients (therefore those of $x_n^{\alpha}, x_n^{\beta}, \ldots, x_n^{\varepsilon}$) are designated by $a_\omega, b_\omega, \ldots, e_\omega$. All following considerations refer to integral polynomials in the indeterminates $x_1, \ldots, x_n, a_1, \ldots, e_\omega$.

In Section 80 we encountered a polynomial T in $a_1, \ldots, e_\omega$ alone with the property

$$x_i^{\tau} T \equiv 0 (f_1, \ldots, f_r) \tag{1}$$

for a suitable i and τ. Such polynomials T are called *inertia forms*, a nomenclature due to Hurwitz. Each form contained in the resultant system of Section 80 is an inertia form.

Inertia forms may also be characterized as follows: set

$$\begin{aligned} f_1 &= f_1^* + a_\omega x_n^{\lambda}, \\ &\cdots\cdots \\ f_r &= f_r^* + e_\omega x_n^{\nu}, \end{aligned}$$

If we substitute

$$(2_i) \qquad \begin{cases} a_\omega = -\dfrac{f_1^*}{x_n^\alpha}, \\ \cdots\cdots\cdots \\ e_\omega = -\dfrac{f_r^*}{x_n^\varepsilon} \end{cases}$$

in (1), the forms $f_1, \ldots, f_r$ all vanish. Hence the left side of congruence (1) must also vanish. But x_i is not affected by substitution (2). Hence T must vanish after this substitution, that is,

$$(3) \qquad T\left(a_1, \ldots, -\frac{f_1^*}{x_n^\alpha}; \ldots; e_1, \ldots, -\frac{f_r^*}{x_n^\varepsilon}\right) = 0.$$

This conclusion follows as soon as we assume that congruence (1) is valid for *one* x_i.

Conversely, if for any polynomial $T(a_1, \ldots, a_\omega, \ldots, e_1, \ldots, e_\omega)$ relation (3) is satisfied, we can arrange T according to powers of $a_\omega + \frac{f_1^*}{x_n^\alpha}, \ldots, e_\omega + \frac{f_r^*}{x_n^\varepsilon}$ and show by means of (3) that the term independent of these powers vanishes. Hence it follows that

$$T \equiv 0\left(a_\omega + \frac{f_1^*}{x_n^\alpha}, \ldots, e_\omega + \frac{f_r^*}{x_n^\varepsilon}\right)$$

in the domain of fractions with denominators x_n^λ. On multiplying through by the highest power of x_n that appears in these denominators, all terms become integral and we obtain

$$x_n^\tau T \equiv 0(f_1, \ldots, f_r).$$

Hence if (1) is valid for one x_i, (3) is also; and if (3) is valid, (1) is also with x_n instead of x_i. It follows immediately that if (1) is valid for one x_i, (1) is also true for x_n. But the index n does not play a special role. Hence from the validity of (1) for one x_i it follows that (1) is satisfied by all other x_j. Therefore, (1) and (3) are equivalent, i.e., *inertia forms may be defined either by equation* (3) *or by* (1).

Obviously the sum and difference of two inertia forms as well as any multiple of an inertia form are inertia forms. Hence the inertia forms T form an *ideal* $\mathfrak{T}$.

The ideal $\mathfrak{T}$ is a prime ideal. Thus if a product $T_1 T_2$ has property (3), one of these factors also must satisfy (3).

The inertia forms may be used as the resultant system of Section 80. Thus if the forms $f_1, \ldots, f_r$ have a (non-trivial) common zero and we substitute this zero in (1), the member on the right vanishes. Since not all x_i are zero it follows that $T = 0$ for every inertia form. Conversely, if *all* inertia forms of a particular system $f_1, \ldots, f_r$ vanish, the resultant system in particular vanishes, and consequently the f_i have a common zero. Hence if the ideal $\mathfrak{T}$ of the inertia forms has a basis, this basis may also be used as a resultant system. This fact will be used in the next section.

We shall now prove:

If the number r of forms f_i is less than the number of variables n, then there is no inertia form distinct from zero. If $r = n$, there is no inertia form independent of e_ω and distinct from zero.

By the first half of this theorem it follows immediately that the resultant system of less than n forms vanishes identically. Hence in this case there always exists a common zero.

PROOF. First let $r < n$. If T were an inertia form distinct from zero, by (3) the quantities

$$-\frac{f_1^*}{x_n^\alpha}, \ldots, -\frac{f_r^*}{x_n^\varepsilon}$$

would be algebraically dependent relative to the polynomial domain of the elements $a_1, \ldots, a_{\omega-1}, \ldots, e_1, \ldots, e_{\omega-1}$. This result would also be true if we were to set $x_n = 1$.

Similarly, in the case $r = n$, if we were to assume that the hypothesis was false, the quantities

$$-\frac{f_1^*}{x_n^\alpha}, \quad -\frac{f_{n-1}^*}{x_n^\delta}$$

(where δ denotes the degree of the form f_{n-1}) would be algebraically dependent (f_n^* does not occur since T should be independent of e_ω). Here also we could set $x_n = 1$.

In each case therefore there would be a sequence of polynomials

$$[-f_1^*]_{x_n=1}, \ldots, [-f_s^*]_{x_n=1} \qquad (s < n)$$

algebraically dependent in relation to the polynomial domain of the $a_1, \ldots, a_{\omega-1}, \ldots, e_1, \ldots, e_{\omega-1}$. We shall now prove the following

LEMMA. *When a sequence of polynomials $f_1, \ldots, f_s$ in the indeterminates $a_1, \ldots, a_p, x_1, \ldots, x_q$ is algebraically dependent relative to the polynomial domain $\mathsf{K}[a_1, \ldots, a_p]$, where K is a domain of integrity, this dependence is also valid for every specialization $a_p = \alpha (\alpha \in \mathsf{K})$.*

PROOF OF LEMMA. By hypothesis a relation

$$F(a_1, \ldots, a_p, f_1, \ldots, f_s) = 0 \tag{4}$$

exists where F is a polynomial such that if $z_1, \ldots, z_s$ are indeterminates,

$$F(a_1, \ldots, a_p, z_1, \ldots, z_s) \neq 0 \tag{5}$$

We may assume that the polynomial $F(a,z)$ is not divisible by the factor $a_p - \alpha$; otherwise we could reduce (4) and (5) by this factor. Hence under this assumption F does not vanish for the substitution $a_p = \alpha$,

$$F(a_1, \ldots, a_{p-1}, \alpha, z_1, \ldots, z_s) \neq 0.$$

Furthermore the validity of (4) is preserved by the substitution $a_p = \alpha$. This proves the lemma.

On applying this lemma successively it follows that we may specialize several or all of the indeterminates $a_1, \ldots, a_{\omega-1}, \ldots, e_1, \ldots, e_{\omega-1}$ without losing the algebraic dependency.

We can now easily complete the proof that was interrupted by this lemma. We specialize the elements $a_1, \ldots, a_{\omega-1}, \ldots, e_{\omega-1}$ so that the forms $f_1^*, \ldots, f_s^*$ go over into $x_1^\alpha, \ldots, x_s^\delta$. Since $s < n$ these expressions remain unchanged by the previous substitution $x_n = 1$. Since the specialization does not alter the algebraic dependency the expressions $x_1^\alpha, \ldots, x_s^\delta$ must be algebraically dependent. But the latter are obviously independent. Hence our assumption is false and the theorem is proved.

However the result just proved for $r < n$ is not valid for $r = n$. Instead we have:

If $r = n$, there is a non-vanishing inertia form D_e. It is homogeneous in $a_1, \ldots, a_\omega$, in $b_1, \ldots, b_\omega$, etc., and of degree $L_n = l_1 l_2 \ldots l_{n-1}$ in $e_1, \ldots, e_\omega$.

PROOF. Let

$$\sum_1^n (l_\iota - 1) = l - 1.$$

The totality of power products in x_ι of degree l may be arranged as follows:

first, all power products which contain $x_1^{l_1}$;

then, all which contain $x_2^{l_2}$ but not $x_1^{l_1}$, etc.;

finally, all which contain $x_n^{l_n}$, but neither $x_1^{l_1}$ nor $x_2^{l_2}$, etc.

This process yields all power products of degree l since only those may be omitted which contain x_1 at most to the $(l_1 - 1)$-th power, etc., finally x_n at most to the $(l_n - 1)$-th power. These power products have at most the degree $\sum(l_\iota - 1)$ and therefore not the degree l. Let us designate the power products so obtained by

$$H_{l-l_1}^{(\nu)} x_1^{l_1}, H_{l-l_2}^{(\nu)} x_2^{l_2}, \ldots, H_{l-l_n}^{(\nu)} x_n^{l_n}, \tag{6}$$

where the $H_{l-l_\iota}^{(\nu)}$ designate power products of degree $l - l_\iota$. We note that the last category H_{l-l_n} contains only power products of degree $< l_1$ in $x_1, \ldots, < l_{n-1}$ in x_{n-1}, while the degree in x_n is determined by the condition that the total degree shall be $l - l_n$. Hence the last category contains exactly $l_1 l_2 \ldots l_{n-1}$ power products.

We now form all forms

$$H_{l-l_\iota}^{(\nu)} f_\iota. \tag{7}$$

There are evidently exactly as many of these as there are power products (6) of degree l. The matrix of the coefficients of the forms (7) is therefore square; its determinant D_e has by the specialization $f_\iota = x_\iota^{l_\iota}$ the value 1 and consequently cannot vanish identically. Furthermore D_e is an inertia form. Thus, if we multiply the equations

$$H_{l-l_\iota}^{(\nu)} f_\iota = \sum a_{\nu\mu} H_l^{(\mu)}$$

by the subdeterminants of a column of D_e and add, the left side becomes a linear combination of f_i and the right side $D_e \cdot H_i^{(\mu)}$. Hence if we let $H_i^{(\mu)} = x_i^l$, we obtain

$$D_e x_i^l \equiv 0 (f_1, \ldots, f_r).$$

Finally, D_e is homogeneous in the coefficients of every individual form f_i, and has the degree $L_n = l_1 l_2 \ldots l_{n-1}$ in the coefficients of f_n. This proves the theorem.

For further properties of inertia forms see A. Hurwitz: "Über die Trägheitsformen eines algebraischen Moduls," *Annali di Matematica* (3ª) 20 (1913).

82. THE RESULTANT OF n FORMS in n VARIABLES

Let $f_1, \ldots, f_n$ be n generic forms in $x_1, \ldots, x_n$, i.e., forms with indeterminate coefficients, $\mathfrak{T}$ the ideal generated by the inertia forms. We now seek in $\mathfrak{T}$ a polynomial of lowest possible degree in e_ω. There is such a polynomial and its degree in e_ω is not zero since there is no inertia form independent of e_ω except zero. If it is factored into indecomposable factors, at least one factor must belong to $\mathfrak{T}$ since $\mathfrak{T}$ is a prime ideal. This factor must have the same degree in e_ω as the polynomial under consideration since no polynomial in $\mathfrak{T}$ can have a lower degree in e_ω. We designate this factor by R and prove the theorem:

Every polynomial of the ideal $\mathfrak{T}$ is divisible by R.

PROOF. Arrange R in descending powers of e_ω:

$$R = S e_\omega^\lambda + \cdots \qquad (\lambda > 0,\ S \neq 0).$$

Let T be a polynomial in $\mathfrak{T}$. Since the degree of T in e_ω is at least λ, we can lower its degree in e_ω by multiplying T by S and subtracting an appropriate multiple of R. If we repeat this process until a polynomial is obtained whose degree is less than λ, we arrive at an equation of the form

$$S^\nu T - QR = T'.$$

Here T' also belongs to $\mathfrak{T}$ and its degree in e_ω is $<\lambda$. This implies that T' is zero and that $S^\nu T$ is divisible by R. However R is indecomposable and S is not divisible by R (since S is independent of e_ω). Hence T is divisible by R. Q.E.D.

We have shown that $\mathfrak{T}$ is a principal ideal with basis R. Hence R is uniquely determined up to a constant factor. We call R the *resultant* of the forms $f_1, \ldots, f_n$. This nomenclature is justified by the following remarks. If R vanishes for any specialization of the coefficients of the forms $f_1, \ldots, f_n$, all forms of the ideal $\mathfrak{T}$ must also vanish. In particular all forms of the resultant system of $f_1, \ldots, f_n$ must vanish; this implies that $f_1, \ldots, f_n$ must have a non-trivial zero in common. Conversely, if $f_1, \ldots, f_n$ have a non-trivial zero in common, the right-hand side of the identity

$$x_i^\tau R = A_1 f_1 + \cdots + A_n f_n$$

must vanish for this zero, hence the left-hand side must also. But there is at least

one x_i which does not vanish. Hence R must vanish. In view of the remarks made in the previous sections, R may be called a *resultant* of the forms $f_1, \ldots, f_n$ since $R = 0$ *is a necessary and sufficient condition for the existence of a non-trivial solution.*

We shall now prove a theorem on resultants which will be particularly useful in degree determinations.

If f_1 *is specialized to* $g \cdot h$, *where* g *and* h *are arbitrary forms of degree* μ, ν $(\mu + \nu = l_1)$, *then* R *is divisible by the product*

$$R_g \cdot R_h = R(g, f_2, \ldots, f_n) \cdot R(h, f_2, \ldots, f_n).$$

PROOF. From

$$x_n^j R = A_1 f_1 + \cdots + A_n f_n$$

it follows that

$$x_n^j \cdot R(gh, f_2, \ldots, f_n) = A_1 gh + A_2 f_2 + \cdots + A_n f_n.$$

Hence $R(gh, f_2, \ldots, f_n)$ belongs to the ideal $\mathfrak{T}_g$ generated by the forms $g, f_2, \ldots, f_n$ as well as to the corresponding ideal $\mathfrak{T}_h$. This means that $R(gh, f_2, \ldots, f_n)$ is divisible by R_g as well as by R_h, and (since these are both irreducible and distinct) by $R_g \cdot R_h$. Q.E.D.

Now let $f_1, \ldots, f_{n-1}$ be specialized as products of linear forms. By successive application of the above theorem it follows that R is divisible by a product of $L_n = l_1 l_2 \ldots l_{n-1}$ subresultants. By an earlier theorem each of these subresultants contains the e_i explicitly. Hence the product has at least the degree L_n in the e_i. On the other hand we have already seen that R has at most degree L_n in the e_i. Hence its degree is exactly L_n.

As in the case of D_e (Section 81), we may form D_a, D_b, ... by arranging the forms $f_1, \ldots, f_n$ so that f_1, respectively f_2, etc. occupies the last place. Then D_a has degree $L_1 = l_2 l_3 \ldots l_n$ in the a_i, D_b has degree $L_2 = l_1 l_3 \ldots l_n$ in the b_i, etc. Also $D_a, D_b, \ldots, D_e$ are each divisible by R and R has degree L_1 in a_i, degree L_2 in b_i, etc. The definition of R as a basis of the ideal $\mathfrak{T}$ does not depend on the ordering of the forms $f_1, \ldots, f_n$. Furthermore R has the highest degree which a common divisor of $D_a, D_b, \ldots, D_e$ can have. Hence:

R is the greatest common divisor of the polynomials $D_a, D_b, \ldots, D_e$.

D_e has by the specialization $f_i = x_i^{l_i}$ $(i = 1, \ldots, n)$ the value 1, and R is a divisor of D_e. Hence for this specialization R has the value ± 1, i.e., R contains a term

$$\pm a_1^{L_1} \ldots e_\omega^{L_n}.$$

We normalize R so that the sign of this "principal term" comes out with the plus sign.

The statement made earlier, i.e., that R is divisible by $R_g R_h$ for $f_1 = g \cdot h$, can now be sharpened to

$$R_{gh} = R_g R_h.$$

This can be seen by comparing the degrees and the principal terms of both members.

We recapitulate:

n generic forms in n variables have a resultant R which is an indecomposable integral polynomial in their (indeterminate) coefficients and may be defined as a basis of the ideal of their inertia forms. The vanishing of this resultant for particular $f_1, \ldots, f_n$ *with coefficients in a field is necessary and sufficient for the existence of a solution of the system of equations* $f_1 = 0, \ldots, f_n = 0$ *distinct from the zero solution. The resultant is homogeneous in the coefficients of* f_1 *of degree* $L_1 = l_2 \ldots l_n$, *etc. It contains a principal term* $a_1^{L_1} \ldots a_\omega^{L_n}$ *and takes on by the specialization* $f_i = x_i^{l_i}$ *the value 1. By the specialization* $f_1 = g \cdot h$, R *becomes equal to the product* $R_g \cdot R_h$. *Finally R is the greatest common divisor of the n known determinants* $D_a, D_b, \ldots, D_e$.

EXERCISES. 1. In the case of two forms in two variables show that the resultant agrees with the Sylvester resultant (Section 27).

2. In the case of a form f of degree l and $n - 1$ linear forms

$$\sum b_i x_i, \ldots, \sum e_i x_i$$

the resultant has the value

$$f(X_1, \ldots, X_n),$$

where $X_1, \ldots, X_n$ are the $(n - 1)$-rowed subdeterminants of the matrix

$$\begin{pmatrix} b_1 & \ldots & b_n \\ \ldots & \ldots & \ldots \\ e_1 & \ldots & e_n \end{pmatrix}.$$

3. The resultant is absolutely indecomposable.

4. In the forms $f_1, \ldots, f_n$ introduce new variables by a linear substitution with non-vanishing determinant

$$x_i = \sum a_{ik} x_k'.$$

Show that the resultant of the transformed forms in $x_1', \ldots, x_n'$ is equal to the resultant of $f_1, \ldots, f_n$ up to a factor dependent on the a_{ik}.

For further properties of the resultant see the text quoted earlier (Section 28 and Section 78) of F. S. Macaulay: *Modular Systems*, as well as that of E. Fischer: "Über die Cayleysche Eliminationsmethode." *Math. Z.*, Vol. 26 (1927) pp. 497-550.

83. THE u-RESULTANT AND THE THEOREM OF BEZOUT

By a *solution ray* (cf. Section 80) of a system of homogeneous equations we understand the totality of solutions $\{\lambda\xi_1, \ldots, \lambda\xi_n\}$ which are proportional to a fixed non-trivial solution $\{\xi_1, \ldots, \xi_n\}$. We assume now that the system of equations

(1) $$f_1 = 0; \ldots, f_r = 0$$

has only a finite number of solution rays $\{\xi_1^{(\alpha)}, \ldots, \xi_n^{(\alpha)}\}$ $(\alpha = 1, \ldots, q)$, and seek to determine these rays.

To the polynomials $f_1, \ldots, f_r$ we add the linear form with indeterminate coefficients

$$l = u_1 x_1 + \cdots + u_n x_n$$

and form the resultant system $b_1(u), \ldots, b_t(u)$ of the forms $f_1, \ldots, f_r, l$. This resultant system vanishes for particular $u_1, \ldots, u_n$ if and only if a solution $\{\xi^{(\alpha)}\}$ of (1) also satisfies the condition

$$l_\alpha = u_1 \xi_1^{(\alpha)} + \cdots + u_n \xi_n^{(\alpha)} = 0.$$

In other words: the common zeros of the forms $b_1(u), \ldots, b_t(u)$ (as forms in the u) are exactly the zeros of the product $\prod_\alpha l_\alpha$.

By Hilbert's Nullstellensatz (Section 79) we have on the one hand

(2) $$(b_i(u))^{r_i} \equiv 0 \quad (\prod_\alpha l_\alpha) \qquad (i = 1, \ldots, t),$$

and on the other hand that

(3) $$(\prod_\alpha l_\alpha)^r \equiv 0 \quad (b_1(u), \ldots, b_t(u)).$$

Now the l_α are linear forms in the u and therefore are indecomposable. From (2) the $b_i(u)$, and consequently their greatest common divisor $D(u)$, are divisible by all the linear factors l_α. But by (3) we have

$$(\prod_\alpha l_\alpha)^r \equiv 0 \quad (D(u)).$$

Hence $D(u)$ can contain no other linear factors but these l_α, therefore

(4) $$D(u) = \prod l_\alpha^{\varrho_\alpha}, \quad \varrho_\alpha > 0.$$

This means that *the linear forms l_α which determine the solution rays of* (1) *are found by factoring the form $D(u)$*. The form $D(u)$, which is the greatest common divisor of the resultant system of $f_1, \ldots, f_r$ and l, is called the *u-resultant* of $f_1, \ldots, f_r$.

Now let us consider the case of $n-1$ homogeneous equations in n variables which have a finite number of solution rays. If we add to this system the linear form l, we obtain n forms which have a single resultant $R(u)$. Naturally $R(u)$ is the same as the u-resultant and factors according to (4). The solutions appear with known *multiplicities* ϱ_α. The sum of the ϱ_α is the degree of $R(u)$ and therefore the product of the degrees of the forms $f_1, \ldots, f_{n-1}$ (cf. Section 82). We have thus proved the *theorem of Bezout*:

If $n-1$ homogeneous equations in n variables have only a finite number of solution rays, the sum of the multiplicities defined by (4) *of the solution rays is equal to the product of the degrees of the equations.*

For $n = 3$ and $n = 4$ the following geometric theorem is involved in this theorem: the sum of the multiplicities of the intersection points of two algebraic curves in the projective plane, respectively, three algebraic surfaces in the projective space, is equal to the product of the degrees of these curves, respectively, surfaces. The multiplicities are positive integers which are defined by the exponents of the linear factors of $R(u)$.

EXERCISE. Show that the first result of this section may be stated for homogeneous equations in two sequences of variables $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_m)$, if we replace the linear form l by $\sum\sum u_{ik} x_i y_k$.

For further remarks on the Theorem of Bezout see B. L. v. d. Waerden, *Einführung in die algebraische Geometrie*, Bd. LI of this series, Berlin 1939, especially Section 17 and Section 41.

CHAPTER XII

GENERAL IDEAL THEORY OF COMMUTATIVE RINGS

84. BASIS CONDITION AND DIVISOR CHAIN CONDITION

In this chapter we shall investigate the divisibility properties of the ideals of commutative rings and determine the extent to which the simple laws that are valid in a domain such as integers may be carried over to more general rings. In order to avoid situations that are unduly complicated, we shall restrict our investigations to rings in which every ideal has a finite basis. As we shall see, this condition is satisfied in a great many important cases.

We say that the *basis condition is valid* in a ring $\mathfrak{o}$ when every ideal in $\mathfrak{o}$ has a finite basis.

The basis condition is satisfied in every field since (0) and (1) are the only ideals that exist in a field. It is valid in the ring of integers, in every principal ideal ring, and in every finite ring. We shall see later that it is valid in every residue class ring $\mathfrak{o}/\mathfrak{a}$ whenever it is valid in $\mathfrak{o}$. Finally, we have the following theorem which goes back essentially to Hilbert:

If the basis condition is valid in the ring $\mathfrak{o}$ *which contains an identity element, then it is valid in the polynomial domain* $\mathfrak{o}[x]$.

PROOF. Let $\mathfrak{A}$ be an ideal in $\mathfrak{o}[x]$. The coefficients of the highest powers of x in the polynomials of $\mathfrak{A}$, together with zero, form an ideal in $\mathfrak{o}$. Thus, if α and β are the leading coefficients of polynomials a, b:

$$a = \alpha x^n + \cdots,$$

$$b = \beta x^m + \cdots,$$

and if we assume that $n \geqq m$, then

$$a - bx^{n-m} = (\alpha x^n + \cdots) - (\beta x^n + \cdots)$$

$$= (\alpha - \beta)x^n + \cdots$$

is also a polynomial in $\mathfrak{A}$ and $\alpha - \beta$ is either its leading coefficient or zero. Similarly, if α is the leading coefficient of a, then $\lambda\alpha$ is either the leading coefficient of λa or zero.

This ideal $\mathfrak{a}$, consisting of the leading coefficients, has by hypothesis a basis $(\alpha_1, \ldots, \alpha_r)$. Let us say that α_i is the leading coefficient of the polynomial

$$a_i = \alpha_i x^{n_i} + \cdots$$

of degree n_i and that n is the largest of the finitely many integers n_i.

The polynomials a_i are assumed to be elements of the basis of $\mathfrak{A}$ which we are trying to construct. We shall now determine what other polynomials are necessary for a basis.

If

$$f = \alpha x^N + \cdots$$

is a polynomial of $\mathfrak{A}$ of degree $N \geqq n$, α must belong to the ideal $\mathfrak{a}$:

$$\alpha = \sum \lambda_i \alpha_i .$$

Now form the polynomial

$$f_1 = f - \sum (\lambda_i x^{N-n_i}) a_i .$$

The coefficient of x^N in this polynomial is

$$\alpha - \sum \lambda_i \alpha_i = 0;$$

hence f_1 has degree $< N$. Therefore the polynomial f may be replaced modulo $(a_1, \ldots, a_r)$ by a polynomial of lower degree. We can continue this process until we arrive at a polynomial of degree less than n. Consequently, from now on, it is sufficient to consider only polynomials of bounded degrees $(<n)$.

The coefficients of x^{n-1} in the polynomials of degree $\leqq n-1$ in $\mathfrak{A}$ form, together with zero, an ideal $\mathfrak{a}_{n-1}$. Let

$$(\alpha_{r+1}, \ldots, \alpha_s)$$

be a basis of this ideal. Furthermore, let α_{r+i} be the leading coefficient of the polynomial

$$a_{r+i} = \alpha_{r+i} x^{n-1} + \cdots$$

We now assume that the polynomials $a_{r+1}, \ldots, a_s$ are also elements of the basis under construction. Then every polynomial of degree $\leqq n-1$ may be replaced modulo $(a_{r+1}, \ldots, a_s)$ by a polynomial of degree $\leqq n-2$; as above we need only to subtract a suitably chosen linear combination

$$\sum \lambda_{r+i} a_{r+i}.$$

Let us continue in this manner. The coefficients of x^{n-2} in the polynomials of degree $\leqq n-2$ form, together with zero, an ideal $\mathfrak{a}_{n-2}$, whose basis elements $\alpha_{s+1}, \ldots, \alpha_t$ belong to the polynomials $a_{s+1}, \ldots, a_t$. We again assume that these polynomials are elements of the basis under construction. Finally, we arrive at an ideal $\mathfrak{a}_0$ consisting only of constants belonging to $\mathfrak{A}$; its basis elements $(\alpha_{v+1}, \ldots, \alpha_w)$ belong to the polynomials $a_{v+1}, \ldots, a_w$. Hence every polynomial of $\mathfrak{A}$ must be congruent to zero modulo

$$(a_1, \ldots, a_r, a_{r+1}, \ldots, a_s, \ldots, a_{v+1}, \ldots, a_w),$$

that is, the polynomials $a_1, \ldots, a_v$ form a basis of the ideal $\mathfrak{A}$ and the basis condition is satisfied.

By applying this theorem n times we immediately obtain the following generalization:

If the basis condition is valid in a ring $\mathfrak{o}$ *with an identity element, then it is also valid in the polynomial domain* $\mathfrak{o}[x_1, \ldots, x_n]$ *where* $x_1, \ldots, x_n$ *are indeterminates and* n *is finite.*

The most important special cases are: the polynomial domain over the ring of integers $C[x_1, \ldots, x_n]$ and every polynomial domain $K[x_1, \ldots, x_n]$ with coefficients in a field K. For all these domains every ideal has a finite basis.

Hilbert states his theorem only for these cases and in a form which seems perhaps to be more general, namely:

In every subset $\mathfrak{M}$ *of* $\mathfrak{o}$ *(not only in every ideal) there is a finite number of elements* $m_1, \ldots, m_r$ *such that every element* m *of* $\mathfrak{M}$ *can be written in the form*

$$\lambda_1 m_1 + \cdots + \lambda_r m_r \qquad (\lambda_i \text{ in } \mathfrak{o})$$

However, this condition is an immediate consequence of the basis condition for ideals. Thus, if $\mathfrak{A}$ is the ideal generated by $\mathfrak{M}$, then $\mathfrak{A}$ has first of all a basis

$$\mathfrak{A} = (a_1, \ldots, a_s).$$

Every element a_i depends (since it is an element of the ideal generated by $\mathfrak{M}$) on a finite number of elements of $\mathfrak{M}$:

$$a_i = \sum_k \lambda_{ik} m_{ik}.$$

Hence all elements of $\mathfrak{A}$ are linearly dependent on a finite number of the elements m_{ik}; in particular this is valid for the elements of $\mathfrak{M}$.

It is important that the basis condition is equivalent to the following "divisor chain condition." [1]

Divisor Chain Condition, First Statement

If a chain of ideals $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ *in* $\mathfrak{o}$ *is given and if every* $\mathfrak{a}_{i+1}$ *is a proper divisor of* $\mathfrak{a}_i$*:*

$$\mathfrak{a}_i \subset \mathfrak{a}_{i+1},$$

the chain breaks off after a finite number of terms.

This is equivalent to

Divisor Chain Condition, Second Statement

If an infinite chain of divisors $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ *is given:*

[1] This is also referred to as the "ascending chain condition."

$$\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$$

all terms must be equal after a certain n:

$$\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots.$$

We shall first show that the divisor chain condition follows from the basis condition.

Let $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ be an infinite chain such that $\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$ for all i. The union $\mathfrak{v}$ of all ideals $\mathfrak{a}_i$ is an ideal. Thus, if a and b lie in $\mathfrak{v}$, say that a is in $\mathfrak{a}_n$ and b in $\mathfrak{a}_m$, then a and b are both in $\mathfrak{a}_N$, where N is the larger of the numbers n and m. Hence $a - b$ lies in $\mathfrak{a}_N$ and therefore in $\mathfrak{v}$. Furthermore, if a is in $\mathfrak{v}$, say in $\mathfrak{a}_n$, then λa is also in $\mathfrak{a}_n$ and hence in $\mathfrak{v}$.

By the hypothesis the ideal $\mathfrak{v}$ has a basis $(a_1, \ldots, a_r)$. Every a_i lies in an ideal $\mathfrak{a}_{n_i}$. If n is the largest of the numbers n_i, then $a_1, \ldots, a_r$ all lie in $\mathfrak{a}_n$. Since all elements of $\mathfrak{v}$ depend linearly on $a_1, \ldots, a_r$, all elements of $\mathfrak{v}$ lie in $\mathfrak{a}_n$ and hence

$$\mathfrak{v} = \mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots.$$

Conversely, the basis condition follows from the divisor chain condition. Let $\mathfrak{a}$ be an ideal, a_1 an arbitrary element of $\mathfrak{a}$. If a_1 does not generate the whole ideal, there is an element in $\mathfrak{a}$ which does not lie in (a_1). Let a_2 be such an element. Then

$$(a_1) \subset (a_1, a_2).$$

If a_1 and a_2 still do not generate the whole ideal $\mathfrak{a}$, there is a third element a_3 in $\mathfrak{a}$ which does not lie in (a_1, a_2), etc. Continuing in this manner we obtain a divisor chain

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots$$

which must break off after a finite (say r) number of steps. It follows that

$$(a_1, a_2, \ldots, a_r) = \mathfrak{a};$$

hence $\mathfrak{a}$ has a finite basis.[2]

If the divisor chain condition is valid in a ring $\mathfrak{o}$, *it is also valid in every residue class ring* $\mathfrak{o}/\mathfrak{a}$.

PROOF. An ideal $\bar{\mathfrak{b}}$ in $\mathfrak{o}/\mathfrak{a}$ is a set of residue classes. If we form the set-union of all these residue classes, we obtain an ideal $\mathfrak{b}$ in $\mathfrak{o}$. Conversely, let $\mathfrak{b}$ uniquely determine $\bar{\mathfrak{b}}$ by the relation

$$\bar{\mathfrak{b}} = \mathfrak{b}/\mathfrak{a}.$$

A chain of ideals $\bar{\mathfrak{b}}_1 \subset \bar{\mathfrak{b}}_2 \subset \bar{\mathfrak{b}}_3 \subset \ldots$ in $\mathfrak{o}/\mathfrak{a}$ is determined in this manner by a chain of ideals $\mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \mathfrak{b}_3 \subset \ldots$ in $\mathfrak{o}$. Since the latter breaks off after a finite number of terms, the former must do the same.

[2] In this proof we have used the axiom of choice. Cf. O. Teichmüller, *Deutsche Mathematik*, Vol. 4 (1939) p. 567.

This proves the statement made at the beginning of this section, namely, that the basis condition in $\mathfrak{o}$ implies the basis condition in $\mathfrak{o}/\mathfrak{a}$.

The divisor chain condition may be stated in two other forms, which are frequently more useful in applications:

Divisor Chain Condition, Third Statement: Maximal Condition

If the divisor chain condition is valid in $\mathfrak{o}$, *then in every non-empty set of ideals there is a maximal ideal, i.e., an ideal which is contained in no other ideal of the set.*

PROOF. In every non-empty set of ideals let one ideal be marked. Now if we assume that in a set $\mathfrak{M}$ of ideals there is no maximal ideal, then every ideal of the set must be contained in another ideal of the set. There is in $\mathfrak{M}$ one of the marked ideals, say $\mathfrak{a}_1$. Furthermore, the set of those ideals of $\mathfrak{M}$ which contain $\mathfrak{a}_1$ and $\neq \mathfrak{a}_1$ must contain a marked ideal, say $\mathfrak{a}_2$, etc. Continuing we are led to an infinite chain

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \ldots$$

which contradicts the hypothesis.

Divisor Chain Condition, Fourth Statement: Principle of Divisor Induction

If the divisor chain condition is valid in $\mathfrak{o}$ *and a property E is valid for every ideal* $\mathfrak{a}$ (*in particular for the unit ideal*) *as soon as it is satisfied by all proper divisors of* $\mathfrak{a}$, *then the property E is valid for all ideals.*

PROOF. Let us assume that the property E is not valid for an ideal. By the third statement of the divisor chain condition there must be a maximal ideal $\mathfrak{a}$ which does not satisfy property E. But on account of the maximality, all proper divisors of $\mathfrak{a}$ must satisfy the property E. Hence $\mathfrak{a}$ must also, which is a contradiction.

85. PRODUCTS AND QUOTIENTS OF IDEALS

As in Section 17 we understand by the *greatest common divisor* (G.C.D.) or the *sum* of the ideals $\mathfrak{a}, \mathfrak{b}, \ldots$ the ideal $(\mathfrak{a}, \mathfrak{b}, \ldots)$ generated by their set-union, and similarly by the *least common multiple* (L.C.M.) the intersection $[\mathfrak{a}, \mathfrak{b}, \ldots] = \mathfrak{a} \cap \mathfrak{b} \cap \ldots$. The same notation as for the sum of ideals shall be used to denote the ideal generated by an element and an ideal:

$$(\mathfrak{a}, b) = (\mathfrak{a}, (b)).$$

It is obvious that $(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{b}, \mathfrak{a})$, $((\mathfrak{a}, \mathfrak{b},) \mathfrak{c}) = (\mathfrak{a}, (\mathfrak{b}, \mathfrak{c})) = (\mathfrak{a}, \mathfrak{b}, \mathfrak{c})$, etc. Furthermore

$$((a_1, a_2, \ldots), (b_1, b_2, \ldots)) = (a_1, a_2, \ldots, b_1, b_2, \ldots),$$

that is, *we obtain a basis for the greatest common divisor when we write one after another the bases of the individual ideals.*

If the elements of an ideal $\mathfrak{a}$ are multiplied by those of an ideal $\mathfrak{b}$, the products ab (in contrast to the sums) generally do not form an ideal.[3] The ideal generated by the products ab is called the *product* of the ideals $\mathfrak{a}$, $\mathfrak{b}$ and is denoted by $\mathfrak{a} \cdot \mathfrak{b}$ or $\mathfrak{a}\mathfrak{b}$. It consists of all sums $\sum a_i b_i$ (a_i in $\mathfrak{a}$, b_i in $\mathfrak{b}$).

It is obvious that

$$\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{b} \cdot \mathfrak{a},$$

$$(\mathfrak{a} \cdot \mathfrak{b}) \cdot \mathfrak{c} = \mathfrak{a} \cdot (\mathfrak{b} \cdot \mathfrak{c}).$$

Hence we can operate with products of ideals as with usual products. In particular we may speak of *powers* $\mathfrak{a}^\varrho$ of an ideal; these are defined by

$$\mathfrak{a}^1 = \mathfrak{a}; \qquad \mathfrak{a}^{\varrho+1} = \mathfrak{a} \cdot \mathfrak{a}^\varrho.$$

If $\mathfrak{a} = (a_1, \ldots, a_n)$ and $\mathfrak{b} = (b_1, \ldots, b_m)$, the product $\mathfrak{a}\mathfrak{b}$ is evidently generated by the products $a_i b_k$. Hence *we obtain a basis for the product by multiplying all the basis elements of one factor by all basis elements of the other.*

In particular for principal ideals we have

$$(a) \cdot (b) = (ab),$$

hence in the domain of the elements of $\mathfrak{o}$ the definition of product coincides with the usual one.

The product $\mathfrak{a} \cdot (b)$ of an arbitrary ideal and a principal ideal consists of all products ab where a is in $\mathfrak{a}$. Therefore we simply write $\mathfrak{a}b$ or $b\mathfrak{a}$.

A further rule is the "distributive law of ideals"

$$\mathfrak{a} \cdot (\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a} \cdot \mathfrak{b}, \mathfrak{a} \cdot \mathfrak{c}). \tag{1}$$

Thus, since $\mathfrak{a} \cdot (\mathfrak{b}, \mathfrak{c})$ is generated by the products $a(b + c)$ and

$$a(b + c) = ab + ac,$$

then all such products lie in $(\mathfrak{a} \cdot \mathfrak{b}, \mathfrak{a} \cdot \mathfrak{c})$. Conversely, $(\mathfrak{a} \cdot \mathfrak{b}, \mathfrak{a} \cdot \mathfrak{c})$ is generated by the products ab and the products ac, which all lie in $\mathfrak{a} \cdot (\mathfrak{b}, \mathfrak{c})$.

Rule (1) is also valid when several or infinitely many ideals stand in the parenthesis instead of $\mathfrak{b}, \mathfrak{c}$.

Since all products ab lie in $\mathfrak{a}$, it follows that

$$\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a}$$

and similarly

$$\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{b}.$$

Hence

$$\mathfrak{a} \cdot \mathfrak{b} \subseteq [\mathfrak{a}, \mathfrak{b}],$$

that is, *the product is divisible by the least common multiple.*

[3] EXAMPLE. In a polynomial domain, let $\mathfrak{a} = (x, y)$ and $\mathfrak{b} = (x^2, y)$. Then x^3 and y^2 are products of the form $a \cdot b$ but $x^3 - y^2$ is not.

In the ring of integers the product of the least common multiple and greatest common divisor of two ideals $\mathfrak{a}$, $\mathfrak{b}$ is equal to the product $\mathfrak{a}\mathfrak{b}$. This is not valid in an arbitrary ring; instead we have

$$[\mathfrak{a} \cap \mathfrak{b}] \cdot (\mathfrak{a}, \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}. \tag{2}$$

PROOF.

$$[\mathfrak{a} \cap \mathfrak{b}] \cdot (\mathfrak{a}, \mathfrak{b}) = ([\mathfrak{a} \cap \mathfrak{b}] \cdot \mathfrak{a}, [\mathfrak{a} \cap \mathfrak{b}] \cdot \mathfrak{b}) \subseteq (\mathfrak{b} \cdot \mathfrak{a}, \mathfrak{a} \cdot \mathfrak{b}) = \mathfrak{a} \cdot \mathfrak{b}.$$

The ideal $\mathfrak{o}$, which contains *all* elements of the given ring, is called according to Section 16 a *unit ideal*. Naturally we have

$$\mathfrak{a} \cdot \mathfrak{o} \subseteq \mathfrak{a}.$$

Conversely, if $\mathfrak{o}$ contains an identity e, we also have

$$\mathfrak{a} = \mathfrak{a} \cdot e \subseteq \mathfrak{a} \cdot \mathfrak{o},$$

therefore

$$\mathfrak{a} \cdot \mathfrak{o} = \mathfrak{a}.$$

In this case the ideal $\mathfrak{o}$ plays the role of an identity with respect to multiplication. It is generated by the identity element.

It is always true that

$$(\mathfrak{a}, \mathfrak{o}) = \mathfrak{o}; \qquad \mathfrak{a} \cap \mathfrak{o} = \mathfrak{a}.$$

By the *quotient ideal* $\mathfrak{a}:\mathfrak{b}$, where $\mathfrak{a}$ is an ideal, we understand the totality of elements γ of $\mathfrak{o}$ such that

$$\gamma b \equiv 0 (\mathfrak{a}) \text{ for all } b \text{ in } \mathfrak{b}. \tag{3}$$

This totality is an ideal. Thus, if γ and δ satisfy (3), so does $\gamma - \delta$; and if γ satisfies (3), so does $r\gamma$. Here it is assumed that $\mathfrak{a}$ is an ideal. However, $\mathfrak{b}$ need not be an ideal; it may be an arbitrary set of elements or a single element.

The definition of quotient ideal implies, if $\mathfrak{a}$ and $\mathfrak{b}$ are ideals, that

$$\mathfrak{b} \cdot (\mathfrak{a}:\mathfrak{b}) \subseteq \mathfrak{a}.$$

In the ring of integers the quotient ideal of two principal ideals (a), $(b) \neq (0)$ is constructed out of the factors of the number a which are not also factors of b; for instance:

$$(12):(2) = (6),$$
$$(12):(4) = (3),$$
$$(12):(8) = (3),$$
$$(12):(5) = (12).$$

In other words, we divide a in the usual sense by the greatest common divisor (a, b).

In general rings a corresponding rule is valid:

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

This may be easily proved and is not very important for our purposes.

Obviously $\mathfrak{a} \subseteq \mathfrak{a}:\mathfrak{b}$, since every element of $\mathfrak{a}$ satisfies (3). There are therefore two extreme cases:

$$\mathfrak{a}:\mathfrak{b} = \mathfrak{o} \quad \text{and} \quad \mathfrak{a}:\mathfrak{b} = \mathfrak{a}.$$

The first case occurs among others when $\mathfrak{b} \subseteq \mathfrak{a}$ since for every γ we have under this assumption

$$\gamma\mathfrak{b} \equiv 0(\mathfrak{b}) \equiv 0(\mathfrak{a}).$$

The second case means that if $\gamma\mathfrak{b} \equiv 0(\mathfrak{a})$, then $\gamma \equiv 0(\mathfrak{a})$. Hence the congruence $\gamma\mathfrak{b} \equiv 0(\mathfrak{a})$ may be written without $\mathfrak{b}$. In this case we say that $\mathfrak{b}$ is *prime relative to* (relativ prim zu) $\mathfrak{a}$ or prime to $\mathfrak{a}$; however, we will seldom use this expression which may easily be a source of confusion, and usually we will explicitly write the equation $\mathfrak{a}:\mathfrak{b} = \mathfrak{a}$. In the case of integers a and b, both $\neq 0$, this criterion may obviously be stated as follows:

$$\gamma b \equiv 0(a) \text{ implies } \gamma \equiv 0(a)$$

only if a and b have no common prime factors. In more general cases however the expression "prime relative to" is *not symmetric*; for instance, if $\mathfrak{a}$ is a prime ideal and $\mathfrak{b}$ is a prime ideal distinct from $\mathfrak{o}$ and a proper divisor of $\mathfrak{a}$, then

$$\mathfrak{a}:\mathfrak{b} = \mathfrak{a}, \text{ so that } \mathfrak{b} \text{ is prime relative to } \mathfrak{a},$$

$$\mathfrak{b}:\mathfrak{a} = \mathfrak{o}, \text{ so that } \mathfrak{a} \text{ is not prime relative to } \mathfrak{b}.$$

For example,

$$(0):(2) = (0),$$

$$(2):(0) = (1).$$

The following rule is important:

(4) $$[\mathfrak{a}_1, \ldots, \mathfrak{a}_r]:\mathfrak{b} = [\mathfrak{a}_1:\mathfrak{b}, \ \ldots, \mathfrak{a}_r:\mathfrak{b}].$$

PROOF. If

$$\gamma\mathfrak{b} \subseteq [\mathfrak{a}_1, \quad , \mathfrak{a}_r],$$

then

$$\gamma\mathfrak{b} \subseteq \mathfrak{a}_i \text{ for every } i$$

and conversely.

EXERCISES. 1. Prove the following rules:

$$(\mathfrak{a}:\mathfrak{b}):\mathfrak{c} = \mathfrak{a}:\mathfrak{b}\mathfrak{c} = (\mathfrak{a}:\mathfrak{c}):\mathfrak{b},$$

$$\mathfrak{a}:(\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a}:\mathfrak{b}) \cap (\mathfrak{a}:\mathfrak{c}).$$

2. Show that the following three statements are equivalent:

a) $\mathfrak{a}:\mathfrak{b}_1 = \mathfrak{a}$ and $\mathfrak{a}:\mathfrak{b}_2 = \mathfrak{a}$;

b) $\mathfrak{a}:[\mathfrak{b}_1 \cap \mathfrak{b}_2] = \mathfrak{a}$;

c) $\mathfrak{a}:\mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{a}$.

86. PRIME IDEALS AND PRIMARY IDEALS

We have already defined a prime ideal as an ideal whose residue class ring contains no divisors of zero.

In the ring of integers every integer $a > 0$ is the product of powers of distinct prime numbers

$$a = p_1^{e_1} \dots p_r^{e_r}, \tag{1}$$

and accordingly every ideal (a) is the product of powers of prime ideals:

$$(a) = (p_1)^{e_1} \dots (p_r)^{e_r}.$$

In more general rings we can not expect that the decomposition of its ideals will be as simple as this. For example, in the polynomial domain of the indeterminate x over the ring of integers the ideal $(4, x)$, which is not prime, has beside 0 only one prime divisor, i.e., $(2, x)$; however, the ideal $(4, x)$ cannot be expressed as a power of $(2, x)$. Hence in general an ideal will not have a representation as a product; at most an ideal will have a representation as the L.C.M. (intersection) of components,[4] similar to the representation of (a) as the L.C.M. which follows from (1):

$$(a) = [(p_1^{e_1}), \dots, (p_r^{e_r})].$$

The ideals $(p_k^{e_k})$ have the following characteristic property: if a product ab is divisible by $p_k^{e_k}$ and the factor a is not, then the other factor b must contain at least a factor of $p_k^{e_k}$. This means that a power b^e must be divisible by $p_k^{e_k}$. Hence,

$$ab \equiv 0 (p_k^{e_k}),$$

$$a \not\equiv 0 (p_k^{e_k})$$

implies

$$b^e \equiv 0 (p_k^{e_k}).$$

Ideals with this property are called *primary ideals.*

An ideal $\mathfrak{q}$ *is said to be primary if*

$$ab \equiv 0 (\mathfrak{q}), \quad a \not\equiv 0 (\mathfrak{q})$$

implies that there is a ϱ *such that*

$$b^\varrho \equiv 0 (\mathfrak{q}).$$

This definition may also be stated as follows:

In the residue class ring modulo $\mathfrak{q}$ *if* $\bar{a}\bar{b} = 0$ *and* $\bar{a} \neq 0$, *then a power* $\bar{b}^\varrho$ *vanishes.*

If $\bar{a}\bar{b} = 0$ and $\bar{a} \neq 0$, then b is a zero divisor. If a ring element b has the property that a power b^ϱ vanishes, the element is said to be *nilpotent.* Hence we may also say:

[4] An L.C.M. representation is in certain cases more useful than a representation as a product, particularly if we wish to decide whether an element b is divisible by an ideal $\mathfrak{m}$, i.e., belongs to $\mathfrak{m}$. If $\mathfrak{m} = [\mathfrak{a}_1, \dots, \mathfrak{a}_r]$, b belongs to $\mathfrak{m}$ if and only if b belongs to all $\mathfrak{a}_\nu$.

An ideal is primary if in its residue class ring every divisor of zero is nilpotent.

It follows immediately that this definition is a slight modification of the definition of a prime ideal; for, in the residue class ring modulo a prime ideal every divisor of zero must not only be nilpotent but also vanish.

We shall see that for general rings the primary ideals play the same role as the powers of prime numbers do in the ring of integers. In particular under very general assumptions it shall be shown that every ideal may be represented as the intersection of primary ideals and that by such representations the fundamental structure properties of ideals may be exhibited.

A primary ideal is not necessarily a power of a prime ideal. This has already been illustrated by the ideal $(4, x)$, introduced at the beginning of this section, which may easily be shown to be primary. The converse is also valid; for in the ring of polynomials $a_0 + a_1 x \cdots + a_n x^n$ with integers as coefficients for which a_1 is divisible by 3, $\mathfrak{p} = (3x, x^2, x^3)$ is a prime ideal but $\mathfrak{p}^2 = (9x^2, 3x^3, x^4, x^5, x^6)$ is not primary since

$$9 \cdot x^2 \equiv 0 (\mathfrak{p}^2),$$

$$x^2 \not\equiv 0 (\mathfrak{p}^2),$$

$$9^\varrho \not\equiv 0 (\mathfrak{p}^2)$$

for every ϱ.

Properties of Primary Ideals Independent of the Divisor Chain Condition

I. *To every primary ideal* $\mathfrak{q}$ *there exists a prime ideal divisor* $\mathfrak{p}$ *which may be defined as follows:* $\mathfrak{p}$ *is the totality of elements* b *such that a power* b^ϱ *lies in* $\mathfrak{q}$.

PROOF. First, $\mathfrak{p}$ is an ideal. Thus, if $b^\varrho \equiv 0 (\mathfrak{q})$, then $(rb)^\varrho \equiv 0 (\mathfrak{q})$, and if $b^\varrho \equiv 0 (\mathfrak{q})$ and $c^\sigma \equiv 0 (\mathfrak{q})$, then

$$(b - c)^{\varrho+\sigma-1} \equiv 0 (\mathfrak{q}),$$

since in the development of $(b - c)^{\varrho+\sigma-1}$ every summand contains either b^ϱ or c^σ.

Secondly, $\mathfrak{p}$ is prime. Thus, if

$$ab \equiv 0 (\mathfrak{p}),$$

$$a \not\equiv 0 (\mathfrak{p}),$$

then there is a ϱ such that

$$a^\varrho b^\varrho \equiv 0 (\mathfrak{q})$$

and

$$a^\varrho \not\equiv 0 (\mathfrak{q}).$$

Hence there must be a σ such that

$$b^{\varrho\sigma} \equiv 0 (\mathfrak{q}).$$

Therefore

$$b \equiv 0(\mathfrak{p}).$$

Thirdly, $\mathfrak{p}$ is a divisor of $\mathfrak{q}$:

$$\mathfrak{q} \equiv 0(\mathfrak{p});$$

since the elements of $\mathfrak{q}$ have the property that a power lies in $\mathfrak{q}$.

$\mathfrak{p}$ is said to be *the prime ideal belonging to* $\mathfrak{q}$, $\mathfrak{q}$ a primary ideal belonging to $\mathfrak{p}$. As a consequence of the definition of primary ideals we have:

II. *If* $ab \equiv 0(\mathfrak{q})$ *and* $a \not\equiv 0(\mathfrak{q})$, *then* $b \equiv 0(\mathfrak{p})$.

To some extent the following is the converse of this theorem:

III. *If* $\mathfrak{p}$ *and* $\mathfrak{q}$ *are ideals and have the property that*

1. $ab \equiv 0(\mathfrak{q})$ *and* $a \not\equiv 0(\mathfrak{q})$ *implies* $b \equiv 0(\mathfrak{p})$,

2. $\mathfrak{q} \equiv 0(\mathfrak{p})$,

3. $b \equiv 0(\mathfrak{p})$ *implies* $b^{\varrho} \equiv 0(\mathfrak{q})$,

then $\mathfrak{q}$ *is primary and* $\mathfrak{p}$ *the prime ideal belonging to* $\mathfrak{q}$.

PROOF. If $ab \equiv 0(\mathfrak{q})$ and $a \not\equiv 0(\mathfrak{q})$, then (by 1. and 3.) $b^{\varrho} \equiv 0(\mathfrak{q})$. Hence $\mathfrak{q}$ is primary. We must now show that $\mathfrak{p}$ contains all the elements b for which a power b^{ϱ} lies in $\mathfrak{q}$. One half of this result follows from 3. It remains to show that the relation $b^{\varrho} \equiv 0(\mathfrak{q})$ implies $b \equiv 0(\mathfrak{p})$. Let ϱ be the smallest natural number for which $b^{\varrho} \equiv 0(\mathfrak{q})$. If $\varrho = 1$ our result is proved by 2. If $\varrho > 1$ we write $b \cdot b^{\varrho-1} \equiv 0(\mathfrak{q})$. In this case $b^{\varrho-1} \not\equiv 0(\mathfrak{q})$ and hence (by 1.) $b \equiv 0(\mathfrak{p})$.

In specific cases this theorem simplifies the proof that an ideal is primary and that a particular prime ideal belongs to it. Furthermore it shows what properties are needed to uniquely determine the prime ideal belonging to a primary ideal.

Property II is also valid when a and b are replaced by ideals $\mathfrak{a}$ and $\mathfrak{b}$:

IV. *If* $\mathfrak{ab} \equiv 0(\mathfrak{q})$ *and* $\mathfrak{a} \not\equiv 0(\mathfrak{q})$, *then* $\mathfrak{b} \equiv 0(\mathfrak{p})$.

Thus let $\mathfrak{b} \not\equiv 0(\mathfrak{p})$. Then there is an element b in $\mathfrak{b}$ which is not in $\mathfrak{p}$, and similarly an element a in $\mathfrak{a}$ which is not in $\mathfrak{q}$. The product ab must however be in $\mathfrak{ab}$ and hence in $\mathfrak{q}$. This contradicts the earlier proofs.

In the same manner we may prove a corresponding theorem for prime ideals:

If $\mathfrak{ab} \equiv 0(\mathfrak{p})$ *and* $\mathfrak{a} \not\equiv 0(\mathfrak{p})$, *then* $\mathfrak{b} \equiv 0(\mathfrak{p})$.

As a corollary we have [it may be proved by $(h-1)$ applications of this theorem]:

If $\mathfrak{a}^h \equiv 0(\mathfrak{p})$, *then* $\mathfrak{a} \equiv 0(\mathfrak{p})$.

Another corollary of Theorem IV is:

IV'. *If* $\mathfrak{b} \not\equiv 0(\mathfrak{p})$, *then* $\mathfrak{q}:\mathfrak{b} = \mathfrak{q}$.

The residue class ring $\mathfrak{o}/\mathfrak{q}$ contains (since $\mathfrak{p} \supseteq \mathfrak{q}$) the ideal $\mathfrak{p}/\mathfrak{q}$. The latter ideal consists of all nilpotent elements, and in case $\mathfrak{q} \neq \mathfrak{o}$ also all zero divisors.

Properties of Primary Ideals Under the Assumption of the Divisor Chain Condition

If $\mathfrak{p}$ is the prime ideal belonging to $\mathfrak{q}$, a power of every element of $\mathfrak{p}$ lies in $\mathfrak{q}$. The smallest exponent that is needed for this is dependent on the chosen element and could increase without bound. However, if we assume that the divisor chain condition is valid in the ring $\mathfrak{o}$, the exponents can not increase without bound because of the following theorem:

V. *A power* $\mathfrak{p}^\varrho$ *is divisible by* $\mathfrak{q}$:

$$\mathfrak{p}^\varrho \equiv 0(\mathfrak{q}).$$

PROOF. Let $(\mathfrak{p}_1, \ldots, \mathfrak{p}_r)$ be a basis for $\mathfrak{p}$ and let $\mathfrak{p}_1^{\varrho_1}, \ldots, \mathfrak{p}_r^{\varrho_r}$ lie in $\mathfrak{q}$. If we set

$$\varrho = \sum_1^r (\varrho_i - 1) + 1,$$

$\mathfrak{p}^\varrho$ is generated by all products of the $\mathfrak{p}_i$, ϱ at a time. In each such product at least one factor $\mathfrak{p}_i$ must occur more than $(\varrho_i - 1)$ times, and therefore at least ϱ_i times. All generators of $\mathfrak{p}^\varrho$ are in $\mathfrak{q}$. This proves the theorem.

Between a primary ideal $\mathfrak{q}$ and the prime ideal $\mathfrak{p}$ belonging to it there exist the following relations:

$$\text{(2)} \qquad \begin{cases} \mathfrak{q} \equiv 0(\mathfrak{p}), \\ \mathfrak{p}^\varrho \equiv 0(\mathfrak{q}). \end{cases}$$

The smallest number ϱ for which these relations are valid is called the *exponent* of $\mathfrak{q}$. The exponent is in particular an upper bound of the exponents of the powers to which the elements of $\mathfrak{p}$ must be raised (at least) in order to obtain elements of $\mathfrak{q}$.

If $\mathfrak{q}$ is primary, equations (2) are characteristic for the prime ideal $\mathfrak{p}$ belonging to it. Thus, let us assume that there is a second prime ideal $\mathfrak{p}'$ which satisfies (2) with an exponent ϱ'. Since

$$\begin{cases} \mathfrak{p}^\varrho \subseteq \mathfrak{q} \subseteq \mathfrak{p}' \text{ implies } \mathfrak{p} \subseteq \mathfrak{p}', \\ \mathfrak{p}'^{\varrho'} \subseteq \mathfrak{q} \subseteq \mathfrak{p} \text{ implies } \mathfrak{p}' \subseteq \mathfrak{p}, \end{cases}$$

then $\mathfrak{p}' = \mathfrak{p}$. The relations (2) are however not characteristic of primary ideals since it may be true that (2) is valid for a non-primary $\mathfrak{q}$ (cf. the following Exercise 1).

VI. *If* $\mathfrak{a}\mathfrak{b} \equiv 0(\mathfrak{q})$ *and* $\mathfrak{a} \not\equiv 0(\mathfrak{q})$, *then there is a power* $\mathfrak{b}^\sigma \equiv 0(\mathfrak{q})$.

PROOF. It is sufficient to choose $\sigma = \varrho$. If $\mathfrak{a}\mathfrak{b} \equiv 0(\mathfrak{q})$ and $\mathfrak{a} \not\equiv 0(\mathfrak{q})$, it follows, as we have proved earlier, that $\mathfrak{b} \equiv 0(\mathfrak{p})$ and hence

$$\mathfrak{b}^\varrho \equiv 0(\mathfrak{p}^\varrho) \equiv 0(\mathfrak{q}).$$

An ideal $\mathfrak{q}$ with the property just considered is said to be *strongly primary*, in contrast to the *weakly primary* ideals or primary ideals which were defined earlier. If the divisor chain

condition is valid, the two concepts coincide; for, as we have already seen, the primary ideals in this case are also strongly primary, and the converse follows easily by specializing the ideals $\mathfrak{a}$, $\mathfrak{b}$ to principal ideals (a), (b). If the divisor chain condition is not valid, every strongly primary ideal is also weakly primary, but the converse need not be valid.

EXAMPLE. In the polynomial domain of infinitely many indeterminates $x_1, x_2, x_3, \ldots$ the ideal

$$\mathfrak{q} = (x_1, x_2^2, x_3^3, \quad)$$

is primary and the prime ideal belonging to it is

$$\mathfrak{p} = (x_1, x_2, x_3, \ldots).$$

These two results may be easily established by Theorem III. Thus $\mathfrak{q}$ consists of all polynomials in which the constant term is omitted and in every term one or more x_ν occurs with the exponent ν at least, while $\mathfrak{p}$ consists of all polynomials without a constant term. Now if $a \not\equiv 0(\mathfrak{q})$ and $b \not\equiv 0(\mathfrak{p})$, then b contains a constant term $b_0 \neq 0$ and a one term in which every x_ν has an exponent $< \nu$. Among these terms of a we seek a term of lowest degree; when this term is multiplied by the constant b_0 we obtain a term of lowest degree which actually occurs in ab and in which every x_ν has an exponent $< \nu$. Hence it follows that $ab \not\equiv 0(\mathfrak{q})$. This proves assumption 1 of Theorem III. Furthermore, if $b \equiv 0(\mathfrak{p})$, the constant term is omitted in b; if x_ω is the last of the indeterminates $x_1, x_2, \ldots$ which actually occurs in the polynomial b (b contains only a finite number of x_ν), then all terms in b^{ω^2} have at least degree ω^2. In every term therefore one x_ν at least occurs to the ω-th power; accordingly b^{ω^2} is in $\mathfrak{q}$. Finally, since $\mathfrak{q} \equiv 0(\mathfrak{p})$ all assumptions of Theorem III are satisfied.

Nevertheless $\mathfrak{p}^\varrho \not\equiv 0(\mathfrak{q})$ no matter how large we assume ϱ to be since $\mathfrak{p}^\varrho$ contains the element $x_{\varrho+1}^\varrho$ which is not in $\mathfrak{q}$.

EXERCISES. 1. The ideal $\mathfrak{a} = (x^2, 2x)$ in the domain of polynomials of a single variable x with integers as coefficients is not primary. Nevertheless $(x)^2 \equiv 0(\mathfrak{a}) \equiv 0(x)$ and (x) is a prime ideal.

2. If $\mathfrak{o}$ has an identity element, then $\mathfrak{o}$ is itself the unique primary ideal belonging to the prime ideal $\mathfrak{o}$.

3. If $\mathfrak{o}^*$ is a subring of $\mathfrak{o}$ and $\mathfrak{q}$ is a primary ideal in $\mathfrak{o}$ belonging to the prime ideal $\mathfrak{p}$, then $\mathfrak{q} \cap \mathfrak{o}^*$ is a primary ideal in $\mathfrak{o}^*$ belonging to the prime ideal $\mathfrak{p} \cap \mathfrak{o}^*$.

87. THE GENERAL DECOMPOSITION THEOREM

Let us assume that the divisor chain condition is valid in the ring $\mathfrak{o}$, i.e., every divisor chain of ideals breaks off after a finite number of terms. From this assumption follows the "principle of divisor induction."

An ideal $\mathfrak{m}$ is said to be *reducible* if it can be represented as the intersection of two proper divisors:

$$\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}, \qquad \mathfrak{a} \supset \mathfrak{m}, \qquad \mathfrak{b} \supset \mathfrak{m}.$$

If such a representation is not possible, the ideal is said to be *irreducible.*

The prime ideals are examples of irreducible ideals. Thus, if a prime ideal $\mathfrak{p}$ had a representation

$$\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b}, \qquad \mathfrak{a} \supset \mathfrak{p}, \qquad \mathfrak{b} \supset \mathfrak{p},$$

then

$$\mathfrak{a}\mathfrak{b} \equiv 0(\mathfrak{a} \cap \mathfrak{b}) \equiv 0(\mathfrak{p}), \qquad \mathfrak{a} \not\equiv 0(\mathfrak{p}), \qquad \mathfrak{b} \not\equiv 0(\mathfrak{p}),$$

which would contradict the assumption that the ideal is prime.

By means of the divisor chain condition we may now prove the *first decomposition theorem:*

Every ideal is the intersection of a finite number of irreducible ideals.

PROOF. The theorem is obviously valid for irreducible ideals. Hence let $\mathfrak{m}$ be reducible:

$$\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}, \qquad \mathfrak{a} \supset \mathfrak{m}, \qquad \mathfrak{b} \supset \mathfrak{m}.$$

If we assume that the theorem is valid for all proper divisors of $\mathfrak{m}$, then it is valid in particular for $\mathfrak{a}$ and $\mathfrak{b}$. Hence let us say that

$$\mathfrak{a} = [\mathfrak{i}_1, \ldots, \mathfrak{i}_s],$$

$$\mathfrak{b} = [\mathfrak{i}_{s+1}, \ldots, \mathfrak{i}_r].$$

This means that $\mathfrak{m} = [\mathfrak{i}_1, \ldots, \mathfrak{i}_s, \mathfrak{i}_{s+1}, \ldots, \mathfrak{i}_r]$;

hence the theorem is also valid for $\mathfrak{m}$. Since the theorem is valid for the unit ideal (which is always irreducible), it is valid in general by the "principle of divisor induction."

The representation by irreducible ideals gives rise to a representation by primary ideals as a consequence of the following theorem:

Every irreducible ideal is primary.

PROOF. Let us assume that $\mathfrak{m}$ is not primary. We shall now show that $\mathfrak{m}$ is reducible.

Since $\mathfrak{m}$ is not primary, there are two elements a and b with the property

$$ab \equiv 0(\mathfrak{m}),$$

$$a \not\equiv 0(\mathfrak{m}),$$

$$b^\varrho \not\equiv 0(\mathfrak{m}) \text{ for every } \varrho.$$

By the divisor chain condition the sequence of quotient ideals

$$\mathfrak{m}:b, \qquad \mathfrak{m}:b^2, \ldots$$

breaks off after a while, i.e., for a certain k we have

$$\mathfrak{m}:b^k = \mathfrak{m}:b^{k+1}.$$

We now state that

$$\mathfrak{m} = (\mathfrak{m}, a) \cap (\mathfrak{m}, \mathfrak{o}b^k): \tag{1}$$

The two ideals on the right-hand side are divisors of $\mathfrak{m}$, and indeed proper divisors since the first one contains a and the second contains b^{k+1}. We have to show that every element common to these two ideals must belong to $\mathfrak{m}$. Let c be such an element. As an element of $(\mathfrak{m}, \mathfrak{o}b^k)$ it has the form

$$c = m + rb^k.$$

Secondly, as an element of $(\mathfrak{m}, a)$ it has the property

$$cb \equiv 0(\mathfrak{m}b, ab) \equiv 0(\mathfrak{m}).$$

Hence we have

$$mb + rb^{k+1} = cb \equiv 0(\mathfrak{m}),$$
$$rb^{k+1} \equiv 0(\mathfrak{m})$$

and, since $\mathfrak{m}:b^{k+1} = \mathfrak{m}:b^k$:

$$rb^k \equiv 0(\mathfrak{m}),$$
$$c = m + rb^k \equiv 0(\mathfrak{m}).$$

This proves (1); hence $\mathfrak{m}$ is reducible.

Since every ideal is representable as the intersection of a finite number of irreducible ideals and every irreducible ideal is primary, we have

Every ideal is representable as the intersection of a finite number of primary ideals.

This theorem may be sharpened further. First, we can strike out successively from the representation

$$\mathfrak{m} = [\mathfrak{q}_1, \ \ldots, \mathfrak{q}_r]$$

all superfluous ideals $\mathfrak{q}_i$, i.e., all those which include the intersection of the remaining ideals. Thereby we arrive at an *irredundant* representation, i.e., one in which no component $\mathfrak{q}_i$ includes the intersection of the remaining. In such a representation it may still happen that some primary components form a primary ideal when collected together, i.e., their intersection is again a primary ideal. When this is the case, it is a consequence of the following theorems:

1. *The intersection of a finite number of primary ideals, which belong to the same prime ideal, is again primary and belongs to the same prime ideal.*

2. *An irredundant intersection of a finite number of primary ideals, which do not all belong to the same prime ideal, is not primary.*

The validity of these theorems is independent of the divisor chain condition.

PROOF OF 1. Our proof is based on Theorem III (Section 86). Let

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r],$$

where $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ all belong to $\mathfrak{p}$. If

$$ab \equiv 0(\mathfrak{m}), \quad a \not\equiv 0(\mathfrak{m}),$$

then

$$ab \equiv 0(\mathfrak{q}_\nu)$$

for all ν and

$$a \not\equiv 0(\mathfrak{q}_\nu)$$

for at least one ν. Hence $b \equiv 0(\mathfrak{p})$.

Secondly, it is evident that

$$\mathfrak{m} \equiv 0(\mathfrak{q}_\nu) \equiv 0(\mathfrak{p}).$$

Finally, if $b \equiv 0(\mathfrak{p})$, then

$$b^{\varrho_\nu} \equiv 0(\mathfrak{q}_\nu) \text{ for all } \nu.$$

Hence if $\varrho = \max \varrho_\nu$, then

$$b^{\varrho} \equiv 0(\mathfrak{q}_\nu) \text{ for all } \nu,$$

$$b^{\varrho} \equiv 0(\mathfrak{m}).$$

We have thus shown that all three properties stated in Theorem III are valid. Therefore $\mathfrak{m}$ is primary and $\mathfrak{p}$ is the prime ideal belonging to it.

PROOF OF 2. Let an irredundant representation

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r] \qquad (r \geqq 2),$$

be given such that at least two of the prime ideals $\mathfrak{p}_\nu$ are distinct, where $\mathfrak{p}_1$ belongs to $\mathfrak{q}_\nu$. From here on we shall assume that in this representation each set of primary ideals belonging to the same prime ideal is replaced by their intersection which is a primary ideal. The representation that is thereby obtained remains irredundant.

Among the finitely many prime ideals $\mathfrak{p}_\nu$ there is a minimal one, i.e., one which contains none of the remaining ideals. Let us say that it is $\mathfrak{p}_1$. Since $\mathfrak{p}_1$ does not contain the ideals $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$, there is an element a_ν such that

$$\left.\begin{aligned} a_\nu &\not\equiv 0(\mathfrak{p}_1), \\ a_\nu &\equiv 0(\mathfrak{p}_\nu) \end{aligned}\right\} \qquad (\nu = 2, 3, \ldots, r).$$

Hence for ϱ sufficiently large, we have

$$a_\nu^{\varrho} \equiv 0(\mathfrak{q}_\nu).$$

If $\mathfrak{q}_1 = \mathfrak{m}$, the representation $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ is redundant (for $\mathfrak{q}_2, \ldots, \mathfrak{q}_r$ are superfluous). Hence there is in $\mathfrak{q}_1$ an element q_1 such that

$$q_1 \not\equiv 0(\mathfrak{m}).$$

The product

$$q_1(a_2 \ldots a_r)^{\varrho}$$

is in $\mathfrak{q}_1$ as well as in $\mathfrak{q}_2, \ldots, \mathfrak{q}_r$ and therefore in $\mathfrak{m}$. q_1 however is not in $\mathfrak{m}$. Hence if $\mathfrak{m}$ is assumed to be primary, then:

$$(a_2 \ldots a_r)^{\varrho\sigma} \equiv 0(\mathfrak{m}),$$

$$(a_2 \ldots a_r)^{\varrho\sigma} \equiv 0(\mathfrak{p}_1),$$

and, since $\mathfrak{p}_1$ is prime,

$$a_\nu \equiv 0(\mathfrak{p}_1)$$

for at least one ν which is a contradiction.

If in an irredundant representation

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

all prime ideals $\mathfrak{p}_\nu$ are distinct where $\mathfrak{p}_\nu$ belongs to $\mathfrak{q}_\nu$, the intersection of two or more primary ideals $\mathfrak{q}_\nu$ cannot form a primary ideal. We call such a representation a *representation by greatest primary ideals.* These greatest primary ideals are also called the *primary components* of $\mathfrak{m}$.

Every irredundant representation $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ may be transformed into a representation by greatest primary ideals by collecting together the primary ideals belonging to the same prime ideal. This proves the *second decomposition theorem:*

Every ideal has an irredundant representation as the intersection of a finite number of greatest primary components. These primary components belong to actually distinct prime ideals.

This "second decomposition theorem," proved for polynomial domains by E. Lasker and in general by E. Noether, is the most important result of the general ideal theory. Applications of this theorem will be found throughout Chapter XIII. In the next section we shall investigate what may be said about the uniqueness of the primary components.

EXERCISES. 1. Decompose the ideal $(9, 3x + 3)$ into primary components in the domain of polynomials in a single indeterminate with integers as coefficients.

2. To every ideal $\mathfrak{a}$ there is a product of powers of prime ideals $\mathfrak{p}_1^{\varrho_1} \cdot \mathfrak{p}_2^{\varrho_2} \cdot \ldots \mathfrak{p}_h^{\varrho_h}$ which is divisible by $\mathfrak{a}$ and such that each $\mathfrak{p}_\nu$ is a divisor of $\mathfrak{a}$.

3. If the ring $\mathfrak{o}$ has an identity, every ideal $\mathfrak{a}$ distinct from $\mathfrak{o}$ is divisible by at least one prime ideal distinct from $\mathfrak{o}$.

4. In the domain of polynomials in a single indeterminate with integers as coefficients the ideal $(4, 2x, x^2)$ is primary, but reducible. [show that $(4, 2x, x^2) = (4, x) \cap (2, x^2)$.]

88. THE UNIQUENESS THEOREMS

The decomposition of an ideal into greatest primary components is not unique.

EXAMPLE. The ideal

$$\mathfrak{m} = (x^2, xy)$$

in the polynomial domain $\mathsf{K}[x, y]$ consists of all polynomials which are divisible by x and do not contain linear terms. The totality of all polynomials which are divisible by x is the prime ideal

$$\mathfrak{q}_1 = (x).$$

The totality of all polynomials in which the linear and constant terms are omitted is the primary ideal

$$\mathfrak{q}_2 = (x^2, xy, y^2).$$

Hence

$$\mathfrak{m} = [\mathfrak{q}_1, \mathfrak{q}_2].$$

This is an irredundant representation and since the prime ideals belonging to $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are distinct, namely, equal to (x) and (x, y) respectively, this is also a representation by greatest primary ideals.

However, besides this representation there is still another:

$$\mathfrak{m} = [\mathfrak{q}_1, \mathfrak{q}_3],$$

where

$$\mathfrak{q}_3 = (x^2, y),$$

for in order that a polynomial lie in $\mathfrak{m}$ it is sufficient to require that the polynomial be divisible by x and that the term with x be omitted. If K is an infinite field, there are infinitely many representations of this type:

$$\mathfrak{m} = [\mathfrak{q}_1, \mathfrak{q}^{(\lambda)}], \quad \mathfrak{q}^{(\lambda)} = (x^2, y + \lambda x).$$

All decompositions of $\mathfrak{m}$, here obtained, have the same *number* of primary components and the prime ideals belonging to these components, namely,

$$(x), (x, y),$$

are the same. This is valid in general:

FIRST UNIQUENESS THEOREM. In two irredundant representations of an ideal $\mathfrak{m}$ *by greatest primary components the number of components is the same and the prime ideals belonging to these components are also the same (though the components themselves need not be the same).*

PROOF. For a primary ideal the statement is trivial. We can therefore set up an induction on the number of primary components which appear in at least one representation of the ideal under consideration.

Let

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l] = [\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{l'}]. \tag{1}$$

Among the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_l, \mathfrak{p}'_1, \ldots, \mathfrak{p}'_{l'}$ belonging to the primary ideals choose a maximal ideal, i.e., one which is contained (divided) by no other. Let us assume that it occurs on the left-hand side and let us say that it is $\mathfrak{p}_1$. We will now show that it also must occur on the right-hand side. Otherwise we could, in (I), form the quotients modulo $\mathfrak{q}_1$:

$$[\mathfrak{q}_1 : \mathfrak{q}_1, \ldots, \mathfrak{q}_l : \mathfrak{q}_1] = [\mathfrak{q}'_1 : \mathfrak{q}_1, \ldots, \mathfrak{q}'_{l'} : \mathfrak{q}_1].$$

Now (for all $\nu > 1$) $\mathfrak{q}_1 \not\equiv 0 (\mathfrak{p}_\nu)$, since otherwise $\mathfrak{p}_1 \equiv 0 (\mathfrak{p}_\nu)$ contrary to the assumption that $\mathfrak{p}_1$ is a maximal ideal. Similarly, for all ν it follows that $\mathfrak{q}_1 \not\equiv 0 (\mathfrak{p}'_\nu)$. By Theorem IV′ (Section 86) we have

$$\mathfrak{q}_\nu : \mathfrak{q}_1 = \mathfrak{q}_\nu \quad (\nu = 2, \ldots, l),$$
$$\mathfrak{q}'_\nu : \mathfrak{q}_1 = \mathfrak{q}'_\nu \quad (\nu = 1, \ldots, l').$$

Furthermore, since $\mathfrak{q}_1 : \mathfrak{q}_1 = \mathfrak{o}$, it follows that

$$[\mathfrak{o}, \mathfrak{q}_2, \ldots, \mathfrak{q}_l] = [\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{l'}].$$

The right member is equal to $\mathfrak{m}$; hence the left member is also. As $\mathfrak{o}$ may be omitted, we have

$$\mathfrak{m} = [\mathfrak{q}_2, \ldots, \mathfrak{q}_l].$$

Consequently the first of the two representations (1) is redundant, contrary to the assumption.

Every maximal prime ideal occurs therefore on *both* sides.

Let us now assume that $l \leqq l'$. We shall show that $l = l'$ and (by a suitable ordering) $\mathfrak{p}'_\nu = \mathfrak{p}_\nu$. Let us assume that these results are valid for ideals which may be represented by fewer than l primary ideals. We arrange the $\mathfrak{q}$ and $\mathfrak{q}'$ so that $\mathfrak{p}_1 = \mathfrak{p}'_1$ is the maximal prime ideal belonging to $\mathfrak{q}_1$ and $\mathfrak{q}'_1$ respectively.

In both sides of (1) form quotients modulo the product $\mathfrak{q}_1\mathfrak{q}'_1$:

$$[\mathfrak{q}_1 : \mathfrak{q}_1\mathfrak{q}'_1, \ldots, \mathfrak{q}_l : \mathfrak{q}_1\mathfrak{q}'_1] = [\mathfrak{q}'_1 : \mathfrak{q}_1\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{l'} : \mathfrak{q}_1\mathfrak{q}'_1].$$

It follows that

$$\left.\begin{aligned} \mathfrak{q}_\nu : \mathfrak{q}_1\mathfrak{q}'_1 &= \mathfrak{q}_\nu \\ \mathfrak{q}'_\nu : \mathfrak{q}_1\mathfrak{q}'_1 &= \mathfrak{q}'_\nu \end{aligned}\right\} \quad (\nu > 1).$$

Furthermore, since $\mathfrak{q}_1\mathfrak{q}'_1$ is divisible by $\mathfrak{q}_1$ and $\mathfrak{q}'_1$, we have

$$\mathfrak{q}_1 : \mathfrak{q}_1\mathfrak{q}'_1 = \mathfrak{o},$$
$$\mathfrak{q}'_1 : \mathfrak{q}_1\mathfrak{q}'_1 = \mathfrak{o}.$$

Hence

$$[\mathfrak{q}_2, \ldots, \mathfrak{q}_l] = [\mathfrak{q}'_2, \ldots, \mathfrak{q}'_{l'}].$$

But the left and right sides are irredundant representations by greatest primary components. Hence by the induction hypothesis we have $l' - 1 = l - 1$, i.e., $l' = l$. Furthermore, by a suitable ordering we have $\mathfrak{p}_\nu = \mathfrak{p}'_\nu$ for all $\nu > 1$. Since $\mathfrak{p}_1 = \mathfrak{p}'_1$, the proof is completed.

The ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$, which are uniquely determined by the theorem just proved and are the prime ideals belonging to the irredundant representation $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l]$, are called *the prime ideals belonging to the ideal* $\mathfrak{a}$. Their most important property is the following:

If an ideal $\mathfrak{a}$ *is divisible by no one of the prime ideals belonging to an ideal* $\mathfrak{b}$, *then* $\mathfrak{b} : \mathfrak{a} = \mathfrak{b}$ *and conversely.*

PROOF. Let $\mathfrak{b} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l]$ be an irredundant representation. First, assume that $\mathfrak{a} \not\equiv 0 (\mathfrak{p}_i)$ for $i = 1, \ldots, l$, where $\mathfrak{p}_i$ belongs to $\mathfrak{q}_i$. Then

$$\mathfrak{q}_i : \mathfrak{a} = \mathfrak{q}_i,$$
$$\mathfrak{b} : \mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l] : \mathfrak{a}$$
$$= [\mathfrak{q}_1 : \mathfrak{a}, \ldots, \mathfrak{q}_l : \mathfrak{a}]$$
$$= [\mathfrak{q}_1, \ldots, \mathfrak{q}_l] = \mathfrak{b}.$$

Conversely, let $\mathfrak{b}:\mathfrak{a} = \mathfrak{b}$. If $\mathfrak{a} \equiv 0(\mathfrak{p}_i)$ for one i, say $\mathfrak{a} \equiv 0(\mathfrak{p}_1)$, then $\mathfrak{a}^\varrho \equiv 0(\mathfrak{q}_1)$, and

$$\mathfrak{a}^\varrho \cdot [\mathfrak{q}_2, \ldots, \mathfrak{q}_l] \equiv 0([\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_l]) \equiv 0(\mathfrak{b}).$$

Consequently, since in every congruence (mod $\mathfrak{b}$) $\mathfrak{a}$ may be omitted and therefore also $\mathfrak{a}^\varrho$,

$$[\mathfrak{q}_2, \ldots, \mathfrak{q}_l] \equiv 0(\mathfrak{b})$$

contrary to the assumption that the representation is irredundant.

An important special case is obtained if we specialize $\mathfrak{a}$ to be a principal ideal (a):

If an element a is not divisible by a prime ideal belonging to an ideal $\mathfrak{b}$, then $\mathfrak{b}:a = \mathfrak{b}$; i.e., $ac \equiv 0(\mathfrak{b})$ implies $c \equiv 0(\mathfrak{b})$.

We may state the general theorem in another way if we also represent $\mathfrak{a}$ as the intersection of primary ideals $[\mathfrak{q}_1', \ldots, \mathfrak{q}_{l'}']$. $\mathfrak{a}$ is divisible by $\mathfrak{p}_i$ if and only if one $\mathfrak{q}_j'$ is,[5] in other words, if one $\mathfrak{p}_j'$ is. Hence we have

If no prime ideal belonging to $\mathfrak{a}$ is divisible by a prime ideal belonging to $\mathfrak{b}$, then $\mathfrak{b}:\mathfrak{a} = \mathfrak{b}$, and conversely.

The theorem will be applied in this form in order to prove the second uniqueness theorem, i.e., the uniqueness of the "isolated component ideals."

By a *component ideal* of an ideal $\mathfrak{a}$ we understand any intersection of primary ideals which appear in an irredundant representation of the ideal $\mathfrak{a}$ by greatest primary ideals.

Let

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l]$$

be an irredundant representation and

$$\mathfrak{a}_1 = [\mathfrak{q}_1, \ldots, \mathfrak{q}_k], \quad \text{or} = \mathfrak{o}, \text{ if } k = 0,$$
$$\mathfrak{a}_2 = [\mathfrak{q}_{k+1}, \ldots, \mathfrak{q}_l], \text{or} = \mathfrak{o}, \text{ if } k = l.$$

Then

$$\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2,$$

and $\mathfrak{a}_1$ is a component ideal of $\mathfrak{a}$.

The component ideal $\mathfrak{a}_1$ is said to be *isolated* if no prime ideal $\mathfrak{p}_{k+j}$ belonging to $\mathfrak{a}_2$ is divisible by a $\mathfrak{p}_i$ belonging to $\mathfrak{a}_1$.

We say that a prime ideal belonging to $\mathfrak{a}$ is *imbedded* if it is a divisor of an other prime ideal belonging to $\mathfrak{a}$. Then an isolated component ideal of $\mathfrak{a}$ may also be defined as one such that the set of prime ideals belonging to it either contains no imbedded prime ideals or contains for every imbedded ideal at least all the prime ideals in which it is imbedded.

[5] Since it is clear that if $\mathfrak{q}_j'$ is divisible by $\mathfrak{p}_i$ so also is $\mathfrak{a}$, and if $\mathfrak{a} \equiv 0(\mathfrak{p}_i)$, then $\mathfrak{q}_1' \cdots \mathfrak{q}_{l'}' \equiv 0([\mathfrak{q}_1', \ldots, \mathfrak{q}_{l'}']) \equiv 0(\mathfrak{p}_i)$ so that one $\mathfrak{q}_j'$ is divisible by $\mathfrak{p}_i$.

SECOND UNIQUENESS THEOREM. Every isolated component ideal of an ideal $\mathfrak{a}$ *is uniquely determined by giving the prime ideals belonging to it (hence by a subset of all prime ideals belonging to* $\mathfrak{a}$ *).*

PROOF. Let two representations be given

$$\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1' \cap \mathfrak{a}_2', \tag{2}$$

where $\mathfrak{a}_1'$ has the same prime ideals belonging to it as $\mathfrak{a}_1$. Moreover let $\mathfrak{a}_1$ and $\mathfrak{a}_1'$ be isolated components. Then by the theorem proved above:

$$\mathfrak{a}_1 : \mathfrak{a}_2 = \mathfrak{a}_1,$$
$$\mathfrak{a}_1' : \mathfrak{a}_2 = \mathfrak{a}_1'.$$

Hence on forming quotients modulo $\mathfrak{a}_2$ it follows by (2) that

$$\mathfrak{a} : \mathfrak{a}_2 = \mathfrak{a}_1 = \mathfrak{a}_1' \cap (\mathfrak{a}_2' : \mathfrak{a}_2),$$

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_1'.$$

Similarly,

$$\mathfrak{a}_1' \subseteq \mathfrak{a}_1,$$

Hence

$$\mathfrak{a}_1 = \mathfrak{a}_1',$$

Q.E.D.

In particular the *isolated primary components* of an ideal (i.e., the primary components belonging to the non-imbedded prime ideals) are uniquely determined.

89. THEORY OF RELATIVELY PRIME IDEALS

In the following we shall assume that the ring $\mathfrak{o}$ has an identity. This identity generates the unit ideal $\mathfrak{o}$:

$$\mathfrak{o} = (1).^{6}$$

Two ideals $\mathfrak{a}$, $\mathfrak{b}$ are said to be *relatively prime* if they have no common divisor except $\mathfrak{o}$, i.e., their greatest common divisor is $\mathfrak{o}$:

$$(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}.$$

Hence every element of $\mathfrak{o}$ may be represented as the sum of an element of $\mathfrak{a}$ and one of $\mathfrak{b}$.

Such a representation exists if and only if the identity (the generating element of $\mathfrak{o}$) may be represented as a sum

$$1 = a + b \tag{1}$$

[6] This representation implies

$$\mathfrak{o}^2 = (1) \cdot (1) = (1).$$

Hence $\mathfrak{o}^2 = \mathfrak{o}$ which need not be true in rings without an identity element.

(a in $\mathfrak{a}$, b in $\mathfrak{b}$). Then

$$(2)\qquad \begin{cases} a \equiv 1\,(\mathfrak{b}), & b \equiv 0\,(\mathfrak{b}), \\ a \equiv 0\,(\mathfrak{a}), & b \equiv 1\,(\mathfrak{a}). \end{cases}$$

If two primary ideals $\mathfrak{q}_1$, $\mathfrak{q}_2$ are relatively prime, the prime ideals $\mathfrak{p}_1$, $\mathfrak{p}_2$ belonging to them are also (every common divisor of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ is also a common divisor of $\mathfrak{q}_1$ and $\mathfrak{q}_2$). Furthermore, the converse is valid: *if* $\mathfrak{p}_1$ *and* $\mathfrak{p}_2$ *are relatively prime, so also are* $\mathfrak{q}_1$, $\mathfrak{q}_2$. For, if

$$1 = p_1 + p_2,$$

then the $(\varrho + \sigma - 1)$-th power gives

$$1 = p_1^{\varrho+\sigma-1} + \cdots + p_2^{\varrho+\sigma-1}.$$

Hence if we choose ϱ and σ so that p_1^{ϱ} lies in $\mathfrak{q}_1$ and p_2^{σ} in $\mathfrak{q}_2$, every term of the sum on the right lies either in $\mathfrak{q}_1$ or in $\mathfrak{q}_2$, that is,

$$1 = q_1 + q_2.$$

If two ideals are relatively prime, they are prime relative to one another in both directions.

PROOF. Let $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$, and $a + b = 1$. It is sufficient to show that $\mathfrak{a}:\mathfrak{b} \subseteq \mathfrak{a}$. If x belongs to $\mathfrak{a}:\mathfrak{b}$, then $x\mathfrak{b} \subseteq \mathfrak{a}$. Hence $xb \equiv 0\,(\mathfrak{a})$, and

$$x(a + b) \equiv 0\,(\mathfrak{a}),$$
$$x \cdot 1 \equiv 0\,(\mathfrak{a}).$$

Consequently x belongs to $\mathfrak{a}$. Q.E.D.

The converse is not valid as seen by the following example taken from the polynomial domain $\mathsf{K}[x, y]$: the ideals (x) and (y) are prime to each other but not relatively prime

$$\begin{cases} (x, y) \neq \mathfrak{o}, \\ (x):(y) = (x), \\ (y):(x) = (y). \end{cases}$$

If $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime, we may solve congruences simultaneously as in the theory of numbers. Let the two congruences

$$f(\xi) \equiv 0\,(\mathfrak{a}),$$
$$g(\xi) \equiv 0\,(\mathfrak{b}) \qquad (f(x), g(x) \in \mathfrak{o}[x])$$

be given. It will be assumed that each congruence has a solution. If we say that $\xi \equiv \alpha$ is a solution of the first, $\xi \equiv \beta$ a solution of the second congruence, then we can obtain an element ξ which satisfies both congruences. Thus, form

$$\xi = b\alpha + a\beta,$$

where a and b are the elements constructed earlier, i.e., satisfy equations (1) and (2).

Since $\xi \equiv \alpha(\mathfrak{a})$ and $\xi \equiv \beta(\mathfrak{b})$, ξ is a solution of the two given congruences.

The least common multiple of two relatively prime ideals is equal to their product.

PROOF. In Section 85 it was proved that

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b},$$

$$[\mathfrak{a} \cap \mathfrak{b}] \cdot (\mathfrak{a}, \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}.$$

If $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ and an identity element exists, the second equation simplifies to

$$\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}.$$

Hence

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}, \qquad \text{Q.E.D.}$$

In order to extend this theorem to more than two pairwise relatively prime ideals we must first establish a lemma.

If $\mathfrak{a}$ is relatively prime to $\mathfrak{b}$ and to $\mathfrak{c}$, then $\mathfrak{a}$ is relatively prime to the product $\mathfrak{b}\mathfrak{c}$ and to the intersection $\mathfrak{b} \cap \mathfrak{c}$.

PROOF. If

$$a + b = 1,$$

$$a' + c = 1,$$

then

$$(a + b)(a' + c) = 1,$$

$$aa' + ac + a'b + bc = 1,$$

$$a'' + bc = 1,$$

where $a'' = aa' + ac + a'b$ is again an element of $\mathfrak{a}$. Hence

$$(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) = \mathfrak{o}$$

and

$$(\mathfrak{a}, \mathfrak{b} \cap \mathfrak{c}) = \mathfrak{o}.$$

This proves both statements.

If $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ are pairwise relatively prime ideals and if we assume that

$$[\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}] = \mathfrak{a}_1 \ldots \mathfrak{a}_{n-1}$$

is valid, then

$$\begin{aligned}[\mathfrak{a}_1, \ldots, \mathfrak{a}_n] &= [\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}] \cap \mathfrak{a}_n \\ &= (\mathfrak{a}_1 \ldots \mathfrak{a}_{n-1}) \cap \mathfrak{a}_n \\ &= \mathfrak{a}_1 \ldots \mathfrak{a}_{n-1}\ \mathfrak{a}_n.\end{aligned}$$

Hence by induction we have the theorem:

The least common multiple of a finite number of pairwise relatively prime ideals is equal to their product.

The previous remark concerning the solution of congruences modulo relatively prime ideals is also valid for several pairwise relatively prime ideals:

It is always possible to determine ξ *by the congruences*

$$\xi \equiv \alpha_i (\mathfrak{a}_i) \qquad (i = 1, 2, \ldots, r)$$

whenever $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_r$ *are pairwise relatively prime ideals.*

PROOF BY INDUCTION. Let η be determined by

$$\eta \equiv \alpha_i (\mathfrak{a}_i) \qquad (i = 1, 2, \ldots, r-1).$$

Then ξ may be determined by

$$\begin{cases} \xi \equiv \eta([\mathfrak{a}_1, \ldots, \mathfrak{a}_{r-1}]), \\ \xi \equiv \alpha_r (\mathfrak{a}_r), \end{cases}$$

since $\mathfrak{a}_r$ is relatively prime to $[\mathfrak{a}_1, \ldots, \mathfrak{a}_{r-1}]$.

If the divisor chain condition is valid in $\mathfrak{o}$, *every ideal may be represented as the intersection of pairwise relatively prime ideals which are themselves no longer representable as the intersection of pairwise relatively prime proper divisors.*

Let

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

be an irredundant representation of the given ideal $\mathfrak{a}$ by primary ideals. Let $\mathfrak{a}_1$ be the intersection of all the primary ideals which are not pairwise relatively prime to a fixed ideal. From the remaining ideals, let the ideals $\mathfrak{a}_2, \ldots, \mathfrak{a}_s$ be formed successively in the same manner. We will show that the representation

$$\mathfrak{a} = [\mathfrak{a}_1, \ldots, \mathfrak{a}_s] \tag{3}$$

has the desired property. First, $\mathfrak{a}_i$ and $\mathfrak{a}_k$ for $i \neq k$ are actually relatively prime since the components of $\mathfrak{a}_i$ are relatively prime to those of $\mathfrak{a}_k$. Secondly, it is impossible to represent $\mathfrak{a}_1$, let us say, as the intersection of two pairwise relatively prime proper divisors. For, if such a representation exists:

$$\mathfrak{a}_1 = \mathfrak{b} \cap \mathfrak{c} = \mathfrak{b}\mathfrak{c},$$
$$(\mathfrak{b}, \mathfrak{c}) = \mathfrak{o},$$

every prime ideal belonging to $\mathfrak{a}_1$ must be a divisor of $\mathfrak{b}\mathfrak{c}$, hence either of $\mathfrak{b}$ or of $\mathfrak{c}$. Now among these prime ideals there is one that is not pairwise relatively prime to the remaining. Hence if this one divides $\mathfrak{b}$, let us say, then all remaining prime ideals must also divide $\mathfrak{b}$ and not $\mathfrak{c}$; otherwise $\mathfrak{b}$ and $\mathfrak{c}$ would not be relatively prime. But the primary components belonging to these prime ideals divide $\mathfrak{b}\mathfrak{c}$; therefore they must divide $\mathfrak{b}$ (since their prime ideals do not divide $\mathfrak{c}$). Hence it follows that the intersection $\mathfrak{a}_1$ is also a divisor of $\mathfrak{b}$:

$$\mathfrak{b} \subseteq \mathfrak{a}_1;$$

contrary to the assumption that $\mathfrak{b}$ shall be a proper divisor of $\mathfrak{a}_1$.

Our theorem shows that the representation (3) may also be written as the product

$$\mathfrak{a} = \mathfrak{a}_1 \mathfrak{a}_2 \dots \mathfrak{a}_s .$$

EXERCISES. 1. Prove the "third uniqueness theorem" which predicates the unique determination of the ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_s$ which appear in the representation (3) with the prescribed properties. [Show that this third uniqueness theorem is a consequence of the second] .

To every multiplicative decomposition of an ideal $\mathfrak{a}$ there is associated an additive decomposition of the ring $\mathfrak{o}$ and of the residue class ring $\mathfrak{o}/\mathfrak{a}$. We prove first:

If $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ *are pairwise relatively prime ideals and*

$$\mathfrak{a} = \mathfrak{a}_1 \dots \mathfrak{a}_r = [\mathfrak{a}_1, \dots, \mathfrak{a}_r],$$

$$\mathfrak{b}_\nu = \mathfrak{a}_1 \dots \mathfrak{a}_{\nu-1}\, \mathfrak{a}_{\nu+1} \dots \mathfrak{a}_r = [\mathfrak{a}_1, \dots, \mathfrak{a}_{\nu-1}, \mathfrak{a}_{\nu+1}, \dots, \mathfrak{a}_r],$$

then $$\mathfrak{o} = (\mathfrak{b}_1, \dots, \mathfrak{b}_r).$$

Furthermore, the additive representation of every element of $\mathfrak{o}$ *as a sum of elements of* $\mathfrak{b}_1, \dots, \mathfrak{b}_r$ *is unique modulo* $\mathfrak{a}$.

PROOF. The definition of $\mathfrak{a}$ and $\mathfrak{b}_\nu$ implies $\mathfrak{a} = \mathfrak{a}_\nu \cap \mathfrak{b}_\nu = \mathfrak{a}_\nu \cdot \mathfrak{b}_\nu$.

Let b be an arbitrary element of $\mathfrak{o}$. Determine $b_1, \dots, b_{r-1}$ by the congruences

$$b_\nu \equiv b \,(\mathfrak{a}_\nu), \qquad b_\nu \equiv 0 \,(\mathfrak{b}_\nu)$$

Then for $\nu = 1, 2, \dots, r-1$.

$$b \equiv \sum_1^{r-1} b_\lambda \;(\mathfrak{a}_\nu) .$$

Hence, if we set $b - \sum_1^{r-1} b_\lambda = b_r$, we obtain $b_r \equiv 0 (\mathfrak{a}_\nu)$ for $\nu = 1, 2, \dots, r-1$,

This implies $b_r \equiv 0 (\mathfrak{b}_r)$

and that

$$b = \sum_1^r b_\nu$$

is a representation with the required properties. Now if two such representations

$$b = \sum_1^r b_\nu = \sum_1^r b'_\nu$$

are given, then

$$b_\mu \equiv b'_\mu \;(\mathfrak{a}_\mu) .$$

since all $\mathfrak{b}_\nu$ with $\nu \neq \mu$ are congruent to zero modulo $\mathfrak{a}_\mu$. Hence the difference $b_\mu - b'_\mu$ belongs to $\mathfrak{a}_\mu$ as well as to $\mathfrak{b}_\mu$, and consequently to $\mathfrak{a} = \mathfrak{a}_\mu \cap \mathfrak{b}_\mu$. Therefore $b_\mu \equiv b'_\mu (\mathfrak{a})$ which completes the proof.

If we now go over to the residue class ring $\bar{\mathfrak{o}} = \mathfrak{o}/\mathfrak{a}$ by replacing each element b by the residue class $\bar{b}$ belonging to it, and similarly set $\bar{\mathfrak{b}}_\nu = \mathfrak{b}_\nu/\mathfrak{a}$, $\bar{\mathfrak{a}}_\nu = \mathfrak{a}_\nu/\mathfrak{a}$, then a unique representation of each element $\bar{b}$ of $\bar{\mathfrak{o}}$ in the form

$$\bar{b} = \bar{b}_1 + \bar{b}_2 + \dots + \bar{b}_r; \qquad \bar{b}_\nu \in \bar{\mathfrak{b}}_\nu .$$

is obtained.

Since the representation is unique, the sum $\bar{\mathfrak{o}} = (\bar{\mathfrak{b}}_1, \dots, \bar{\mathfrak{b}}_r)$ is *direct* in the sense of Section 47. Furthermore, $\bar{\mathfrak{a}}_\nu \cdot \bar{\mathfrak{b}}_\nu = (0)$. Hence, since every $\bar{\mathfrak{b}}_\mu (\mu \neq \nu)$ is a subset of $\bar{\mathfrak{a}}_\nu$,

$$\bar{\mathfrak{b}}_\mu \cdot \bar{\mathfrak{b}}_\nu = 0$$

The ring $\bar{\mathfrak{o}} = \mathfrak{o}/\mathfrak{a}$ *appears therefore as the direct sum of the rings* $\bar{\mathfrak{b}}_1, \dots, \bar{\mathfrak{b}}_r$, *which mutually annul one another.*

To every b of $\mathfrak{o}$ there is associated a $\bar{b}$ and to every $\bar{b}$ again a $\bar{b}_1$. Both correspondences

are ring homomorphisms. Hence the correspondence $b \to \bar{b}_1$ is also a ring homomorphism. If $\bar{b}_1 = 0$, then $\bar{b} \in \bar{a}_1$, and therefore $b \in a_1$, and conversely. Hence by the Homomorphism Theorem

$$\bar{b}_1 \cong o/a_1.$$

Similarly, for every ν: $\bar{b}_\nu \cong o/a_\nu$.

EXERCISES. 2. If we apply the decomposition (4) to the identity 1 of $\bar{o}$, then

$$1 = \bar{e}_1 + \bar{e}_2 + \quad + e_r; \quad \bar{e}_\nu^2 = \bar{e}_\nu; \quad \bar{e}_\mu \bar{e}_\nu = 0 \text{ for } \mu \neq \nu.$$

The $\bar{e}_\nu$ are the identity elements of the rings b_ν.

90. SINGLE-PRIMED IDEALS

Let o be a ring with an identity element.

The unit ideal o is always a prime ideal. What primary ideals belong to the unit ideal? The answer is: only o itself; for, if q is a primary ideal belonging to o, then $1 \in o$, $1^\varrho \in q$, and therefore $q = o$.

Let $[q_1, \ldots, q_r]$ be a representation of $a \neq o$ as an intersection of primary ideals. If the unit ideal occurs among the prime ideals $\mathfrak{p}_i$ belonging to the primary ideals, the q_i belonging to the unit ideal must also be equal to o and therefore is superfluous in the intersection-representation. Hence *if the representation* $a = [q_1, \ldots, q_r]$ *is irredundant and* $a \neq o$, *the unit ideal cannot occur among the prime ideals belonging to* a.

It immediately follows if the divisor chain condition is valid in o and therefore if every ideal a has a representation as the intersection of primary ideals:

Every ideal $a \neq o$ *possesses at least one prime ideal divisor* $\mathfrak{p} \neq o$. *If the ideal* a *is not primary, it actually possesses at least two prime ideal divisors* $\neq o$.

An ideal which possesses no more than one prime ideal divisor besides o is said to be *single-primed* (einartig), a nomenclature due to Dedekind. By the previous theorem every single-primed ideal q is primary. Moreover, the prime ideal $\mathfrak{p}$ belonging to the single-primed ideal q is a maximal ideal. Thus, if $a' \neq o$ were a proper divisor of $\mathfrak{p}$, then a' would have a prime divisor $\mathfrak{p}' \neq o$ which would also be a proper divisor of $\mathfrak{p}$. Hence q would have two prime ideal divisors $\mathfrak{p}$ and $\mathfrak{p}'$ distinct from one another and from o, contrary to the assumption that q is single-primed.

We have

$$\mathfrak{p}^\varrho \equiv 0 (q). \tag{1}$$

Conversely, if (1) is valid and $\mathfrak{p}$ is maximal, then q is single-primed. For, if $\mathfrak{p}'$ is an arbitrary prime ideal divisor of q, then (1) implies

$$\mathfrak{p}^\varrho \equiv 0 (\mathfrak{p}'),$$

hence

$$\mathfrak{p} \equiv 0 (\mathfrak{p}'),$$

therefore either $\mathfrak{p}' = \mathfrak{p}$ or $\mathfrak{p}' = \mathfrak{o}$. This means that $\mathfrak{q}$ has no prime ideal divisor other than $\mathfrak{p}$ and $\mathfrak{o}$.

The concepts:

1. single-primed ideal,
2. primary ideal belonging to a maximal prime ideal $\mathfrak{p}$,
3. divisor of a power $\mathfrak{p}^\varrho$ of a maximal prime ideal $\mathfrak{p}$,

are therefore equivalent. Furthermore:

If the ideal $\mathfrak{m}$ has an isolated single-primed primary component $\mathfrak{q}$, such that $\mathfrak{p}$ is the prime ideal belonging to it and ϱ is its exponent, then

$$\mathfrak{q} = (\mathfrak{m}, \mathfrak{p}^\sigma). \tag{2}$$

for every integer $\sigma \geqq \varrho$.

PROOF. If

$$\mathfrak{m} \equiv 0(\mathfrak{q})$$

and

$$\mathfrak{p}^\sigma \equiv 0(\mathfrak{q}),$$

then

$$(\mathfrak{m}, \mathfrak{p}^\sigma) \equiv 0(\mathfrak{q}). \tag{3}$$

On the other hand, let

$$\mathfrak{m} = [\mathfrak{q}, \mathfrak{q}_2, \ldots, \mathfrak{q}_s]$$

be a representation of $\mathfrak{m}$ by primary components. The ideal $(\mathfrak{m}, \mathfrak{p}^\sigma)$ is single-primed, and therefore primary; the prime ideal belonging to it is $\mathfrak{p}$. The product $\mathfrak{q}\mathfrak{q}_2 \ldots \mathfrak{q}_s$ is divisible by $(\mathfrak{m}, \mathfrak{p}^\sigma)$; however $\mathfrak{q}_2 \ldots \mathfrak{q}_s$ is not divisible by $\mathfrak{p}$ since by assumption $\mathfrak{q}$ is isolated. Hence $\mathfrak{q}$ must be divisible by $(\mathfrak{m}, \mathfrak{p}^\sigma)$:

$$\mathfrak{q} \equiv 0(\mathfrak{m}, \mathfrak{p}^\sigma). \tag{4}$$

From (3) and (4) follows (2).

COROLLARY. For $\sigma \geqq \varrho$ we have

$$\mathfrak{p}^\sigma \equiv 0(\mathfrak{q}) \equiv 0(\mathfrak{m}, \mathfrak{p}^{\sigma+1}),$$

hence

$$\mathfrak{p}^\sigma \equiv 0(\mathfrak{m}, \mathfrak{p}^{\sigma+1}). \tag{5}$$

For $\sigma < \varrho$ the relation (5) is no longer valid. Thus, if

$$\mathfrak{p}^\sigma \equiv 0(\mathfrak{m}, \mathfrak{p}^{\sigma+1})$$

for a $\sigma < \varrho$, we would obtain on multiplying by $\mathfrak{p}^{\varrho-\sigma-1}$

$$\mathfrak{p}^{\varrho-1} \equiv 0(\mathfrak{m}\mathfrak{p}^{\varrho-\sigma-1}, \mathfrak{p}^\varrho) \equiv 0(\mathfrak{m}, \mathfrak{q}) \equiv 0(\mathfrak{q}),$$

contrary to the definition of the exponent ϱ.

Hence the exponent ϱ of $\mathfrak{q}$ is the smallest number σ for which (5) is valid.

There are domains of integrity $\mathfrak{o}$ with an identity in which (the divisor chain

condition is valid and) every prime ideal distinct from the null ideal is maximal. For instance, the principal ideal rings (cf. Section 19) have this property as well as certain "orders" in number and function fields to be defined later; the ring $C[\sqrt{-3}]$ is a typical example. In these rings *all primary ideals except the null ideal are single-primed.* Furthermore, in these domains any two prime ideals distinct from one another and from (0) are also relatively prime. This implies that any two primary ideals belonging to distinct prime ideals $\neq (0)$ are also relatively prime. Finally, all primary components of an ideal are isolated and therefore are uniquely determined. Hence: *every ideal distinct from the null ideal may be represented uniquely as the intersection of relatively prime single-primed primary ideals.* By Section 89 this intersection is equal to the product

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r] = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdots \mathfrak{q}_r.$$

By the theorems at the end of Section 89 the residue class ring $\mathfrak{o}/\mathfrak{a}$ is a direct sum of rings which mutually annul one another and are isomorphic to the residue class rings $\mathfrak{o}/\mathfrak{q}_\nu$. The latter residue class rings are *primary*, i.e., in these rings every zero divisor is nilpotent.

In principal ideal rings the primary ideals $\mathfrak{q}_i$ are also powers of prime ideals. Whether this is also the case in more general rings depends on a condition which we will investigate later, namely, the condition of "integral closure" (Section 100).

The ideal theory of the domains of integrity mentioned above, in which every prime ideal except (0) is maximal, is substantially simpler to derive than the general theory of ideals of Sections 86 to 88. This was shown by W. Krull. Thus, by the divisor chain condition we can easily show that to every ideal $\mathfrak{a}$ there is a product of power products of prime ideals such that each prime ideal is a divisor of $\mathfrak{a}$ and the product is divisible by $\mathfrak{a}$ (cf. Section 102, Lemma 1):

$$\mathfrak{p}_1^{\varrho_1} \cdot \mathfrak{p}_2^{\varrho_2} \cdots \mathfrak{p}_r^{\varrho_r} \equiv \mathfrak{o}(\mathfrak{a})$$
$$\mathfrak{a} \equiv \mathfrak{o}(\mathfrak{p}_i) \qquad (i = 1, \ldots, r).$$

If $\mathfrak{a} = \mathfrak{q}$ is single-primed, there is beside $\mathfrak{o}$ at most one $\mathfrak{p}_i = \mathfrak{p}$. This prime ideal has the property $\mathfrak{p}^\varrho \equiv \mathfrak{o}(\mathfrak{q})$ Thereby we have derived anew the characterization given above: a single-primed ideal is a divisor of powers of a prime ideal. If $\mathfrak{a} \neq (0)$ is not single-primed, the prime ideals $\mathfrak{p}_i$ as well as their powers $\mathfrak{p}_i^{\varrho_i}$ are relatively prime to one another. Consequently, the ideals $\mathfrak{q}_i = (\mathfrak{a}, \mathfrak{p}_i^{\varrho_i})$ are also relatively prime and their intersection is equal to their product:

$$[\mathfrak{q}_1, \ldots, \mathfrak{q}_r] = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r$$

$\mathfrak{a}$ is divisible by all $\mathfrak{q}_i$, and therefore by their intersection. On the other hand, if the product

$$\mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r = (\mathfrak{a}, \mathfrak{p}_1^{\varrho_1}) \cdot (\mathfrak{a}, \mathfrak{p}_2^{\varrho_2}) \cdots (\mathfrak{a}, \mathfrak{p}_r^{\varrho_r})$$

on the right side is expanded according to the distributive law (Section 85), we obtain a sum of ideals which are all divisible by $\mathfrak{a}$. Hence

$$\mathfrak{a} \equiv \mathfrak{o}(\mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r) \equiv \mathfrak{o}(\mathfrak{a}),$$

therefore

$$\mathfrak{a} = [\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r] = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r$$

The $\mathfrak{q}_i$, as divisors of $\mathfrak{p}_i^{\varrho_i}$, are evidently divisible by no prime ideal other than $\mathfrak{p}_i$ and $\mathfrak{o}$, that is, the $\mathfrak{q}_i$ are single-primed. The uniqueness of the $\mathfrak{q}_i$ follows from the fact that every decomposition $\mathfrak{a} = [\mathfrak{q}_1', \mathfrak{q}_2', \ldots, \mathfrak{q}_r']$ implies $\mathfrak{q}_i' = (\mathfrak{a}, \mathfrak{p}_i^{\sigma})$, as seen above.

CHAPTER XIII

THEORY OF POLYNOMIAL IDEALS

In this chapter the general ideal theory of (commutative) polynomial domains shall be developed. Besides the general theory of ideals we shall assume as known only the theory of fields (Chap. 5) and what precedes it.

91. ALGEBRAIC MANIFOLDS

Let K be a commutative field. A sequence of n elements $\{\xi_1, \ldots, \xi_n\}$ of an arbitrary algebraic extension field of K is said to be a *point* of the n-dimensional space R_n. The point $\{\xi_1, \ldots, \xi_n\}$ is denoted simply by ξ ; the ξ_ν are called its *coordinates.*

Let $\mathfrak{o} = \mathsf{K}[x_1, \ldots, x_n]$ be the polynomial domain of the n indeterminates $x_1, \ldots, x_n$. Its elements are polynomials and will be denoted by $f = f(x) = f(x_1, \ldots, x_n)$, g, h, ... A point ξ is said to be a *zero* of the polynomial $f(x)$ if $f(\xi) = f(\xi_1, \ldots, \xi_n) = 0$. The common zeros of an arbitrary number of polynomials $f_1, \ldots, f_r$, that is, the solutions of a system of equations

$$f_1(\xi) = 0, \ldots, f_r(\xi) = 0, \tag{1}$$

is said to form an *algebraic manifold* $\mathfrak{M}$, when this set is not empty. The following are well known examples: the "algebraic curves" in a plane and the "algebraic surfaces" in space, each of which is represented by a single equation $f(\xi_1, \xi_2) = 0$ and $f(\xi_1, \xi_2, \xi_3) = 0$ respectively; the "space curves" which are determined by two equations, etc. Also, a single point ξ with coordinates in K forms an algebraic manifold as well as the whole space R_n.

In Chapter XI we explained how the solutions of (1) could actually be determined. Here we will be concerned with other problems, namely, what general theorems can be stated for algebraic manifolds and, in particular, how can algebraic manifolds be classified as curves, surfaces, etc. by their "dimension."

Let $f_1, \ldots, f_r$ be the "polynomials defining" the algebraic manifold $\mathfrak{M}$. If the ideal $\mathfrak{a} = (f_1, \ldots, f_r)$, is formed, then all points of the manifold (zeros of $f_1, \ldots, f_r$) are also zeros of all polynomials $f = g_1 f_1 + \cdots + g_r f_r$ of this ideal.

Hence $\mathfrak{M}$ may also be characterized as the totality of all zeros common to the polynomials of the ideal $\mathfrak{a}$ or, more concisely, of all *zeros of the ideal* $\mathfrak{a}$. By Hilbert's Basis Theorem (Section 84) we may also assume that $\mathfrak{a}$ has a finite basis since every ideal in $\mathfrak{o}$ has a finite basis. Hence *an algebraic manifold* $\mathfrak{M}$ *consists of those points* ξ *which are zeros of an ideal* $\mathfrak{a}$ *in* $\mathsf{K}[x_1, \ldots, x_n]$. We call $\mathfrak{M}$ *the zero manifold of* $\mathfrak{a}$ or simply *the manifold of* $\mathfrak{a}$.

An ideal which contains $\mathfrak{a}$ (divisor of $\mathfrak{a}$) defines a submanifold of $\mathfrak{M}$. It may happen however that distinct ideals define the same algebraic manifold $\mathfrak{M}$; for instance, $\mathfrak{a}$ and $\mathfrak{a}^2$ always have the same manifold $\mathfrak{M}$. Among all the ideals having the same algebraic manifold, there is one of particular importance: the totality of *all* polynomials f which are zero at all points of the manifold $\mathfrak{M}$. This totality includes all ideals which define the manifold $\mathfrak{M}$. Furthermore, it is itself an ideal since if f vanishes over all of $\mathfrak{M}$, so also must every multiple of f, and if f and g both vanish over $\mathfrak{M}$, so also must $f - g$. The manifold of this ideal is $\mathfrak{M}$. This ideal is said to be the *ideal belonging* to the manifold.

If a polynomial f is zero at all points of a manifold $\mathfrak{M}$, we say that the polynomial f *contains* the manifold $\mathfrak{M}$ (since in this case the manifold $f = 0$ contains the manifold $\mathfrak{M}$). Hence the ideal belonging to a manifold $\mathfrak{M}$ consists of all polynomials which contain the manifold $\mathfrak{M}$.

The *intersection* $\mathfrak{M} \cap \mathfrak{N}$, if it is not empty, of two algebraic manifolds $\mathfrak{M}$ and $\mathfrak{N}$ is again an algebraic manifold. Thus, if $\mathfrak{M}$ is defined by the ideal $\mathfrak{a}=(f_1, \ldots, f_r)$ and $\mathfrak{N}$ by the ideal $\mathfrak{b} = (g_1, \ldots, g_s)$, the intersection $\mathfrak{M} \cap \mathfrak{N}$ is evidently the manifold defined by the ideal $(\mathfrak{a}, \mathfrak{b}) = (f_1, \ldots, f_r, g_1, \ldots, g_s)$.

Likewise, the *set-union* of two algebraic manifolds $\mathfrak{M}, \mathfrak{N}$ is an algebraic manifold; it is defined by the intersection ideal (L.C.M.) $\mathfrak{a} \cap \mathfrak{b}$ (or also by the product $\mathfrak{a} \cdot \mathfrak{b}$). This may be shown as follows. On the one hand, every point of the union is either a zero of all polynomials in $\mathfrak{a}$ or a zero of all polynomials in $\mathfrak{b}$, and therefore in every case a zero of all polynomials in $\mathfrak{a} \cap \mathfrak{b}$ (and particularly of those in $\mathfrak{a} \cdot \mathfrak{b}$). On the other hand, if a point ξ does not belong to the union $\mathfrak{M} \vee \mathfrak{N}$, there is in $\mathfrak{a}$ a polynomial f and similarly in $\mathfrak{b}$ a polynomial g which does not vanish at the point ξ. Hence the product fg, which belongs to $\mathfrak{a} \cap \mathfrak{b}$ (and $\mathfrak{a} \cdot \mathfrak{b}$), does not vanish at the point ξ; this means that ξ is not a zero of $\mathfrak{a} \cap \mathfrak{b}$ (or $\mathfrak{a} \cdot \mathfrak{b}$). Therefore, the zeros of $\mathfrak{a} \cap \mathfrak{b}$ (as well as of $\mathfrak{a} \cdot \mathfrak{b}$) are the points of $\mathfrak{M} \vee \mathfrak{N}$ and only these.

The union of a finite number of algebraic manifolds (for instance, a finite number of points, curves, etc.) is again an algebraic manifold.

A manifold which may be represented as the union of two proper submanifolds is said to be *composite* or *reducible*. A non-composite manifold is said to be *indecomposable* or *irreducible*.

The decision regarding the reducibility of a manifold depends in particular on the ground field K. For instance, in the field of rational numbers the pair of points

$\xi_1 = 0$, $\xi_2 = \pm\sqrt{2}$ forms an irreducible manifold, the zero manifold of the ideal $(x_1, x_2^2 - 2)$. However, by the adjunction of $\sqrt{2}$ this manifold may be decomposed into two constitutents (points).

A criterion for irreducibility is given by: *A manifold $\mathfrak{M}$ is irreducible if and only if the ideal belonging to $\mathfrak{M}$ is prime, i.e., if from "fg contains $\mathfrak{M}$" follows: "either f or g contains $\mathfrak{M}$."*

PROOF. First, assume that $\mathfrak{M}$ is reducible: $\mathfrak{M} = \mathfrak{M}_1 \vee \mathfrak{M}_2$, where $\mathfrak{M}_1$ and $\mathfrak{M}_2$ are proper submanifolds of $\mathfrak{M}$. In the ideal belonging to $\mathfrak{M}_1$ there is a polynomial f which does not contain $\mathfrak{M}$, since otherwise $\mathfrak{M}_1 \supseteq \mathfrak{M}$. Similarly, in the ideal belonging to $\mathfrak{M}_2$ there is a polynomial g which does not contain $\mathfrak{M}$. The product fg contains $\mathfrak{M}_1$ and $\mathfrak{M}_2$, and therefore $\mathfrak{M}$. Hence the ideal belonging to $\mathfrak{M}$ is not prime.

Secondly, let $\mathfrak{M}$ be irreducible. Now, if a product fg were to contain $\mathfrak{M}$ without f or g doing likewise, then $\mathfrak{M}$ could be represented as the union of the two proper submanifolds $\mathfrak{M}_1$ and $\mathfrak{M}_2$ defined as follows: $\mathfrak{M}_1$ consists of all points of $\mathfrak{M}$ which satisfy the equation $f = 0$, and $\mathfrak{M}_2$ all points of $\mathfrak{M}$ which satisfy the equation $g = 0$. Thus, every point ξ of $\mathfrak{M}$ belongs to $\mathfrak{M}_1$ or to $\mathfrak{M}_2$ since $f(\xi)g(\xi) = 0$ implies $f(\xi) = 0$ or $g(\xi) = 0$. This contradicts the assumption that $\mathfrak{M}$ is irreducible.

The fact that the ideal belonging to an irreducible manifold is a prime ideal gives us an intuitive insight regarding the large number of prime ideals that are possible, and also how a prime ideal may be divisible by another. For instance, in the plane we may start with the null ideal which belongs to the manifold consisting of the whole plane. As its divisors we have the prime principal ideals (f) which belong to the indecomposable curves $f = 0$. Then, as divisors of these we have the prime ideals which belong to points (or systems of conjugate points when the field K is not algebraically closed). Finally, as divisor of all prime ideals we have the unit ideal which has no zeros.

The fact that there are no prime ideals other than the prime ideals belonging to irreducible manifolds and the unit ideal $\mathfrak{o}$ follows very easily if we assume that Hilbert's Nullstellensatz (Section 79) is known. Thus, let $\mathfrak{p}$ be a prime ideal distinct from the unit ideal, and $\mathfrak{M}$ its zero manifold. If a polynomial f vanishes over all of $\mathfrak{M}$, then by Hilbert's Nullstellensatz $f^\varrho \equiv 0(\mathfrak{p})$. Hence, since $\mathfrak{p}$ is prime, $f \equiv 0(\mathfrak{p})$. Consequently, $\mathfrak{p}$ is the ideal belonging to the manifold $\mathfrak{M}$, and $\mathfrak{M}$ must be irreducible since otherwise $\mathfrak{p}$ would not be prime.

In a later section we will give another proof of the theorem that every prime ideal distinct from the unit ideal is the ideal belonging to its manifold, and thereby derive conversely a new proof of Hilbert's Nullstellensatz.

EXERCISE. 1. Decompose the manifold of the ideal $(x_1^2 + x_2^2 - 1,\ x_1^2 - x_3^2 - 1)$ into irreducible constitutents

a) over the rational number field Γ;

b) over the Gaussian number field $\Gamma(i)$;

c) over the field of all algebraic numbers.

In geometry we very frequently make the transition from the usual "open" or "affine" n-dimensional space R_n to the projective space S_n, whose points are determined by $n+1$ homogeneous coordinates $\xi_0, \xi_1, \ldots, \xi_n$ which are not all zero and which may be multiplied (cf. p. 7, footnote 6) by a factor distinct from zero. To every point $\{\xi_1, \ldots, \xi_n\}$ of R_n there corresponds the point $\{1, \xi_1, \ldots, \xi_n\}$ of the projective space S_n; hence we may consider R_n as a part of S_n which together with the "improper hyperplane" $\xi_0 = 0$ fills up all of S_n.

To every ideal $\mathfrak{a}$ of $\mathsf{K}[x_1, \ldots, x_n]$ there corresponds an ideal $\mathfrak{a}^*$ of $\mathsf{K}_1[x_0, \ldots, x_n]$ which is generated by those forms (homogeneous polynomials) $F(x_0, \ldots, x_n)$ that give rise to polynomials of $\mathfrak{a}$ by the substitution $x_0 = 1$. Such an ideal, which is generated by homogeneous polynomials, is called a *homogeneous ideal* or H-ideal. In particular we refer to $\mathfrak{a}^*$ as the *H-ideal belonging to* $\mathfrak{a}$. The H-ideals have the property that if $\{\xi_0, \ldots, \xi_n\}$ is a zero, then $\{\lambda\xi_0, \ldots, \lambda\xi_n\}$ $(\lambda \neq 0)$ is also. In this case we say that the point ξ of S_n is a zero of the H-ideal. The zeros of an H-ideal in the projective space form the *manifold of the H-ideal in the projective space.*

To every algebraic manifold $\mathfrak{M}$ in R_n there is a (smallest) algebraic manifold $\mathfrak{M}^*$ in S_n which includes it. This manifold may be constructed as follows: let $\mathfrak{a}$ be the ideal belonging to $\mathfrak{M}$, $\mathfrak{a}^*$ the H-ideal belonging to $\mathfrak{a}$, and $\mathfrak{M}^*$ the manifold in S_n belonging to $\mathfrak{a}^*$. The proof that $\mathfrak{M}^*$ actually includes $\mathfrak{M}$ and is the smallest manifold in S_n of this kind is left to the reader, since it is similar to the proof that $\mathfrak{M}$ consists of those points of $\mathfrak{M}^*$ which do not lie in the improper hyperplane.

If $\mathfrak{M}$ is irreducible, obviously $\mathfrak{M}^*$ is also.

EXERCISES. 2. Prove the above statements.

3. If a polynomial f belongs to an H-ideal, the homogeneous constitutents of distinct degrees, in which f can be decomposed additively, belong to the H-ideal.

4. Every H-ideal has an ideal basis consisting of a finite number of forms.

92. ALGEBRAIC FUNCTIONS

In the next section we shall show how to represent points of an algebraic manifold as algebraic functions of parameters. To introduce this investigation we make the following remarks about algebraic functions in general.

By a *rational function field* we understand the field $\mathsf{K}(t_1, \ldots, t_r)$ of rational functions of the indeterminates $t_1, \ldots, t_r$. By an *algebraic function field* we understand an arbitrary algebraic extension of the rational function field $\mathsf{K}(t_1, \ldots, t_r)$. The elements of such a field are called *algebraic functions* of $t_1, \ldots, t_r$.

Let $\varphi = \dfrac{f(t_1, \ldots, t_r)}{g(t_1, \ldots, t_r)}$ (f and g are polynomials) be a rational function. It is clear what is meant by the *value* of this function for the special values $\tau_1, \ldots, \tau_r$ in the field K: the τ may actually be substituted for the t in the definition of φ as long as $g(\tau_1, \ldots, \tau_r)$ does not vanish:

$$\varphi(\tau_1, \ldots, \tau_r) = \frac{f(\tau_1, \ldots, \tau_r)}{g(\tau_1, \ldots, \tau_r)}.$$

The values $\tau_1, \ldots, \tau_r$ may also be taken from an algebraic extension field Ω of K; in this case the φ-value will belong to this extension field. Since a Ω may

always be chosen with an arbitrary number of elements, for every τ_r there are infinitely many values at our disposal. Hence there always exists $\tau_1, \ldots, \tau_r$ such that $g(\tau_1, \ldots, \tau_r) \neq 0$.

In regard to algebraic functions the concept of the value of a function is not as obvious; for, even though the algebraic functions as elements of a field are connected with the indeterminates $t_1, \ldots, t_r$ by certain equations, they cannot be explicitly expressed in terms of $t_1, \ldots, t_r$. If f is a function of the field, f satisfies an irreducible equation

$$a_0(t)f^h + a_1(t)f^{h-1} + \cdots + a_h(t) = 0, \tag{1}$$

where $a_0, \ldots, a_h$ are rational functions of $t_1, \ldots, t_r$ (with coefficients in K) which may naturally be assumed to be rational integral functions and relatively prime. If we substitute for $t_1, \ldots, t_r$ arbitrary values $\tau_1, \ldots, \tau_r$ from K, or from $\Omega \supseteq \mathsf{K}$, then all roots φ of the specialized equation (1) in a suitable algebraic extension field are considered as *function values* of f. These values always exist as soon as $a_0(\tau) \neq 0$. Hence in general the function f is *many-valued:* to every set of argument values there correspond many function values.

If we have to consider simultaneously several functions $f_1, \ldots, f_s$ in a function field, we may adjoin $f_1, \ldots, f_s$ successively to $\mathsf{K}(t_1, \ldots, t_r)$. Every f_k satisfies in $\mathsf{K}(t_1, \ldots, t_r, f_1, \ldots, f_{k-1})$ an irreducible equation

$$\begin{cases} f_k^{m_k} + a_{k1}(t_1, \ldots, t_r, f_1, \ldots, f_{k-1}) f_k^{m_k-1} + \cdots \\ \quad + a_{km_k}(t_1, \ldots, t_r, f_1, \ldots, f_{k-1}) = 0, \end{cases} \tag{2}$$

whose coefficients are rational in $t_1, \ldots, t_r, f_1, \ldots, f_{k-1}$. Since f_{k-1} is an algebraic quantity, every rational function of $f_1, \ldots, f_{k-1}$ may be written as a rational integral function in f_{k-1}, then rational integral in f_{k-2}, etc., finally also in f_1. We are permitted therefore to assume that the denominators of the rational functions $a_{k\mu}$ depend only on $t_1, \ldots, t_r$. Let $V(t_1, \ldots, t_r)$ be a common multiple of these denominators.

We define an *allowable system of argument values* of the functions $f_1, \ldots, f_s$ as a system of values $\tau_1, \ldots, \tau_r$ in an algebraic extension field Ω of K which satisfies the condition $V(\tau_1, \ldots, \tau_r) \neq 0$. Then a *system of function values belonging* to these arguments is a system of values $\varphi_1, \ldots, \varphi_s$ in Ω which satisfies equations (2) with τ instead of t and φ instead of f:

$$\begin{cases} \varphi_k^{m_k} + a_{k1}(\tau_1, \ldots, \tau_r, \varphi_1, \ldots, \varphi_{k-1}) \varphi_k^{m_k-1} + \cdots \\ \quad + a_{km_k}(\tau_1, \ldots, \tau_r, \varphi_1, \ldots, \varphi_{k-1}) = 0. \end{cases} \tag{3}$$

It is clear that by a suitable choice of the extension field to every system of allowable argument values we may find a system of function values belonging to these arguments. For in a suitable algebraic extension field every algebraic equation has at least one solution and the equations (3) determine the sequence of values $\varphi_1, \varphi_2, \ldots, \varphi_s$ (in many ways).

The following theorem is now valid: *if an algebraic relation* $F(t_1, \ldots, t_r, f_1, \ldots, f_s) = 0$ *is valid in the function field, then the same relation* $F(\tau_1, \ldots, \tau_r, \varphi_1, \ldots, \varphi_s) = 0$ *is valid for all allowable argument values and function values belonging to the arguments.* Here F shall always designate a polynomial with coefficients in K.

PROOF. For $s = 0$ the theorem is trivial since every equation $F(t_1, \ldots, t_r) = 0$, which is valid identically in the indeterminates $t_1, \ldots, t_r$ is also valid for arbitrary special values of the indeterminates. We will therefore make an induction on s and assume that the theorem is valid for all polynomials F which contain only $t_1, \ldots, t_r, f_1, \ldots, f_{s-1}$.

In the equation $F(t_1, \ldots, t_r, f_1, \ldots, f_s) = 0$ let us replace the last function f_s by an indeterminate z. Then $F(t_1, \ldots, t_r, f_1, \ldots, f_{s-1}, z)$ is divisible by the irreducible polynomial

$$h(z) = z^{m_s} + a_{s1}(t_1, \ldots, t_r, f_1, \ldots, f_{s-1}) z^{m_s-1} + \cdots + a_{sm_s}(t_1, \ldots, t_r, f_1, \ldots, f_{s-1})$$

which has f_s as a zero by (2). Let the division be actually carried out. Then no denominators will appear except those which in $h(z)$ already occur in the denominator. Hence the fact that $F(t_1, \ldots, z)$ is divisible by $h(z)$ can be expressed as a rational integral relation in $t_1, \ldots, t_r, f_1, \ldots, f_{s-1}, z$ on multiplying by the product of these denominators. In this relation equate the coefficients of like powers of z in both members. We thereby obtain rational integral relations in $t_1, \ldots, t_r, f_1, \ldots, f_{s-1}$ which must also be valid, by the induction hypothesis, when $t_1, \ldots, t_r, f_1, \ldots, f_{s-1}$ are replaced by $\tau_1, \ldots, \tau_r, \varphi_1, \ldots, \varphi_{s-1}$. But the product of the denominators, by which we have just multiplied, does not vanish when the t are replaced by the τ. Hence, after the substitution we may again divide by this product and obtain the result that $F(\tau_1, \ldots, \tau_r, \varphi_1, \ldots, \varphi_{s-1}, z)$ is divisible by the specialized polynomial $h(z)$, that is, by

$$z^{m_s} + a_{s1}(\tau_1, \ldots, \tau_r, \varphi_1, \ldots, \varphi_{s-1}) z^{m_s-1} + \cdots + a_{sm_s}(\tau_1, \ldots, \tau_s, \varphi_1, \ldots, \varphi_{s-1})$$

Consequently, (3) implies $F(\tau_1, \ldots, \tau_r, \varphi_1, \ldots, \varphi_s) = 0$. Q.E.D.

The converse of the theorem just proved is also valid: *if the relation* $F(\tau_1, \ldots, \tau_r, \varphi_1, \ldots, \varphi_s) = 0$ *is valid for all allowable argument values and function values belonging to these arguments, then* $F(t_1, \ldots, t_r, f_1, \ldots, f_s) = 0$.

PROOF. Assume that $F(t_1, \ldots, t_r, f_1, \ldots, f_s) \neq 0$. Then we may form the function

$$f_{s+1} = \frac{1}{F(t_1, \ldots, t_r, f_1, \ldots, f_s)}$$

and find for the functions $f_1, \ldots, f_s, f_{s+1}$ a system of allowable argument values $\tau_1, \ldots, \tau_r$ and function values $\varphi_1, \ldots, \varphi_s, \varphi_{s+1}$. The relation

$$1 = f_{s+1} \cdot F(t_1, \ldots, t_r, f_1, \ldots, f_s)$$

must remain valid by the specialization $t_\lambda \to \tau_\lambda$, $f_\nu \to \varphi_\nu$. However, by assumption $F_i(\tau_1, \ldots, \tau_r, \varphi_1, \ldots, \varphi_s) = 0$. Hence we have

$$1 = 0,$$

which is absurd.

93. THE ZEROS OF A PRIME IDEAL

If $\xi_1, \ldots, \xi_n$ are algebraic functions of $t_1, \ldots, t_r$, the function values $\xi'_1, \ldots, \xi'_n$ belonging to the special allowable argument values $\tau_1, \ldots, \tau_r$ determine a point ξ' in R_n; these points ξ' may either completely fill up an algebraic manifold or almost completely. We then speak of a *parametric representation* of the manifold by the algebraic functions $\xi_1, \ldots, \xi_n$ of the parameters $t_1, \ldots, t_r$.

Our aim is to investigate more exactly whether every system of algebraic functions defines in this manner a manifold and whether every manifold permits such a parametric representation. We will answer these questions only after we have investigated the algebraic properties of the functions $\xi_1, \ldots, \xi_n$ themselves. Our immediate concern is with a prime ideal which will later turn out to be the ideal belonging to the manifold represented by the parametric representation.

THEOREM 1. *If* $\Omega = \mathsf{K}(\xi_1, \ldots, \xi_n)$ *is an extension field of a field* K, *then the polynomials* f *in* $\mathfrak{o} = \mathsf{K}[x_1, \ldots, x_n]$, *for which* $f(\xi_1, \ldots, \xi_n) = 0$, *form a prime ideal in* $\mathfrak{o}$.

PROOF. If $f(\xi_1, \ldots, \xi_n) = 0$ and $g(\xi_1, \ldots, \xi_n) = 0$, then

$$f(\xi_1, \ldots, \xi_n) - g(\xi_1, \ldots, \xi_n) = 0.$$

If $f(\xi_1, \ldots, \xi_n) = 0$, then $f(\xi_1, \ldots, \xi_n)\, g(\xi_1, \ldots, \xi_n) = 0$.

Hence the polynomials under consideration form an ideal.

If $f(\xi_1, \ldots, \xi_n)\, g(\xi_1, \ldots, \xi_n) = 0$ and $g(\xi_1, \ldots, \xi_n) \neq 0$, then $f(\xi_1, \ldots, \xi_n) = 0$ since a field has no zero divisors.

Hence the ideal is prime.

EXAMPLE. Let $\xi_1, \ldots, \xi_n$ be linear functions of an indeterminate λ with coefficients in the field K of complex numbers:

$$\xi_i = \alpha_i + \beta_i \lambda. \tag{1}$$

Then the prime ideal referred to in the theorem consists of all polynomials $f(x_1, \ldots, x_n)$ for which $f(\alpha_1 + \beta_1\lambda, \ldots, \alpha_n + \beta_n\lambda)$ vanishes identically in λ, or (geometrically speaking) of all polynomials that vanish at all points of the line with the parametric representation (1) in the n-dimensional space. This example may be used to illustrate all theorems of this and the following sections.

THEOREM 2. *If* $\mathfrak{p}$ *denotes the prime ideal of Theorem* 1, *then* Ω *is isomorphic to the residue class field* Π *of* $\mathfrak{o}$ *modulo* $\mathfrak{p}$, *and in fact there is a map-*

ping such that the elements $x_1, \ldots, x_n$ *correspond to the elements* $\xi_1, \ldots, \xi_n$.

PROOF. Let Ω' be the ring of those elements of Ω which may be written as polynomials in $\xi_1, \ldots, \xi_n$. $\Omega = \mathsf{K}(\xi_1, \ldots, \xi_n)$ is the quotient field of Ω'. Let each element $f(\xi_1, \ldots, \xi_n)$ of Ω' be mapped on the element of the residue class ring $\mathfrak{o}/\mathfrak{p}$ which has the function $f(x_1, \ldots, x_n)$ as a representative. Then $f(\xi_1, \ldots, \xi_n) - g(\xi_1, \ldots, \xi_n) = 0$ implies $f(x_1, \ldots, x_n) - g(x_1, \ldots, x_n) \equiv 0(\mathfrak{p})$ or $f(x_1, \ldots, x_n) \equiv g(x_1, \ldots, x_n)$ $(\mathfrak{p})$, and conversely. Hence the correspondence is one-to-one. It is clear that sums and products go into sums and products. Hence the Ω' is isomorphic to $\mathfrak{o}/\mathfrak{p}$ so that the quotient fields Ω and Π must be isomorphic.

THEOREM 3. *To every prime ideal* $\mathfrak{p}$ *in* $\mathfrak{o}$ *distinct from* $\mathfrak{o}$ *there is a field* $\Omega = \mathsf{K}(\xi_1, \ldots, \xi_n)$ *such that* $\mathfrak{p}$ *consists of all polynomials* f *of* $\mathfrak{o}$ *for which* $f(\xi_1, \ldots, \xi_n) = 0$.

PROOF. Let the polynomials in $\mathfrak{o}$ be mapped on the elements of a new set $\mathfrak{o}'$, which includes the coefficient field K, such that two polynomials congruent modulo $\mathfrak{p}$ shall correspond to the same element, two that are not congruent shall correspond to different elements, and the elements of K correspond to themselves. This is always possible since two elements of K are congruent modulo $\mathfrak{p}$ if and only if they are equal since $\mathfrak{p} \neq \mathfrak{o}$. Denote the images of the elements $x_1, \ldots, x_n$ under this correspondence by $\xi_1, \ldots, \xi_n$.

The set $\mathfrak{o}'$ is a single-valued image of the residue class ring of $\mathfrak{o}$ modulo $\mathfrak{p}$. Hence, if we define in $\mathfrak{o}'$ an addition and a multiplication which correspond to the addition and multiplication respectively in the residue class ring, then $\mathfrak{o}'$ is isomorphic to the residue class ring. This means that it has no zero divisors and permits the formation of a quotient field Ω. In Ω, $f(\xi_1, \ldots, \xi_n) = 0$ if and only if $f(x_1, \ldots, x_n) \equiv 0(\mathfrak{p})$. Q.E.D.

By Theorem 3 for every prime ideal $\mathfrak{p}$ distinct from $\mathfrak{o}$ the field $\Omega = \mathsf{K}(\xi_1, \ldots, \xi_n)$ may be constructed, by Theorem 1 it exists *only* for prime ideals, and by Theorem 2 it is uniquely determined except for isomorphisms. Its generators ξ_i have the property that $f(\xi_1, \ldots, \xi_n) = 0$ if and only if $f \equiv 0(\mathfrak{p})$. This field is called the *zero field* (*Nullstellenkörper*) of $\mathfrak{p}$; the sequence $\{\xi_1, \ldots, \xi_n\}$ is called the *generic zero* of $\mathfrak{p}$. By a *zero* of an ideal $\mathfrak{m}$ we mean a sequence $\{\eta_1, \ldots, \eta_n\}$ of elements in an extension field of K such that $f(\eta_1, \ldots, \eta_n) = 0$ whenever $f \equiv 0(\mathfrak{m})$. Every zero of a prime ideal distinct from the generic zero is called a *particular zero.*

By Section 91 the ideal belonging to an irreducible algebraic manifold $\mathfrak{M}$ is a prime ideal $\mathfrak{p}$. Every zero ξ of this prime ideal is a point of the manifold since it satisfies the equations of the manifold. Strictly speaking we have a point (in the sense of Section 91) only if its coordinates $\xi_1, \ldots, \xi_n$ are algebraic over K. However, if by a "point" in an extended sense we mean any sequence of elements $\xi_1, \ldots, \xi_n$ in an arbitrary extension field of K, then every zero of $\mathfrak{p}$ may be considered as a point of $\mathfrak{M}$. In particular, if ξ is a generic zero of $\mathfrak{p}$, ξ is called a generic point of $\mathfrak{M}$.

If we go back to the definition of generic zero and of the prime ideal belonging to it, then: *a point (in the extended sense) ξ is a generic point of $\mathfrak{M}$ if every algebraic equation $f(\xi_1, \ldots, \xi_n) = 0$ with coefficients in K which is valid for ξ is valid for all points of $\mathfrak{M}$, and conversely.*

Furthermore, by Theorem 3: *every irreducible manifold possesses a generic point.*

By Theorem 2 this point is uniquely determined except for isomorphisms, that is, if ξ and η are two generic points of $\mathfrak{M}$, there is an isomorphism $\mathsf{K}(\xi_1, \ldots, \xi_n) \cong \mathsf{K}(\eta_1, \ldots, \eta_n)$ which takes $\xi_1, \ldots, \xi_n$ into $\eta_1, \ldots, \eta_n$.

We now ask whether to every point ξ in the extended sense there belongs a manifold $\mathfrak{M}$ which has ξ as a generic point.

Let $\xi_1, \ldots, \xi_n$ be elements of an extension field of K. If $\xi_1, \ldots, \xi_d$, let us say, are algebraically independent and $\xi_{d+1}, \ldots, \xi_n$ are algebraically dependent on $\xi_1, \ldots, \xi_d$, then all ξ_j are algebraic functions of $\xi_1, \ldots, \xi_d$ and the latter functions behave as indeterminates. Hence the generality of our results will not be affected if we assume that $\xi_1, \ldots, \xi_n$ are algebraic functions of the indeterminates $t_1, \ldots, t_d$.

Now if $\tau_1, \ldots, \tau_d$ are allowable argument values of the functions $\xi_1, \ldots, \xi_n$ in the sense of Section 92 and $\eta_1, \ldots, \eta_n$ are the function values belonging to these argument values, then by Section 92 every algebraic equation $f(\xi) = 0$ which is valid for the point ξ is also valid for all points η, and conversely. Furthermore, by Theorem 1 the polynomials f with the property $f(\xi) = 0$ form a prime ideal $\mathfrak{p}$, and ξ is the generic zero of this prime ideal. We have therefore shown: if f belongs to $\mathfrak{p}$, then $f(\eta) = 0$ for all points η constructed as above, and conversely.

Let the zero manifold of $\mathfrak{p}$ be $\mathfrak{M}$. The points η constructed above all belong to $\mathfrak{M}$. If a polynomial f belongs to $\mathfrak{p}$, f is zero at all points of $\mathfrak{M}$. Conversely: if a polynomial is zero at all points of $\mathfrak{M}$, f in particular is zero at the points η constructed above, and therefore f belongs to the ideal $\mathfrak{p}$. This implies: $\mathfrak{p}$ is the ideal belonging to $\mathfrak{M}$. Since $\mathfrak{p}$ is prime, $\mathfrak{M}$ is irreducible. Finally, since ξ is a generic zero of $\mathfrak{p}$, ξ is a generic point of $\mathfrak{M}$.

Hence we have proved:

THEOREM 4. *Every point ξ in the extended sense is a generic point of a uniquely determined irreducible algebraic manifold. By Theorem* 1 *the prime ideal belonging to ξ is the ideal belonging to this manifold.*

From the proof we may also deduce the sense in which we may speak of a parametric representation of $\mathfrak{M}$. Thus, the ξ_ν should be thought of as algebraic functions of the parameters $t_1, \ldots, t_d$ and for each special value τ of the parameter as determining a fixed point η which belongs to $\mathfrak{M}$. These points need not fill up the whole manifold $\mathfrak{M}$. However they lie so thickly in $\mathfrak{M}$ that every polynomial f, which is zero at all points η, already belongs to $\mathfrak{p}$ and therefore contains the

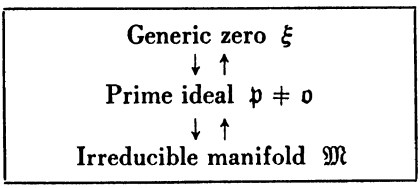
whole of $\mathfrak{M}$. In the example given by (1) the points η actually fill up the whole line $\mathfrak{M}$.

Theorems 3 and 4 further imply:

Every prime ideal $\neq 0$ *is the prime ideal belonging to its manifold which is irreducible.*

The only prime ideal without zeros is 0. Hence this ideal is also determined by its zeros.

The proofs given so far may be combined according to the following scheme:



EXERCISES. 1. In $\mathsf{K}[x_1, x_2, x_3]$ the ideal

$$(x_1x_3 - x_2^2,\ x_2x_3 - x_1^3,\ x_3^2 - x_1^2x_2)$$

is prime and

$$\{t^3, t^4, t^5\}$$

is the generic zero.

2. In $\mathsf{K}[x_1, x_2, x_3]$ the ideal

$$(x_1^2 + x_2^2 - x_3^2,\ x_1^2 - x_2^2 + 1)$$

is prime and

$$\left\{\frac{1-t^2}{2t},\ \frac{1+t^2}{2t},\ \frac{\sqrt{2(1+t^4)}}{2t}\right\}.$$

is the generic zero.

3. In $\mathsf{K}[x_1, x_2, x_3, x_4]$ the ideal

$$(x_1x_4 - x_2x_3,\ x_2^3 - x_1^2x_3,\ x_3^3 - x_2x_4^2,\ x_2^2x_4 - x_1x_3^2)$$

is prime and

$$\{t_1^4, t_1^3t_2, t_1t_2^3, t_2^4\}.$$

is the generic zero.

4. If $\mathfrak{p}$ is a prime ideal in $\mathsf{K}[x_1, \ldots, x_n]$ with the generic zero $\{\xi_1, \ldots, \xi_n\}$, then the H-ideal $\mathfrak{p}^*$ in $\mathsf{K}[x_0, \ldots, x_n]$ (cf. Section 91, end) belonging to $\mathfrak{p}$ is prime with the generic zero $\{\lambda, \lambda\xi_1, \ldots, \lambda\xi_n\}$, where λ is an indeterminate.

94. THE DIMENSION

Let $\xi_1, \ldots, \xi_n$ be algebraic functions of $t_1, \ldots, t_r$. The degree of transcendence s of the system $\{\xi_1, \ldots, \xi_n\}$ (cf. Section 64) is $\leqq r$. The degree of transcendence is exactly equal to r if the $t_1, \ldots, t_r$ also depend algebraically on the ξ ; for instance, if the t belong to the field $\mathsf{K}(\xi_1, \ldots, \xi_n)$, or if $t_1, \ldots, t_r$ are chosen as the $r = s$ algebraically independent ξ, say $\xi_1, \ldots, \xi_s$. In the parametric representation of an algebraic manifold $\mathfrak{M}$ it is very advantageous to choose the parameters $t_1, \ldots, t_r$ in the field $\mathsf{K}(\xi_1, \ldots, \xi_n)$ because the parameters may then be interpreted as functions of the manifold $\mathfrak{M}$ rather than something foreign which is added to it. If the number r of the parameters is larger than the degree of transcendence s, we have "*superfluous parameters.*" The smallest number of parameters which are needed is exactly s. This number is called the *dimension of the manifold* $\mathfrak{M}$ or the *dimension of the prime ideal* $\mathfrak{p}$ *belonging to* $\mathfrak{M}$. Accordingly, the dimension of a prime ideal distinct from the unit ideal is nothing else than the degree of transcendence of its generic zero ξ.

Obviously, the dimension of the prime ideals $\mathfrak{p} \neq \mathfrak{o}$ may be any number from 0 to n. The dimension of the unit ideal $\mathfrak{o}$, which has no zeros, is said to be -1.

If ξ is the generic zero of a prime ideal $\mathfrak{p}$, ξ' an arbitrary zero of this ideal, then to every polynomial $f(\xi)$ in $\mathsf{K}[\xi]$ we can associate the polynomial $f(\xi')$ in $\mathsf{K}[\xi']$. Now, if $f(\xi) = g(\xi)$. then $f(x) \equiv g(x)$ $(\mathfrak{p})$, and so $f(\xi') = g(\xi')$. Hence the correspondence $f(\xi) \to f(\xi')$ is single-valued. Obviously this correspondence takes sums into sums and products into products. Hence it is an *homomorphism:*

$$\mathsf{K}[\xi] \backsim \mathsf{K}[\xi']. \tag{1}$$

If the correspondence is an isomorphism, ξ' is also a generic zero of $\mathfrak{p}$, and conversely.

In a zero-dimensional ideal $\mathfrak{p}$ all ξ are algebraic over K; therefore, all rational functions of the ξ are actually rational integral functions: $\mathsf{K}(\xi) = \mathsf{K}[\xi]$. Hence $\mathsf{K}[\xi]$ is a *field.* Furthermore, if ξ' is an arbitrary zero, the homomorphism (1) must be an isomorphism; for a field can only have homomorphisms that are either one-to-one or have the null ring as its image. Accordingly the following theorem is valid:

In a zero-dimensional prime ideal all zeros are generic and equivalent to one another.[1]

The coordinates $\xi_1, \ldots, \xi_n$ or $\xi_1', \ldots, \xi_n'$ are in this case algebraic quantities (whose degree of transcendence is actually zero). If we think of all zeros as being contained in a common (say algebraically closed) comprehending field Ω, then by (1) they are algebraically conjugate. The number of these conjugate points

[1] That is, they are mapped on one another by an isomorphism which leaves fixed the elements of the ground field K.

in a suitable field Ω is at most equal (and, if $K(\xi)$ is separable, exactly equal) to the degree of the field $K(\xi)$ over K. Hence

A zero-dimensional irreducible algebraic manifold consists of a finite number of algebraically conjugate points.

In particular if the field K is actually algebraically closed, there is only one zero ξ in the field K itself, and the ideal belonging to it is

$$\mathfrak{p} = (x_1 - \xi_1, \ldots, x_n - \xi_n).$$

THEOREM. *The distinct zeros of an r-dimensional prime ideal have a degree of transcendence* $\leqq r$, *and if the degree of transcendence of a zero is exactly r, the zero is generic.*

PROOF. If ξ' is a zero of degree of transcedence s, the homomorphism (1) is valid. If $\xi'_1, \ldots, \xi'_s$ are algebraically independent, then $\xi_1, \ldots, \xi_s$ are also; for. every algebraic relation between the ξ is also valid between the ξ'. This means that $r \geqq s$. If $r = s$, all ξ depend algebraically on $\xi_1, \ldots, \xi_s$. If a polynomial $f(\xi)$, which is itself not zero, were mapped onto zero by the homomorphism (1), then in the field $K(\xi)$ the element $1/f$ could be written in the following special form:

$$\frac{1}{f(\xi_1, \ldots, \xi_n)} = \frac{g(\xi_1, \ldots, \xi_n)}{h(\xi_1, \ldots, \xi_s)}.$$

It would then follow that

$$h(\xi_1, \ldots, \xi_s) = g(\xi_1, \ldots, \xi_n) f(\xi_1, \ldots, \xi_n).$$

But by the homomorphism (1) f is mapped onto 0. Hence $h(\xi_1, \ldots, \xi_s)$ would also be mapped onto 0, that is,

$$h(\xi'_1, \ldots, \xi'_s) = 0,$$

which contradicts the assumption that the $\xi'_1, \ldots, \xi'_s$ are algebraically independent. Hence by the homomorphism (1) no polynomial distinct from zero is mapped onto zero, that is, if $r = s$, (1) is an isomorphism. This means that ξ' is a generic zero.

Every zero ξ' of $\mathfrak{p}$ is the generic zero of some ideal $\mathfrak{p}'$. If $f \equiv 0(\mathfrak{p})$, then $f(\xi') = 0$ which implies that $f \equiv 0(\mathfrak{p}')$; therefore $\mathfrak{p}'$ is a divisor of $\mathfrak{p}$. Conversely, every prime divisor $\mathfrak{p}'$ of $\mathfrak{p}$ distinct from $\mathfrak{o}$ may be obtained in this manner since every ideal $\mathfrak{p}' \neq \mathfrak{o}$ possesses a generic zero ξ'. From the theorem formulated above it immediately follows:

Every divisor $\mathfrak{p}'$ *of* $\mathfrak{p}$ *has a dimension* $r' \leqq r$; *if* $r' = r$, *then* $\mathfrak{p}' = \mathfrak{p}$.

By the dimension of an arbitrary algebraic manifold we understand the maximum of the dimensions of its irreducible constituents. The pure one-dimensional algebraic manifolds are called *curves*, the pure two-dimensional manifolds are called *surfaces*, the pure $(n-1)$-dimensional manifolds are called *hypersurfaces*. The only n-dimensional manifold in R_n is the whole space R_n, the ideal belonging to it is

the null ideal (since if $\xi_1, \ldots, \xi_n$ are algebraically independent, the relation $f(\xi) = 0$ implies $f = 0$).

EXERCISES. 1. A principal ideal (p), where p is a non-constant polynomial which is not factorable, is a $(n-1)$-dimensional prime ideal.

2. Conversely: every $(n-1)$-dimensional prime ideal is a principal ideal.

3. Every d-dimensional prime ideal $\mathfrak{p}$ $(d > 0)$ possesses (at least) one $(d-1)$-dimensional prime ideal divisor. [If $\xi_{d+1}, \ldots, \xi_n$ are algebraic functions of $\xi_1, \ldots, \xi_d$, a particular zero of $\mathfrak{p}$ is formed by specializing ξ_d according to Section 92 while $\xi_1, \ldots, \xi_{d-1}$ remain unchanged.]

If we go from the affine space R_n to the projective space S_n, then by Section 91 every irreducible manifold $\mathfrak{M}$ of R_n (with $\mathfrak{p}$ the prime ideal belonging to $\mathfrak{M}$) corresponds to an $\mathfrak{M}^*$ in S_n which is just like it (with $\mathfrak{p}^*$ the prime ideal belonging to $\mathfrak{M}^*$). If d is the dimension of $\mathfrak{p}$, then $d+1$ is the dimension of $\mathfrak{p}^*$; for, an indeterminate proportionality factor λ raises the degree of transcendence of the generic zero by one (cf. Section 93, Exer. 4). However the dimension of $\mathfrak{M}^*$ is denoted by the number d (not $d+1$); for, from a geometrical point of view $\mathfrak{M}^*$ coincides with $\mathfrak{M}$ except for the improper points occurring in it. If $\mathfrak{M}$ is a curve, let us say, then the image $\mathfrak{M}^*$, which is generated from $\mathfrak{M}$ by the addition of finitely many points, is also called a curve. Hence by the dimension of a manifold in the projective space we always understand the dimension diminished by 1 of the prime ideal belonging to it.

95. THE PRIMARY IDEALS

The main problem in the ideal theory of polynomial domains may be stated as follows: *to determine whether a polynomial f belongs to a given ideal*

$$\mathfrak{m} = (f_1, \ldots, f_r).$$

In solving this problem we will not be interested in developing a procedure that will lead to a solution after a finite number of operations have been carried out even though this is always possible.[2] Instead we will seek a criterion that will give an insight into the structure of the ideal and bring forth the geometric relations existing between the zeros of the ideal and its elements f. Such a criterion was first given by E. Lasker;[3] it depends on the decomposition of the ideal into primary components.

The basic idea of the method of Lasker is as follows: by the decomposition theorems of Section 87 every ideal $\mathfrak{m}$ may be represented as the intersection of primary ideals:

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s].$$

Hence a polynomial f belongs to the ideal $\mathfrak{m}$ if and only if f belongs to all the

[2] Cf. J. König: *Einleitung in die allgemeine Theorie der algebraischen Grössen* (Leipzig: B. G. Teubner 1903), as well as G. Hermann: "Die Frage der endlich vielen Schritte in der Theorie der Polynomideale." *Math. Ann. Vol.* 95 *pp.* 736-788.

[3] Lasker, E.: "Zur Theorie der Moduln und Ideale." *Math. Ann. Vol.* 60 (1905) *pp.* 20-116.

primary ideals $\mathfrak{q}_\nu$. As a result the above problem will be essentially solved as soon as we determine the conditions which a polynomial must satisfy if it is to belong to a primary ideal.

To every primary ideal $\mathfrak{q}$ there belongs by Section 86 a prime ideal $\mathfrak{p}$ and an "exponent" ϱ with the following properties:

1. $$\mathfrak{p}^\varrho - 0(\mathfrak{q}) \equiv 0(\mathfrak{p}).$$

2. If $$fg \equiv 0(\mathfrak{q}) \text{ and } f \not\equiv 0(\mathfrak{p}), \text{ then } g \equiv 0(\mathfrak{q}).$$

Furthermore, the prime ideal $\mathfrak{p}$, if $\mathfrak{q} \neq \mathfrak{o}$, belongs to an irreducible manifold $\mathfrak{M}$. By 1. all zeros of $\mathfrak{q}$ are also zeros of $\mathfrak{p}$ and conversely. *Hence the manifold of a primary ideal $\mathfrak{q} \neq \mathfrak{o}$ is irreducible and equal to the manifold of the prime ideal belonging to it.*

By the decomposition theorems the manifold of an arbitrary ideal $\mathfrak{m}$ is the union of irreducible manifolds, namely, of the manifolds of its primary components. Hence

Every algebraic manifold may be represented as the union of a finite number of irreducible manifolds.

The irreducible manifolds of the primary components of $\mathfrak{m}$ are determined by the prime ideals belonging to these components. Here the "imbedded" prime ideals (Section 88) may be omitted since their manifolds are contained in the manifolds of the non-imbedded ("isolated") prime ideals.[4]

Let $\mathfrak{q}$ be a primary ideal, $\mathfrak{p}$ the prime ideal belonging to it, ϱ its exponent, and $\mathfrak{M}$ its manifold. If f is a polynomial which contains $\mathfrak{M}$, then $f \equiv 0(\mathfrak{p})$, and so $f^\varrho \equiv 0(\mathfrak{q})$. However, if f does not contain $\mathfrak{M}$, we may omit the factor f from every congruence modulo $\mathfrak{q}$ as a consequence of the above property 2. We have here two very important tools which may frequently be used to determine whether $f^\varrho \equiv 0(\mathfrak{q})$ or $g \equiv 0(\mathfrak{q})$. They may be immediately carried over to arbitrary ideals $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s]$ with the help of the decomposition theorems. Thus, if f is a polynomial which contains the manifold $\mathfrak{M}$ of $\mathfrak{m}$, and ϱ is the largest of the exponents of the primary ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$, then

$$f^\varrho \equiv 0(\mathfrak{q}_i) \qquad (\text{for } i = 1, \ldots, s),$$

hence

$$f^\varrho \equiv 0(\mathfrak{m}).$$

We have thereby obtained another proof of *Hilbert's Nullstellensatz* (Section 79). Actually this proof sharpens the theorem by showing that the exponent ϱ depends only on the ideal $\mathfrak{m}$.

On the other hand, if f is a polynomial which does not contain the manifolds of the primary ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$, we may omit f from every congruence

[4] The use of the word "imbedded" arises from this fact.

$$fg \equiv 0(\mathfrak{m})$$

and conclude that

$$g \equiv 0(\mathfrak{m}),$$

since the corresponding congruences are valid for all primary ideals $\mathfrak{q}_\nu$. The condition under which f may be omitted from every such congruence may be concisely written as

$$\mathfrak{m}:(f) = \mathfrak{m},$$

since by Section 88 this is valid if and only if f is not divisible by the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ belonging to $\mathfrak{m}$ (therefore does not contain their irreducible manifolds).

By Section 88 this result may be generalized to any ideal: an ideal $\mathfrak{a}$ satisfies the relation

$$\mathfrak{m}:\mathfrak{a} = \mathfrak{m} \tag{1}$$

if and only if $\mathfrak{a}$ is not divisible by all $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. in other words. *if the manifold of* $\mathfrak{a}$ *contains none of the manifolds of the prime ideals* $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. This theorem is often useful when seeking the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ belonging to a given ideal $\mathfrak{m}$. Thus, if it is suspected that a prime ideal $\mathfrak{p}$ is a $\mathfrak{p}_\nu$, assume that $\mathfrak{a}$ is an ideal which is divisible by $\mathfrak{p}$, for instance $\mathfrak{a} = \mathfrak{p}$, and determine whether the relation (1) or its negation can be proved; that is, whether $g\mathfrak{a} \equiv 0(\mathfrak{m})$ implies $g \equiv 0(\mathfrak{m})$ or not. If (1) is valid, $\mathfrak{p}$ is not a $\mathfrak{p}_\nu$. By this criterion we will prove in Section 98 that the prime ideals belonging to an ideal with r basis elements have exactly the dimension $n - r$ (and therefore are not imbedded) provided that their dimensions do not exceed $n - r$.

By the *dimension* of a primary ideal we mean the dimension of the prime ideal belonging to it (or the dimension of its zero manifold). By the dimension or *highest dimension* of an arbitrary ideal $\mathfrak{a} \neq 0$ we mean the maximum of the dimensions of the primary components (or of the prime ideals belonging to them). This number also represents the dimension of the manifold of $\mathfrak{a}$.

If the dimensions of the primary ideals belonging to $\mathfrak{a}$ are all equal, say equal to d, the ideal $\mathfrak{a}$ is said to be an *unmixed d-dimensional* ideal.

EXERCISES. 1. The ideal $(x_1^2, x_2x_3 + 1)$ is primary with the exponent 2 and $(x_1, x_2x_3 + 1)$ is the prime ideal belonging to it.

2. Every power $\mathfrak{p}^e$ of an irreducible non-constant polynomial $\mathfrak{p}$ generates an $(n - 1)$-dimensional primary ideal. Every non-constant polynomial f generates an unmixed $(n - 1)$-dimensional ideal.

3. If $\mathfrak{p}$ is the prime ideal of Section 93, Exer. 1, then $\mathfrak{p}^2$ is not primary. [The polynomial $(x_2x_3 - x_1^3)^2 - (x_2^2 - x_1x_3)(x_3^2 - x_1^2x_2)$ has a factor x_1 and the other factor does not belong to $\mathfrak{p}^2$.]

96. THE NOETHERIAN THEOREM

With the help of the primary ideal decomposition we shall first solve completely for zero-dimensional ideals the problem of determining the conditions that a polynomial f must satisfy in order to belong to an ideal $\mathfrak{m}$. We start with a *lemma* which is useful in other respects:

If Σ is an extension field of K and $f, f_1, \ldots, f_r$ are polynomials in $\mathsf{K}[x] = \mathsf{K}[x_1, \ldots, x_n]$, then the congruence

$$f \equiv 0 (f_1, \ldots, f_r) \text{ in } \Sigma[x],$$

implies

$$f \equiv 0 (f_1, \ldots, f_r) \text{ in } \mathsf{K}[x].$$

PROOF. Let

$$f = \sum g_i f_i, \tag{1}$$

where the g_i are polynomials with coefficients in Σ. These coefficients are linearly expressible in terms of a finite number of linearly independent elements $1, \omega_1, \omega_2, \ldots$ of Σ with coefficients in K. Every term $g_i f_i$ in (1) thereby takes on the form

$$(g_{i0} + g_{i1}\omega_1 + g_{i2}\omega_2 + \cdots) f_i,$$

where the g_{ik} are polynomials with coefficients in K. Hence (1) may be written as

$$f = \sum g_{i0} f_i + \omega_1 \sum g_{i1} f_i + \omega_2 \sum g_{i2} f_i + \cdots.$$

But the field elements $1, \omega_1, \omega_2, \ldots$ are linearly independent. Hence the coefficients of $1, \omega_1, \omega_2, \ldots$ in the left and right-hand sides must be respectively equal,

$$f = \sum g_{i0} f_i, \qquad \text{Q.E.D.}$$

By this lemma we may always extend the ground field K in any way when seeking an answer to the question: is $f \equiv 0 (f_1, \ldots, f_r)$. In particular we may extend K by the adjunction of zeros of the ideal $(f_1, \ldots, f_r)$. If the congruence in question is valid in the extended domain $\Sigma[x]$, it is also valid before the extension.

A zero-dimensional algebraic manifold always decomposes in a suitable extension of the ground field into distinct isolated points; therefore, when it is advantageous we may always assume that all zero-dimensional prime ideals that occur have only one point as a zero (instead of a system of conjugate points, which is actually the case).

A zero-dimensional prime ideal $\mathfrak{p}$ is maximal; for the residue class ring $\mathfrak{o}/\mathfrak{p}$ is a field by Section 94. This implies that every zero-dimensional primary ideal is single-primed since by Section 90 a primary ideal which belongs to a maximal prime ideal is always single-primed. Furthermore, by the theorems of Section 90 every zero-dimensional isolated primary component $\mathfrak{q}$ of an ideal $\mathfrak{m}$ may be repre-

sented by

$$\mathfrak{q} = (\mathfrak{m}, \mathfrak{p}^{\varrho}) \tag{2}$$

Here the exponent ϱ is the smallest number σ with the property

$$\mathfrak{p}^{\sigma} \equiv 0(\mathfrak{m}, \mathfrak{p}^{\sigma+1}). \tag{3}$$

We will now determine the significance of the relation (2) in the case that the ground field has been so extended that the single-primed ideals $\mathfrak{q}$ under consideration have only one zero $a = \{a_1, \ldots, a_n\}$. (2) implies that $f \equiv 0(\mathfrak{q})$ if and only if

$$f \equiv 0(\mathfrak{m}, \mathfrak{p}^{\varrho}). \tag{4}$$

Now, if $\mathfrak{m}$ has the basis $(f_1, \ldots, f_r)$ and if we set $y_\nu = x_\nu - a_\nu$, then $\mathfrak{p} = (y_1, \ldots, y_n)$. If we think of all polynomials that occur as arranged in ascending powers of the y_ν, then $\mathfrak{p}^{\varrho}$ consists of all those polynomials which contain only power products of the y_ν of degree $\geqq \varrho$. The relation (4) therefore implies that f coincides with a linear combination $\sum g_\nu f_\nu$ except for terms of degree ϱ and higher degree. If we think of the polynomials $f_1, \ldots, f_r$ as multiplied by 1 and by all power products of the y_ν of degree $< \varrho$, and if we designate the polynomials formed by omitting all terms of degree $\geqq \varrho$ by $h_1, \ldots, h_k$, then (4) implies that f except for terms of degree $\leqq \varrho$ is equal to a linear combination of $h_1, \ldots, h_k$ with constant coefficients. This is a condition whose existence or non-existence can be actually established in any case that may occur (with given $\varrho, f_1, \ldots, f_r$ and f). In particular it is valid if there are formal power series $P_1(y), \ldots, P_r(y)$[5] such that

$$f = P_1 f_1 + \cdots + P_r f_r .^{6} \tag{5}$$

In this case for every value of σ we may omit from the power series those terms of degree σ and substantiate the agreement of both members mod $\mathfrak{p}^{\sigma}$. Strictly speaking the power series criterion demands just as much: the two members of (5) need not be exactly equal but should coincide except for terms of degree $\geqq \varrho$.

Similarly, the validity or non-validity of the relation (3) for every σ may be established: it implies that all power products of degree σ may be represented by the polynomials $\sum g_\nu f_\nu$ by omitting the power products of degree $> \sigma$. We may therefore test one after another the values $\sigma = 1, 2, 3, \ldots$ in the given $f_1, \ldots, f_r$ for every zero a until we have found a σ for which (3) is valid. This σ is then the exponent of $\mathfrak{q}$.

For a zero-dimensional ideal $\mathfrak{m}$ all primary components are zero-dimensional and isolated. Hence we may apply to *all* components the above criterion for $f \equiv 0(\mathfrak{q})$. If it is satisfied for all zeros, then $f \equiv 0(\mathfrak{m})$. Accordingly the following theorem is valid:

[5] Naturally we make no assumption regarding their convergence.

[6] This means that both members of (5) coincide when expanded as power products of the y_ν.

If for every zero $a = \{a_1, \ldots, a_n\}$ *of a zero-dimensional ideal* $\mathfrak{m}$ *we determine the exponent* ϱ *as the smallest natural number* σ *for which* (3) *is valid with* $\mathfrak{p} = (x_1 - a_1, \ldots, x_n - a_n)$, *and if a polynomial* f *satisfies the condition* (4) *for all such* $\mathfrak{p}$, *then* $f \equiv 0(\mathfrak{m})$.

This theorem was first announced [7] by Max Noether for the case $\mathfrak{m} = (f_1, f_2)$, where f_1 and f_2 are polynomials in two variables. It is known as the "*Fundamental Theorem of Noether*" and formed the foundation for the "geometrical trend" in the theory of algebraic functions. Noether actually assumed that the power series condition (5) was satisfied by all zeros instead of the weaker relation (4). The condition given here, whereby we need determine the terms only up to the degree $\varrho - 1$ in $y_1, \ldots, y_n$, originated with Bertini,[8] who at the same time gave a bound for the exponent ϱ.[9] The n-dimensional generalization is due to Lasker and Macaulay. We refer to the fact that $f \equiv 0(\mathfrak{m}, \mathfrak{p}^\varrho)$ is a sufficient condition for $f \equiv 0(\mathfrak{q})$ as the *Noetherian condition at the point a*, a designation due to Macaulay.

In order to illustrate the application of the Noetherian Theorem we will now consider a special case in which the Noetherian conditions are especially simple.

Each of the polynomials $f_1, \ldots, f_r$ determines by itself an algebraic manifold (hypersurface) $f_\nu = 0$ in the n-dimensional space. Similarly, the polynomial f determines a hypersurface $f = 0$. If f is decomposed into irreducible factors: $f = \mathfrak{p}_1^{\varrho_1}\mathfrak{p}_2^{\varrho_2}\ldots$, the manifold $f = 0$ is also decomposed into irreducible parts $\mathfrak{p}_1 = 0, \mathfrak{p}_2 = 0, \ldots$, each of which will be counted as often as the exponent appearing in the factorization of f.

If f is expanded for a point a in powers of $y_\nu = x_\nu - a_\nu$ and if the expansion begins with the terms of s-th order $(s \geqq 0)$:

$$f = c_0 y_1^s + c_1 y_1^{s-1} y_2 + \cdots + c_\omega y_n^s + \cdots,$$

then we say that the hypersurface $f = 0$ *has at a an s-fold point.* The terms of s-th order $c_0 y_1^s + \cdots + c_\omega y_n^s$ generate by themselves, when set equal to zero, a hypersurface, which consists of only "straight lines" through a: the *tangential cone* of the hypersurface $f = 0$ at the point a.

The simplest case to which the Noetherian Theorem may be applied is: among the hypersurfaces $f_1 = 0, \ldots, f_r = 0$ which determine the zero-dimensional ideal $\mathfrak{m}$ there are hypersurfaces $f_1 = 0, \ldots, f_n = 0$ each of which has a simple point at a and whose tangent hyperplanes have only the point a in common:

[7] Noether, M.: "Über einen Satz aus der Theorie der algebraischen Funktionen," *Math. Ann. Vol.* 6 (1873) *pp.* 351-359.

[8] Bertini, E.: "Zum Fundamentalsatz aus der Theorie der algebraischen Funktionen." *Math. Ann. Vol.* 34 (1889) *pp.* 447-449.

[9] Sharper bounds were developed by P. Dubreil: Thèse de Doctorat, Paris 1930. Cf. also H. Kapferer: "Notwendige und hinreichende Multiplizitätsbedingungen zum Noetherschen Fundamentalsatz." *Sitzungsber. der Heidelberger Akad.* 1927, 8. *Abhandlung.*

$$f_1 = c_{11}y_1 + \cdots + c_{1n}y_n + \cdots,$$
$$f_2 = c_{21}y_1 + \cdots + c_{2n}y_n + \cdots,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$f_n = c_{n1}y_1 + \cdots + c_{nn}y_n + \cdots;$$

Linear forms $\sum_{\mu=1}^{n} c_{\lambda\mu}y_\mu$ are linearly independent.

In this case if the prime ideal $(x_1 - a_1, \ldots, x_n - a_n)$ is designated by $\mathfrak{p}$, then $y_1, \ldots, y_n$ actually occurs among the linear combinations of $f_1, \ldots, f_n$ modulo $\mathfrak{p}^2$ (that is, by neglecting the terms of the second and higher degrees). In other words,

$$(y_1, \ldots, y_n) \equiv 0((f_1, \ldots, f_n), \mathfrak{p}^2),$$

and therefore

$$\mathfrak{p} \equiv 0(\mathfrak{m}, \mathfrak{p}^2).$$

Hence the ideal $\mathfrak{m}$ has at the point a an isolated primary component $\mathfrak{q}$ of exponent 1, that is, $\mathfrak{q} = \mathfrak{p}$. Every polynomial with the zero a is therefore divisible by $\mathfrak{q}$. If all zeros a of $\mathfrak{m}$ are such "simple intersection points," then a sufficient condition for $f \equiv 0(\mathfrak{m})$ is that f contain all these zeros.

For further special cases and applications of the Noetherian Theorem see my *Einführung in die algebraische Geometrie* (published in this series 1939).

In the geometrical applications of the Noetherian Theorem it frequently happens that the polynomials f, f_1, f_2 arise from the homogeneous polynomials F, F_1, F_2 by the substitution $x_0 = 1$. We may now ask: under what conditions will

$$f = g_1f_1 + g_2f_2 \tag{6}$$

imply

$$F = G_1F_1 + G_2F_2, \tag{7}$$

where G_1 and G_2 are also forms?

In the investigation of this question we shall assume that for $x_0 = 0$ the forms F_1 and F_2 have no non-constant common divisor (therefore no common zero except for the trivial zero $x_1 = 0, x_2 = 0$). By a linear transformation of the three variables x_0, x_1, x_2 this condition can always be satisfied though extensions of the coefficient field K may be required.

On substituting $x_1 \to \frac{x_1}{x_0}$, $x_2 \to \frac{x_2}{x_0}$ in (6) and multiplying by a suitable power of x_0 an equation of the form

$$x_0^h \cdot F = H_1F_1 + H_2F_2, \tag{8}$$

is obtained, where H_1 and H_2 are forms.

We shall transform this equation so that a factor x_0 may be cancelled. If we set $x_0 = 0$ in the left and right members of (8), then

$$0 = H_{10}F_{10} + H_{20}F_{20}$$

By assumption F_{10} and F_{20} are relatively prime. Hence H_{10} must be divisible by F_{20} and H_{20} by F_{10}:

$$H_{10} = G_0 F_{20},$$
$$H_{20} = -G_0 F_{10}.$$

Since H_1 coincides with H_{10} except for terms in x_0, similarly H_2 with H_{20}, F_1 with F_{10}, and F_2 with F_{20}, then

$$H_1 = G_0 F_2 + x_0 K_1,$$
$$H_2 = -G_0 F_1 + x_0 K_2,$$

where K_1 and K_2 are forms. Substituting in (8), we obtain

$$x_0^h F = x_0 K_1 F_1 + x_0 K_2 F_2.$$

In this relation a factor x_0 may be cancelled. On repeating this process h-times we finally arrive at an equation of the form (7).

Hence:

Equation (7) *is valid if and only if the non-homogeneous polynomials arising from* F, F_1, F_2 *satisfy the Noetherian conditions for all zeros common to the forms* F_1 *and* F_2.

If we think of the quantities x_0, x_1, x_2 as homogeneous coordinates of a variable point of the projective plane, then $F = 0$ is a curve which contains all intersection points of the curves $F_1 = 0$ and $F_2 = 0$ and moreover satisfies fixed "Noetherian conditions" at all these points; this means that equation (5) should be valid. This equation is important above all because it gives rise to the following corollary, the "residue theorem":

If a curve $F_2 = 0$ *of degree* m *is intersected by a curve* $F = 0$ *of degree* $n + p$ *in* $m(n + p)$ *points, each by Section* 83 *counted with its proper multiplicity, and if of these* $m(n + p)$ *points* $m \cdot n$ *points are intersections by a curve* $F_1 = 0$ *of degree n, then the remaining* $m \cdot p$ *points are intersections of a curve* $G_1 = 0$ *of degree* p; *it is assumed that the curve* $F = 0$ *satisfies at every one of the* $m \cdot n$ *points the Noetherian conditions of the ideal* (F_1, F_2).

Thus by (7) it clearly follows that the intersection points of $F = 0$ and $F_2 = 0$ are the same as those of $F_1 \cdot G_1 = 0$ and $F_2 = 0$.

97. REDUCTION OF MULTI-DIMENSIONAL IDEALS TO ZERO-DIMENSIONAL IDEALS

In this section we will seek to extend to multi-dimensional ideals the theorems which were proved in Section 96 for zero-dimensional ideals.

The method is as follows: if $\mathfrak{q}$ is a primary ideal in $\mathsf{K}[x]$ of dimension d, $\mathfrak{p}$ the prime ideal belonging to it, $\{\xi_1, \ldots, \xi_n\}$ its generic zero and (let us say) $\xi_1, \ldots, \xi_d$ are algebraically independent,[10] then the ideals $\mathfrak{q}$ and $\mathfrak{p}$ are transformed into zero-dimensional ideals by the substitution $x_1 = \xi_1, \ldots, x_d = \xi_d$. We carry out this substitution in all polynomials q of the ideal $\mathfrak{q}$; thereby the polynomials q go over into polynomials q' in $\mathsf{K}(\xi_1, \ldots, \xi_d)[x_{d+1}, \ldots, x_n]$ which generate an ideal $\mathfrak{q}'$. Obviously it is sufficient to perform the substitution $x_1 = \xi_1, \ldots, x_d = \xi_d$ in the basis polynomials $q_1, \ldots, q_r$; the corresponding polynomials $q_1', \ldots, q_r'$ generate the ideal $\mathfrak{q}'$:

$$\mathfrak{q}' = (q_1', \ldots, q_r').$$

[10] The $\xi_1, \ldots, \xi_d$ may therefore be considered as indeterminates (we could have designated them by $t_1, \ldots, t_d$); the remaining ξ, as algebraic functions of these indeterminates.

The ideal $\mathfrak{q}'$ consists of the polynomials q' divided by polynomials φ in $\xi_1, \ldots, \xi_d$ distinct from zero; for, the polynomials q' form an ideal in $K[\xi_1, \ldots, \xi_d, x_{d+1}, \ldots, x_n]$ which will generate an ideal in $K(\xi_1, \ldots, \xi_d)[x_{d+1}, \ldots, x_n]$ as soon as we permit the denominators φ.

Just as $\mathfrak{q}'$ is generated from $\mathfrak{q}$ so also is an ideal $\mathfrak{p}'$ generated from $\mathfrak{p}$, and in general to every ideal $\mathfrak{m} = (f_1, \ldots, f_r)$ there is an ideal $\mathfrak{m}' = (f_1', \ldots, f_r')$.

Geometrically the substitution $x_1 = \xi_1, \ldots, x_d = \xi_d$ implies that all manifolds under consideration are cut by the linear space $x_1 = \xi_1, \ldots, x_d = \xi_d$, which passes through the generic point of the manifold of $\mathfrak{q}$.

If $f(x_1, \ldots, x_n)$ is a polynomial and $f(\xi_1, \ldots, \xi_d, x_{d+1}, \ldots, x_n)$ belongs to $\mathfrak{q}'$, then by the above

$$f(\xi, x) = \frac{q'}{\varphi(\xi_1, \ldots, \xi_d)} = \frac{q(\xi, x)}{\varphi(\xi)} \qquad q(x) \equiv 0(\mathfrak{q}),$$

therefore

$$q(\xi, x) = \varphi(\xi) f(\xi, x).$$

As $\xi_1, \ldots, \xi_d$ are algebraically independent,

$$q(x) = \varphi(x) f(x) \equiv 0(\mathfrak{q}).$$

If $\varphi(\xi) \neq 0$, then $\varphi(x) \not\equiv 0(\mathfrak{p})$, and consequently

$$f(x) \equiv 0(\mathfrak{q}).$$

Hence in order to determine whether a polynomial $f(x)$ belongs to $\mathfrak{q}$ we need only to investigate whether the corresponding $f' = f(\xi_1, \ldots, \xi_d, x_{d+1}, \ldots, x_n)$ belongs to $\mathfrak{q}'$. Furthermore, $\mathfrak{q}'$ uniquely determines $\mathfrak{q}$.[11]

We now state: *the ideal* $\mathfrak{q}'$ *in* $K(\xi_1, \ldots, \xi_d)[x_{d+1}, \ldots, x_n]$ *is primary; the prime ideal belonging to it is* $\mathfrak{p}'$; *the exponent of* $\mathfrak{q}'$ *is equal to that of* $\mathfrak{q}$; *the generic zero of* $\mathfrak{p}'$ *is* $\{\xi_{d+1}, \ldots, \xi_n\}$ *and the dimension of* $\mathfrak{p}'$ *is* 0.

PROOF. In order to show that $\mathfrak{q}'$ is primary and that $\mathfrak{p}'$ is the prime ideal belonging to this primary ideal, it is sufficient to prove the following three properties:

1. If $f(\xi, x)\, g(\xi, x) \equiv 0(\mathfrak{q}')$ and $f(\xi, x) \not\equiv 0(\mathfrak{p}')$, then $g(\xi, x) \equiv 0(\mathfrak{q}')$.
2. If $f(\xi, x) \equiv 0(\mathfrak{q}')$, then $f(\xi, x) \equiv 0(\mathfrak{p}')$.
3. If $f(\xi, x) \equiv 0(\mathfrak{p}')$, then $f(\xi, x)^\varrho \equiv 0(\mathfrak{q}')$.

For all three properties we may assume that f and g are rational integral functions of $\xi_1, \ldots, \xi_d$ since in any other case we need only multiply by a suitable $\varphi(\xi)$. Then, by the above remarks, in all these congruences we may replace the ξ by the x, $\mathfrak{q}'$ by $\mathfrak{q}$, $\mathfrak{p}'$ by $\mathfrak{p}$ since for instance $f(\xi, x) \equiv 0(\mathfrak{q}')$ is equivalent to $f(x) \equiv 0(\mathfrak{q})$, etc. After this substitution is performed, 1., 2., 3. simply state that $\mathfrak{q}$ is

---

[11] This is also valid, as the proof shows, for any other primary ideal $\mathfrak{r}$ with the property that $x_1, \ldots, x_d$ are independent modulo the prime ideal $\mathfrak{s}$ belonging to it, i.e., if $\varphi(x_1, \ldots, x_d) \neq 0$, then $\varphi \not\equiv 0(\mathfrak{s})$. If there is on the contrary a $\varphi(x_1, \ldots, x_d) \neq 0$ in $\mathfrak{s}$, then $\varphi(x)^\varrho \equiv 0(\mathfrak{r})$. Hence

$$1 = \varphi(\xi)^{-\varrho} \varphi(\xi)^\varrho \equiv 0(\mathfrak{r}'),$$

consequently $\mathfrak{r}'$ is the unit ideal.

primary and $\mathfrak{p}$ is the prime ideal belonging to it, which we know to be true. These relations also show that the exponents of $\mathfrak{q}'$ and $\mathfrak{q}$ coincide.

In order to show that $\{\xi_{d+1}, \ldots, \xi_n\}$ is the generic zero of $\mathfrak{p}'$, we only have to prove that if

$$f(\xi_1, \ldots, \xi_d, \xi_{d+1}, \ldots, \xi_n) = 0,$$

where f is rational in $\xi_1, \ldots, \xi_d$, rational integral in $\xi_{d+1}, \ldots, \xi_n$, then

$$f(\xi, x) \equiv 0(\mathfrak{p}')$$

and conversely. Now f may be assumed to be rational integral in $\xi_1, \ldots, \xi_d$. Then $f(\xi, x) \equiv 0(\mathfrak{p}')$ is equivalent to $f(x) \equiv 0(\mathfrak{p})$; therefore this part of the theorem is settled by observing that $\{\xi_1, \ldots, \xi_n\}$ is the generic zero of $\mathfrak{p}$.

Finally the zero-dimensionality of $\mathfrak{p}'$ follows from the fact that $\xi_{d+1}, \ldots, \xi_n$ are algebraic over $K(\xi_1, \ldots, \xi_d)$. This completes the proof of the theorem.

In the same manner we may show that *if* $\mathfrak{q}$ *is a primary component of an ideal* $\mathfrak{m} = (f_1, \ldots, f_r)$, *then* $\mathfrak{q}'$ *is also a primary component of the corresponding ideal* $\mathfrak{m}' = (f_1', \ldots, f_r')$.

Thus, let $\mathfrak{m} = [\mathfrak{q}, \mathfrak{q}_2, \ldots, \mathfrak{q}_s]$ be an irredundant representation of $\mathfrak{m}$ by greatest primary components. Then $\mathfrak{m}' = [\mathfrak{q}', \mathfrak{q}_2', \ldots, \mathfrak{q}_s']$; for, the polynomial $f(\xi, x)$ of $\mathfrak{m}'$ or of $[\mathfrak{q}', \mathfrak{q}_2', \ldots]$ may be transformed, if multiplied by a suitable polynomial $\varphi(\xi_1, \ldots, \xi_d) \neq 0$, into an element $g(\xi, x)$ such that $g(x_1, \ldots, x_d, x_{d+1}, \ldots, x_n)$ belongs to $\mathfrak{m}$ or to $\mathfrak{q}$ and $\mathfrak{q}_2, \ldots, \mathfrak{q}_s$ respectively. If $\mathfrak{q}'$ were superfluous in the representation $\mathfrak{m}' = [\mathfrak{q}', \mathfrak{q}_2', \ldots, \mathfrak{q}_s']$, then $[\mathfrak{q}_2', \ldots, \mathfrak{q}_s'] \equiv 0(\mathfrak{q}')$. On setting $\mathfrak{m}_1 = [\mathfrak{q}_2, \ldots, \mathfrak{q}_s]$, it would follow that $\mathfrak{m}_1' = [\mathfrak{q}_2', \ldots, \mathfrak{q}_s'] \equiv 0(\mathfrak{q}')$. If f is an arbitrary element of $\mathfrak{m}_1$, then $f' \equiv 0(\mathfrak{m}_1') \equiv 0(\mathfrak{q}')$, and $f \equiv 0(\mathfrak{q})$. This would imply that $\mathfrak{m}_1 \equiv 0(\mathfrak{q})$; that is, $\mathfrak{q}$ would be superfluous in the representation of $\mathfrak{m}$, contrary to the assumption that the representation of $\mathfrak{m}$ is irredundant. Hence in the representation $\mathfrak{m}' = [\mathfrak{q}', \mathfrak{q}_2', \ldots, \mathfrak{q}_s']$ $\mathfrak{q}'$ cannot be superfluous. On omitting any $\mathfrak{q}_\nu'$ that may be superfluous, an irredundant representation is obtained in which $\mathfrak{q}'$ occurs. Furthermore, if $\mathfrak{p}_\nu$ is the prime ideal belonging to $\mathfrak{q}_\nu$ and $\mathfrak{p}_\nu'$ is the prime ideal belonging to $\mathfrak{q}_\nu'$, then $\mathfrak{p} \neq \mathfrak{p}_\nu$ and therefore, in view of the uniqueness noted earlier (footnote p. 66), $\mathfrak{p}' \neq \mathfrak{p}_\nu'$. In the case $\mathfrak{p}_\nu' = \mathfrak{o}$ we still have $\mathfrak{p}' \neq \mathfrak{p}_\nu'$ even though the uniqueness property is no longer valid. Hence in the representation of $\mathfrak{m}'$ the primary ideal $\mathfrak{q}'$ is the only one belonging to $\mathfrak{p}'$. This means that $\mathfrak{q}'$ is a primary component of $\mathfrak{m}'$.

In a similar manner, it may be easily shown: if $\mathfrak{q}$ is an *isolated* component of $\mathfrak{m}$, then $\mathfrak{q}'$ is *also an isolated component* of $\mathfrak{m}$.

The method developed for reducing a primary ideal to a zero-dimensional one provides us with the tools for determining whether a particular polynomial f belongs to a given ideal $\mathfrak{m} = (f_1, \ldots, f_r)$. If it is assumed, once and for all, that the decomposition of $\mathfrak{m}$ into primary components is given by

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s],$$

the procedure may be described as follows. First, we seek for every primary component $\mathfrak{q}$ the associated zero-dimensional ideal $\mathfrak{q}'$. Next, we extend the ground field to the field $\mathsf{K}(\xi_1, \ldots, \xi_d)$; in this field $\mathfrak{q}'$ decomposes into primary ideals $\mathfrak{q}'_\nu$ each of which has only one zero $a^{(\nu)}$. Finally, by the methods of Section 96 we determine by means of the "Noetherian conditions"

$$f' \equiv 0(\mathfrak{q}', \mathfrak{p}'^{\varrho}_\nu), \qquad \mathfrak{p}'_\nu = (x_{d+1} - a^{(\nu)}_{d+1}, \ldots, x_n - a^{(\nu)}_n), \tag{1}$$

whether the polynomial f' belongs to the ideals $\mathfrak{q}'_\nu = (\mathfrak{q}', \mathfrak{p}'^{\varrho}_\nu)$ and thus to the ideal $\mathfrak{q}'$. Since the zeros of the $\mathfrak{p}'_\nu$ are conjugate relative to $\mathsf{K}(\xi_1, \ldots, \xi_d)$, the $\mathfrak{p}'_\nu$ as well as the $\mathfrak{q}'_\nu$ are conjugate relative to $\mathsf{K}(\xi_1, \ldots, \xi_d)$; hence for every $\mathfrak{q}'$ it is sufficient to investigate *one* $\mathfrak{q}'_\nu$. This means that we have to adjoin only one zero belonging to each $\mathfrak{q}'$. Let $\{\xi_{d+1}, \ldots, \xi_n\}$ be such a zero. Then $\mathfrak{p}'_\nu$ is replaced by the prime ideal

$$\mathfrak{p}_\xi = (x_{d+1} - \xi_{d+1}, \ldots, x_n - \xi_n);$$

and condition (1) may be stated more appropriately as

$$f' \equiv 0(\mathfrak{m}', \mathfrak{p}^{\varrho}_\xi), \tag{2}$$

since (2) is also necessary for $f \equiv 0(\mathfrak{m})$ and (1) immediately follows from (2). The condition (2), which must be satisfied by every primary component $\mathfrak{q}$ of $\mathfrak{m}$, is known as the *criterion of* Hentzelt or *Hentzelt's Nullstellensatz.*

If $\mathfrak{q}$ is an isolated component of $\mathfrak{m}$, so that $\mathfrak{q}'$ is an isolated component of $\mathfrak{m}'$, we may determine, as in Section 90, the exponent ϱ by the condition

$$\mathfrak{p}^{\varrho}_\xi \equiv 0(\mathfrak{m}', \mathfrak{p}^{\varrho+1}_\xi).$$

The conditions (1) for $f \equiv 0(\mathfrak{q})$ enable us to clarify the geometrical significance of the primary ideals: to belong to a primary ideal imposes certain conditions on the leading coefficients in the expansion of the polynomial f in powers of $x_1 - \xi_1, \ldots, x_n - \xi_n$, where ξ is a generic point of an irreducible manifold $\mathfrak{M}$. For instance, the conditions could be that f should vanish at this generic point, or that the hypersurface $f = 0$ should rest at this generic point on another hypersurface containing $\mathfrak{M}$, etc.

EXERCISES. 1. Using the method developed for reducing an ideal to a zero-dimensional one, prove that every $(n-1)$-dimensional primary ideal in $\mathsf{K}[x_1, \ldots, x_n]$ is a principal ideal.

2. Every unmixed $(n-1)$-dimensional ideal in $\mathsf{K}[x_1, \ldots, x_n]$ is a principal ideal and conversely.

98. UNMIXED IDEALS

An unmixed ideal has been defined as an ideal whose primary components have the same dimension d. Hence the primary components of an unmixed ideal must be isolated; their manifolds and generic points are readily obtained by means of the elimination theory (Section 78), and the criterions for $f \equiv 0(\mathfrak{m})$ take on the simple form derived in the previous section. Hence

it is very important to be able to establish from the beginning that a particular ideal is unmixed. We will first set up a criterion by which we can determine whether an ideal possesses zero-dimensional components.

If $\mathfrak{m} = (f_1, \ldots, f_r)$ is an ideal in $\mathfrak{o} = K[x]$ and $\mathfrak{M}$ is the ideal generated by $\mathfrak{m}$ (with the same basis) in $\mathfrak{O} = \Omega[x]$, where Ω is a suitable (algebraically closed would be most suitable) algebraic extension field of K, then by the lemma of Section 96 the intersection $\mathfrak{M} \cap \mathfrak{o}$ is equal to $\mathfrak{m}$. If $\mathfrak{M}$ is decomposed into primary components:

$$\mathfrak{M} = [\mathfrak{Q}_1, \mathfrak{Q}_2, \quad , \mathfrak{Q}_s], \tag{1}$$

then

$$\mathfrak{m} = \mathfrak{M} \cap \mathfrak{o} = [\mathfrak{Q}_1, \mathfrak{Q}_2, \quad \ldots, \mathfrak{Q}_s, \mathfrak{o}]$$

$$= [\mathfrak{Q}_1 \cap \mathfrak{o}, \mathfrak{Q}_2 \cap \mathfrak{o}, \quad ., \mathfrak{Q}_s \cap \mathfrak{o}]^{12} \tag{2}$$

We now have:

If $\mathfrak{Q}$ is primary and $\mathfrak{P}$ the prime ideal belonging to it, then $\mathfrak{Q} \cap \mathfrak{o}$ is primary in the ring $\mathfrak{o}$ and $\mathfrak{P} \cap \mathfrak{o}$ is its prime ideal.[13]

The proof is based on the three well-known criterions:

1. If $fg \equiv 0(\mathfrak{Q} \cap \mathfrak{o})$, $f \not\equiv 0(\mathfrak{P} \cap \mathfrak{o})$, then $g \equiv 0(\mathfrak{Q} \cap \mathfrak{o})$;
2. If $f \equiv 0(\mathfrak{Q} \cap \mathfrak{o})$, then $f \equiv 0(\mathfrak{P} \cap \mathfrak{o})$;
3. If $f \equiv 0(\mathfrak{P} \cap \mathfrak{o})$, then $f^{\varrho} \equiv 0(\mathfrak{Q} \cap \mathfrak{o})$,

for f and g in $\mathfrak{o}$.

Furthermore: *if ξ is the generic zero of $\mathfrak{P}$ (in an extension field of Ω), then ξ is also the generic zero of $\mathfrak{P} \cap \mathfrak{o}$.* For, if $\mathfrak{P}$ consists of all polynomials of $\mathfrak{O}$ with the zero ξ , $\mathfrak{P} \cap \mathfrak{o}$ consists of all polynomials of $\mathfrak{o}$ with the zero ξ.

COROLLARY. The dimension of $\mathfrak{P}$ is equal to that of $\mathfrak{P} \cap \mathfrak{o}$.

Hence if $\mathfrak{M}$ is the intersection (1) of primary ideals of prescribed dimensions, then $\mathfrak{m}$ is the intersection (2) of primary ideals of the same dimensions. In particular: if $\mathfrak{M}$ has no zero-dimensional components, then $\mathfrak{m}$ has none, and if $\mathfrak{M}$ is unmixed, so also is $\mathfrak{m}$. (The converse is also valid though it is not as easy to prove and is of no importance for us.)

The decision as to whether $\mathfrak{M}$ possesses a k-dimensional component may be reduced by the method of Section 97 to a decision regarding zero-dimensional components. By a suitable choice of the field Ω the zero-dimensional components of $\mathfrak{M}$ have only the one zero a; the prime ideal belonging to it is $\mathfrak{p} = (x_1 - a_1, \quad ., x_n - a_n)$, and the decision as to whether there is a primary component belonging to $\mathfrak{p}$ depends on whether

$$\mathfrak{M}\,\mathfrak{p} = \mathfrak{M}$$

is valid, that is, whether

$$f\mathfrak{p} \equiv 0(\mathfrak{M})$$

implies

$$f \equiv 0(\mathfrak{M}).$$

If l is an arbitrary linear combination of $x_1 - a_1, \ldots, x_n - a_n$, then $f\mathfrak{p} \subseteq \mathfrak{M}$ implies $fl \equiv 0(\mathfrak{M})$. Hence, if we can prove (for a suitably chosen l) that $fl \equiv 0(\mathfrak{M})$ implies $f \equiv 0(\mathfrak{M})$, then the ideal $\mathfrak{M}$ as well as $\mathfrak{m}$ itself possesses no zero-dimensional primary components with the zero a. The method of proof is the same as that used in Section 96 (small type) in order to show that $x_0^h F = H_1F_1 + H_2F_2$ implies $F = G_1F_1 + G_2F_2$. The general theorem that may be obtained by this method of proof is as follows:

[12] The ideals $\mathfrak{Q}_\nu \cap \mathfrak{o}$ need not be distinct. Thus, two (relative to K) conjugate $\mathfrak{Q}_\nu$ have the same intersection with $\mathfrak{o}$.

[13] In order to avoid misunderstandings, I will prove that the converse is not valid: that is, if $\mathfrak{Q} \cap \mathfrak{o}$ is primary, $\mathfrak{Q}$ need not be. In fact there are examples (cf. Section 91) of prime ideals $\mathfrak{m}$ in $\mathfrak{o}$ which by extension of the ground field K to Ω decompose into distinct primary components.

If the ideal $(f_1, \ldots, f_r)$ is distinct from 0, has r basis elements, and dimension $d \leqq n - r$, then it is an unmixed $(n - r)$-dimensional ideal.

For $r = 1$ this theorem is known by Section 95 (Exercise 2). Hence we proceed by complete induction on r and assume in the case of $r - 1$ basis polynomials that the theorem is valid for every number of variables n.

We have to show that the ideal $(f_1, \ldots, f_r)$ for $k < n - r$ has no k-dimensional primary components. Let us suppose that q were such a component. By the method of Section 97 we can reduce the dimension of q to zero; this reduces the number of variables n and the highest dimension d of $(f_1, \ldots, f_r)$ by exactly k without affecting the assumption $d \leqq n - r$. Hence it only remains to prove that such an ideal $(f_1, \ldots, f_r)$, if $n - r > 0$, has no zero-dimensional primary components. In view of the earlier remarks it may be assumed that each of the zero-dimensional primary components in question possesses only one zero a in the (possibly extended) ground field.

We show first that by the assumption $d \leqq n - r$ the basis polynomials $f_1, \ldots, f_r$ may be so chosen that every one of the ideals $(f_1, \ldots, f_i)$ has at most the dimension $n - i$. For $i = 1$ and $f_1 \neq 0$ this condition is obviously satisfied. Let us assume that we have already shown that $(f_1, \ldots, f_{i-1})$ has a dimension $\leqq n - i + 1$. In every one of the irreducible $(n - i + 1)$-dimensional manifolds of the ideal $(f_1, \ldots, f_{i-1})$ (in case there are any) we choose a point which does not belong to the manifold of $(f_1, \ldots, f_r)$. At each of these points at least one of the polynomials $f_i, f_{i+1}, \ldots, f_r$ does not vanish. Hence a linear combination $f_i^* = f_i + \mu_{i+1} f_{i+1} + \ldots + \mu_r f_r$ can be formed which will vanish at no one of these points. We choose this linear combination as the i-th basis element instead of f_i, then the ideal $(f_1, \ldots, f_{i-1}, f_i^*)$ has at most the dimension $n - i$, while the ideal $(f_1, \ldots, f_r)$ remains unchanged by the substitution.

For the actual proof that $(f_1, \ldots, f_r)$ does not possess a zero-dimensional component at a, we choose a linear polynomial

$$l = (x_1 - a_1) + c_2(x_2 - a_2) + \ldots + c_n(x_n - a_n),$$

where the c are determined so that l assumes the value zero at none of the generic zeros of the $(n - r)$-dimensional prime ideals belonging to $(f_1, \ldots, f_r)$ and of the $(n - r + 1)$-dimensional prime ideals belonging to $(f_1, \ldots, f_{r-1})$. To complete the proof we have only to show that

$$lf \equiv 0 (f_1, \ldots, f_r)$$

implies

$$f \equiv 0 (f_1, \ldots, f_r).$$

By the substitution

$$x_1 = a_1 - \sum_{\nu=2}^{n} c_\nu (x_\nu - a_\nu)$$

l goes into 0 and every polynomial f into a polynomial $f_0 \equiv f \pmod{l}$. By assumption

$$lf = g_1 f_1 + \ldots + g_r f_r; \tag{3}$$

on applying the substitution, (3) becomes

$$0 = g_{10} f_{10} + \ldots + g_{r0} f_{r0}. \tag{4}$$

The ideal $(f_{10}, \ldots, f_{r-1,0})$ in $K[x_2, \ldots, x_n]$ is at most $(n - r)$-dimensional because of the choice of l. Hence by the induction hypothesis it is an unmixed $(n - r)$-dimensional ideal, and f_{r0} contains no $(n - r)$-dimensional manifold of this ideal. Therefore (4) implies that

$$g_{r0} \equiv 0 \ (f_{10}, \ldots, f_{r-1,0})$$

which means

$$g_r \equiv h_r l \ (f_1, \ldots, f_{r-1}).$$

Substituting in (3), this gives

$$lf \equiv h_r l f_r \ (f_1, \ldots, f_{r-1}),$$

$$l(f - h_r f_r) \equiv 0 \quad (f_1, \ldots, f_{r-1}).$$

Since the ideal $(f_1, \ldots, f_{r-1})$ is unmixed and l is distinct from zero at the generic zeros of the primary ideals belonging to this ideal, we have

$$f - h_r f_r \equiv 0 \quad (f_1, \ldots, f_{r-1}),$$

$$f \equiv 0 \quad (f_1, \ldots, f_r).$$

This completes the proof.

EXERCISES. 1. If f_1 and f_2 have no non-constant common divisor and $(f_1, f_2) \neq 0$, then the ideal (f_1, f_2) is an unmixed $(n-2)$-dimensional ideal.

2. Under the assumptions of Exercise 1 if the "tangential spaces" of the hypersurfaces $f_1 = 0$ and $f_2 = 0$ (for definitions, cf. Section 96) are distinct at the generic points of the irreducible constituents of the manifold of the ideal (f_1, f_2), then $f \equiv 0 (f_1, f_2)$ if and only if f contains this manifold.

3. What conditions must be satisfied by a polynomial f in order that it should belong to the ideal

$$(x_1^2 + x_2^2 - x_3^2,\ x_1 + x_4,\ x_2 + x_4).$$

For further theorems regarding unmixed ideals see the tract of F. S. Macaulay: *Algebraic Theory of Modular Systems.* Cambridge Tracts in Mathematics 19, Cambridge 1916.

CHAPTER XIV

INTEGRAL ALGEBRAIC QUANTITIES

The development of the theory of ideals has historically two starting points: the theory of integral algebraic numbers and the theory of polynomial ideals. These two theories have been developed to solve entirely different problems. In the theory of polynomial ideals the central problems have been to determine the zeros of an ideal and to establish the necessary and sufficient conditions that a polynomial belong to an ideal; while in the theory of integral algebraic numbers it is the problem of factorization. The following remarks will illustrate how this latter problem arises.

In the ring of the numbers $a + b\sqrt{-5}$, where a and b are rational integral numbers, the unique factorization theorem is not valid. For instance, the number 9 has two substantially different factorizations into indecomposable [1] factors:

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).^{2}$$

This fact led Dedekind (following the lead of Kummer who reinstated unique factorization in cyclotomic fields by the introduction of certain "ideal numbers") to extend the domain of the elements to that of the ideals (he was the first to use this nomenclature). He could then show that in this domain every ideal is uniquely expressible as the product of prime ideals. In the above case, if we introduce the prime ideals

$$\mathfrak{p}_1 = (3, 2 + \sqrt{-5}), \quad \mathfrak{p}_2 = (3, 2 - \sqrt{-5}),$$

[1] The statement that the numbers 3 and $2 \pm \sqrt{-5}$ are indecomposable follows readily from the fact that their norm (cf. Section 41) is 9. If they were factorable, either both factors must have the norm ± 3 or one factor has the norm ± 1. A number $a + b\sqrt{-5}$ cannot have ± 3 as a norm since

$$a^2 + 5b^2 = \pm 3$$

is impossible for integers a and b. A number with the norm ± 1 is one of the units ± 1 since

$$a^2 + 5b^2 = \pm 1$$

is satisfied only if $a = \pm 1, b = 0$.

[2] We have already seen (Section 19, Exer. 5) that in the ring of numbers $a + b\sqrt{-3}$ the number 4 has two different factorizations, but that the factorization becomes unique if the number

$$\varrho = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-3}$$

is adjoined to the ring (cf. Section 18, Exer. 5). However, for the ring $C[\sqrt{-5}]$ it will be shown that such a finite extension inside its quotient field is impossible.

we may easily show that

$$(3) = \mathfrak{p}_1\mathfrak{p}_2; \qquad (2+\sqrt{-5}) = \mathfrak{p}_1^2; \qquad (2-\sqrt{-5}) = \mathfrak{p}_2^2,$$

Hence the principal ideal (9) has the (unique) factorization:

$$(9) = \mathfrak{p}_1^2\mathfrak{p}_2^2.$$

In this chapter the "classical" (Dedekind) theory of ideals of the integral quantities of a field will be developed in the modern axiomatic form due to E. Noether.[3] The representation does not assume the general theory of ideals developed in the twelfth chapter, though we shall refer to the mutual relations.

99. FINITE $\mathfrak{R}$-MODULES

We consider modules relative to a (not necessarily commutative) ring $\mathfrak{R}$, that is, modules with $\mathfrak{R}$ as a (left-)multiplicative domain. Usually the modules under consideration are either contained in $\mathfrak{R}$ itself (therefore left ideals in $\mathfrak{R}$) or in an extension ring $\mathfrak{S}$.

By a *finite* $\mathfrak{R}$*-module* we mean a module $\mathfrak{M}$ which is generated by a finite *module basis* $(a_1, \ldots, a_h)$, i.e., all its elements may be expressed linearly by $a_1, \ldots, a_h$ with coefficients in $\mathfrak{R}$ and coefficients that are integers:

$$(1) \qquad m = r_1a_1 + \cdots + r_ha_h + n_1a_1 + \cdots + n_ha_h$$

$$(r_\nu \in \mathfrak{R},\ n_\nu \text{ integers}).$$

(If $\mathfrak{R}$ has an identity which is also an identity operator the terms $n_1a_1, \ldots, n_ha_h$ are naturally superfluous.) In this case we write $\mathfrak{M} = (a_1, \ldots, a_h)$.

We say that the *divisor chain condition* is valid in a module $\mathfrak{M}$ if every chain of submodules $\mathfrak{M}_1, \mathfrak{M}_2, \ldots$ of $\mathfrak{M}$ for which every consequent properly contains (divides) the preceding:

$$\mathfrak{M}_1 \subset \mathfrak{M}_2 \subset \cdots,$$

breaks off after a finite number of steps.

THEOREM. *If the divisor chain condition is valid in* $\mathfrak{M}$, *then every submodule of* $\mathfrak{M}$ *has a finite basis, and conversely.*

This theorem is a generalization of the theorems of Section 84 concerning the basis of an ideal and the divisor chain condition and is proved in the same way. Since we do not assume that Chapter 12 is known, we shall sketch the proof.

In order to find a basis for a submodule $\mathfrak{N}$, we first seek in $\mathfrak{N}$ an element a_1; if $(a_1) = \mathfrak{N}$, we are through. Otherwise, we choose in $\mathfrak{N}$ an element a_2 which is not contained in (a_1); if $(a_1, a_2) = \mathfrak{N}$, we are through. Otherwise, we choose an element a_3, etc. If we now assume that the chain of modules

[3] Noether, E.: "Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern." *Math. Ann. Vol.* 96 (1926) *pp.* 26-61.

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots$$

breaks off after a finite number of terms, $\mathfrak{N}$ has a finite basis.

Conversely, if every submodule of $\mathfrak{M}$ has a finite basis and

$$\mathfrak{M}_1 \subset \mathfrak{M}_2 \subset \cdots$$

is a chain of submodules of $\mathfrak{M}$, the set-union $\mathfrak{B}$ of all $\mathfrak{M}_\nu$ is again a submodule and so must have a finite basis:

$$\mathfrak{B} = (a_1, \ldots, a_r).$$

However, all a_ν are already contained in an $\mathfrak{M}_\omega$ of the chain. Hence $\mathfrak{B} \subseteq \mathfrak{M}_\omega$ and so $\mathfrak{B} = \mathfrak{M}_\omega$, i.e., the chain breaks off with $\mathfrak{M}_\omega$.

A sufficient condition for the divisor chain condition to be valid in $\mathfrak{M}$ is given by the following theorem:

If the divisor chain condition is valid for the left ideals in $\mathfrak{R}$ and $\mathfrak{M}$ is a finite $\mathfrak{R}$-module, then the divisor chain condition is valid for $\mathfrak{R}$-modules in $\mathfrak{M}$.

This is equivalent to (by the previous theorem):

If every left ideal in $\mathfrak{R}$ has a finite ideal basis and $\mathfrak{M}$ has a finite $\mathfrak{R}$-module basis, then every submodule of $\mathfrak{M}$ also has a finite $\mathfrak{R}$-module basis.

The proof is entirely analogous to the proof of Hilbert's Basis Theorem (Section 84). Let $\mathfrak{M} = (a_1, \ldots, a_h)$ and let $\mathfrak{N}$ be a submodule of $\mathfrak{M}$. Every element of $\mathfrak{N}$ may be written in the form (1). In the expression (1) if the last $2h - l$ of the $2h$ coefficients $r_1, \ldots, n_h$ (in other words, the $(l+1)$-st to the $(2h)$-th coefficients inclusive) are zero, we say that the *expression has length* $\leqq l$. We now consider all expressions of length $\leqq l$ occurring in $\mathfrak{N}$. It follows immediately that their l-th coefficients (r_l or n_{l-h}) form a left ideal in $\mathfrak{R}$ or in the ring C of integers. This ideal has a finite basis

$$(b_{l1}, \ldots, b_{ls_l}).$$

Every $b_{l\nu}$ is the last (l-th) coefficient (r_l or n_{l-h}) of an expression (1) which we denote by $B_{l\nu}$:

$$B_{l\nu} = r_1 a_1 + \cdots + b_{l\nu} a_l \quad \text{or} \quad = r_1 a_1 + \cdots + b_{l\nu} n_{l-h}.$$

We state that the totality of the $B_{l\nu} (l = 1, \ldots, 2h;\ \nu = 1, \ldots, s_l)$ forms a basis for $\mathfrak{N}$. Thus, every element (1) of $\mathfrak{N}$ of length l may be transformed into an element without its last (l-th) coefficient by subtracting a linear combination of the $B_{l1}, \ldots, B_{ls_l}$ (with coefficients in $\mathfrak{R}$ or C depending on the value of l). Thereby the element is reduced to an element of smaller length. In the same manner the latter elements may be further reduced in length until by successive subtractions of linear combinations of the $B_{\lambda\nu}$ we are left with zero. Hence every element of $\mathfrak{N}$ may be written as a linear combination of the $B_{l\nu}$. Q.E.D. If one of the ideals $(b_{l1}, \ldots, b_{ls_l})$ should be the null ideal, the corresponding $B_{l\nu}$ would be entirely superfluous in the basis.

REMARKS. If $\mathfrak{R}$ has an identity which is also a unity operator the terms $n_1 a_1, \ldots, n_h a_h$ in (1) may be omitted and the proof correspondingly simplified.

In particular if $\mathfrak{R}$ is a principal ideal ring, every ideal in $\mathfrak{R}$ has a basis consisting of only one element. This means that for every l there is only one b_l and so only one B_l. In this case therefore there is a basis $(B_1, \ldots, B_h)$ consisting of just as many basis elements as are contained in the original basis of $\mathfrak{M}$. If $(a_1, \ldots, a_h)$ is a linearly independent basis of $\mathfrak{M}$, we can easily show that $(B_1, \ldots, B_h)$, where the B_l for which $b_l = 0$ are omitted, is also a linearly independent basis (cf. Section 108).

100. INTEGRAL QUANTITIES WITH RESPECT TO A RING

Let $\mathfrak{R}$ be a subring of a ring $\mathfrak{T}$.

An element t of $\mathfrak{T}$ is said to be *integral with respect to* $\mathfrak{R}$ if all powers [4] of t belong to a finite $\mathfrak{R}$-module $(a_1, \ldots, a_m)$, i.e., if all powers of t may be expressed linearly by a finite number of elements $a_1, \ldots, a_m$ of $\mathfrak{T}$ in the form

$$t^\varrho = r_1 a_1 + \cdots + r_m a_m + n_1 a_1 + \cdots + n_m a_m \tag{1}$$

$$(r_\nu \in \mathfrak{R},\ n_\nu \text{ integers}).$$

In particular every element r of $\mathfrak{R}$ is integral with respect to $\mathfrak{R}$, since $r, r^2, r^3, \ldots$ belong to the $\mathfrak{R}$-module (r). Also the identity of $\mathfrak{T}$, when there is one, is always integral with respect to $\mathfrak{R}$.

If $\mathfrak{T}$ is a field, it contains the quotient field P of $\mathfrak{R}$. Then all powers of an integral quantity t depend linearly on a finite number of elements $a_1, \ldots, a_m$ with coefficients in P; for, P not only contains the ring $\mathfrak{R}$ but also the identity. Hence there are only a finite number of powers of t that are linearly independent with respect to P; in other words, t is algebraic over P. Consequently, instead of "integral quantity" we may say *integral algebraic quantity*. However an algebraic quantity is not necessarily an integral algebraic quantity; for example, the number $\frac{1}{2}$ or $\sqrt{\frac{1}{2}}$ is algebraic over the field of rational numbers but is not integral with respect to the ring of integers.

Let $\mathfrak{R}$ be a ring in which the divisor chain condition is valid for left ideals. Then by Section 99 the divisor chain condition is also valid for the submodules of the finite $\mathfrak{R}$-module $(a_1, \ldots, a_m)$. Hence the chain of modules

$$(t) \subseteq (t, t^2) \subseteq \cdots$$

must contain modules that are not distinct, i.e., there is a power of t which may be expressed linearly by lower powers:

$$t^h = r_1 t + \cdots + r_{h-1} t^{h-1} + n_1 t + \cdots + n_{h-1} t^{h-1} \tag{2}$$

[4] In this section a power is always understood to have a positive exponent.

Conversely, let t be an element of $\mathfrak{T}$ which for a suitable h has a representation such as (2) with coefficients in $\mathfrak{R}$ or C. Then all higher powers of t may be expressed linearly, by successive applications of (2), in terms of the finite number of powers $t, t^2, \ldots, t^{h-1}$. Hence t is integral according to our definition. We have thus proved:

If the divisor chain condition is valid in $\mathfrak{R}$ for left ideals, then the existence of an equation such as (2) is necessary and sufficient in order that t be integral with respect to $\mathfrak{R}$.

Equation (2), when $\mathfrak{T}$ is a field, gives a new meaning to the algebraicness of t. If $\mathfrak{R}$ has an identity, we may augment the powers of t by $t^0 = 1$ and thereby omit the tail end $n_1 t + \cdots + n_{h-1} t^{h-1}$ of (2). Hence instead of (2) we obtain the simpler equation

$$t^h - r_{h-1} t^{h-1} - \cdots - r_0 = 0$$

which has the characteristic property that the coefficient of the highest power of t is one.

EXAMPLES. *Integral algebraic numbers* are those algebraic numbers which are integral with respect to the ring C of the ordinary integers. Hence an integral algebraic number satisfies an equation with coefficients that are integers and leading coefficient 1. *Integral algebraic functions* of $x_1, \ldots, x_n$ are those functions in an algebraic extension field of $\mathsf{K}(x_1, \ldots, x_n)$ which are integral with respect to the polynomial domain $\mathsf{K}[x_1, \ldots, x_n]$; K is here a fixed ground field. *Absolutely integral algebraic functions* of $x_1, \ldots, x_n$ are functions which are integral with respect to the polynomial domain $C[x_1, \ldots, x_n]$ with integer coefficients.

In a commutative ring $\mathfrak{T}$ the sum, difference, and product of two quantities integral with respect to $\mathfrak{R}$ are again integral. In other words, *the quantities in $\mathfrak{T}$ integral with respect to $\mathfrak{R}$ form a ring $\mathfrak{S}$.*

PROOF. If all powers of s are linearly expressible in terms of $a_1, \ldots, a_m$ and all powers of t by $b_1, \ldots, b_n$, then all powers of $s + t$, $s - t$ or $s \cdot t$ are linearly expressible in terms of $a_1, \ldots, a_m, b_1, \ldots, b_n, a_1 b_1, a_1 b_2, \ldots, a_m b_n$.

Let us now assume that the divisor chain condition is valid for the ideals of the ring $\mathfrak{S}$. Then we can prove the *Theorem of the Transitivity of Integralness:*

If $\mathfrak{S}$ is the ring of integral quantities in the commutative ring $\mathfrak{T}$ (with respect to the subring $\mathfrak{R}$) and the element t of $\mathfrak{T}$ is integral with respect to $\mathfrak{S}$, then t is also integral with respect to $\mathfrak{R}$ (i.e., belongs to $\mathfrak{S}$). In other words, *if t satisfies an equation such as (2) whose coefficients r_ν are integral with respect to $\mathfrak{R}$, then t is itself integral with respect to $\mathfrak{R}$.*

PROOF. By the repeated application of equation (2) all powers $t^{h+\lambda}$ may be expressed linearly in terms of $t, t^2, \ldots, t^{h-1}$ with coefficients which are either integers or integral rational functions in the power products of the r_ν. For every r_ν there exists a finite number of quantities in $\mathfrak{T}$ such that all the powers of r_ν

are linearly expressible in terms of these quantities with coefficients that are either in $\mathfrak{R}$ or integers. Hence all power products of the r_ν are linearly expressible in terms of a finite number of products of these finitely many quantities. Let each of these products be multiplied by $t, t^2, \ldots, t^{h-1}$. Then these products together with $t, t^2, \ldots, t^{h-1}$ are finite in number and all powers of t may be expressed linearly in terms of these products with coefficients that are either in $\mathfrak{R}$ or integers.

A ring $\mathfrak{S}$ is said to be *integrally closed in an extension ring* $\mathfrak{T}$ *if every* quantity of $\mathfrak{T}$ which is integral with respect to $\mathfrak{S}$ belongs to $\mathfrak{S}$. In particular, a domain of integrity $\mathfrak{S}$ which is integrally closed in its quotient field Σ is simply described as *integrally closed.* This means, as may be easily seen, that an element t of Σ belongs to $\mathfrak{S}$ if and only if all powers t^ϱ may be represented by fractions with a fixed denominator from $\mathfrak{S}$. Thus, all powers of an integral element t are linearly expressible in terms of a finite number of elements of Σ which may always be brought to a common denominator. Conversely, if all powers of t are representable as fractions with denominator s, they are all linearly expressible in terms of the one element s^{-1}.

By the above theorem it now follows, if $\mathfrak{T}$ is assumed to be commutative, that *the ring* $\mathfrak{S}$ *of all quantities of* $\mathfrak{T}$ *integral with respect to* $\mathfrak{R}$ *is always integrally closed in* $\mathfrak{T}$,[5] *as soon as the divisor chain condition is valid for the ideals of* $\mathfrak{S}$.

A sufficient, but in no way a necessary criterion, for the integral closure of a domain of integrity is given by the following theorem:

A domain of integrity with an identity, in which the unique factorization theorem is valid, is integrally closed in its quotient field.

PROOF. Every element of the quotient field may be represented as a fraction a/b such that a and b have no prime factor in common. If all powers of a/b are transformed, when multiplied by a single quantity c into quantities without denominators, then ca^n and therefore c must be divisible by b^n for every n. But this is possible only if b is a unit. Hence $a/b = ab^{-1}$ belongs to the domain of integrity.

By this theorem the following domains of integrity are integrally closed: all principal ideal rings (in particular the ring C of integers), every polynomial domain with integer coefficients, and every polynomial domain over a commutative field K.

---

[5] This theorem may also be proved without the assumption of the divisor chain condition if we assume instead that $\mathfrak{R}$ is integrally closed in its quotient field P and $\mathfrak{T}$ is a finite extension field of P. For the proof $\mathfrak{T}$ will be extended to a Galois field $\mathfrak{T}'$ over P and $\mathfrak{S}$ to the ring $\mathfrak{S}'$ of integral quantities of $\mathfrak{T}'$. If an element t is integral with respect to $\mathfrak{S}$, and hence with respect to $\mathfrak{S}'$, so also are the quantities conjugate to t (relative to P) and the elementary symmetric functions of these conjugate quantities, that is, the coefficients of the defining equation of t. By the integral closure of $\mathfrak{R}$ these coefficients belong to $\mathfrak{R}$. Hence t is integral with respect to $\mathfrak{R}$ and so $t \in \mathfrak{S}$.

EXERCISES. 1. The roots of unity of a field are always integral with respect to every subring.

2. Which numbers of the Gaussian number field $\Gamma(i)$ are integral with respect to C? Which numbers of the field $\Gamma(\varrho)$, where $\varrho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$ is a cube root of unity?

3. If the domain of integrity $\mathfrak{R}$ is integrally closed, the polynomial domain $\mathfrak{R}[x]$ is also integrally closed.

101. THE INTEGRAL QUANTITIES OF A FIELD

Let $\mathfrak{R}$ be a domain of integrity, P its quotient field, Σ a commutative finite extension field of P, and $\mathfrak{S}$ the ring of the quantities of Σ integral with respect to $\mathfrak{R}$. Evidently $\mathfrak{S}$ is an extension ring of $\mathfrak{R}$. The relations existing between the rings $\mathfrak{R}$, $\mathfrak{S}$ and the fields P, Σ may be represented schematically by

$$\begin{array}{ccc} \mathfrak{R} & \subset & \mathfrak{S} \\ \cap & & \cap \\ \mathsf{P} & \subset & \Sigma. \end{array}$$

These relations will be valid throughout this section. By the term "integral" we always mean: integral with respect to $\mathfrak{R}$.

EXAMPLE. If $\mathfrak{R}$ is the ring of the ordinary integers, then P is the field of rational numbers, Σ a number field (finite over P) and $\mathfrak{S}$ the ring of integral algebraic numbers of the field Σ.

If $\mathfrak{R}$ is a polynomial domain: $\mathfrak{R} = \mathsf{K}[x_1, \ldots, x_n]$, then P is the field of rational functions, Σ is generated by the adjunction of a finite number of algebraic functions, and $\mathfrak{S}$ consists of the integral algebraic functions of the field Σ. Etc.

Our aim is to investigate the theory of ideals in $\mathfrak{S}$. This means that we must first establish the role played by the divisor chain condition for the ideals of $\mathfrak{S}$. Specifically, we will ask whether the divisor chain condition carries over to $\mathfrak{S}$ if it is valid in $\mathfrak{R}$. By the theorems of Section 99 this transfer is valid as soon as an $\mathfrak{R}$-module basis exists for $\mathfrak{S}$. This will therefore be our first objective.

First a preliminary theorem:

If σ is an element of Σ, then $\sigma = s/r$, where $s \in \mathfrak{S}$, $r \in \mathfrak{R}$.

PROOF. The element σ satisfies an equation with coefficients in P. These coefficients are fractions with respect to $\mathfrak{R}$. They are transformed into quantities of $\mathfrak{R}$ when multiplied by the product of the denominators:

$$r_0\sigma^m + r_1\sigma^{m-1} + \cdots + r_m = 0.$$

If we set $r_0 = r$ and multiply by r^{m-1}, then

$$(r\sigma)^m + r_1(r\sigma)^{m-1} + r_2 r(r\sigma)^{m-2} + \cdots + r_m r^{m-1} = 0.$$

Hence $r\sigma$ is integral with respect to $\mathfrak{R}$. If we set $r\sigma = s$, the proof is completed.

This theorem implies that Σ is the quotient field of $\mathfrak{S}$.

If an element ξ is integral, then all conjugates of ξ (in an extension field of Σ normal with respect to P) are also integral.

PROOF. By assumption all powers of ξ may be expressed linearly in terms of a finite number of quantities of Σ. Under an isomorphism of Σ these quantities have a finite number of images, and all powers of the conjugate of ξ determined by the isomorphism are linearly expressible in terms of these images.

Since sums and products of integral quantities are integral, the elementary symmetric functions of ξ and its conjugates are also integral. Hence

If in the equation irreducible over P, which is satisfied by an integral quantity ξ, the leading coefficient is made equal to 1, then all remaining coefficients are integral with respect to $\mathfrak{R}$. In particular, if $\mathfrak{R}$ is integrally closed in P, then all these coefficients lie in $\mathfrak{R}$.

If $\mathfrak{R}$ is integrally closed, this theorem gives us a convenient tool for determining whether an element ξ is integral. Thus, instead of forming all equations which are satisfied by ξ and examining this totality for an equation with integral coefficients, it is sufficient to take the single irreducible equation with leading coefficient 1. If its coefficients are integral, ξ is also; otherwise, ξ is not integral.

We now make the following restrictive assumptions:

I. *$\mathfrak{R}$ is integrally closed in its quotient field P.*

II. *In $\mathfrak{R}$ the divisor chain condition is valid for ideals.*

III. *Σ is a separable extension of P.*

By III, as seen in Section 40, Σ is generated by a "primitive element" σ: $\Sigma = \mathsf{P}(\sigma)$. By the above theorem, $\sigma = \frac{s}{r}$ $(s \in \mathfrak{S}, r \in \mathfrak{R})$; therefore the integral quantity s also generates the field. s satisfies an equation of n-th degree, where n is the degree of the field (Σ/P). Every element ξ of Σ may be represented in the form

$$\xi = \sum_{0}^{n-1} \varrho_k s^k \qquad (\varrho_k \in \mathsf{P}). \tag{1}$$

Now by Section 38, s has exactly n conjugates (in a normal extension field of P including Σ). If s in (1) is replaced by its conjugates s_ν, then the conjugates ξ_ν of ξ are given by

$$\xi_\nu = \sum_{0}^{n-1} \varrho_k s_\nu^k \qquad (\nu = 1, 2, \ldots, n). \tag{2}$$

The determinant of this system of equations is:

$$D = |s_\nu^k| = \prod_{\lambda<\mu} (s_\lambda - s_\mu),$$

by the Vandermonde Determinant Theorem. Its square is a symmetric function of the s_ν and therefore is contained in P. Furthermore, since the conjugates s_ν are all distinct, $D \neq 0$. Hence we can solve the system of equations (2):

$$\varrho_k = \frac{\sum S_{k\nu}\xi_\nu}{D},$$

where the $S_{k\nu}$ and D are polynomials in the s_ν, and so integral with respect to $\mathfrak{R}$. On multiplying this equation by D^2, we obtain

$$D^2\varrho_k = \sum_\nu D S_{k\nu}\xi_\nu. \tag{3}$$

Now let us assume that ξ is an element of $\mathfrak{S}$, that is, an integral quantity. Then the ξ_ν and consequently the right member of (3) are integral. However, the left member is an element of P. Hence since $\mathfrak{R}$ is integrally closed in P, $D^2\varrho_k$ must lie in $\mathfrak{R}$. If we set $D^2\varrho_k = r_k$, then $\varrho_k = r_k D^{-2}$ and by (1)

$$\xi = \sum_0^{n-1} r_k D^{-2} s^k.$$

Hence every element ξ of $\mathfrak{S}$ may be expressed linearly in terms of $D^{-2}s^0, D^{-2}s^1, \ldots, D^{-2}s^{n-1}$ with coefficients in $\mathfrak{R}$. In other words, $\mathfrak{S}$ is contained in the finite $\mathfrak{R}$-module

$$\mathfrak{M} = (D^{-2}s^0, D^{-2}s^1, \ldots, D^{-2}s^{n-1}).$$

Therefore by the theorems of Section 99 $\mathfrak{S}$, *as well as every submodule of* $\mathfrak{S}$ *and especially every ideal in* $\mathfrak{S}$, *has a finite module basis with respect to* $\mathfrak{R}$. This implies that the *divisor chain condition is valid for the* $\mathfrak{R}$*-modules and especially for the ideals in* $\mathfrak{S}$. If $\mathfrak{R}$ is a principal ideal ring, $\mathfrak{S}$ and every submodule of $\mathfrak{S}$ actually have a linearly independent $\mathfrak{R}$-module basis.

The same result is valid even though III is not satisfied provided that we assume that Σ is an inseparable extension (of characteristic p) such that the root ring $\mathfrak{R}^{\frac{1}{p^\nu}}$ is finite over $\mathfrak{R}$, where the root ring (similarly to the root field of Section 39) consists of the p-th roots of the elements of $\mathfrak{R}$. This is true in all cases of practical interest. For instance, if $\mathfrak{R}$ is a polynomial domain: $\mathfrak{R} = \mathsf{K}[x_1, \ldots, x_n]$, and K is obtained from the prime field Π by the adjunction of a finite number of algebraic or transcendental elements $\vartheta_1, \ldots, \vartheta_r$.

$$\mathsf{K} = \Pi(\vartheta_1, \ldots, \vartheta_r),$$

then

$$\mathfrak{R}^{\frac{1}{p^\nu}} = \mathsf{K}^{\frac{1}{p^\nu}}\left[x_1^{\frac{1}{p^\nu}}, \ldots, x_n^{\frac{1}{p^\nu}}\right]$$

$$= \Pi\left(\vartheta_1^{\frac{1}{p^\nu}}, \ldots, \vartheta_r^{\frac{1}{p^\nu}}\right)\left[x_1^{\frac{1}{p^\nu}}, \ldots, x_n^{\frac{1}{p^\nu}}\right];$$

therefore $\mathfrak{R}^{\frac{1}{p^\nu}}$ has a finite $\mathfrak{R}$-module basis consisting of the elements

$$\vartheta_1^{\alpha_1 : p^\nu}, \ldots, \vartheta_r^{\alpha_r \cdot p^\nu}, x_1^{\beta_1 \cdot p^\nu}, \ldots, x_n^{\beta_n : p^\nu}\begin{pmatrix} 0 \leqq \alpha_i < p, \\ 0 \leqq \beta_k < p \end{pmatrix}.$$

If the finiteness condition is satisfied instead of III, the finiteness of $\mathfrak{S}$ may be proved as follows:

First, the finiteness of $\mathfrak{R}^{1\cdot p}$ over $\mathfrak{R}$ implies by the isomorphism $\mathfrak{R} \cong \mathfrak{R}^{1:p}$ (cf. Section 39) that $\mathfrak{R}^{1\cdot p^2}$ is finite over $\mathfrak{R}^{1:p}$, etc. Continuing in this manner we conclude finally that $\mathfrak{R}^{1\cdot p^e}$ is finite over $\mathfrak{R}$.

Now let Δ be the largest separable extension of P which is contained in Σ. Let e be the exponent of Σ. Then Σ lies between Δ and $\Delta^{1\cdot p^e}$.

If $\mathfrak{D}$ is the ring of integral quantities in Δ, then $\mathfrak{D}^{1:p^e}$ is the ring of integral quantities in $\Delta^{1:p^e}$; for, an element of $\Delta^{1:p^e}$ is integral if and only if its p^e-th power is integral. Hence the ring $\mathfrak{S}$ lies between $\mathfrak{D}$ and $\mathfrak{D}^{1:p^e}$. Furthermore, $\mathfrak{D}$ is finite over $\mathfrak{R}$ by the above proof since here it behaves just as a separable extension. Because of the isomorphism

$$\mathfrak{D} \cong \mathfrak{D}^{1:p^e}$$

$\mathfrak{D}^{1:p^e}$ is thereby finite over $\mathfrak{R}^{1:p^e}$. However, by assumption $\mathfrak{R}^{1:p^e}$ is finite over $\mathfrak{R}$. Hence $\mathfrak{D}^{1:p^e}$ is also finite over $\mathfrak{R}$. Hence as before $\mathfrak{S}$ is imbedded in a finite $\mathfrak{R}$-module. From here on all our earlier conclusions are valid.

By an $\mathfrak{R}$-*order* in Σ we mean a subring of Σ which includes $\mathfrak{R}$ and is a finite $\mathfrak{R}$-module. By the above $\mathfrak{S}$ is an $\mathfrak{R}$-order and every ring between $\mathfrak{R}$ and $\mathfrak{S}$ is also. Conversely, by the definition of integralness every $\mathfrak{R}$-order $\mathfrak{T}$ in Σ contains only integral elements, i.e., it is in $\mathfrak{S}$. Consequently, $\mathfrak{S}$ may be characterized as the most comprehending $\mathfrak{R}$-order in Σ. Hence $\mathfrak{S}$ is called the *principal order* of the field Σ. When we use the terminology "ideals of the field," "units of the field," etc., we always mean the ideals of $\mathfrak{S}$, the units of $\mathfrak{S}$, etc. By Section 100 $\mathfrak{S}$ is integrally closed in Σ.

The results of this section are valid for the most part if Σ is assumed to be, instead of a field, a commutative hypercomplex system over P which can be represented as a sum of fields which mutually annul one another. These results are not valid however in non-commutative hypercomplex systems over P; the reason for the failure is due mainly to the fact that the sum of two integral quantities need no longer be integral. The totality of the integral quantities is therefore not an order. Though every order contains only integral quantities there is no principal order including all orders. Under suitable assumptions on Σ there exists distinct maximal $\mathfrak{R}$-orders such that every $\mathfrak{R}$-order, and so every integral element, is contained in at least one maximal $\mathfrak{R}$-order. For the theory of ideals of these maximal $\mathfrak{R}$-orders see M. Deuring, *Algebren*, Ergebn. Math. Vol. 4, Heft 1 (1935).

In all $\mathfrak{R}$-orders of Σ the divisor chain condition is valid by the proof given above. Hence for these orders the decomposition and uniqueness theorems of Sections 87 and 88 (representation of all ideals as the intersection of primary ideals) are also valid.

An important simplification of this theory of ideals is brought about by Section 90, final remarks, if in the order $\mathfrak{o}$ every prime ideal, which is distinct from the null ideal, is maximal. The following theorem is valid when this is the case:

If in $\mathfrak{R}$ *every prime ideal* $\neq (0)$ *is maximal, then in every* $\mathfrak{R}$*-order* $\mathfrak{o}$ *every prime ideal* $\neq (0)$ *is maximal.*

PROOF. Let $\mathfrak{p}$ be a prime ideal in $\mathfrak{o}$ which contains an element t distinct from zero. Let the equation which is satisfied by t of lowest possible degree with coefficients in $\mathfrak{R}$ and leading coefficient 1 be given by

$$t^h + a_1 t^{h-1} + \cdots + a_h = 0,$$

where $a_h \neq 0$ since otherwise t could be cancelled from all terms of this equation. It follows that $a_h \equiv 0(t) \equiv 0(\mathfrak{p})$; hence a_h belongs to the intersection $\mathfrak{p} \cap \mathfrak{R}$. This intersection is a prime ideal in $\mathfrak{R}$; for, if a product of two elements of $\mathfrak{R}$ belongs to $\mathfrak{R} \cap \mathfrak{p}$, and therefore to $\mathfrak{p}$, then one factor must belong to $\mathfrak{p}$ and so to $\mathfrak{R} \cap \mathfrak{p}$. Since a_h belongs to the prime ideal $\mathfrak{R} \cap \mathfrak{p}$, this prime ideal is distinct from the null ideal and therefore it is maximal.

Now, let $\mathfrak{a}$ be a proper divisor of $\mathfrak{p}$ and u an element of $\mathfrak{a}$ which does not belong to $\mathfrak{p}$. Then u satisfies an equation

$$u^l + b_1 u^{l-1} + \cdots + b_l = 0$$

and therefore a congruence of lowest degree given by

$$u^k + c_1 u^{k-1} + \cdots + c_k \equiv 0(\mathfrak{p}),$$

where $c_k \not\equiv 0(\mathfrak{p})$ since otherwise u could be cancelled. It follows that $c_k \equiv 0(u) \equiv 0(\mathfrak{a})$, hence c_k belongs to the intersection $\mathfrak{a} \cap \mathfrak{R}$ without belonging to $\mathfrak{p} \cap \mathfrak{R}$. The intersection $\mathfrak{a} \cap \mathfrak{R}$ is therefore a proper divisor of $\mathfrak{p} \cap \mathfrak{R}$; consequently it is equal to the unit ideal $\mathfrak{R}$. Hence $\mathfrak{a}$ contains the identity element so that $\mathfrak{a} = \mathfrak{o}$. Q.E.D.

The assumptions of this theorem are satisfied if $\mathfrak{R}$ is a principal ideal ring (ring of integers, polynomial domain in one variable). In this case $\mathfrak{o}$ has the property that every ideal distinct from the null- and unit ideals may be represented uniquely as the product of primary ideals which are relatively prime and distinct from $\mathfrak{o}$.

In regard to the principal order $\mathfrak{S}$ it is further valid, as we shall see, that the primary ideals are powers of prime ideals, and therefore, *every ideal is the product of powers of prime ideals.* We shall give a direct proof of this fundamental result of the "classical" Dedekind theory of ideals because of its significance in the theory of number- and function fields. This proof will not assume the concept of primary ideals or the general theory of ideals. This shall be done in the next section by a method due to W. Krull.[6]

EXERCISES. 1. If $\mathfrak{R}$ is a principal ideal ring, $(\omega_1, \ldots, \omega_n)$ the linearly independent basis of an order $\mathfrak{o}$ (such a basis always exists in this case), and $(\omega_1^{(i)}, \ldots, \omega_n^{(i)})$ are the conjugate bases in a normal extension field of P, then the "field discriminant"

$$D = \begin{vmatrix} \omega_1^{(1)} \ldots \omega_n^{(1)} \\ \cdots\cdots\cdots \\ \omega_1^{(n)} \ldots \omega_n^{(n)} \end{vmatrix}^2$$

is integral, rational and distinct from zero.

2. Let $\Sigma = \mathsf{P}(\sqrt{d})$ and $\mathfrak{R}$ be integrally closed in P. Prove that the numbers $\xi = a + b\sqrt{d}$ are integral with respect to $\mathfrak{R}$ if and only if the trace and norm:

$$S(\xi) = \xi + \xi' = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a,$$
$$N(\xi) = \xi \cdot \xi' = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$$

both belong to $\mathfrak{R}$.

3. In Exercise 2, if $\mathfrak{R} = \mathsf{K}[x]$ is a domain of polynomials in one indeterminate

[6] Krull, W.: "Zur Theorie der allgemeinen Zahlringe." *Math. Ann. Vol.* 99 (1928) *pp.* 51-70.

and d is a polynomial which contains no multiple factors, then $\xi = a + b\sqrt{d}$ is integral only if a and b belong to $\mathfrak{R}$.

4. In Exercise 2, if $\mathfrak{R} = C$ is the ring of integers and d is a square-free integer, then a basis of the principal order consists of the numbers $1, \sqrt{d}$ if $d \not\equiv 1(4)$; of the numbers $1, \frac{1+\sqrt{d}}{2}$ if $d \equiv 1(4)$.

102. AXIOMATIC FOUNDATION OF THE CLASSICAL THEORY OF IDEALS

Let $\mathfrak{o}$ be a domain of integrity (commutative ring with no zero divisors) in which the following three axioms are satisfied:

I. The divisor chain condition for ideals.

II. All prime ideals distinct from the null ideal are maximal.

III. $\mathfrak{o}$ is integrally closed in its quotient field Σ.

Examples of such rings are: 1. the principal ideal rings; 2. the principal orders which arise from principal ideal rings by finite extensions of the quotient field according to the scheme of Section 101 (for instance, the principal orders in number fields and function fields of one variable).

Elements of Σ which are integral with respect to $\mathfrak{o}$ must lie in $\mathfrak{o}$ by III and will be simply called integral. In particular the identity of Σ is always integral; consequently, $\mathfrak{o}$ is a domain of integrity with an identity.

We now consider, besides the ideals of $\mathfrak{o}$ (or $\mathfrak{o}$-modules in $\mathfrak{o}$), the $\mathfrak{o}$-modules in Σ, i.e., subclasses of Σ such that if a and b are elements of the subclass, then $a - b$ is also, and similarly for a and ra (where r is integral). In case such an $\mathfrak{o}$-module has a finite module basis we also call it a *fractional ideal.* If an $\mathfrak{o}$-module $\mathfrak{a}$ contains only integral quantities ($\mathfrak{a} \subseteq \mathfrak{o}$), it is an ideal in the usual sense or, as we now say, an *integral ideal.*

By the *sum* or the G.C.D. $(\mathfrak{a}, \mathfrak{b})$ of two $\mathfrak{o}$-modules $\mathfrak{a}$ and $\mathfrak{b}$ we mean (as with ideals) the module of all sums $a + b$. where $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. Similarly, by the product $\mathfrak{a}\mathfrak{b}$ we mean the module generated by all products ab, i.e., the totality of all sums $\sum a_\nu b_\nu$.

Sums and products of $\mathfrak{o}$-modules with finite basis also have a finite basis.

In the following theorems the German letters will only be used to designate *integral ideals in* $\mathfrak{o}$ *distinct from the null ideal,* while the letter $\mathfrak{p}$ will always stand for a prime ideal $\neq (0)$.

LEMMA. 1. *To every ideal* $\mathfrak{a}$ *there are prime ideals* $\mathfrak{p}_i$ *which are divisors of* $\mathfrak{a}$ *such that the product of the prime ideals is divisible by* $\mathfrak{a}$ *:*

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \equiv 0(\mathfrak{a}).^7$$

[7] This theorem depends only on the divisor chain condition.

FIRST PROOF. If we assume that the general decomposition theorems (Section 87) are known, then

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s],$$
$$\mathfrak{p}_i^{e_i} \equiv 0(\mathfrak{q}_i),$$
$$\prod_1^s \mathfrak{p}_i^{e_i} \equiv 0([\mathfrak{q}_1, \ldots, \mathfrak{q}_s]) \equiv 0(\mathfrak{a}).$$

SECOND PROOF. Without using primary ideals we may proceed as follows.

If $\mathfrak{a}$ is prime, the lemma is true. If $\mathfrak{a}$ is not prime, there is a product of two principal ideals $\mathfrak{b}\mathfrak{c}$ such that

$$\mathfrak{b}\mathfrak{c} \equiv 0(\mathfrak{a}), \qquad \mathfrak{b} \not\equiv 0(\mathfrak{a}), \qquad \mathfrak{c} \not\equiv 0(\mathfrak{a}).$$

The ideals $\mathfrak{b}' = (\mathfrak{b}, \mathfrak{a})$, $\mathfrak{c}' = (\mathfrak{c}, \mathfrak{a})$ are proper divisors of $\mathfrak{a}$ and

$$\mathfrak{b}'\mathfrak{c}' = (\mathfrak{b}, \mathfrak{a}) \cdot (\mathfrak{c}, \mathfrak{a}) = (\mathfrak{b}\mathfrak{c}, \mathfrak{b}\mathfrak{a}, \mathfrak{a}\mathfrak{c}, \mathfrak{a}^2) \equiv 0(\mathfrak{a}, \mathfrak{a}, \mathfrak{a}) \equiv 0(\mathfrak{a}).$$

Now, if we assume that the lemma is valid for the ideals $\mathfrak{b}'$ and $\mathfrak{c}'$, there is a product $\mathfrak{p}_1 \ldots \mathfrak{p}_s \equiv 0(\mathfrak{b}')$ and another product $\mathfrak{p}_{s+1} \ldots \mathfrak{p}_r \equiv 0(\mathfrak{c}')$. The product $\mathfrak{p}_1 \ldots \mathfrak{p}_s\mathfrak{p}_{s+1} \ldots \mathfrak{p}_r$ is then $\equiv 0(\mathfrak{b}' \cdot \mathfrak{c}') \equiv 0(\mathfrak{a})$ and therefore the lemma is also valid for $\mathfrak{a}$. Hence, if the lemma were not valid for an ideal $\mathfrak{a}$, it would not be valid for one of the two proper divisors $\mathfrak{b}'$ or $\mathfrak{c}'$; in the same manner, there would be a proper divisor for which the lemma would not be valid, etc.; we thereby would obtain an infinite chain of proper divisors which is impossible by Axiom I. Hence the lemma is valid for every ideal $\mathfrak{a}$.

LEMMA. 2. *If* $\mathfrak{p}$ *is prime, then* $\mathfrak{a}\mathfrak{b} \equiv 0(\mathfrak{p})$ *implies* $\mathfrak{a} \equiv 0(\mathfrak{p})$ *or* $\mathfrak{b} \equiv 0(\mathfrak{p})$.[8]

PROOF. Let $\mathfrak{a} \not\equiv 0(\mathfrak{p})$ and $\mathfrak{b} \not\equiv 0(\mathfrak{p})$. Then there is an element a in $\mathfrak{a}$ and an element b in $\mathfrak{b}$ such that neither element belongs to $\mathfrak{p}$. However, the product ab is in $\mathfrak{a}\mathfrak{b}$ and so in $\mathfrak{p}$. This is a contradiction since $\mathfrak{p}$ is a prime ideal.

We designate by $\mathfrak{p}^{-1}$ the totality of quantities a (integral or fractional) for which $a\mathfrak{p}$ is integral.[9] Evidently $\mathfrak{p}^{-1}$ is an $\mathfrak{o}$-module.

LEMMA. 3. *If* $\mathfrak{p} \neq \mathfrak{o}$, *then there is a non-integral element in* $\mathfrak{p}^{-1}$.

PROOF. Let c be an arbitrary element of $\mathfrak{p}$ distinct from zero. By Lemma 1. there is a product of prime ideals

$$\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r \equiv 0(c).$$

We may assume that this product is irredundant, i.e., that there is no subproduct as $\mathfrak{p}_2 \ldots \mathfrak{p}_r \equiv 0(c)$. Since the product $\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r$ is divisible by $\mathfrak{p}$, there must be a factor, say $\mathfrak{p}_1$, which is divisible by $\mathfrak{p}$ and therefore equal to $\mathfrak{p}$.

Consequently,

$$\mathfrak{p}\mathfrak{p}_2 \ldots \mathfrak{p}_r \equiv 0(c),$$
$$\mathfrak{p}_2 \ldots \mathfrak{p}_r \not\equiv 0(c).$$

[8] Cf. Section 86.

[9] $a\mathfrak{p}$ stands for the totality of all products ac with $c \in \mathfrak{p}$.

Hence there is an element b in $\mathfrak{p}_2 \ldots \mathfrak{p}_r$ which does not belong to (c). For this element we have

$$\mathfrak{p} b \equiv 0(\mathfrak{p}\mathfrak{p}_2 \ldots \mathfrak{p}_r) \equiv 0(c).^{10}$$

Hence $\mathfrak{p}\frac{b}{c}$ is integral; therefore $\frac{b}{c}$ lies in $\mathfrak{p}^{-1}$. However, since $b \not\equiv 0(c)$, $\frac{b}{c}$ is not integral. Q.E.D.

THEOREM. 1. *If* $\mathfrak{p} \neq \mathfrak{o}$, *then*

$$\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{o}.$$

PROOF. The definition of $\mathfrak{p}^{-1}$ implies $\mathfrak{o} \subseteq \mathfrak{p}^{-1}$. Hence $\mathfrak{p} = \mathfrak{o}\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p}$. The integral ideal $\mathfrak{p}\mathfrak{p}^{-1}$ is a divisor of $\mathfrak{p}$; hence it is either $= \mathfrak{p}$ or $= \mathfrak{o}$. Let us suppose that

$$\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{p}.$$

It would then follow: $\mathfrak{p} \cdot (\mathfrak{p}^{-1})^2 = (\mathfrak{p}\mathfrak{p}^{-1})\mathfrak{p}^{-1} = \mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, and similarly $\mathfrak{p}(\mathfrak{p}^{-1})^3 = \mathfrak{p}$, etc. Therefore, if $a \neq 0$ is an arbitrary element of $\mathfrak{p}$ and b an element of $\mathfrak{p}^{-1}$, then $ab^e \in \mathfrak{p}(\mathfrak{p}^{-1})^e$ is integral and therefore all powers of b may be represented as fractions with the same denominator a. Hence b is integral. This is valid for every b in $\mathfrak{p}^{-1}$, contrary to Lemma 3.

We are now able to prove the main factorization theorem:

THEOREM. 2. *Every ideal* $\mathfrak{a}$ *is a product of prime ideals.*

PROOF. We may assume that $\mathfrak{a} \neq \mathfrak{o}$. By Lemma 1., let

$$\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r \equiv 0(\mathfrak{a}), \tag{1}$$

where the number r is chosen as small as possible, i.e., there is no shorter product $\equiv 0(\mathfrak{a})$. Furthermore, let $\mathfrak{p}$ be an arbitrary prime ideal divisor of $\mathfrak{a}$ distinct from $\mathfrak{o}$ (by Lemma 1. there must be such an ideal). Then the product $\mathfrak{p}_1 \ldots \mathfrak{p}_r$ is divisible by $\mathfrak{p}$. Hence (by Lemma 2.) there is a $\mathfrak{p}_i$ which is divisible by $\mathfrak{p}$ and, as this $\mathfrak{p}_i$ is maximal, $\mathfrak{p}_i = \mathfrak{p}$. Let us assume that $\mathfrak{p}_1$ is the prime ideal $\mathfrak{p}$. If we multiply (1) by $\mathfrak{p}^{-1}$, then

$$\mathfrak{p}_2 \ldots \mathfrak{p}_r \equiv 0(\mathfrak{p}^{-1}\mathfrak{a}) \equiv 0(\mathfrak{o});$$

therefore $\mathfrak{p}^{-1}\mathfrak{a}$ is an integral ideal which divides a product of less than r prime ideals. Now, if we make an induction on r, i.e., if we assume that the theorem is true for ideals which divide a product of less than r prime ideals $\neq (0)$ (for ideals which divide *one* prime ideal $\neq (0)$ the theorem is valid), then the theorem is valid in particular for $\mathfrak{p}^{-1}\mathfrak{a}$, that is

$$\mathfrak{p}^{-1}\mathfrak{a} = \mathfrak{p}_2' \ldots \mathfrak{p}_s'.$$

On multiplying both sides by $\mathfrak{p}$ the desired representation for $\mathfrak{a}$ is obtained.

The uniqueness of this representation follows from

---

[10] This proof may also be shortened if we assume that the general theory of ideals is known. Thus, if $c \equiv 0(\mathfrak{p})$, $\mathfrak{p}$ occurs among the prime ideals belonging to (c), and so by Section 88 $(c):\mathfrak{p} \neq (c)$, i.e., there is an element b not belonging to (c) for which $\mathfrak{p}b \equiv 0(c)$.

THEOREM. 3. *If* $\mathfrak{a} \equiv 0(\mathfrak{b})$ *and* $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$, $\mathfrak{b} = \mathfrak{p}_1' \dots \mathfrak{p}_s'$, *then every prime ideal distinct from* $\mathfrak{o}$ *which occurs in the representation of* $\mathfrak{b}$, *also occurs in the representation of* $\mathfrak{a}$ *and at least as often.*

PROOF. Let $\mathfrak{p}_1' \neq \mathfrak{o}$. Since $\mathfrak{p}_1'$ is a divisor of $\mathfrak{a}$, we conclude as before that $\mathfrak{p}_1'$ must occur among the $\mathfrak{p}_\nu$. Let us say that $\mathfrak{p}_1 = \mathfrak{p}_1'$. Then

$$\mathfrak{p}_1^{-1}\mathfrak{a} \equiv 0(\mathfrak{p}_1^{-1}\mathfrak{b}),$$
$$\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{p}_2 \dots \mathfrak{p}_r,$$
$$\mathfrak{p}_1^{-1}\mathfrak{b} = \mathfrak{p}_2' \dots \mathfrak{p}_s'.$$

If we assume the statement as valid for smaller values of s (for $s = 0$, $\mathfrak{b} = \mathfrak{o}$ it is trivial), then each of the ideals $\mathfrak{p}_2', \dots, \mathfrak{p}_s'$ distinct from $\mathfrak{o}$ occurs at least as often among $\mathfrak{p}_2, \dots, \mathfrak{p}_r$. The theorem follows immediately.

COROLLARY. 1. *The representation of an ideal* $\mathfrak{a}$ *as a product of prime ideals is unique except for the order of the factors and for the factor* $\mathfrak{o}$.

2. *Divisibility implies product representation: if* $\mathfrak{a} \equiv 0(\mathfrak{b})$, *then* $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ *with integral* $\mathfrak{c}$.

$\mathfrak{c}$ may be taken as the product of those prime factors of $\mathfrak{a}$ which are left over when we strike out of the representation of $\mathfrak{a}$ those of $\mathfrak{b}$ (each as often as it occurs in $\mathfrak{b}$).

If $\mathfrak{o}$ is a commutative ring *with* zero divisors, the whole theory of this section is valid without essential modifications if we limit ourselves to those ideals which do not consist of only zero divisors. The Axioms I and II must be assumed as valid for these non-zero divisor ideals, while in Axiom III the quotient field must be replaced by the *quotient ring*, i.e., by the ring of all fractions a/b where b is not a zero divisor. It can be shown that Theorems 1., 2., 3. are valid for the non-zero divisor ideals.

EXERCISE. 1. Decompose into its prime ideal factors the principal ideals (2) and (3) in the principal order of the number field $\Gamma(\sqrt{-5})$.

103. CONVERSE AND EXTENSION OF THE RESULTS

We have seen (Section 102) that Theorems 2. and 3. follow from Axioms I to III. These two theorems imply the unique decomposition of the ideal into prime factors. The converse is also valid.

Let $\mathfrak{o}$ *be a domain of integrity with an identity. In* $\mathfrak{o}$ *let every ideal* $\mathfrak{a}$ [11] *be representable as a product of prime ideals:* $\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r$. *Furthermore, if* $\mathfrak{a}$ *is divisible by* $\mathfrak{b}$, *then in every decomposition of* $\mathfrak{a}$ *let every factor distinct from* $\mathfrak{o}$ *occur at least as often as in a decomposition of* $\mathfrak{b}$. *Then Axioms I to III are valid in* $\mathfrak{o}$.

PROOF. The chain condition (Axiom I) follows immediately from the fact that every ideal $\mathfrak{a} = \mathfrak{p}_1^{\sigma_1} \dots \mathfrak{p}_r^{\sigma_r}$ has only the finitely many divisors $\mathfrak{b} = \mathfrak{p}_1^{\tau_1} \dots \mathfrak{p}_r^{\tau_r}$

[11] German letters again represent integral ideals $\neq (0)$.

($\sigma_i \leqq \varrho_i$). In particular a prime ideal $\mathfrak{p}$ has only $\mathfrak{p}$ and $\mathfrak{o}$ as divisors; therefore, Axiom II is also satisfied.

In order to prove Axiom III (the integral closure of $\mathfrak{o}$ in its quotient field Σ), let us assume that λ is an element of Σ which is integral with respect to $\mathfrak{o}$. Then λ^m, let us say, is linearly expressible by $\lambda^0, \ldots, \lambda^{m-1}$, in other words, lies in the $\mathfrak{o}$-module $\mathfrak{l} = (\lambda^0, \lambda^1, \ldots, \lambda^{m-1})$. If $\lambda = a/b$, $\mathfrak{l}$ may be transformed into an integral ideal on multiplying by $\mathfrak{b} = (b^{m-1})$. Furthermore, $\mathfrak{l}$ evidently satisfies the equation $\mathfrak{l}^2 = \mathfrak{l}$. On multiplying by $\mathfrak{b}^2$, we obtain

$$(\mathfrak{l}\mathfrak{b})^2 = (\mathfrak{l}\mathfrak{b})\mathfrak{b}.$$

The uniqueness implies

$$\mathfrak{l}\mathfrak{b} = \mathfrak{b}.$$

On multiplying both sides by $b^{-(m-1)}$,

$$\mathfrak{l} = \mathfrak{o}.$$

λ is therefore an element of $\mathfrak{o}$. Q.E.D.

We will now consider in detail some extensions of Theorems 2. and 3. which also belong to the classical theory of ideals.

The fact that divisibility implies product representation allows us to compute the greatest common divisor and the least common multiple of ideals in the same manner as in the case of whole numbers, i.e., by means of the decomposition into prime factors.

Let $\mathfrak{a}$ and $\mathfrak{b}$ be two arbitrary ideals:

$$\mathfrak{a} = \mathfrak{p}_1^{\varrho_1} \ldots \mathfrak{p}_r^{\varrho_r},$$
$$\mathfrak{b} = \mathfrak{p}_1^{\sigma_1} \ldots \mathfrak{p}_r^{\sigma_r}$$

(where in both cases all prime factors are written down which occur in either $\mathfrak{a}$ or $\mathfrak{b}$, possibly with exponents zero). Every common divisor contains only prime factors which appear in these sequences. If $\mathfrak{p}_i$, let us say, does occur, it can only be raised to an exponent $\leqq \tau_i$, where τ_i is the smaller of the numbers ϱ_i, σ_i. The greatest common divisor $(\mathfrak{a}, \mathfrak{b})$ must be divisible by every common divisor, in particular by $\mathfrak{p}^{\tau_i}$. Hence it must be equal to

$$\mathfrak{p}_1^{\tau_1} \ldots \mathfrak{p}_r^{\tau_r}.$$

Similarly, the least common multiple (the intersection) $\mathfrak{a} \cap \mathfrak{b}$ of $\mathfrak{a}$ and $\mathfrak{b}$ is the ideal

$$\mathfrak{p}_1^{\mu_1} \ldots \mathfrak{p}_r^{\mu_r},$$

where μ_i is the larger of the numbers ϱ_i, σ_i.

THEOREM. 4. *If* $\mathfrak{a} \equiv 0(\mathfrak{b})$, *then there is in* $\mathfrak{b}$ *an element* d *such that*

$$(\mathfrak{a}, d) = \mathfrak{b}.$$

PROOF. Let

$$\mathfrak{a} = \mathfrak{p}_1^{\varrho_1} \dots \mathfrak{p}_r^{\varrho_r},$$

$$\mathfrak{b} = \mathfrak{p}_1^{\sigma_1} \dots \mathfrak{p}_r^{\sigma_r}. \qquad (0 \leqq \sigma_i \leqq \varrho_i)$$

We have to choose d so that d is divisible by $\mathfrak{b}$ but has no further divisor in common with $\mathfrak{a}$. We set

$$\mathfrak{c} = \mathfrak{p}_1^{\sigma_1+1} \dots \mathfrak{p}_r^{\sigma_r+1},$$

$$\mathfrak{c}_i = \mathfrak{c}.\mathfrak{p}_i = \mathfrak{p}_1^{\sigma_1+1} \dots \mathfrak{p}_i^{\sigma_i} \dots \mathfrak{p}_r^{\sigma_r+1}.$$

Then $\mathfrak{c}_i \not\equiv 0(\mathfrak{c})$. Hence there is an element d_i which is in $\mathfrak{c}_i$ but not in $\mathfrak{c}$. Then

$$d_i \equiv 0(\mathfrak{p}_j^{\sigma_j+1}) \quad \text{for} \quad j \neq i,$$

$$d_i \not\equiv 0(\mathfrak{p}_i^{\sigma_i+1}).$$

The sum

$$d = d_1 + \dots + d_r$$

is divisible by $\mathfrak{b}$ (since all d_i are). However

$$d \equiv d_i \not\equiv 0(\mathfrak{p}^{\sigma_i+1});$$

hence d has only the factors of $\mathfrak{b}$ in common with $\mathfrak{a}$.

COROLLARIES.

1. *In the residue class ring* $\mathfrak{o}/\mathfrak{a}$ *every ideal* $\mathfrak{b}/\mathfrak{a}$ *is a principal ideal.* Thus $\mathfrak{b}/\mathfrak{a}$ is generated by the residue class $\mathfrak{a} + d$.

2. *Every ideal* $\mathfrak{b}$ *possesses a basis* (a, d) *with two basis elements, where* $a \neq 0$ *may be arbitrarily chosen in* $\mathfrak{b}$.

Thus, let a be any element of $\mathfrak{b}$ distinct from zero and $\mathfrak{a} = (a)$. The above theorem implies $(a, d) = \mathfrak{b}$.

3. *Every ideal* $\mathfrak{b}$ *may be transformed into a principal ideal on multiplying by an ideal* $\mathfrak{b}$ *relatively prime to a given ideal* $\mathfrak{c}$.

PROOF. We set $\mathfrak{a} = \mathfrak{c}\mathfrak{b}$. The above theorem implies

$$(\mathfrak{a}, d) = \mathfrak{b}. \tag{1}$$

Since d is divisible by $\mathfrak{b}$, we can set

$$(d) = \mathfrak{b}\mathfrak{d}.$$

Then by (1):

$$(\mathfrak{c}\mathfrak{d}, \mathfrak{b}\mathfrak{d}) = \mathfrak{d}.$$

$\mathfrak{c}$ and $\mathfrak{d}$ must therefore be relatively prime.

EXERCISE. 1. Let $\mathfrak{O}$ be the ring of all quotients a/b, where a and b are integral and b is not divisible by fixed prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$. Then to every ideal $\mathfrak{a}$ of $\mathfrak{o}$ there corresponds an ideal $\mathfrak{A}$ of $\mathfrak{O}$ consisting of the fractions a/b with $a \in \mathfrak{a}$. To the ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ there correspond the prime ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_r$, all remaining prime ideals of $\mathfrak{o}$ correspond to the unit ideal $\mathfrak{O}$. Every ideal in $\mathfrak{O}$ is uniquely representable as a power product of the ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_r$. Moreover, in $\mathfrak{O}$ every ideal is a principal ideal.

Results Dependent on Valuation Theory

To every prime ideal $\mathfrak{p}$ of a ring $\mathfrak{o}$, which satisfies the Axioms of Section 102, there belongs by Section 73 a $\mathfrak{p}$-*adic valuation* of the quotient field Σ. Thus by Section 73 a $\mathfrak{p}$-adic valuation exists as soon as the following two properties of the prime ideal $\mathfrak{p}$ are valid:

A. All powers $\mathfrak{p}$, $\mathfrak{p}^2$, . are distinct and their intersection contains only zero;

B. If an element a in $\mathfrak{o}$ is exactly divisible by $\mathfrak{p}^\alpha$ and b is exactly divisible by $\mathfrak{p}^\beta$, then ab is exactly divisible by $\mathfrak{p}^{\alpha+\rho}$.

The property A implies that every element $a \neq 0$ is exactly divisible by a uniquely determined power $\mathfrak{p}^\alpha$. This is always the case in our rings since we have only to factor the principal ideal $a\mathfrak{o}$ into prime factors and then determine which power $\mathfrak{p}^\alpha$ occurs in this factorization. Similarly, it is clear that property B is valid.

The $\mathfrak{p}$-adic valuation of the element a/b as defined in Section 73 is

$$\varphi\left(\frac{a}{b}\right) = e^{-\alpha+\beta}$$

when a is exactly divisible by $\mathfrak{p}^\alpha$ and b is exactly divisible by $\mathfrak{p}^\beta$. If we go over to the logarithms $w(c) = -\log\varphi(c)$, then

$$w\left(\frac{a}{b}\right) = \alpha - \beta.$$

An equivalent valuation (cf. Section 74) is given by

$$w\left(\frac{a}{b}\right) = \sigma \cdot (\alpha - \beta),$$

where σ is an arbitrary positive real number.

We now show that the $\mathfrak{p}$-adic valuations are the only ones by which all elements of $\mathfrak{o}$ have non-negative values, in other words:

If $w(c) = -\log\varphi(c)$ is a non-trivial exponential valuation of Σ, by which all elements a of $\mathfrak{o}$ have non-negative values $w(a)$, then it is equivalent to a $\mathfrak{p}$-adic valuation, where $\mathfrak{p}$ is a prime ideal of $\mathfrak{o}$.

PROOF. The totality of the elements of $\mathfrak{o}$ whose values are positive is evidently a prime ideal in $\mathfrak{o}$. Let π be an element of $\mathfrak{o}$ which is exactly divisible by the first power of $\mathfrak{p}$. Then if a is exactly divisible by $\mathfrak{p}^\alpha$, we have

$$a\mathfrak{o} = \mathfrak{p}^\alpha\mathfrak{c}. \tag{2}$$

In $\mathfrak{c}$ there is an element c not divisible by $\mathfrak{p}$. By (2) $\pi^\alpha c$ is divisible by a:

$$\pi^\alpha c = ab. \tag{3}$$

The left member and the factor a on the right are each exactly divisible by $\mathfrak{p}^\alpha$. Hence b cannot be divisible by $\mathfrak{p}$ and so $w(b) = 0$. Similarly $w(c) = 0$. Hence by (3),

$$w(a) = w(\pi^\alpha) = \alpha w(\pi).$$

Since $w(\pi)$ is a positive constant, the valuation $w(a)$ is equivalent to that given by $w'(a) = \alpha$.

EXERCISES. 2. If all elements of the ring $\mathfrak{S}$ are integral with respect to the subring $\mathfrak{R}$ and P, Σ are the quotient fields of $\mathfrak{R}$ and $\mathfrak{S}$, then every continuation of a $\mathfrak{p}$-adic valuation of P to Σ is equivalent to a $\mathfrak{P}$-adic valuation of Σ. The prime ideal $\mathfrak{P}$ of $\mathfrak{S}$, which belongs to this valuation, is a divisor of the prime ideal $\mathfrak{p}$ of $\mathfrak{R}$.

3. Conversely: if a prime ideal $\mathfrak{P}$ of the extension ring $\mathfrak{S}$ is a divisor of the prime ideal $\mathfrak{p}$ of the subring $\mathfrak{R}$ and if to $\mathfrak{P}$ corresponds a $\mathfrak{P}$-adic valuation and to $\mathfrak{p}$ a $\mathfrak{p}$-adic valuation, then the first is equivalent to a continuation of the latter.

For the further evaluation of the relation between the theory of ideals and the theory of valuations, first considered by K. Hensel, we refer to *Zahlentheorie* by H. Hasse in this series.

104. FRACTIONAL IDEALS

In Section 102 a *fractional ideal* was defined as an $\mathfrak{o}$-module in the quotient field Σ which has a finite basis. Hence the ideals in $\mathfrak{o}$, i.e., "integral ideals," are fractional ideals.

Let $(\sigma_1, \ldots, \sigma_r)$ be a basis of a fractional ideal. On multiplying by a suitable denominator the elements of the basis, and therefore the ideal itself, can all be made integral.

Conversely, if an $\mathfrak{o}$-module $\mathfrak{a}$ can be made integral on multiplying by an integral quantity $b \neq 0$, then $b\mathfrak{a}$ as an integral ideal has a finite basis

$$b\mathfrak{a} = (a_1, \ldots, a_r),$$

which implies

$$\mathfrak{a} = \left(\frac{a_1}{b}, \ldots, \frac{a_r}{b}\right).$$

Hence we have proved:

An $\mathfrak{o}$-module in Σ is a finite, and therefore fractional, ideal if and only if it can be transformed into an integral ideal on multiplying by an integral quantity $b \neq 0$.

We have already seen that if $\mathfrak{a}$ and $\mathfrak{b}$ have a finite basis then $\mathfrak{a} \cdot \mathfrak{b}$ and $(\mathfrak{a}, \mathfrak{b})$ also have a finite basis and therefore are fractional ideals. This is also true of the *module quotient* $\mathfrak{a}:\mathfrak{b}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are integral ideals and $\mathfrak{b} \neq (0)$.[12] For, if $b \neq 0$ is an arbitrary element of $\mathfrak{b}$, then

$$b \cdot (\mathfrak{a}:\mathfrak{b}) \subseteq \mathfrak{b} \cdot (\mathfrak{a}:\mathfrak{b}) \subseteq \mathfrak{a} \subseteq \mathfrak{o};$$

accordingly $\mathfrak{a}:\mathfrak{b}$ is transformed into an integral ideal on multiplying by b.

In particular $\mathfrak{o}:\mathfrak{p} = \mathfrak{p}^{-1}$ is always a fractional ideal.

Every integral or fractional ideal $\neq (0)$ has an inverse.

PROOF. Let $\mathfrak{c}$ be an integral or fractional ideal $\neq (0)$, and $b \neq 0$ be so chosen that $b\mathfrak{c}$ is integral:

$$b\mathfrak{c} = \mathfrak{a}. \tag{1}$$

Now if $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r$ and (1) is multiplied by $\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \ldots \mathfrak{p}_r^{-1}$, then by Theorem 1 (Section 102)

$$(\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \ldots \mathfrak{p}_r^{-1}b)\,\mathfrak{c} = \mathfrak{o}.$$

This proves the existence of the inverse

$$\mathfrak{c}^{-1} = \mathfrak{p}_1^{-1} \ldots \mathfrak{p}_r^{-1}b.$$

This theorem implies: *the integral and fractional ideals $\neq (0)$ form an Abelian group.*

The equation $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ can be solved uniquely for $\mathfrak{c}$. The solution is designated by $\mathfrak{a}^{-1}\mathfrak{b}$ or $\mathfrak{b}/\mathfrak{a}$.

[12] By the module quotient $\mathfrak{a}:\mathfrak{b}$ (in Σ) we mean the totality of the elements λ of Σ for which $\lambda\mathfrak{b} \subseteq \mathfrak{a}$

The earlier theorems imply further:

Every fractional ideal is representable as the quotient of two integral ideals, in other words, in the form

$$\frac{\mathfrak{p}_1' \cdots \mathfrak{p}_s'}{\mathfrak{p}_1'' \cdots \mathfrak{p}_t''}.$$

In this expression we may cancel every ideal which occurs in the numerator as well as the denominator.

Every fractional principal ideal (λ) has a representation as the quotient of two integral principal ideals with the property: if r arbitrary prime ideals are given, then no one of these occurs in the numerator as well as the denominator.

PROOF. Let

$$(\lambda) = \frac{\mathfrak{p}_1' \cdots \mathfrak{p}_s'}{\mathfrak{p}_1'' \cdots \mathfrak{p}_t''},$$

be a reduced representation and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ the r given prime ideals. If we transform the denominator into a principal ideal (d) on multiplying by an ideal $\mathfrak{b}$ relatively prime to the product $\mathfrak{p}_1 \ldots \mathfrak{p}_r$, then

$$(\lambda) = \frac{\mathfrak{b}\mathfrak{p}_1' \cdots \mathfrak{p}_s'}{\mathfrak{b}\mathfrak{p}_1'' \cdots \mathfrak{p}_t''} = \frac{\mathfrak{b}\mathfrak{p}_1' \cdots \mathfrak{p}_s'}{(d)},$$

and therefore

$$\mathfrak{b}\mathfrak{p}_1' \ldots \mathfrak{p}_2' = (\lambda d).$$

Hence the numerator becomes in every case a principal ideal. None of the ideals $\mathfrak{p}_1, \ldots \mathfrak{p}_r$ occurs in the numerator as well as the denominator.

EXERCISE. The ideal fraction $\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{b}/\mathfrak{a}$ is equal to the module quotient $\mathfrak{b}:\mathfrak{a}$.

For the further development of the theory of ideals in number fields we refer to the book of E. Hecke: *Vorlesungen uber die Theorie der algebraischen Zahlen*, Leipzig 1923. For the theory of ideals in function fields and their applications we refer to the fundamental work of Dedekind and Weber: *Crelles Journal Vol.* 92 (1882) *pp.* 181-290, as well as to the treatise of M. Deuring appearing in this series.

105. IDEAL THEORY OF ARBITRARY INTEGRALLY CLOSED DOMAINS OF INTEGRITY

There are many important domains of integrity which actually satisfy Axioms I and III of Section 102 but not Axiom II. Examples of such domains are: the polynomial domain $K[x_1, \ldots, x_n]$ in more than one variable, the polynomial domain with integer coefficients $C[x_1, \ldots, x_n]$, and their finite integrally closed extensions (principal orders). In all these rings a prime ideal distinct from the null- and unit ideals has a prime ideal as a divisor which is also distinct from the null- and unit ideals. Hence in these rings the theory of ideals of Section 102 is not valid. However we will show that its main results remain unchanged provided that we replace the relation of equality for ideals by a "quasi-equality" relation, which we will immediately define.[13]

[13] This theory was developed by the author in *Math. Ann. 101 (1929)*. It was brought to a more refined form by E. Artin and will be published here in this form for the first time.

Let $\mathfrak{o}$ be a domain of integrity which is integrally closed in its quotient field Σ. In the following the German letters will designate fractional ideals distinct from the null ideal, i.e., $\mathfrak{o}$-modules in Σ which become integral when multiplied by a non-vanishing quantity of $\mathfrak{o}$. The inverse ideal $\mathfrak{a}^{-1}$ again denotes the totality of those elements r of Σ for which $r\mathfrak{a}$ is integral.

We define: $\mathfrak{a}$ is *quasi-equal* to $\mathfrak{b}$ if $\mathfrak{a}^{-1} = \mathfrak{b}^{-1}$ in symbols, $\mathfrak{a} \sim \mathfrak{b}$. The relation $\sim$ is evidently reflexive, symmetric, and transitive.

Similarly, $\mathfrak{a}$ is said to be a *quasi-divisor* of $\mathfrak{b}$, $\mathfrak{b}$ a *quasi-multiple* of $\mathfrak{a}$, if $\mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}$, in other words, if $\mathfrak{a}^{-1}\mathfrak{b}$ is integral; in symbols, $\mathfrak{a} \leqq \mathfrak{b}$ or $\mathfrak{b} \geqq \mathfrak{a}$.

The simplest properties of the symbols $\leqq$ and $\sim$ are:

1. If $\mathfrak{a} \supseteq \mathfrak{b}$, then $\mathfrak{a} \leqq \mathfrak{b}$ (proof is obvious).

2. If $\mathfrak{a}$ is a principal ideal: $\mathfrak{a} = (a)$, then $\mathfrak{a} \leqq \mathfrak{b}$ implies conversely $\mathfrak{a} \supseteq \mathfrak{b}$. Thus, in this case $\mathfrak{a}^{-1} = (a^{-1})$. Hence the assumption that $\mathfrak{a}^{-1}\mathfrak{b}$ is integral implies that $a^{-1}\mathfrak{b}$ is integral, i.e., that all elements of $\mathfrak{b}$ are divisible by a.

3. If $\mathfrak{a} \leqq \mathfrak{b}$ and at the same time $\mathfrak{a} \geqq \mathfrak{b}$, then $\mathfrak{a} \sim \mathfrak{b}$.

4. All quasi-multiples $\mathfrak{b}$ of $\mathfrak{a}$, especially all $\mathfrak{b}$ quasi-equal to $\mathfrak{a}$ have the property $\mathfrak{b} \subseteq (\mathfrak{a}^{-1})^{-1}$. (This is an immediate consequence of the integralness of $\mathfrak{b}\mathfrak{a}^{-1}$.)

In particular $\mathfrak{a} \subseteq (\mathfrak{a}^{-1})^{-1}$. By 1. this implies that $\mathfrak{a} \geqq (\mathfrak{a}^{-1})^{-1}$. On the other hand, $\mathfrak{a}^{-1}(\mathfrak{a}^{-1})^{-1}$ is integral. Hence $\mathfrak{a} \leqq (\mathfrak{a}^{-1})^{-1}$, and

5. $$\mathfrak{a} \sim (\mathfrak{a}^{-1})^{-1}.$$

By 4. and 5. $(\mathfrak{a}^{-1})^{-1}$ is *the most comprehending ideal quasi-equal to* $\mathfrak{a}$. We designate it by $\mathfrak{a}^*$

6. If $\mathfrak{a} \leqq \mathfrak{b}$, then $\mathfrak{a}\mathfrak{c} \leqq \mathfrak{b}\mathfrak{c}$. For, since $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c}\mathfrak{a}$ is integral, $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c} \subseteq \mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}$. Hence $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c}\mathfrak{b}$ is integral, or $\mathfrak{c}\mathfrak{a} \leqq \mathfrak{c}\mathfrak{b}$.

7. If $\mathfrak{a} \sim \mathfrak{b}$, then $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{c}$ (Consequence of 6.)

8. If $\mathfrak{a} \sim \mathfrak{b}$ and $\mathfrak{c} \sim \mathfrak{d}$, then $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$ (For by 7. $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$.)

By the class of an ideal we mean the union of all ideals quasi-equal to the ideal. Then by 8. the class of the product $\mathfrak{a}\mathfrak{c}$ is dependent only on the class of $\mathfrak{a}$ and the class of $\mathfrak{c}$. We can therefore define the *product* of the two latter classes as the class of the product $\mathfrak{a}\mathfrak{c}$.

9. The unit class with respect to the class-multiplication is the class of those ideals which are quasi-equal to the unit ideal $\mathfrak{o}$; since for every $\mathfrak{a}$ we have $\mathfrak{a}\mathfrak{o} = \mathfrak{a}$.

10. All quasi-multiples of $\mathfrak{o}$, especially all ideals of the unit class, are integral. (This is a special case of 2. obtained by setting $a = 1$.) As a consequence we have that all ideals quasi-equal to an integral ideal are again integral.

We will now prove the most important property of the inverses:

11. $$\mathfrak{a}\mathfrak{a}^{-1} \sim \mathfrak{o}.$$

It is clear that $\mathfrak{a}\mathfrak{a}^{-1} \geqq \mathfrak{o}$ since $\mathfrak{a}\mathfrak{a}^{-1}$ is integral. We must now prove that $\mathfrak{a}\mathfrak{a}^{-1} \leqq \mathfrak{o}$, or $(\mathfrak{a}\mathfrak{a}^{-1})^{-1} \subseteq \mathfrak{o}$. If λ belongs to $(\mathfrak{a}\mathfrak{a}^{-1})^{-1}$, then $\lambda\mathfrak{a}\mathfrak{a}^{-1}$ is integral. Hence $\lambda\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$, $\lambda^2\mathfrak{a}^{-1} \subseteq \lambda\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$, etc., in general $\lambda^n\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$ and therefore $\lambda^n\mathfrak{a}^{-1}\mathfrak{a}$ is integral. If μ is an arbitrary element of $\mathfrak{a}^{-1}\mathfrak{a}$, then all powers of λ become integral on multiplying by μ. Due to the integral closure of $\mathfrak{o}$, this implies, exactly as at the corresponding point in Section 102, that λ is itself integral.

By 11. it follows that, with respect to the class-multiplication defined above, the class of $\mathfrak{a}^{-1}$ represents an inverse to the class of $\mathfrak{a}$: the product of the classes of $\mathfrak{a}$ and $\mathfrak{a}^{-1}$ is the unit class. Hence

THEOREM. 1. *The classes of quasi-equal ideals form a group.*

The following two rules permit us to characterize quasi-divisibility and quasi-equality as divisibility and equality respectively except for factors of the unit class.

12. $\mathfrak{a} \geqq \mathfrak{b}$ implies $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{d}$ if $\mathfrak{c} \sim \mathfrak{o}$ and $\mathfrak{d}$ is integral. In particular, $\mathfrak{a} \sim \mathfrak{b}\mathfrak{d}$.

13. $\mathfrak{a} \sim \mathfrak{b}$ implies $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{d}$ if $\mathfrak{c} \sim \mathfrak{o}$ and $\mathfrak{d} \sim \mathfrak{o}$.

Thus in both cases $\mathfrak{a}(\mathfrak{b}\mathfrak{b}^{-1}) = \mathfrak{b}(\mathfrak{a}\mathfrak{b}^{-1})$.

The greatest common divisor $(\mathfrak{a}, \mathfrak{b})$ is obviously a quasi-divisor of $\mathfrak{a}$ as well as of $\mathfrak{b}$. We now show:

14. Every common quasi-divisor of $\mathfrak{a}$ and $\mathfrak{b}$ is a quasi-divisor of $(\mathfrak{a}, \mathfrak{b})$. For, if $\mathfrak{c}$ is such a divisor, $\mathfrak{c}^*$ is a common divisor of $\mathfrak{a}$ and $\mathfrak{b}$, and therefore a divisor of $(\mathfrak{a}, \mathfrak{b})$

Two integral ideals $\mathfrak{a}$, $\mathfrak{b}$ are said to be *quasi-relatively prime* if $(\mathfrak{a}, \mathfrak{b}) \sim \mathfrak{o}$, in other words, if every integral common quasi-divisor of $\mathfrak{a}$ and $\mathfrak{b}$ is quasi-equal to $\mathfrak{o}$.

15. If $\mathfrak{a}$ is quasi-relatively prime to $\mathfrak{b}$ and to $\mathfrak{c}$, it is also to the product $\mathfrak{bc}$ Thus

$$(\mathfrak{a}, \mathfrak{b}) \cdot (\mathfrak{a}, \mathfrak{c}) = (\mathfrak{a}^2, \mathfrak{ac}, \mathfrak{ba}, \mathfrak{bc}) \equiv \mathfrak{o}(\mathfrak{a}, \mathfrak{bc})$$

The left-hand side is $\sim \mathfrak{o}$, therefore the right-hand side must also be.

We will now prove a result due to E. Artin.

THEOREM. 2. *REFINEMENT THEOREM. If two factorizations of an integral ideal* $\mathfrak{a}$ *are given:*

$$\mathfrak{a} \sim \mathfrak{b}_1 \mathfrak{b}_2 \dots \mathfrak{b}_m \sim \mathfrak{c}_1 \mathfrak{c}_2 \dots \mathfrak{c}_n, \tag{1}$$

then the two products may be further decomposed until the factors coincide except for the order of the factors and for quasi-equality:

$$\mathfrak{b}_\lambda \sim \prod_\mu \mathfrak{b}_{\lambda\mu}, \qquad \mathfrak{c}_\mu \sim \prod_\lambda \mathfrak{b}_{\lambda\mu}. \tag{2}$$

PROOF. Let $(\mathfrak{b}_1, \mathfrak{c}_1) = \mathfrak{b}_{11}$. By 12. $\mathfrak{b}_1 \sim \mathfrak{b}_{11}\mathfrak{b}_1'$ and $\mathfrak{c}_1 \sim \mathfrak{b}_{11}\mathfrak{c}_1'$. Hence $\mathfrak{b}_{11} = (\mathfrak{b}_1, \mathfrak{c}_1) \sim (\mathfrak{b}_{11}\mathfrak{b}_1', \mathfrak{b}_{11}\mathfrak{c}_1') = \mathfrak{b}_{11}(\mathfrak{b}_1', \mathfrak{c}_1')$, and therefore $(\mathfrak{b}_1', \mathfrak{c}_1') \sim \mathfrak{o}$ Again let $(\mathfrak{b}_1', \mathfrak{c}_2) = \mathfrak{b}_{12}$. By 12. $\mathfrak{b}_1' \sim \mathfrak{b}_{12}\mathfrak{b}_1''$ and $\mathfrak{c}_2 = \mathfrak{b}_{12}\mathfrak{c}_2'$, as before, it follows that $(\mathfrak{b}_1'', \mathfrak{c}_2') \sim \mathfrak{o}$. Continuing in this way we finally obtain $\mathfrak{b}_1 = \mathfrak{b}_{11}\mathfrak{b}_{12} \dots \mathfrak{b}_{1n}\mathfrak{d}$ and $\mathfrak{c}_\mu = \mathfrak{b}_{1\mu}\mathfrak{c}_\mu'$ $(\mu = 1, 2, \dots, n)$. If this is substituted in (1), then

$$\mathfrak{b}_{11}\mathfrak{b}_{12} \dots \mathfrak{b}_{1n}\mathfrak{d}\mathfrak{b}_2 \dots \mathfrak{b}_m \sim \mathfrak{b}_{11}\mathfrak{c}_1'\mathfrak{b}_{12}\mathfrak{c}_2' \dots \mathfrak{b}_{1n}\mathfrak{c}_n'$$

By the group property $\mathfrak{b}_{11} \dots \mathfrak{b}_{1n}$ may be cancelled:

$$\mathfrak{d}\mathfrak{b}_2 \dots \mathfrak{b}_m \sim \mathfrak{c}_1'\mathfrak{c}_2' \dots \mathfrak{c}_n'$$

Here $\mathfrak{d}$ is quasi-relatively prime to all $\mathfrak{c}_\mu'$, and therefore to the product $\mathfrak{c}_1'\mathfrak{c}_2' \dots \mathfrak{c}_n'$. But $\mathfrak{d}$ occurs as a factor on the left-hand side and therefore is a quasi-divisor of the product $\mathfrak{c}_1'\mathfrak{c}_2' \dots \mathfrak{c}_n'$. Hence $\mathfrak{d} \sim \mathfrak{o}$ and the factor $\mathfrak{d}$ may also be omitted:

$$\mathfrak{b}_2 \dots \mathfrak{b}_m \sim \mathfrak{c}_1'\mathfrak{c}_2' \dots \mathfrak{c}_n'$$

We may now repeat the procedure with $\mathfrak{b}_2, \dots, \mathfrak{b}_m$ until we arrive at the factorization given in (2).

From now on all German letters shall represent *integral* ideals distinct from the null ideal. Such an ideal $\mathfrak{p}$ is said to be *irreducible* if it is not quasi-equal to $\mathfrak{o}$ and in every product representation $\mathfrak{p} \sim \mathfrak{ab}$ one factor belongs to the unit class. By 12. this is equivalent to saying that if $\mathfrak{p}$ is not quasi-equal to $\mathfrak{o}$, it has no quasi-divisors except those which are quasi-equal to $\mathfrak{p}$ or quasi-equal to $\mathfrak{o}$.

Let $\mathfrak{p}$ be an irreducible ideal and $\mathfrak{p}^*$ the most comprehending ideal quasi-equal to $\mathfrak{p}$. Then every integral proper divisor of $\mathfrak{p}^*$ must be non-quasi-equal to $\mathfrak{p}$, and therefore quasi-equal to $\mathfrak{o}$. Every ideal quasi-divisible by $\mathfrak{p}$ or $\mathfrak{p}^*$ is by 4. divisible by $\mathfrak{p}^*$. Hence

16. $\mathfrak{p}^*$ is a prime ideal. Thus, if a product $\mathfrak{bc}$ of two principal ideals $\mathfrak{b}$ and $\mathfrak{c}$ is divisible by $\mathfrak{p}^*$, but $\mathfrak{b}$ is not divisible by $\mathfrak{p}^*$, then $(\mathfrak{b}, \mathfrak{p}^*)$ is a proper divisor of $\mathfrak{p}^*$, and therefore quasi-equal to $\mathfrak{o}$. Hence

$$\mathfrak{c} = \mathfrak{o}\mathfrak{c} \sim (\mathfrak{b}, \mathfrak{p}^*)\mathfrak{c} = (\mathfrak{bc}, \mathfrak{p}^*\mathfrak{c}) \geqq (\mathfrak{p}^*, \mathfrak{p}^*) = \mathfrak{p}^*.$$

Consequently, $\mathfrak{c}$ is quasi-divisible by $\mathfrak{p}^*$ and is therefore divisible by $\mathfrak{p}^*$.

If we further assume that the divisor chain condition is valid in $\mathfrak{o}$, then

17. Every chain of integral ideals $\mathfrak{a}_1 > \mathfrak{a}_2 > \dots$, where each subsequent ideal is a proper quasi-divisor of the preceding one (i.e., quasi-divisor and not quasi-equal), breaks off after a finite number of steps. For, if we replace the ideals $\mathfrak{a}_1, \mathfrak{a}_2, \dots$ by their most comprehending quasi-equals $\mathfrak{a}_1^*, \mathfrak{a}_2^*, \dots$, we obtain a chain of integral ideals $\mathfrak{a}_1^* \subset \mathfrak{a}_2^* \subset \dots$ which must break off by the divisor chain condition.

We may formulate the "quasi-divisor chain condition" 17. also as a "principle of divisor induction" (cf. Section 84, Fourth Statement of the divisor chain condition). By this principle it

follows without difficulty that every integral ideal is quasi-equal to a product of irreducible ideals (cf. the corresponding induction proof in Section 19). The uniqueness of the factorization is contained as a special case in the Refinement Theorem (Theorem 2); it may also be proved directly (as in Section 19) by the fact that $\mathfrak{a}\,\mathfrak{b} \geqq \mathfrak{p}^*$ implies $\mathfrak{a} \geqq \mathfrak{p}^*$ or $\mathfrak{b} \geqq \mathfrak{p}^*$ (cf. 16). Hence

THEOREM. 3. *Every integral ideal distinct from the null ideal is quasi-equal to a uniquely determined product of irreducible ideals* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ *except for the order of the factors and for quasi-equality* (the ideals may also be chosen as the prime ideals $\mathfrak{p}_1^*, \mathfrak{p}_2^*, \ldots, \mathfrak{p}_r^*$).

By 2. two principal ideals are quasi-divisible or quasi-equal only if they are divisible or equal respectively. By Theorem 3. in the domain consisting of the classes of the principal ideals together with the classes of the non-principal ideals the unique factorization theorem is valid, in other words, in this domain the aim of the "classical theory of ideals" is fulfilled.

However, in order to establish the relation of the theory just obtained to the general theory of ideals and to the special theory of ideals of Section 102, we must investigate which prime ideals are irreducible and which ideals are quasi-equal to $\mathfrak{o}$.

We have seen: if $\mathfrak{p}$ is irreducible, $\mathfrak{p}^*$ is prime. We shall now show:

18. No proper multiple of such a $\mathfrak{p}^*$ distinct from the null ideal is prime. Thus, if $\mathfrak{a}$ is such a multiple, then $\mathfrak{a} \geqq \mathfrak{p}^*$: hence by 12 $\mathfrak{a}\,\mathfrak{c} = \mathfrak{p}^*\,\mathfrak{b}$ with $\mathfrak{c} \sim \mathfrak{o}$. Since in the factorization of $\mathfrak{b}$ a prime factor occurs at least as often as in that of $\mathfrak{a}$, then $\mathfrak{b} \equiv \mathfrak{o}(\mathfrak{a})$; similarly $\mathfrak{p}^* \equiv \mathfrak{o}(\mathfrak{a})$ but $\mathfrak{p}^*\mathfrak{b} \equiv \mathfrak{o}(\mathfrak{a})$. Therefore $\mathfrak{a}$ is not prime.

We now consider the factorization of an arbitrary prime ideal $\mathfrak{p}$. Either $\mathfrak{p} \sim \mathfrak{o}$, or in the factorization $\mathfrak{p} \sim \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r$ there occurs an irreducible factor $\mathfrak{p}_1$. Then $\mathfrak{p} \geqq \mathfrak{p}_1$, and therefore $\mathfrak{p} \subseteq \mathfrak{p}_1^*$. But, since a proper multiple of $\mathfrak{p}_1^*$ can not be prime, then $\mathfrak{p} = \mathfrak{p}_1^*$. It follows that $\mathfrak{p}^* = (\mathfrak{p}_1^*)^* = \mathfrak{p}_1^* = \mathfrak{p}$. Hence

19. Every prime ideal $\mathfrak{p}$ is either quasi-equal to $\mathfrak{o}$ or irreducible and equal to the $\mathfrak{p}^*$ belonging to it.

In the second case $\mathfrak{p}$ has no proper prime ideal multiples distinct from the null ideal. On the other hand we will show that in the first case there is one.

20. If $\mathfrak{p} \sim \mathfrak{o}$, there is an irreducible proper prime ideal multiple $\mathfrak{p}_\nu^*$ of $\mathfrak{p}$. Thus, if $p \neq 0$ is an element of $\mathfrak{p}$ and $(p) \sim \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_r \sim \mathfrak{p}_1^*\mathfrak{p}_2^* \ldots \mathfrak{p}_r^*$ is its factorization, then by 2. $\mathfrak{p}_1^*\mathfrak{p}_2^* \ldots \mathfrak{p}_r^* \equiv \mathfrak{o}(p) \equiv \mathfrak{o}(\mathfrak{p})$. Hence there is a $\mathfrak{p}_\nu^* \equiv \mathfrak{o}(\mathfrak{p})$. We have however that $\mathfrak{p}_\nu^* \neq \mathfrak{p}$ since otherwise $\mathfrak{p}_\nu^* \sim \mathfrak{o}$ would be valid.

We say that a prime ideal is a *higher* prime ideal if it has no prime ideal multiples distinct from the null ideal; on the contrary a *lower* prime ideal if it has such a prime ideal multiple. Then we may summarize 18., 19., and 20. by

THEOREM. 4. *Every higher prime ideal* $\mathfrak{p}$ *is irreducible and equal to its* $\mathfrak{p}^*$; *every lower prime ideal is quasi-equal to* $\mathfrak{o}$.

An ideal, which does not belong to the unit class, is by the Factorization Theorem 3. divisible by at least one higher prime ideal $\mathfrak{p} = \mathfrak{p}^*$. An ideal of the unit class is however divisible by no higher prime ideal. This is a pure ideal-theoretic (i.e., in the domain of integral ideals) characterization of the unit class.

In the rings investigated in Section 102 a prime ideal distinct from (0) is only divisible by itself and by $\mathfrak{o}$ because of Axiom II. Hence these rings contain no lower prime ideals except $\mathfrak{o}$. Since every ideal $\mathfrak{a} \neq \mathfrak{o}$ is divisible by a prime ideal distinct from $\mathfrak{o}$ (PROOF: we seek among the divisors of $\mathfrak{a}$ distinct from $\mathfrak{o}$ the most comprehending one; it is maximal and therefore prime), then $\mathfrak{a}$ can not be quasi-equal to $\mathfrak{o}$. Hence the unit class contains only the unit ideal $\mathfrak{o}$ By 12. it follows further that quasi-divisibility and divisibility are equivalent; this fact, or 13., implies that quasi-equality and equality are likewise equivalent. Consequently, the theory of ideals of Section 102 is contained as a special case in the theory developed above.

The connection to the general theory of ideals of Chapter 12 is now easily established. First, it is easy to see that every primary ideal, for which the prime ideal belonging to it is a lower prime ideal, must be quasi-equal to $\mathfrak{o}$. Let us designate such primary ideals as *lower* and the remaining as *higher primary ideals.* Then an ideal $\mathfrak{a}$ is quasi-equal to $\mathfrak{o}$ if and only if all its

primary components are lower. If two ideals $\mathfrak{a}$ and $\mathfrak{b}$ have the same higher primary components (but not necessarily the same lower ones), they are quasi-equal. Among the ideals quasi-equal to $\mathfrak{a}$ there is a most comprehending ideal $\mathfrak{a}^*$; we obtain it by omitting all lower primary components in the factorization $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$. Hence we may interpret the Factorization and Uniqueness Theorems of this section so that from now on all lower primary components are neglected and consideration is given only to the higher ones. The higher primary ideals are divisible only by a higher prime ideal and therefore in its factorization must produce by Theorem 2 a power of a prime ideal; that is, *every higher primary ideal is quasi-equal to a power of a prime ideal.* The basis of this fact rests naturally on the integral closure of the ring $\mathfrak{o}$.

EXAMPLE. The ring $C[x, \sqrt{2x}]$ is integrally closed in the quotient field $\Gamma(\sqrt{2x})$ and satisfies all assumptions of this section. In the domain of the principal ideals the principal ideal $(2x)$ has the two substantially different factorizations:

$$(2x) = (2) \cdot (x) = (\sqrt{2x})^2.$$

Hence in the domain of the principal ideals there is *no* unique factorization; for this, the introduction of ideals is necessary. The prime ideals $\mathfrak{p}_1 = (x, \sqrt{2x})$ and $\mathfrak{p}_2 = (2, \sqrt{2x})$ are not quasi-equal to $\mathfrak{o}$, since their inverses $\mathfrak{p}_1^{-1}$ and $\mathfrak{p}_2^{-1}$ contain the non-integral elements $\frac{\sqrt{2x}}{x}$ and $\frac{\sqrt{2x}}{2}$ respectively. The prime ideal $\mathfrak{p}_3 = (2, x, \sqrt{2x})$ is a proper divisor of $\mathfrak{p}_1$ and of $\mathfrak{p}_2$, and therefore quasi-equal to $\mathfrak{o}$. Hence

$$\mathfrak{p}_1^2 = (x^2, x\sqrt{2x}, 2x) = (x) \cdot (x, \sqrt{2x}, 2) = (x) \cdot \mathfrak{p}_3 \sim (x),$$

$$\mathfrak{p}_2^2 = (2^2, 2\sqrt{2x}, 2x) = (2) \cdot (2, \sqrt{2x}, x) = (2) \cdot \mathfrak{p}_3 \sim (2),$$

$$\mathfrak{p}_1\mathfrak{p}_2 = (2x, 2\sqrt{2x}, x\sqrt{2x}) = (\sqrt{2x}) \cdot (\sqrt{2x}, 2, x) = (\sqrt{2x}) \cdot \mathfrak{p}_3 \sim (\sqrt{2x}).$$

The principal ideals (x) and (2) are primary; though they are not powers of prime ideals, they are quasi-equal to powers of prime ideals. The principal ideal $(\sqrt{2x})$ is the L.C.M. of $\mathfrak{p}_1$ and $\mathfrak{p}_2$; though it is not equal to their product, it is quasi-equal to the product. This example shows the necessity of introducing quasi-equality instead of equality if we wish to obtain the factorization of the principal ideals into prime factors.

EXERCISES. 1. All results of this section are also valid for rings with zero divisors if we replace the quotient field by the quotient ring and limit ourselves to the non-zero divisor ideals (cf. Section 102, end).

2. Theorem 1. implies conversely that the ring $\mathfrak{o}$ is integrally closed (cf. Seetion 103).

3. Prove the integral closure of the residue class ring

$$\mathfrak{o} = K[x, y, z]/(xy - z^2)$$

and decompose the principal ideals (x), (y), (z) in $\mathfrak{o}$ into prime factors.

4. Extend Theorem 4. of Section 103 and its corollaries to more general integrally closed rings.

5. Prove $\mathfrak{a}:\mathfrak{b} \sim \mathfrak{a}\mathfrak{b}^{-1}$.

For a further generalization of the results of this section, see H. Prüfer, *J. reine u. angew. Math. Vol. 168 (1932)*, as well as P. Lorenzen, *Math. Z. Vol. 45 (1939)*.

Summary of the Theory of Ideals

The following summary shows the significance of the Axioms I (divisor chain condition), II (every prime ideal is maximal), III (integral closure) formulated in Section 102 in the theory of ideals for domains of integrity.

I implies: every ideal has a L.C.M. of primary ideals; the prime ideals belonging to the ideal are unique.

I and II imply: every ideal is the product of (single-primed) primary ideals; these are unique.

I and III imply: every ideal is quasi-equal to the product of powers of prime ideals; unique except for quasi-equality.

I, II, III imply: every ideal is the product of powers of prime ideals; these are unique.

For the further development of the theory of ideals we refer, above all others, to the treatise of W. Krull, Idealtheorie, *Ergebn. Math.* IV 3 (1935).

CHAPTER XV

LINEAR ALGEBRA

The linear algebra deals with *linear forms* (with coefficients in a ring K), with *modules* of such linear forms and with their homomorphisms or *linear transformations*. The theory is divided into different parts corresponding to the different assumptions which may be made regarding the basic underlying ring or field K. We will start our investigation with a section that is valid for arbitrary (also non-commutative) rings K.

The representation of linear algebra to be given here rests entirely on the theory of groups with operators (Chap. 6); otherwise, it uses only the foundations (Chap. 1 to 3).

106. MODULES. LINEAR FORMS. VECTORS. MATRICES

Let K be a ring with an identity ε; in this section the ring elements will be denoted by small Greek letters and at times will be called "*scalars.*"

Let $\mathfrak{M}$ be a K-(right)module, i.e., an additive Abelian group with K as a right multiplicative domain satisfying the following rules besides the group axioms:

$$(a + b)\lambda = a\lambda + b\lambda,$$
$$a(\lambda + \mu) = a\lambda + a\mu,$$
$$a \cdot \lambda\mu = a\lambda \cdot \mu.^{1}$$

Here the elements of $\mathfrak{M}$ are denoted by small Latin letters. From the distributive rules we may prove the usual rules regarding subtraction, the multiplicative properties of the minus sign, and the fact that a product is zero if one of its factors is zero (it could be the zero of K or that of $\mathfrak{M}$).

[1] The fact that the multipliers are written on the right is an arbitrary matter. In other words, all theorems that are to be proved are also valid when the multipliers stand on the left. The last rule however should be written as

$$\lambda\mu \cdot a = \lambda \cdot \mu a$$

which states that the multiplication by $\lambda\mu$ is to be performed by multiplying first by μ and then by λ instead of the reverse order as done above. Hence the operators are written on the right- or left-hand sides according as the operation: first Λ, then M, is to be designated by $\Lambda\mathsf{M}$ or $\mathsf{M}\Lambda$ respectively.

The identity of K need not be a unity operator: for certain a the product $a\varepsilon$ may be distinct from a. (For example, all rules are satisfied if we define $a\lambda = 0$ for every a and λ.) In this case however we may always set

$$a = (a - a\varepsilon) + a\varepsilon. \tag{1}$$

The first term $a - a\varepsilon$ is annihilated if multiplied on the right by ε; the second term reproduces itself under this multiplication by ε. The first terms form a submodule $\mathfrak{M}_0$ of $\mathfrak{M}$ which is annihilated by ε and therefore by every element $\varepsilon\lambda$ of K; the second terms $a\varepsilon$ form a submodule $\mathfrak{M}_1$ which has ε as a unity operator. These two submodules have only the zero in common; for, zero is the only element which can be annihilated and reproduced at the same time. Furthermore, the representation (1) shows that $\mathfrak{M}$ is the direct sum $\mathfrak{M}_0 + \mathfrak{M}_1$. Hence, if we split from $\mathfrak{M}$ the uninteresting part $\mathfrak{M}_0$, we will be left with a module which has ε as a unity operator. *From now on we will assume that the identity of* K *is also a unity operator for* $\mathfrak{M}$: $a\varepsilon = a$ for every a, and this identity will henceforth be denoted by 1.

The module $\mathfrak{M}$ is said to be *finite* (over K) if its elements may be represented linearly in the form

$$u_1\lambda_1 + \cdots + u_n\lambda_n$$

by means of a finite number of elements $u_1, \ldots, u_n$. In this case we write

$$\mathfrak{M} = (u_1\mathsf{K}, \ldots, u_n\mathsf{K}) \text{ or } \mathfrak{M} = (u_1, \ldots, u_n).$$

If we further assume that the u_i are *linearly independent*: that is, $\sum u_i\alpha_i = 0$ implies $\alpha_i = 0$, then $\mathfrak{M}$ is called an (*n-termed*) *module of linear forms* or an *n-dimensional vector space* (cf. Section 14).

K is said to be the *coefficient domain;* the u_j form a system of *basis elements.* By the linear independence of the u_j every element of $\mathfrak{M}$ is *uniquely* expressible as a linear form $\sum u_j\lambda_j$; for, if $\sum u_j\lambda_j = \sum u_j\mu_j$, then

$$\sum u_j(\lambda_j - \mu_j) = 0, \quad \text{so that } \lambda_j - \mu_j = 0 \quad \text{or} \quad \lambda_j = \mu_j.$$

The uniquely defined ring elements $\lambda_1, \ldots, \lambda_n$ are called the *components* of the vector $a = \sum u_j\lambda_j$.

Two modules of linear forms which have the same coefficient domain K *and the same number of basis elements are operator isomorphic.* Thus, we may map every basis element u_j of one module on a basis element v_j of the other module and the linear form $\sum u_j\lambda_j$ on the linear form $\sum v_j\lambda_j$.

An operator homomorphism which maps a module of linear forms $\mathfrak{M} = (u_1, \ldots, u_m)$ into a module of linear forms $\mathfrak{N} = (v_1, \ldots, v_n)$ is said to be a *linear mapping* or *linear transformation.* The mapping is completely determined when the image element of every basis element u_j

$$u_j' = \sum_1^n v_i\alpha_{ij} \qquad (j = 1, \ldots, m) \tag{2}$$

is given, therefore when the *matrix*

$$A = (\alpha_{ij}) = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1m} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nm} \end{pmatrix}$$

is given.[2] Thus, the image of $a = \sum u_j \lambda_j$ is $a' = \sum u'_j \lambda_j$. Under changes of the basis $(u_1, \ldots, u_m)$ or $(v_1, \ldots, v_n)$ one and the same linear transformation may be represented by different matrices (cf. Exercise 6. that follows). In spite of this we often denote a linear transformation by the same symbol A which denotes the associated matrix.

The image of an element u of $\mathfrak{M}$ under the mapping determined by the matrix A is denoted by Au. Hence in the case (2):

$$Au_j = \sum v_i \alpha_{ij}.$$

In general, the matrix A is "rectangular"; it is square only when $m = n$, for instance, in the case of a linear mapping of $\mathfrak{M}$ into itself.

The combination of the mapping of $\mathfrak{M} = (u_1, \ldots, u_m)$ into $\mathfrak{N} = (v_1, \ldots, v_n)$ with associated matrix A followed by the mapping of $\mathfrak{N}$ into $\mathfrak{P} = (w_1, \ldots, w_p)$ determined by a matrix B leads to

$$B(Au_j) = B\Big(\sum_i v_i \alpha_{ij}\Big) = \sum_i (Bv_i)\,\alpha_{ij} = \sum_h \sum_i w_h \beta_{hi} \alpha_{ij},$$

therefore to the *matrix product* $C = BA$ defined by

$$\gamma_{hj} = \sum_i \beta_{hi} \alpha_{ij}.$$

Hence for $u \in \mathfrak{M}$ we have

$$BA \cdot u = B \cdot Au.$$

The product AB has a sense only if the number of columns of A is equal to the number of rows of B. If this is the case, the matrix product represents, by the preceding remarks, exactly the product AB of the associated mappings.

The *sum* of two linear mappings of $\mathfrak{M}$ into $\mathfrak{N}$ is defined by

$$(A + B)u = Au + Bu;$$

the associated matrix has the elements $\alpha_{ik} + \beta_{ik}$ and is called the *sum of the matrices* A and B; it has a sense when A and B have the same number of rows and the same number of columns.

From the definitions of sum and product we have the following rules (which are valid only if the sums and products that appear have a sense):

$$A \cdot BC = AB \cdot C,$$

$$A + (B + C) = (A + B) + C,$$

[2] In forming equations (2) from the matrix A it should be noted that according to our notation the m equations (2) correspond to the m columns of A; the elements of a column (reading from top to bottom) are the coefficients of an equation (2).

$$A(B + C) = AB + AC,$$
$$(B + C)A = BA + CA.$$

With the help of the matrices $(u_1 \dots u_m)$, $(v_1 \dots v_n)$, etc. consisting of a single row we may write the system of equations (2) in the matrix form:

$$(u'_1 \dots u'_m) = (v_1 \dots v_n) \cdot A.$$

Accordingly a linear form $\sum u_i \lambda_i$ may be written as the product of a *row* $(u_1 \dots u_m)$ by a *column* $\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix}$. The linear form $\sum u_j \lambda_j$ is transformed by the linear mapping A into

$$\sum A u_j \lambda_j = \sum\sum v_i \alpha_{ij} \lambda_j;$$

the coefficients or components of the transformed form are

$$\lambda'_i = \sum \alpha_{ij} \lambda_j.$$

We may write this formula also as a matrix equation:

$$\begin{pmatrix} \lambda'_1 \\ \vdots \\ \lambda'_n \end{pmatrix} = A \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix}.$$

A mapping of $\mathfrak{M} = (u_1, \dots, u_n)$ into itself is given by a square matrix:

$$u'_j = \sum u_i \alpha_{ij}. \tag{3}$$

As seen above the square matrices form a ring; this ring may be regarded as a (left-) operator domain of the vector space.

It may happen that the u'_j, defined by (3), again form a basis for $\mathfrak{M}$. A necessary condition for this is, *first*, that they be linearly independent; that is, if

$$\sum u'_j \mu_j = 0 \quad \text{or} \quad \sum_i \sum_j u_i \alpha_{ij} \mu_j = 0$$

or finally $\sum_j \alpha_{ij} \mu_j = 0$, then $\mu_j = 0$; in other words, between the columns

$$\begin{pmatrix} \alpha_{11} \\ \vdots \\ \alpha_{n1} \end{pmatrix}, \quad \begin{pmatrix} \alpha_{12} \\ \vdots \\ \alpha_{n2} \end{pmatrix}, \dots$$

no linear relation exists unless all coefficients μ_j are equal to zero. This may be stated in still an other way: the matrix A shall be annihilated on the right by no column $\begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$ distinct from zero. This statement implies that A shall be annihilated by no multi-columned matrix $B + 0$ (that is, $AB + 0$ if $B + 0$), and we may say that A is *not a left zero divisor*. *Secondly*, it is also necessary that conversely all u_i be expressible in terms of the u'_i:

(4) $$u_k = \sum u'_j \beta_{jk}.$$

This means that if the formula (3) is substituted in (4), the identity relation

$$u_k = \sum u_i \alpha_{ij} \beta_{jk}$$

must follow, i.e., the product $A \cdot B$ must be the *identity matrix*

$$E = \begin{pmatrix} \varepsilon & & 0 \\ & \varepsilon & \\ & \ddots & \\ 0 & & \varepsilon \end{pmatrix}:$$

$AB = E$. We have therefore proved:

(3) *represents a new basis if and only if the matrix A is not a left zero divisor and possesses a right inverse B.*

If these conditions are satisfied, the relation between the basis u, u', and therefore also that between the matrices A, B, is reversible; that is, it is also true that

$$BA = E.$$

Furthermore, it follows that A is also not a right zero divisor. Thus, if the product SA were equal to zero for a row $S \neq 0$, it would follow that

$$0 = SAB = SE = S \neq 0.$$

Finally, the fact that A is not a left zero divisor implies that A can possess only *one* right inverse.

Hence we may denote the unique right (and left) inverse matrix, which was called B up to now, by A^{-1}. We say that a matrix A which satisfies the indicated conditions *is invertible in* K, and summarize the above statements:

The transition to a new basis requires an invertible matrix.

Another interpretation of the linear transformations may be obtained if we think of the quantities $u_1, \ldots, u_n$ as indeterminates in a polynomial domain $\mathsf{K}[u_1, \ldots, u_n]$. The formulae (3), (4) then indicate a *linear substitution* by which we introduce a new indeterminate u' in the polynomial domain. By the substitution (4) every form $f(u_1, \ldots, u_n)$ goes over to a form $f'(u'_1, \ldots, u'_n)$, in particular a linear form $\sum u_k \lambda_k$ to a linear form:

$$\sum u_k \lambda_k = \sum \sum u'_j \beta_{jk} \lambda_k = \sum u'_j \lambda'_j,$$

where the new coefficients are given by

(5) $$\lambda'_j = \sum_k \beta_{jk} \lambda_k.$$

On the other hand if we give to the variables u_i special values μ_i from the field K and form by (3)

(6) $$\mu'_k = \sum \mu_j \alpha_{jk},$$

this is also a linear transformation in a vector space or module of linear forms (whose operator domain must this time be written on the *left* because the coefficients of the transformation stand on the *right* of the vector components), whose matrix is the reflected or transposed[3] matrix A^T of A.

[3] Transposing means to interchange the rows and columns or rotate about the principal diagonal.

The two transformations (5), (6) are united to one another by the condition that the sum $\sum \mu_k \lambda_k$ remain invariant:

$$\sum \mu_k \lambda_k = \sum \mu'_k \lambda'_k,$$

and are said to be *contragredient to one another.* The matrix A^T of (6) is the transpose inverse or the inverse transpose of the matrix B of (5):

$$A^T = (B^{-1})^T = (B^T)^{-1}.$$

EXERCISES. 1. If a square matrix has a right and a left inverse, it is invertible (hence the two inverses are equal and unique).

2. The invertible n-rowed matrices in a ring K with an identity form a group: the *full linear group* $GL(n, \mathsf{K})$ or the automorphism group of an n-termed module of linear forms.

3. All n-rowed square matrices in K form a ring, the *complete matrix ring* in K or the endomorphism ring of an n-termed module of linear forms. This ring has a linearly independent basis with respect to K which consists of the matrices C_{ij} that have a 1 at the intersection of the i-th row and j-th column and zero everywhere else.

4. If a linear mapping of $\mathfrak{M} = (u_1, \ldots, u_n)$ in $\mathfrak{N} = (v_1, \ldots, v_n)$ is represented by the matrix A and if we introduce a new basis by

$$(u'_1 \ldots u'_n) = (u_1 \ldots u_n) P,$$

$$(v'_1 \ldots v'_n) = (v_1 \ldots v_n) Q,$$

then the same transformation, referred to the new basis, is represented by the matrix

$$A' = Q^{-1} A P.$$

5. If a matrix A of n rows and m columns is divided arbitrarily into rectangular "small blocks" such as:

$$A = \left(\begin{array}{c|c|c} \alpha_{11} \cdots & \alpha_{1i} \cdots & \alpha_{1j} \cdots \alpha_{1m} \\ \vdots & & \vdots \\ \hline \alpha_{k1} & & \vdots \\ \vdots & & \vdots \\ \hline \alpha_{n1} \cdots & \cdots & \cdots \alpha_{nm} \end{array}\right) = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \end{pmatrix},$$

and if a matrix B of m rows and q columns is also divided so that the position of the horizontal cuts in B coincide with the position $(1, i, j)$ of the vertical cuts of A:

$$B = \left(\begin{array}{c|c|c} \beta_{11} \cdots & \beta_{1k} \cdots & \cdots \beta_{1q} \\ \vdots & & \vdots \\ \hline \beta_{i1} & & \vdots \\ \vdots & & \vdots \\ \hline \beta_{j1} & & \vdots \\ \vdots & & \vdots \\ \beta_{m1} \cdots & \cdots & \cdots \beta_{mq} \end{array}\right) = \begin{pmatrix} B_{11} & B_{12} & B_{13} \\ B_{21} & B_{22} & B_{23} \\ B_{31} & B_{32} & B_{33} \end{pmatrix},$$

then we may carry out the multiplication of A and B as if the small blocks A_{ij}, B_{ik} were elements:

$$AB = \begin{pmatrix} \sum A_{1j}B_{j1} & \sum A_{1j}B_{j2} & \sum A_{1j}B_{j3} \\ \sum A_{2j}B_{j1} & \sum A_{2j}B_{j2} & \sum A_{2j}B_{j3} \end{pmatrix}.$$

107. MODULES WITH RESPECT TO A SKEW FIELD. LINEAR EQUATIONS

We now assume that K is a skew field, the module $\mathfrak{M}$ is finite, and the identity is a unity operator. If the basis elements $u_1, \ldots, u_n$ are linearly dependent: $\sum u_i \lambda_i = 0$, where, let us say, $\lambda_n \neq 0$, we may multiply the equation by λ_n^{-1} and express u_n linearly in terms of the remaining basis elements. Hence $u_1, \ldots, u_{n-1}$ also form a basis. Continuing thus, we finally arrive at a linearly independent basis. Hence every finite module under consideration is a module of linear forms.

A module distinct from the null module is called (as in the case of ordinary Abelian groups) *simple* if it has no proper submodules except for the null module. We have the theorem: *a simple* K*-module is* 1*-termed, and a* 1*-termed* K*-module is simple.*

PROOF. 1. Let $\mathfrak{M}$ be simple. Then every element $u \neq 0$ must generate the entire module. Hence $\mathfrak{M}$ is 1-termed.

2. Let $\mathfrak{M}$ be 1-termed: $\mathfrak{M} = (u)$. If $\mathfrak{N} \neq (0)$ is a submodule and $u\lambda$ is an element of $\mathfrak{N}$ distinct from zero, then $\mathfrak{N}$ also contains $u\lambda\lambda^{-1} = u$; consequently $\mathfrak{M} = \mathfrak{N}$. Hence $\mathfrak{M}$ is simple.

An n-termed module is a direct sum of simple modules $(u_1) = u_1\mathsf{K}, \ldots, (u_n) = u_n\mathsf{K}$. The submodules $(u_1, \ldots, u_n), (u_1, \ldots, u_{n-1}), \ldots, (u_1), (0)$ form a series with 1-termed, and so simple. factor modules and therefore a *composition series. Hence the number n, if the module is n-termed, is equal to the length of the composition series and therefore independent of the choice of the basis.*

The number of basis elements of a K-module is also said to be *the (linear) rank of the module with respect to* K.

In Section 33 we arrived at the uniqueness of the linear rank in another way. The earlier result, that every basis of a submodule may be expanded to a basis of the entire module, is nothing else but the group-theoretic law that every submodule appears in a composition series. The continuation of a basis of a submodule to a basis of $\mathfrak{M}$ may be accomplished by choosing the omitted basis elements from the u_j (that is, from a basis of $\mathfrak{M}$ given beforehand); by Section 47 this follows from the fact that the module $\mathfrak{M}$ is the direct sum of simple modules of rank one. This statement is also the Replacement Theorem of Section 33; therefore this theorem has now been derived by group-theoretic methods.

A proper submodule of $\mathfrak{M}$ has a composition series of smaller length, and therefore it has a smaller rank. Hence we have: *any n linearly independent elements* $v_k = \sum u_i \alpha_{ik}$ *of* $\mathfrak{M}$ *generate* $\mathfrak{M}$ *itself,* since they can generate no proper submodule. The assumption of linear independence implies that the matrix A is not a left zero divisor; the conclusion that the v form a new basis for $\mathfrak{M}$ proves however that the matrix is invertible. Hence, *if a square matrix in a field* K *is not a left zero divisor, then it is invertible.* In this case the matrix is said to be *regular*; however, if it is a left zero divisor (therefore not invertible and so a right zero divisor), we call it *singular.* These designations are applicable to matrices in a domain of integrity $\mathfrak{R}$, since such a system may always be imbedded in a field. Regular matrices need not be invertible in the domain of integrity $\mathfrak{R}$; however in the quotient field K they are invertible. Singular matrices are not only zero divisors in the field, but also in the ring; for, we may always make a column, which annihilates a matrix, integral on multiplying by a common denominator.

The *theory of linear equations* rests on the Replacement Theorem. A system of linear equations may be given as

$$l_i(\xi) = \beta_i, \tag{1}$$

where the l_i are m linear forms in the n unknowns ξ_k :

$$l_i(\xi) = \sum \alpha_{ik} \xi_k .^4$$

If we replace the ξ_k by indeterminates x_k, then the l_i become linear forms in these indeterminates:

$$l_i = \sum \alpha_{ik} x_k . \tag{2}$$

The number r of linearly independent linear forms l_i is said to be the *rank* of the system of equations. Obviously, the system of equations has a solution only if all linear relations $\sum \mu_i l_i = 0$, which (identically in the indeterminates x) exist between the linear forms l_i, also exist between the right-hand members β_i. If this is the case and all l_i are dependent, let us say, on $l_1, \ldots, l_r$, then all equations (1) are consequences of the first r among them. We must have $r \leqq n$ since there can be no more than n linearly independent linear forms in $x_1, \ldots, x_n$. By the Replacement Theorem we may supplement the $l_1, \ldots, l_r$ with $n - r$ of the indeterminates x_i, say $x_{r+1}, \ldots, x_n$, in order to obtain a basis for all linear forms of the x. This means that

$$x_i = \sum_{r+1}^{n} \gamma_{ij} x_j + \sum_{1}^{r} \delta_{ik} l_k \qquad (i = 1, \ldots, r). \tag{3}$$

THEOREM. *All solutions of the equations* (1) *are found by first replacing in* (3) *the* l_i *by* β_i *and the* $x_{r+1}, \ldots, x_n$ *by entirely arbitrary elements* $\xi_{r+1}, .$

[4] The indeterminates are written for the moment on the right of the coefficients which naturally does not matter for the application of the module theorems.

. . ., ξ_n in K *and then determining the values* $\xi_1, \ldots, \xi_r$ *of* $x_1, \ldots, x_r$ *by* (3).

For the proof we note that the $l_1, \ldots, l_r, x_{r+1}, \ldots, x_n$ form a linearly independent basis for the module $(x_1, \ldots, x_n)$. Hence, if we substitute (3) in (2), an identity relation in the $l_1, \ldots, l_r, x_{r+1}, \ldots, x_n$ must appear which must remain valid when we replace the l_i by β_i and the x_j by arbitrary ξ_j. Hence the ξ, thus found, are solutions of (1). Similarly, if we substitute (2) in (3), an identity relation in the x must appear which remains valid when the x are replaced by those ξ which satisfy (1). Hence all solutions of (1) may be obtained by the indicated rule.

It follows that the criterion for solvability given above is also sufficient and that the rank of the system of equations is equal to the number of unknowns for which we can solve after the values of the remaining unknowns are arbitrarily chosen.

In the case of a commutative field K, the *theory of determinants* furnishes explicit solution formulae and algebraic criteria for the solvability and linear dependence of linear equations. For this we refer to the appropriate text-books. In particular we call attention to the following criterion for a matrix to be regular which is valid in this theory: *a square matrix A is regular in a commutative field or domain of integrity if its determinant* $|A|$ *is distinct from zero.* Moreover, if the determinant is a unit of the domain of integrity, then the matrix is also invertible in the domain of integrity; for in the solution formulae the determinant occurs only in the denominator.

The converse of this theorem follows when we apply the multiplication law of determinants:

$$|AB| = |A| \cdot |B|$$

to the case $AB = E$, $|E| = 1$. Therefore: *in a domain of integrity a matrix is invertible if and only if its determinant is a unit* (unimodular matrices).

EXERCISES. 1. A system of homogeneous equations $\sum \alpha_{ik} \xi_k = 0$ always has a solution in a field and all solutions $\{\xi_1, \ldots, \xi_n\}$, considered as vectors, are themselves linear combinations (with coefficients which are written on the right of the vectors) of $n - r$ particular linearly independent solutions. For $r = n$ only the null solution exists.

2. Between the ranks n, m of a K-module and a submodule, and the rank f of the factor module (residue classes) there exists the relation $f = n - m$.

3. Between the ranks n, m of two submodules of a K-module, the rank s of their sum, and the rank d of their intersection there exists the relation

$$s + d = n + m.$$

THE PROJECTIVE SPACE. The submodules of rank one of an n-termed module of linear forms or vectors are designated as *lines* of the vector space $R_n(K)$ or as *points* of the projective $(n-1)$-dimensional space $S_{n-1}(K)$. The components (determined except for a factor of proportionality) of a generated vector are called the *homogeneous coordinates* of the point. The

lines of a submodule form a *linear subspace* in the projective space. By Exercise 1. it now follows that r independent linear homogeneous equations in the coordinates determine a subspace of dimension $n - r - 1$. Furthermore, since the intersection of submodules is again a submodule, it follows that the intersection of linear spaces is again a linear space (or empty). Finally, by Exercise 3. it follows that between the dimensions l,m of two linear subspaces, the dimension d of their intersection, and the dimension s of the smallest linear space including both there exists the relation

$$d + s = l + m$$

(with $d = -1$ if the intersection is empty).

108. MODULES IN EUCLIDEAN RINGS. ELEMENTARY DIVISORS

We now assume that the ring K is commutative and Euclidean in the sense of Section 18. Hence every ring element $a \neq 0$ is associated with an "absolute value" $g(a)$ such that $g(ab) \geqq g(a)$, and a division process is possible. By Section 18 every ideal in K is also a principal ideal. We now prove the

THEOREM. *Let $\mathfrak{M}$ be a module of linear forms with respect to K which has the linearly independent basis $(u_1, \ldots, u_n)$. Then every submodule $\mathfrak{N}$ of $\mathfrak{M}$ is again a module of linear forms with at most n basis elements.*

PROOF. For the null module $\mathfrak{M} = (0)$ the theorem is trivial. Let us assume that the theorem has been proved for $(n-1)$-termed modules $\mathfrak{M}$.

If $\mathfrak{N}$ only contains linear forms in $u_1, \ldots, u_{n-1}$, the theorem is true by the induction hypothesis. However, if $\mathfrak{N}$ contains a linear form $u_1\lambda_1 + \cdots + u_n\lambda_n$ with $\lambda_n \neq 0$, the totality of the λ_n, which occur, is a right ideal in K, and therefore a principal ideal (μ_n) with $\mu_n \neq 0$. Hence there exists in $\mathfrak{N}$ a form $l = u_1\mu_1 + \cdots + u_n\mu_n$ such that if a multiple $l\alpha$ of l is subtracted from any other form $u_1\lambda_1 + \cdots + u_n\lambda_n$ the last coefficient λ_n will vanish. The linear forms in $u_1, \ldots, u_{n-1}$, that remain after the subtraction, belong to $\mathfrak{N}$ and form a submodule which by the induction hypothesis has a linearly independent basis $(l_1, \ldots, l_{m-1})$, $m - 1 \leqq n - 1$. It obviously follows that $l_1, \ldots, l_{m-1}, l$ generate $\mathfrak{N}$.

The $l_1, \ldots, l_{m-1}$ are linearly independent since they were so chosen. If a linear dependence

$$l_1\beta_1 + \cdots + l_{m-1}\beta_{m-1} + l\beta = 0$$

were given with $\beta \neq 0$, on equating the coefficients of u_n we would obtain $\mu_n\beta = 0$ which is not true.

REMARK. The linear independence of the $l_1, \ldots, l_m (l_m = l)$ rests on the fact that every l_i contains, by construction, a u_j which does not occur in l_1 up to l_{i-1}.

EXERCISES. 1. If $\mathfrak{M}$ is a module of linear forms with integer coefficients

and if the submodule $\mathfrak{N}$ is generated by a finite number of linear forms $v_k = \sum u_i \alpha_{ik}$, then a basis $(l_1, \ldots, l_m)$ may be constructed with the above properties in a finite number of steps.

2. Using the basis $(l_1, \ldots, l_m)$ constructed in Exercise 1. deduce a method for determining whether a particular linear form $\beta_1 u_1 + \ldots + \beta_n u_n$ is contained in the module $\mathfrak{N}$; in other words, whether the linear diophantine system of equations

$$\sum \alpha_{ik} \xi_k = \beta_i$$

has a solution in terms of integers ξ_k.

ELEMENTARY DIVISOR THEOREM. *If $\mathfrak{N}$ is a submodule of the module of linear forms $\mathfrak{M}$, then there is a basis $(u_1, \ldots, u_n)$ of $\mathfrak{M}$ and a basis $(v_1, \ldots, v_m)$ of $\mathfrak{N}$ such that*

$$\begin{cases} v_i = u_i \varepsilon_i & (i = 1, \ldots, m) \\ \varepsilon_{i+1} \equiv 0 (\varepsilon_i). \end{cases}$$

PROOF. We start first with an arbitrary basis $(u_1, \ldots, u_n)$ of $\mathfrak{M}$ and an arbitrary basis $(v_1, \ldots, v_m)$ of $\mathfrak{N}$. Let

$$v_k = \sum u_i \alpha_{ik} \quad \text{or} \quad (v_1 \ldots v_m) = (u_1 \ldots u_n) \cdot A .$$

By stepwise changes of the basis we will lead the matrix A into the desired diagonal form

$$(2) \qquad \begin{pmatrix} \varepsilon_1 & & & 0 \\ & \varepsilon_2 & & \\ 0 & & & \\ \cdot & & & \\ \cdot & & & \varepsilon_m \\ 0 & \ldots & \ldots & 0 \end{pmatrix}.$$

The permitted changes are as follows:

1. Interchange of two u or v; this means that two rows or two columns of A are interchanged.

2. Replacement of a u_i by $u_i + u_j \lambda (j \neq i)$; this means that we must subtract from the j-th row of A the i-th row multiplied on the left by λ :

$$v_k = \sum u_i \alpha_{ik} = \cdots + (u_i + u_j \lambda) \alpha_{ik} + \cdots + u_j (\alpha_{jk} - \lambda \alpha_{ik}) + \cdots .$$

3. Replacement of a v_k by $v_k - v_j \lambda (j \neq k)$; this means that we must subtract from the k-th column of A the j-th column multiplied on the right by λ :

$$v_k - v_j \lambda = \sum u_i (\alpha_{ik} - \alpha_{ij} \lambda) .$$

By means of 1., 2., 3. transform the matrix A until *the element of A distinct from zero with the smallest absolute value has an absolute value as small as possible.* By 1. bring this smallest element to the position α_{11}. By 2. make the remaining elements of the first column as small as possible by subtracting suitable multiples of the first row; their absolute values become smaller than $|\alpha_{11}|$, and therefore

are zero. Similarly, by 3. make the elements of the first row equal to zero without altering the first column. After these operations are performed every element of the matrix must be divisible by α_{11}. For let us assume that there is an element, say α_{ik}, which is not divisible by α_{11}. Then by the division algorithm

$$\alpha_{ik} = \alpha_{11} q + r, \quad r \neq 0, \quad g(r) < g(\alpha_{11}).$$

Now by 2. add the first row to the i-th, and by 3. subtract the first column multiplied by q from the k-th. Thereby the element r, with $g(r) < g(\alpha_{11})$, appears in the position (ik). This contradicts the minimal assumption regarding α_{11}.

Hence our matrix has been transformed to a matrix

$$\begin{pmatrix} \alpha_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix},$$

where all elements of A' are multiples of α_{11}. Now, by operations which leave the first row and column unchanged, transform A' as in the case of A. Thereby the divisibility of all elements by α_{11} is not lost and A' becomes a matrix

$$\begin{pmatrix} \alpha_{22} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A'' & \\ 0 & & & \end{pmatrix},$$

where all elements of A'' are divisible by α_{22}. Continuing thus, the desired normal form (2) is obtained after m steps. We note that no one of the matrices A, A', A'', ... can consist only of zeros; for otherwise one of the v_k would equal zero which contradicts the fact that the v form a linearly independent basis for $\mathfrak{R}$ at every stage of the process. This completes the proof of the theorem.

REMARKS. 1. The operations 1. to 3. imply that the matrix A may be multiplied on the left or on the right by a matrix invertible in K. For, if $(u'_1 \dots u'_n) = (u_1 \dots u_n) \cdot B$ and $(v'_1 \dots v'_m) = (v_1 \dots v_m) \cdot C$ are introduced as new bases, then

$$(v'_1 \dots v'_m) = (v_1 \dots v_m) C = (u_1 \dots u_n) A C = (u'_1 \dots u'_n) B^{-1} A C.$$

Hence the Elementary Divisor Theorem implies the existence of two invertible matrices B, C such that $B^{-1} A C$ is a matrix of the form (2).

2. The method employed above may also be used to reduce a matrix A even though the v do not form a linearly independent system; in this case one of the matrices A, A', A'', ... becomes a null matrix and instead of the normal form (2) the more general form

$$B^{-1}AC = \begin{pmatrix} \varepsilon_1 & & 0 \\ & \ddots & \\ & & \varepsilon_r \\ 0 & & 0 \end{pmatrix} \tag{3}$$

is obtained, where r is the rank of A. The divisibility relations of the ε_i remain the same.

3. The k-rowed subdeterminants of the transformed matrix $D = B^{-1}AC$ are known linear functions of the subdeterminants of A, and similarly those of $A = BDC^{-1}$ are linear functions of those of D. Hence the greatest common divisor δ_k of the k-rowed subdeterminants of A is the same as that of D except for a unit. In the case of D we may easily compute the value

$$\delta_k = \varepsilon_1 \varepsilon_2 \cdots \varepsilon_k \qquad (k \leqq r).$$

Hence

$$\delta_k = \delta_{k-1}\varepsilon_k \qquad (1 < k \leqq r). \tag{4}$$

The δ_k are called the *determinantal divisors* of the matrix A, the ε_k the *elementary divisors* of the matrix A. From (4) it now follows: *the elementary divisors are the quotients of two successive determinantal divisors.*

4. The elementary divisors ε_k are uniquely determined by the matrix A except for units. This will be seen in another way in the next section where it will be shown that the elementary divisors (in so far as they are not units) depend only on the factor module $\mathfrak{M}/\mathfrak{N}$, which in turn is naturally determined by A.

EXERCISES. 3. Transform the matrix

$$A = \begin{pmatrix} 4 & 3 & 6 & 2 \\ 2 & 3 & 6 & 4 \\ 6 & 6 & 13 & 5 \end{pmatrix}$$

into the diagonal form (3).

4. Every linear diophantine system of equations

$$\sum_1^n \alpha_{ik}\xi_k = \beta_i \qquad (i = 1, \ldots, m) \tag{5}$$

with integer coefficients α_{ik} and β_i may be transformed by unimodular transformation of the unknowns and the equations to the form

$$\begin{cases} \varepsilon_i \eta_i = \gamma_i & (i = 1, \ldots r;\ \varepsilon_i \neq 0) \\ 0 = \delta_j & (j = r+1, \ldots, m). \end{cases}$$

The conditions for solvability in terms of integers are given by:

$$\gamma_i \equiv 0 (\varepsilon_i); \quad \delta_j = 0.$$

The η_i with $i \leqq r$ are determinable, the remaining η_j are arbitrary. The ξ_k are linear functions of the arbitrary η_j with integer coefficients.

5. A linear system of equations (5) has a solution in terms of integers if and only if the validity of

$$\sum_1^m \lambda_i \alpha_{ik} \equiv 0 (d) \qquad (k = 1, \ldots, n)$$

for arbitrary integers λ_i and d always implies

$$\sum_1^m \lambda_i \beta_i \equiv 0 (d).$$

109. THE FUNDAMENTAL THEOREM OF ABELIAN GROUPS

Let $\mathfrak{G}$ be an additive Abelian group with a finite number of generators, namely a module. If a multiplicative domain K is given for $\mathfrak{G}$, we assume that K has an identity which is also a unity operator (cf. Section 106); however, if no multiplicative domain is given, we take the ring of integers as the multiplicative domain which always satisfies this assumption. We will write the operators on the left of the module elements.

First let $\mathfrak{G}$ be cyclic: $\mathfrak{G} = (g)$. The totality of the μ in K, which annihilate g, is a left ideal $\mathfrak{a}$ of K: if $\mu_1 g = 0$ and $\mu_2 g = 0$ then $(\mu_1 - \mu_2) g = 0$; and if $\mu g = 0$, then $\varkappa \mu g = 0$ for every $\varkappa$ in K. Every λ of K corresponds to a λg , and since

$$(\lambda + \mu) g = \lambda g + \mu g,$$
$$\lambda \mu \cdot g = \lambda \cdot \mu g,$$

the correspondence is an operator homomorphism with respect to K. This implies by the Isomorphism Theorem:

$$\mathfrak{G} \cong \mathsf{K}/\mathfrak{a},$$

or: *a cyclic* K*-module* $\mathfrak{G}$ *is isomorphic to the residue class module of* K *modulo the annihilating left ideal of* $\mathfrak{G}$.

In the case of an ordinary cyclic group $\mathfrak{G}$ we thereby obtain, from a new point of view, the result that $\mathfrak{G}$ is isomorphic to the additive group of integers or to the group of residue classes modulo an integer. If $n > 0$ is the basis element of the ideal $\mathfrak{a}$, then n is the order of the cyclic group (g) or also the order of the element g (cf. Section 7).

The theorem just proved is valid independently of the special assumptions on K. However, if K is commutative and Euclidean, as we shall assume in the following, then we may say much more. In this case the ideal $\mathfrak{a}$ is a principal ideal: $\mathfrak{a} = (\alpha)$. We assume that $\alpha \neq 0$ and factor, if possible, α into two relatively prime factors:

$$\alpha = \varrho\sigma,$$
$$1 = \lambda\varrho + \mu\sigma,$$

and form the cyclic groups $\mathfrak{G}_1 = (\varrho g)$, $\mathfrak{G}_2 = (\sigma g)$. Then $\mathfrak{G}_1$ is annihilated by σ and $\mathfrak{G}_2$ by ϱ. Since

$$g = \lambda\varrho g + \mu\sigma g,$$

$\mathfrak{G}$ is the sum of $\mathfrak{G}_1$ and $\mathfrak{G}_2$. The intersection $\mathfrak{G}_1 \cap \mathfrak{G}_2$ is annihilated by ϱ and by σ, therefore also by $1 = \lambda\sigma + \mu\sigma$ Hence $\mathfrak{G}_1 \cap \mathfrak{G}_2 = (0)$ and the sum is direct:

$$\mathfrak{G} = \mathfrak{G}_1 + \mathfrak{G}_2.$$

If σ or ϱ are again factorable into relatively prime factors, $\mathfrak{G}_1$ or $\mathfrak{G}_2$ may be further decomposed. *Finally, the cyclic group $\mathfrak{G}$ becomes a direct sum of cyclic groups which are annihilated by powers of prime numbers.*[5] *The product of these powers of prime numbers is* α. For groups of this kind we will use the terminology "*prime-power groups.*"

We now go over to the general case, where $\mathfrak{G}$ is a K-module with a finite number of generators $g_1, \ldots, g_n$ and therefore the elements of $\mathfrak{G}$ have the form

$$\lambda_1 g_1 + \cdots + \lambda_n g_n$$

Let $u_1, \ldots, u_n$ be indeterminates and

$$\mathfrak{M} = (u_1, \ldots, u_n)$$

a module of linear forms in these indeterminates. Then every linear form $\sum \lambda_i u_i$ of $\mathfrak{M}$ corresponds to an element $\sum \lambda_i g_i$ of $\mathfrak{G}$; this correspondence is a module homomorphism, and by the Homomorphism Theorem

$$\mathfrak{G} \simeq \mathfrak{M}/\mathfrak{N},$$

where $\mathfrak{N}$ is the submodule of those linear forms $\sum \lambda_i u_i$ for which $\sum \lambda_i g_i = 0$.

As before, let K be a Euclidean field. By Section 108 we can introduce new bases $(v_1, \ldots, v_m)$ and $(u'_1, \ldots, u'_n)$ $(n \geqq m)$ for $\mathfrak{N}$ and $\mathfrak{M}$ such that

$$v_i = \varepsilon_i u'_i \qquad \text{for } i = 1, \ldots, m,$$
$$\varepsilon_{i+1} \equiv 0 (\varepsilon_i).$$

There are elements $h_1, \ldots, h_n$ of $\mathfrak{G}$ (by the above homomorphism) that correspond to the u'. All elements of $\mathfrak{G}$ have the form $\mu_1 h_1 + \cdots + \mu_n h_n$, and such an element is zero if and only if

$$\mu_1 u'_1 + \cdots + \mu_n u'_n \equiv 0 (v_1, \ldots, v_m),$$

that is, if

[5] "Prime number" is short for "prime element of the ring K." In the case of the ordinary Abelian group, it refers to the ordinary prime numbers.

$$\begin{cases} \mu_1 \equiv 0(\varepsilon_1), \\ \cdots\cdots\cdots \\ \mu_m \equiv 0(\varepsilon_m), \end{cases} \qquad \begin{cases} \mu_{m+1} = 0, \\ \cdots\cdots\cdots \\ \mu_n = 0 \end{cases}.$$

Hence a sum $\mu_1 h_1 + \cdots + \mu_n h_n$ is zero only if the individual terms are zero; this means that the coefficients μ_i are divisible by ε_i for $i = 1, \ldots, m$ and zero for $i = m+1, \ldots, n$.

This may also be expressed as follows:

The group $\mathfrak{G}$ *is the direct sum of cyclic groups* $(h_1) + \cdots + (h_n)$, *and the annihilating ideal of* (h_i) *is*

$$(\varepsilon_i) \quad \textit{for} \quad i = 1, \ldots, m,$$
$$(0) \quad \textit{for} \quad i = m+1, \ldots, n.$$

This is the *Fundamental Theorem of Abelian Groups with a finite number of generators.*

In the case of the ordinary Abelian groups the orders of the cyclic groups $(h_1), \ldots, (h_m)$ are the $|\varepsilon_i|$, while the remaining $(h_{m+1}), \ldots, (h_n)$ have infinite orders.

Three supplements to the Fundamental Theorem are necessary:

a) the deletion of the units among the ε_i;

b) the further decomposition of the cyclic groups by prime-power groups;

c) the uniqueness.

a) Let us say ε_1 is a unit. Then (ε_1) is the unit ideal K and $\mathsf{K}h_1 = (0)$. Hence the cyclic group $\mathsf{K}h_1$ may be omitted from the sum decomposition $\mathsf{K}h_1 + \cdots + \mathsf{K}h_n$.

The annihilating ideals (ε_i), (0) which remain after the units are deleted may now be denoted by $\mathfrak{a}_1, \ldots, \mathfrak{a}_q$ *in the reverse order;* then

$$\mathfrak{a}_i \equiv 0(\mathfrak{a}_{i+1}).$$

b) Those groups (h_i), whose annihilating ideal is (0), are isomorphic to K; those, whose annihilating ideal is $(\varepsilon_i) \neq (0)$, may be further split into prime-power groups by the proof given above. The annihilating powers of prime numbers are found by factoring the ε_i. The sum of all groups occurring in the decomposition of $\mathfrak{G}$ which belong to a prime number p is a group $\mathfrak{B}_p$ and consists of those elements of $\mathfrak{G}$ which are annihilated by a sufficiently high power p^e. Therefore: *the groups* $\mathfrak{B}_p$ *are uniquely determined.* If $\mathfrak{U}$ designates the sum of the groups with $\mathfrak{a} = (0)$, then

$$\mathfrak{G} = \sum_p \mathfrak{B}_p + \mathfrak{U}.$$

By further decomposition of the $\mathfrak{B}_p$ we obtain conversely the prime-power groups; these are not determined absolutely uniquely but uniquely except for isomorphism,

as we shall see. There is however in every $\mathfrak{B}_p$ a uniquely determined series of subgroups $\mathfrak{B}_{p,\varrho}$; $\mathfrak{B}_{p,\varrho-1}$; ...; $\mathfrak{B}_{p,0}$, where $\mathfrak{B}_{p,\nu}$ consists of the elements of $\mathfrak{B}_p$ which are annihilated by p^ν. The first group of this series is $\mathfrak{B}_p$; the last consists only of the zero.

The group $\mathfrak{U}$ is not uniquely determined, but it is unique except for isomorphism since

$$\mathfrak{U} \cong \mathfrak{G}/\sum_p \mathfrak{B}_p .$$

c) UNIQUENESS THEOREM. *The annihilating ideals* $\mathfrak{a}_1, \ldots, \mathfrak{a}_q$ *with* $\mathfrak{a}_i \equiv 0(\mathfrak{a}_{i+1})$, *which appear in the direct decomposition* $\mathfrak{G} = \mathfrak{C}_1 + \cdots + \mathfrak{C}_q$, *are uniquely determined by the module* $\mathfrak{G}$ *alone.* (This amounts to saying: the groups $\mathfrak{C}_i$ are uniquely determined except for isomorphism.)

PROOF. The asserted uniqueness will be proved as soon as we have shown that for every power of a prime number p^σ of K we may uniquely determine how many of the ideals $\mathfrak{a}_i$ are divided by this power. Thus, if p^σ divides exactly k of these ideals, they must be the first k, that is, $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$, due to the divisibility relations existing between the ideals. Hence for every power of a prime number p^σ we know not only how many but also which $\mathfrak{a}_i$ are divided by the power; consequently, for every $\mathfrak{a}_i$, which powers of prime numbers divide the ideal. Those $\mathfrak{a}_i$ which are divisible by arbitrarily high powers, are zero, and the remaining are uniquely determined by their prime factor decomposition.

If p^σ divides the annihilating ideal of the cyclic group $\mathfrak{C}_i$, then

$$p^{\sigma-1}\mathfrak{C}_i/p^\sigma\mathfrak{C}_i$$

is a cyclic group with the annihilating ideal (p); therefore a simple group. On the contrary if p^σ does not divide this group, then $p^\sigma\mathfrak{C}_i = p^{\sigma-1}\mathfrak{C}_i$; therefore $p^{\sigma-1}\mathfrak{C}_i/p^\sigma\mathfrak{C}_i = (0)$. Hence $p^{\sigma-1}\mathfrak{G}/p^\sigma\mathfrak{G}$ is a direct sum of k simple groups, where k is the number of the $\mathfrak{a}_i$ divisible by p^σ. Consequently, k is equal to the length of the composition series for $p^{\sigma-1}\mathfrak{G}/p^\sigma\mathfrak{G}$ and so is uniquely determined.

EXERCISES. 1. For the above proof, fill in all the details of the last part.

2. The group $\mathfrak{U}$ constructed in b) is a module of linear forms with respect to the ring C of integers, and the number of its cyclic summands is equal to the rank of $\mathfrak{G}$ (rank = maximum number of linearly independent elements with respect to K).

3. Give a second uniqueness proof using the length of the composition series of the uniquely determined groups constructed in b) and its factor groups. Also the rank of the module $\mathfrak{U}$ (Exer. 2.) may be used.

In the special case of the finite Abelian groups (with the ring of integers as the multiplicative domain) the following direct proof of the Fundamental Theorem may be given by complete induction on the group order.

Let z_0 be an element of highest order. This element generates a cyclic group $\mathfrak{Z}_0$. By the induction hypothesis the factor group $\mathfrak{G}/\mathfrak{Z}_0$ is a direct sum of cyclic groups:

(1) $$\mathfrak{G}/\mathfrak{H}_0 = \bar{\mathfrak{H}}_1 + \cdots + \bar{\mathfrak{H}}_r .$$

$\mathfrak{H}_1$ is generated by a residue class $\bar{z}_1$ from which we choose a representative z_1. Let the annihilating number (order) of $\bar{z}_1$ be a_1. Then $a_1\bar{z}_1 = 0$, $a_1 z_1 \in \mathfrak{H}_0$ and, let us say, $a_1 z_1 \neq b z_0$. If we replace z_1 by $z_1 - q z_0$ (this element is contained in the residue class $\bar{z}_1$), then $a_1(z_1 - q z_0) = b z_0 - q a_1 z_0 = (b - q a_1) z_0$; therefore, we may always replace b by its smallest residue modulo a_1. Hence we assume that $|b| < |a_1|$. If n is the order of z_0, the order of z_1 is equal to $\frac{a_1 n}{(b, n)}$. This value is at most equal to $|n|$ since z_0 was chosen as an element of highest order:

$$\left|\frac{a_1 n}{(b, n)}\right| \leqq |n|$$

$$|a_1| \leqq |(b, n)| \leqq |b| \qquad \text{(in case } b \neq 0\text{)}.$$

However the relation $|a_1| \leqq |b|$ contradicts the assumption $|b| < |a_1|$. Hence $b = 0$. Consequently, $a_1 z_1 = 0$ and the order of z_1 is equal to that of $\bar{z}_1$. This is also valid for the elements $z_2, \ldots, z_r$ defined correspondingly. Due to (1) every element of $\mathfrak{G}$ is congruent modulo $\mathfrak{H}_0$ to a linear combination of the $z_1, \ldots, z_r$:

(2) $$g \equiv c_1 z_1 + \cdots + c_r z_r (\mathfrak{H}_0)$$

and the coefficients c_ν are uniquely determined modulo the orders $a_1, \ldots, a_r$ of $\bar{z}_1, \ldots, \bar{z}_r$ or $z_1, \ldots, z_r$. By (2) it follows that

$$g - (c_1 z_1 + \cdots + c_r z_r) = c_0 z_0 ,$$

where $c_0 z_0$ is uniquely determined. Hence $\mathfrak{G}$ is the direct sum of the cyclic groups $\mathfrak{H}_0, \ldots, \mathfrak{H}_r$ generated by $z_0, \ldots, z_r$.

As above these groups may be further split up into prime-power groups.

We may easily establish that these remarks are also valid when the multiplicative domain is the polynomial ring $\mathsf{P}[u]$. Instead of the values $|a|$ we must work with the degrees of the polynomials. It is assumed that the group $\mathfrak{G}$ has a finite rank with respect to the field P; the complete induction may also be set up regarding this rank. The assumption of the finite rank also implies that for each group element z there are only a finite number of linearly independent elements among the elements $z, uz, u^2 z, \ldots$, in other words, each z is annihilated by a polynomial $f(u) \neq 0$; this fact is needed for the proof of the above statements.

In the same manner we may also prove directly the general case of the Fundamental Theorem, that is, without the use of the elementary divisor theory of Section 108. From such a proof we could derive[6] conversely the Elementary Divisor Theorem of Section 108.

It is entirely unnecessary to mention that all proofs in this section are immediately valid in multiplicative Abelian groups if we write product instead of sum.

For finite Abelian groups the following notation is ordinarily used: for instance, $\mathfrak{A}_{2,2,4,3}$ designates the direct sum (the direct product) of cyclic groups of orders 2, 2, 4, 3 [therefore the annihilating ideals (2), (2), (4), (3)]. It appears useful to extend the notation so that it includes cyclic summands of infinite orders [therefore with the annihilating ideal (0)], and to write, for instance $\mathfrak{A}_{4,0}$ to denote the direct sum of two cyclic groups with the annihilating ideals (4), (0).

EXERCISES. 4. If an Abelian group of order n is cyclic, then n is the smallest number which annihilates all elements of the group; on the contrary if the group is not cyclic, there is a proper divisor of n which has this property.

[6] See H. Prüfer: "Theorie der Abelschen Gruppen." *Math. Z. Vol. 20 (1924) pp. 165-187*, as well as K. Shoda: *Proc. imp. Acad. (Tokyo), Vol. 6 (1930) pp. 217-219.*

5. With the help of 4. prove that the multiplicative group of the residue classes mod p^k, whose numbers are not divisible by p, is a cyclic group, except when $p = 2$ and $k \geqq 3$ for which it has the type $\mathfrak{A}_{2,2^{k-2}}$. [Compute the orders of the elements $1 + p$ and g, where g is a primitive number mod p.]

6. The multiplicative group of the residue classes mod n, whose numbers are relatively prime to n, is isomorphic to the direct product of the corresponding groups modulo the highest power of a prime number dividing n.

110. REPRESENTATIONS AND REPRESENTATION MODULES

By a *representation of a ring* $\mathfrak{o}$ *in terms of linear transformations or in terms of matrices in* K we understand a homomorphism

$$\mathfrak{o} \sim \mathfrak{D},$$

where $\mathfrak{D}$ is a ring of square matrices of degree r. If the homomorphism is an isomorphism, we call it a *true representation.* If $\mathfrak{o}$ and K are both hypercomplex with respect to a field P, we usually require besides ring homomorphism also operator homomorphism with respect to P: if $a \to A$, then $a\varrho \to A\varrho$ for every $\varrho \in \mathsf{P}$.

In the applications K is usually a field. In the hypercomplex case P is contained in the centrum of K.

By a *representation module* of $\mathfrak{o}$ with respect to K we understand a "*double module*" $\mathfrak{M}$ which has $\mathfrak{o}$ as a left and K as a right multiplicative domain with the following properties:

1. $\mathfrak{M}$ is a module of linear forms with respect to K.

$$\mathfrak{M} = u_1\mathsf{K} + \cdots + u_n\mathsf{K}.$$

2. For $a \in \mathfrak{o}$, $u \in \mathfrak{M}$, $\lambda \in \mathsf{K}$, we have

$$a \cdot u\lambda = au \cdot \lambda. \tag{1}$$

The last condition states that the multiplication by a represents an operator homomorphism of the K-module $\mathfrak{M}$, that is, a linear transformation. The linear transformation is given by a square matrix $A = (\alpha_{jk})$:

$$\begin{cases} a \cdot u_k = \sum u_j \alpha_{jk}, \\ a \cdot \sum u_k \lambda_k = \sum\sum u_j \alpha_{jk} \lambda_k. \end{cases} \tag{2}$$

Then to every a of $\mathfrak{o}$ there corresponds a matrix A in K. As a consequence of the module postulate the product and sum of two elements, a, b of $\mathfrak{o}$ also correspond to the product and sum of the associated linear transformations and therefore of their matrices. *Hence the correspondence* $a \to A$ *is a representation of the ring* $\mathfrak{o}$.

Conversely, let $\mathfrak{M}$ be a module of linear forms with respect to K. If a representation of a ring $\mathfrak{o}$ by linear transformations of $\mathfrak{M}$ is given, then $\mathfrak{M}$ is made

into a double module on defining the product $a \cdot u (a \in \mathfrak{o}, u \in \mathfrak{M})$ by (2). Hence on going backwards we conclude that $\mathfrak{M}$ is a *representation module,* since all double module properties and the rule (1) are satisfied.

Every representation module belongs to a representation of $\mathfrak{o}$ *by linear transformations or, after choosing a* K*-basis* $(u_1, \ldots, u_n)$*, by matrices in* K*, and conversely to every representation there is a representation module.*

If we go from the basis $(u_1, \ldots, u_n)$ to an other basis $(u'_1 \ldots, u'_n)$ defined by

$$(u'_1 \ldots u'_n) = (u_1 \ldots u_n) P,$$

then the linear transformation given above is represented by the matrix

$$A' = P^{-1} A P.$$

Hence the ring elements are now mapped on new matrices A'; we call this an *equivalent representation.* Since the transition to an equivalent representation amounts to the transition to another basis for the same (or one that is operator isomorphic to it) representation module, we conclude: *isomorphic representation modules belong to equivalent representations and conversely.*

If $\mathfrak{o}$ and K are both hypercomplex with respect to a commutative field P, which is contained in the centrum of K, and if we require that $a \to A$ implies that $a\varrho \to A\varrho$, then for the representation module we have that

$$a\varrho \cdot u (= \varrho a \cdot u) = au \cdot \varrho.$$

The scalars ϱ of P may therefore be written at any place in a product: they are permutable with all elements.

A system of linear transformations of a module of linear forms $\mathfrak{M}$, especially a representation of a ring, is said to be *reducible,* if all transformations of the system transform a fixed linear subspace $\mathfrak{N} (\neq (0), \neq \mathfrak{M})$ into itself. $\mathfrak{N}$ is then called an *invariant subspace.* In dealing with a representation of a ring $\mathfrak{o}$ if we take $\mathfrak{M}$ to be a double module with respect to $\mathfrak{o}$ and K, then the invariant subspace $\mathfrak{N}$ allows all elements of $\mathfrak{o}$ to act as left operators. This implies: *a representation of a ring is reducible if and only if its associated representation module contains a (double-) submodule* $\mathfrak{N}$.

Now let K be a field. In order to investigate the form of the matrices of a reducible representation we go over to a K-basis for $\mathfrak{N}$ and enlarge it to a K-basis for $\mathfrak{M}$ (cf. Section 107). Hence let

$$\mathfrak{N} = v_1 \mathsf{K} + \cdots + v_r \mathsf{K},$$
$$\mathfrak{M} = v_1 \mathsf{K} + \cdots + v_r \mathsf{K} + w_1 \mathsf{K} + \cdots + w_t \mathsf{K}.$$

The fact that a linear transformation transforms the module $\mathfrak{N}$ into itself indicates that the image of each v is expressed in terms of the v alone:

$$\begin{cases} v_j' = \sum v_i \varrho_{ij}, \\ w_j' = \sum v_i \sigma_{ij} + \sum w_i \tau_{ij}. \end{cases} \tag{3}$$

If we set $R = (\varrho_{ij})$, $S = (\sigma_{ij})$, $T = (\tau_{ij})$, then the transformation is represented by the matrix

$$A = \begin{pmatrix} R & S \\ 0 & T \end{pmatrix}. \tag{4}$$

Hence *a system of matrices is reducible if and only if all matrices of the system may be simultaneously brought into the form* (4) *by a transformation* $A' = P^{-1}AP$ *(choosing a new basis).*

From (3) follows

$$\begin{cases} (v_1' \dots v_r') = (v_1 \dots v_r) \cdot R, \\ (w_1' \dots w_t') \equiv (w_1 \dots w_t) \cdot T \,(\mathrm{mod}\, \mathfrak{N}). \end{cases} \tag{5}$$

This means:

For a reducible representation of a ring $\mathfrak{o}$ *if we interpret the invariant submodule* $\mathfrak{N}$ *and the factor module* $\mathfrak{M}/\mathfrak{N}$ *as representation modules, then the associated representations are given by the components* R *and* T *of* (4).

Let $\mathfrak{N}$ be a maximal invariant submodule $\mathfrak{M}_{l-1}$, in this submodule let $\mathfrak{M}_{l-2}$ be a maximal invariant submodule, etc., until a composition series

$$\mathfrak{M} = \mathfrak{M}_l, \quad \mathfrak{M}_{l-1}, \dots, \mathfrak{M}_0 = (0)$$

is obtained, then the matrices of the representation with respect to a suitable basis take the form

$$\begin{pmatrix} R_{11} & \dots & \dots & R_{1l} \\ 0 & R_{22} & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & R_{ll} \end{pmatrix}. \tag{6}$$

The diagonal blocks R_{ii} produce representations which belong to the composition factors $\mathfrak{M}_i/\mathfrak{M}_{i-1}$; since these composition factors are simple double modules (that is, without invariant submodules), their associated representations are *irreducible.* The process which leads to (6) is referred to as the "*reduction*" (Ausreduzieren) of a representation. According to the Jordan-Hölder Theorem (Section 46) the composition factors are determined uniquely except for the order of the terms and operator isomorphism. Hence the *irreducible components* R_{ii} *of the reduced representation* (6) *are determined uniquely except for the sequential order and equivalent representations.*

In (3) if the σ_{ij} are omitted, then $(w_1, \dots, w_t)$ as well as $(v_1, \dots, v_r)$ is an invariant submodule. In this case $\mathfrak{M}$ is a *direct sum of two invariant submodules* $\mathfrak{N}$, $\mathfrak{Q}$. The matrix (4) then has the form

$$A = \begin{pmatrix} R & 0 \\ 0 & T \end{pmatrix},$$

where R and T belong to the representations adjusted to $\mathfrak{R}$ and $\mathfrak{Q}$, respectively. In this case we say that the representation $a \to A$ is *decomposed* into the representations $a \to R$ and $a \to T$.

If the double module $\mathfrak{M}$ is completely reducible in the sense of Section 47, that is, the direct sum of simple double modules, then the representation adjusted to $\mathfrak{M}$ is given by the matrix

$$\begin{pmatrix} R_{11} & & & 0 \\ & R_{22} & & \\ & & \ddots & \\ 0 & & & R_{ll} \end{pmatrix}, \tag{7}$$

where the individual blocks give rise to irreducible representations which need not be distinct from one another. We call such a representation *completely reducibile.*

Examples of the concepts formulated in this section are furnished by the theory of a single matrix developed in the next section.

EXERCISES. 1. Every (group homomorphism) representation of a (finite or infinite) group by linear substitutions may be enlarged to a (ring homomorphism) representation of the "group ring" (Section 14, Example 3), under the following inference: if the matrices G_i correspond to the elements g_i, then the matrix $\sum G_i \lambda_i$ corresponds to the linear combination $\sum g_i \lambda_i$.

2. If $\mathfrak{o}$ is a ring with an identity and in a representation of $\mathfrak{o}$ if the identity corresponds to the unit matrix, then for the representation module this means that the identity is a unity operator. Show, with the help of a theorem of Section 106, that every representation of $\mathfrak{o}$ decomposes into a representation in which the identity corresponds to the unit matrix and a representation in which every element corresponds to the null matrix:

$$A = \begin{pmatrix} S & 0 \\ 0 & 0 \end{pmatrix}.$$

3. A representation is completely reducible if and only if to every invariant subspace $\mathfrak{R}$ an other $\mathfrak{Q}$, just like it, may be found which together with $\mathfrak{R}$ spans the space $\mathfrak{M}$:

$$\mathfrak{M} = \mathfrak{R} + \mathfrak{Q}.$$

4. If $(u'_1 \dots u'_n) = (u_1 \dots u_n)P$ is a homomorphism of the representation module into itself, then the matrix P is permutable with all matrices of the representation:

$$AP = PA$$

and conversely.

111. NORMAL FORMS OF A MATRIX IN A COMMUTATIVE FIELD

Let $\mathfrak{M} = (u_1, \ldots, u_n)$ be a module of linear forms with respect to the commutative field K and

$$u_k \to v_k = \sum u_i \alpha_{ik}$$ [7]

be a linear transformation of $\mathfrak{M}$ into itself. By the introduction of a new basis

$$(u'_1 \ldots u'_n) = (u_1 \ldots u_n) P$$

(hence P is an invertible matrix in K) we shall bring the matrix $A = (\alpha_{ik})$ to a normal form which is as simple as possible

$$A' = P^{-1} A P.$$

We note that the problem formulated here is different from that in Section 108, where we were dealing with two new bases (v') and (u'), and had set $A' = B^{-1} A C$. Hence our transformation possibilities are now restricted; accordingly, we must make more assumptions regarding K, namely, that K be a field.

We now think of the powers of the matrix A as a meromorphic representation of the powers of an indeterminate x and extend this representation to a representation of the polynomial domain $\mathsf{K}[x]$; namely, to the polynomial

$$f(x) = \sum \alpha_\nu x^\nu$$

corresponds the matrix

$$f(A) = \sum \alpha_\nu A^\nu.$$

The representation is a homomorphism since the powers of A are permutable with one another and with the coefficients α_ν.

This representation determines the representation module $\mathfrak{M}$ if the product of a polynomial in $\mathsf{K}[x]$ with a $u \in \mathfrak{M}$ is defined by

$$(\sum \alpha_\nu x^\nu) u = \sum \alpha_\nu A^\nu u.$$

The representation module $\mathfrak{M}$ is a double module with respect to $\mathsf{K}[x]$ and K; however, since the elements of K are permutable with one another and all others, we may also write them on the left of the elements of $\mathfrak{M}$:

$$u\lambda = \lambda u,$$

therefore $\mathfrak{M}$ may be simply interpreted as a $\mathsf{K}[x]$-module.

Since the polynomial domain $\mathsf{K}[x]$ is a Euclidean domain, the Fundamental Theorem of Section 109 is applicable: [8] the module $\mathfrak{M}$ is the direct sum of

[7] Since K is commutative it is entirely immaterial whether we write the coefficients on the right or left.

[8] This also follows from the short direct proof given at the end of Section 109.

cyclic $K[x]$-modules $(w_1), \ldots, (w_r)$ whose annihilating ideals are either zero or are generated by a single polynomial of $K[x]$. The case of the null ideal is obvious. As to the other case, for every $w = w_\nu$ there are among the quantities $w, xw, x^2w, \ldots$ at most n linearly independent ones; therefore there is a polynomial $\sum \alpha_\nu x^\nu \neq 0$ with the property

$$\sum \alpha_\nu x^\nu w = 0.$$

Hence every $w = w_\nu$ has an annihilating polynomial of lowest degree

$$f_\nu(x) = f(x) = x^k + \alpha_{k-1}x^{k-1} + \cdots + \alpha_0,$$

and

$$f_{\nu+1} \equiv 0 (f_\nu).$$

The quantities $w, xw, \ldots, x^{k-1}w$ are linearly independent with respect to K and may therefore be used as a K-basis for the cyclic $K[x]$-module $(w) = (w, xw, x^2w, \ldots)$. Hence

$$\begin{aligned} Aw &= xw, \\ Axw &= x^2w, \\ &\cdots\cdots\cdots \\ Ax^{k-1}w = x^kw &= -\alpha_0 \cdot w - \alpha_1 \cdot xw - \cdots - \alpha_{k-1} \cdot x^{k-1}w. \end{aligned}$$

This means that the transformation A of the module $(w, xw, \ldots)$ into itself relative to the new basis elements is represented by the matrix

$$A_\nu = \begin{pmatrix} 0 & \cdots & 0 & -\alpha_0 \\ 1 & \ddots & 0 & -\alpha_1 \\ 0 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & -\alpha_{k-1} \end{pmatrix} \tag{1}$$

These matrices are called *companion matrices* (Begleitmatrices); every w_ν determines a companion matrix A_ν of this type. Since $\mathfrak{M}$ is the direct sum of the (w_ν), we obtain for the matrix A the *first Normal Form:*

$$A = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix}, \tag{2}$$

where the blocks A_ν are the companion matrices of type (1).

The Uniqueness Theorem of Section 109 implies that the polynomials $f_\nu(x)$, therefore also the companion matrices A_ν, are *uniquely determined* by the module $\mathfrak{M}$.

The blocks A_ν may be still further "reduced" if we represent the cyclic modules (w_ν) as direct sums of cyclic submodules whose annihilating polynomials

are powers of prime polynomials. The form (2) remains the same, where the companion matrices (1) now belong to powers of prime polynomials $(p(x))^{\varrho}$. (*Second Normal Form.*) Furthermore, these companion matrices are also uniquely determined except for their order in (2). The polynomials $(p(x))^{\varrho}$ are sometimes called *elementary divisors* of the matrix A. This term has, as used here, a meaning different from that in Section 108. The relation between the two concepts will be shown in Section 112.

By the composition series of the cyclic module (w_ν) we may reduce still further the normal form just obtained. Here we will carry out the reduction process only for the case that the prime polynomials $p(x)$ that occur are *linear*, which is always the case when K is an algebraically closed field. Hence let

$$p(x) = x - \lambda,$$
$$f(x) = (x - \lambda)^{\varrho}.$$

As basis elements we use

$$v_1 = (x - \lambda)^{\varrho-1} w,$$
$$v_2 = (x - \lambda)^{\varrho-2} w,$$
$$\cdots\cdots\cdots\cdots$$
$$v_{\varrho} = w;$$

therefore

$$(x - \lambda) v_1 = 0,$$
$$(x - \lambda) v_\mu = v_{\mu-1} \qquad (1 < \mu \leqq \varrho)$$

or

$$\begin{cases} A v_1 = x v_1 = \lambda v_1, \\ A v_\mu = x v_\mu = \lambda x_\mu + v_{\mu-1}. \end{cases} \tag{3}$$

Hence the "blocks" A_1 take on the "reduced" form

$$A_1 = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \\ & & \ddots & \ddots & 0 \\ & & & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix},$$

and similarly, since every w_ν determines a λ_ν, we have

$$A_\nu = \begin{pmatrix} \lambda_\nu & 1 & \cdots & 0 \\ & \ddots & \ddots & \vdots \\ & & \ddots & 1 \\ 0 & & & \lambda_\nu \end{pmatrix}.$$

On inserting these blocks in (2) we obtain the *third Normal Form.* The "*charac-*

teristic roots" [9] λ_ν and the degree ϱ_ν of the blocks are also *uniquely determined.*

All vectors v_u, which belong to the same root λ, generate a module $\mathfrak{B}_\nu$ which is annihilated by a power of $x - \lambda$ (Section 109); this module is called (in the language of vectors) the *subspace belonging to the root* λ. The entire module $\mathfrak{M}$ is the direct sum of these subspaces. Each of these also contains the series of subspaces mentioned in Section 109 which are annihilated by $(x - \lambda)^\varrho$, $(x - \lambda)^{\varrho-1}$, ...,1. The vectors w that are annihilated by $x - \lambda$, which means

$$Aw = \lambda w,$$

are also called *eigenvectors* of the matrix A for the *eigenvalue* λ.

The type of the matrix A is sometimes given by a *scheme* of the following kind: if a characteristic root, say λ_1, occurs in different blocks of degree $\varrho, \sigma, \ldots, \tau$, then we write $\varrho, \sigma, \ldots, \tau$ in parentheses and unite all parentheses belonging to distinct λ_ν by brackets. Thus the scheme [(2 1) 1] indicates the type

$$\begin{pmatrix} \boxed{\begin{matrix}\lambda_1 & 1 \\ 0 & \lambda_1\end{matrix}} & & 0 \\ & \boxed{\lambda_1} & \\ 0 & & \boxed{\lambda_2} \end{pmatrix}.$$

The completely reducible case (cf. Section 110), in which the normal form (2) becomes a diagonal form

$$\begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}, \tag{4}$$

occurs when all ϱ are equal to 1, that is, when the polynomials $f_\nu(x)$, from which the $(f_\nu(x))^\varrho$ are obtained by factoring into prime factors, do not contain multiple factors. Since

$$f_{\nu+1} \equiv 0 (f_\nu),$$

a sufficient condition for this case is that the highest elementary divisor $f_r(x)$ have no multiple factors.

Methods for the actual determination of the characteristic roots and the setting up of the normal forms will be given in the next section.

EXERCISES. 1. The highest elementary divisor $f_r(x)$ may be characterized as the polynomial $f(x)$ of lowest degree with the property

$$f(x)\,\mathfrak{M} = 0 \text{ or } f(A) = 0.$$

2. For an arbitrary matrix A appearing in the second or third Normal Form, determine the totality of the matrices permutable with A. (Cf. Section 110, Exer. 4.)

[9] This term is clarified in the next section.

112. ELEMENTARY DIVISORS AND CHARACTERISTIC FUNCTION

By the transformation

$$A' = P^{-1}AP$$

the matrix $xE - A$ goes over to

$$P^{-1}(xE - A)P = xP^{-1}EP - P^{-1}AP$$
$$= xE - A'.$$

We shall determine the elementary divisors of the matrix $xE - A$ in $\mathsf{K}[x]$ in the sense of Section 108. Since the elementary divisors of a matrix are invariant relative to multiplication by arbitrary invertible matrices, they may be found by using the matrix $xE - A'$, where A' is in the first Normal Form of Section 111. By (1), (2) of Section 111, $xE - A'$ consists of blocks of the form

$$xE_1 - A_1 = \begin{pmatrix} x & 0 & \dots & 0 & \beta_0 \\ -1 & x & \ddots & \vdots & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & x & \beta_{h-2} \\ 0 & \dots & 0 & -1 & x + \beta_{h-1} \end{pmatrix}.$$

To determine the elementary divisors we have to bring this matrix into diagonal form. If we add the second up to the h-th row multiplied by $x, x^2, \dots, x^{h-1}$ respectively to the first row, we obtain:

$$\begin{pmatrix} 0 & 0 & \dots & 0 & f(x) \\ -1 & x & \ddots & \vdots & \beta_1 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & x & \beta_{h-2} \\ 0 & \dots & 0 & -1 & x + \beta_{h-1} \end{pmatrix}.$$

If the first row is sequentially interchanged with all rows, one after the other, until it is in the last position, then only zeros appear under the principal diagonal. It is very easy, by addition of multiples of preceding columns to subsequent ones, to remove all elements which appear above the main diagonal. There remains as a result

$$\begin{pmatrix} -1 & & & 0 \\ & -1 & & \\ & & \ddots & \\ & & & -1 \\ 0 & & & f(x) \end{pmatrix}.$$

Now, if we write all such blocks one after another and permute rows and columns until all -1 occur in the first part of the main diagonal, we obtain the desired diagonal form:

$$\begin{pmatrix} -1 & & & & & & 0 \\ & -1 & & & & & \\ & & \ddots & & & & \\ & & & -1 & & & \\ & & & & f_1(x) & & \\ & & & & & \ddots & \\ 0 & & & & & & f_r(x) \end{pmatrix}.$$

Hence the polynomials $f_\nu(x)$ together with some units are the elementary divisors of $xE - A$. The powers of prime polynomials, in which they factor, are the elementary divisors of the matrix A in the sense of Section 111.

The *characteristic polynomial* (the *characteristic function*) of A

$$\chi(x) = \prod_1^r f_\nu(x)$$

annihilates the module $\mathfrak{M}$, since the factor $f_r(x)$ already does; this means

$$\chi(A) = 0. \tag{1}$$

The characteristic polynomial is the greatest determinantal divisor of $xE - A$, and therefore, except for a constant, equals the determinant $|xE - A|$. The constant is actually equal to the unit; hence

$$\chi(x) = |xE - A|. \tag{2}$$

The *characteristic equation* (1) for the matrix A may be derived directly from (2). Thus

$$xu_k = \sum u_i \alpha_{ik},$$

and the elimination of all u from this system of equations produces (since x and its powers are permutable with the α_{ik});

$$\begin{vmatrix} x - \alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1n} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ -\alpha_{n1} & -\alpha_{n2} & \cdots & x - \alpha_{nn} \end{vmatrix} \cdot u_j = 0$$

or

$$|xE - A| u_j = 0;$$

that is, $\chi(x) = |xE - A|$ annihilates all u_j, and therefore the entire module $\mathfrak{M}$. Q.E.D.

By the above remarks the coefficients of the characteristic function $\chi(x)$ of A

are invariant with respect to the transformation $A \to P^{-1}AP$. The most important ones are the first and last:

the *trace* of A: the coefficient of $-x^{n-1}$:

$$S(A) = \sum \alpha_{ii};$$

the *norm* of A: the coefficient of $(-1)^n x^0$:

$$N(A) = |A|.$$

The roots of the characteristic function are the *characteristic roots* λ_ν, which were already introduced in the previous section [as roots of the polynomial $f_\nu(x)$]. This fact provides us with a practical method for determining the λ_ν and the setting up of the normal forms of the previous sections: we determine first the λ_ν as roots of

$$\chi(x) = |xE - A|,$$

then the v_1 from the linear equations [cf. (3) Section 111]

$$Av_1 = \lambda_\nu v_1.$$

In the case of multiple roots ($\varrho > 1$) the other $v_2, \ldots, v_\varrho$ are found most easily from (3) Section 111; it may be possible to replace the v_1 belonging to the same λ_ν by suitable linear combinations.

The equation $\chi(\lambda) = 0$, whose roots are the λ_ν, appears in many applications and due to its appearance in the theory of secular perturbations it is also called the *secular equation.*

EXERCISES. 1. Determine the normal forms of the matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

2. Give a classification of the projective image of a projective plane into itself:

$$\begin{pmatrix} \xi_1' \\ \xi_2' \\ \xi_3' \end{pmatrix} = A \begin{pmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{pmatrix},$$

and determine the position of the invariant points and lines of this mapping.

113. QUADRATIC AND HERMITIAN FORMS

Let K be a commutative field of characteristic $\neq 2$. In order to study the values which a quadratic form

$$f(x_1, \ldots, x_n) = \sum_i \sum_k \beta_{ik} x_i x_k \qquad (\beta_{ik} = \beta_{ki})$$

assumes for special values $x_i = c_i$ of K, we interpret the $c_1, \ldots, c_n$ as components of a vector u and set

$$f(u, u) = f(c_1, \ldots, c_n) = \sum\sum \beta_{ik} c_i c_k.$$

We form, when $v = (d_1, \ldots, d_n)$ is a second vector, the expression

$$\begin{aligned} f(u + \lambda v, u + \lambda v) &= \sum\sum \beta_{ik} c_i c_k + 2\lambda \sum\sum \beta_{ik} c_i d_k + \lambda^2 \sum\sum \beta_{ik} d_i d_k \\ &= f(u, u) + 2\lambda f(u, v) + \lambda^2 f(v, v), \end{aligned}$$

where

$$f(u, v) = \sum\sum \beta_{ik} c_i d_k.$$

Obviously, the bilinear form $f(u,v)$ is an invariant (that is, independent of the choice of the basis vectors) of the form $f(u,u)$ and is called the *polar form* of $f(u,u)$.

If we refer the vectors u of the space R_n to a new basis $(u'_1, \ldots, u'_n)$, where the u'_i are connected with the old basis vectors $u_1, \ldots, u_n$ by the linear transformation P:

$$u'_j = \sum u_i \pi_{ij},$$

then the components c_i of a vector are transformed, as we proved, by the rule

$$c_i = \sum \pi_{ij} c'_j, \tag{1}$$

and the quadratic form f goes over to

$$f = \sum\sum \beta_{ik} c_i c_k = \sum\sum\sum\sum \beta_{ik} \pi_{ij} \pi_{kl} c'_j c'_l$$

with the coefficients

$$\beta'_{jl} = \sum\sum \beta_{ik} \pi_{ij} \pi_{kl}.$$

These equations may be written in matrix form if we introduce the matrices $A = (\beta_{ik})$ and $A' = (\beta'_{ik})$ and for the matrix $P = (\pi_{ik})$ form the transpose matrix P^T. Thus

$$A' = P^T A P.$$

As we see the matrix of the coefficients of a quadratic form is transformed quite differently from the matrix of a linear transformation, which is given by $A' = P^{-1} A P$ with respect to a new basis.

In order to bring a given quadratic form f by transformations to a form as simple as possible, we choose a vector v_1 such that $f(v_1, v_1) \neq 0$, which is always possible if f is not identically zero. Then the equation $f(v_1, u) = 0$ determines a subspace R_{n-1} of the vector space R_n which does not contain v_1. If we now choose in this subspace, if possible, a vector v_2 such that $f(v_2, v_2) \neq 0$, the equation $f(v_2, u) = 0$ determines together with the previous one a subspace R_{n-2} in R_{n-1} which does not contain v_2. We continue in this manner until we arrive at a subspace R_{n-r} such that $f(u, u) = 0$ for all u in R_{n-r} and therefore [10] $f(u, v) = 0$ for u and v

[10] At this point we use the assumption: characteristic $\neq 2$.

in R_{n-r}. It may happen that $r = n$; then R_{n-r} is the null space. In other cases we arbitrarily choose in R_{n-r} the basis vectors $v_{r+1}, \ldots, v_n$. Then we have

$$\begin{aligned} f(v_i, v_k) &= 0 && (i \neq k), \\ f(v_i, v_i) &= \gamma_i \neq 0 && (i = 1, \ldots, r), \\ f(v_i, v_i) &= 0 && (i = r+1, \ldots, n). \end{aligned}$$

If we refer every vector v to the new basis vectors $v_1, \ldots, v_n$:

$$v = \sum d_i v_i,$$

then

$$f(v, v) = \sum\sum d_i d_k f(v_i, v_k) = \sum_1^r d_i^2 \gamma_i. \tag{2}$$

In this case we say that the form f is *transformed to a sum of squares.*

The vectors w of R_{n-r} have the property

$$f(w, u) = 0 \quad \text{for every } u$$

and are thereby characterized. The space R_{n-r} and its dimension $n - r$ are invariants of the form f. The number r of the squares in (2) is therefore also an invariant: it is called the *rank* of the form f.

We now assume that the field K is ordered (Section 66). The number of negative γ_i in (2) is called the *index of inertia* of f. We will show that the index of inertia is also an invariant (*Law of Inertia of* Sylvester).

Let us assume that the form f, in relation to the basis vectors v_i', has the representation

$$f = \sum_1^r d_i'^2 \gamma_i';$$

let us say that $\gamma_1, \ldots, \gamma_h$ are positive, $\gamma_{h+1}, \ldots, \gamma_r$ negative; similarly $\gamma_1', \ldots, \gamma_k'$ positive and $\gamma_{k+1}', \ldots, \gamma_r'$ negative. If we were now to assume that $k > h$, then the linear equations

$$d_1 = 0, \ldots, d_h = 0, \quad d_{k+1}' = 0, \ldots, d_r' = 0$$

would define a space of more than $n - r$ dimensions. For a vector u of this space, $f(u, u) = \sum_{h+1}^r d_i^2 \gamma_i \leqq 0$. On the other hand $f(u, u) = \sum_1^k d_i'^2 \gamma_i' \geqq 0$. Hence $f(u, u) = 0$ and all d_i and $d_i' = 0$. Consequently u would lie in R_{n-r}. This means that a space of more than $n - r$ dimensions would be contained in one of $n - r$ dimensions, which cannot be true.

If all γ_i in (2) are positive, the form f is said to be *positive definite* in the case $r = n$, *semi-definite* in the case $r < n$. The positive definite forms are characterized by the property that they are positive for every vector $u \neq 0$; the semi-definite by the fact that their values are not always positive, but only $\geqq 0$.

A positive definite form may be transformed, as follows immediately from (2), into the "*primitive form*"

$$E(u, u) = \sum d_i^2$$

by the adjunction of the quantities $\sqrt{\gamma_i}$ to the field K.

The *hermitian forms* are analogous to the quadratic forms. In order to introduce these forms we first adjoin to the ordered field K a square root θ of a negative element α of K, for instance, $\theta = \sqrt{-1}$. We will occasionally call the elements of K "real," in order to distinguish them from $K(\theta)$, since in the applications K is usually the field of real numbers and $\theta = \sqrt{-1}$.

Every element $c = a + b\theta$ has a conjugate $\bar{c} = a - b\theta$. The product $\bar{c}c = a^2 - b^2\theta^2$ is always real and $\geqq 0$, where the equality sign is valid only if $c = 0$.

A *hermitian form* is defined to be the expression

$$H(u, u) = \sum\sum h_{ik}\bar{c}_i c_k \qquad (h_{ik} = h_{ki}).$$

The value of the form H for an arbitrary vector u is always real.

If we form, as at the beginning of this section,

$$H(u + \lambda v, u + \lambda v) = \sum\sum h_{ik}\bar{c}_i c_k + \lambda\sum\sum h_{ik}\bar{c}_i d_k + \bar{\lambda}\sum\sum h_{ik}\bar{d}_i c_k + \lambda\bar{\lambda}\sum\sum h_{ik}\bar{d}_i d_k,$$

then we find as coefficients of λ the *polar form*

$$H(u, v) = \sum\sum h_{ik}\bar{c}_i d_k.$$

We have

$$H(v, u) = \overline{H(u, v)}.$$

By the introduction of a new basis according to formula (1) the matrix H of a hermitian form is transformed as follows:

$$H' = P^\dagger H P,$$

where $P^\dagger = \bar{P}^T$ indicates the conjugate transpose matrix.

Our earlier considerations regarding the representation of the quadratic forms as sums of squares are valid without change for hermitian forms. We find as a normal form

$$H(u, u) = \sum_1^r \bar{c}_i c_i \gamma_i \qquad (\gamma_i \text{ real}). \tag{3}$$

The form H is again said to be *positive definite* if its values $H(u,u)$ are always positive except for $u = 0$, or when $r = n$ and $\gamma_1, \ldots, \gamma_n$ are all positive. By the adjunction of the square roots of the γ_i every positive definite form may be transformed into the *primitive form*

$$E(u, u) = \sum \bar{c}_i c_i.$$

The following discussion is valid for both hermitian and quadratic forms. We shall state our results for hermitian forms; in order to obtain the corresponding theorems for quadratic forms, the elements chosen must belong to K and the dash must be omitted.

We choose a fixed, preferably positive definite, hermitian form $G(u, u)$ of rank n as the *Fundamental Form* and designate its coefficient matrix (g_{ik}) by G. In particular if $G(u, u)$ is the primitive form, then G is the identity matrix E. Two vectors u, v are said to be *perpendicular* if $G(u, v) = 0$. In this case we obviously have $G(v, u) = 0$. The vectors v which are perpendicular to a vector $u \neq 0$ form a linear subspace: *the space perpendicular to u.* If G is positive definite, then $G(u, u) \neq 0$; therefore u itself does not belong to the space perpendicular to R_{n-1}. A system of n basis vectors $v_1, \ldots, v_n$ perpendicular to one another, as would be used in setting up the normal form (3) for $G(u,u)$, is called a *complete orthogonal system* of vectors. The orthogonal system is said to be *normalized* when $G(v_j, v_j) = 1$.

Those linear transformations A which have the property

$$G(Au, v) = G(u, Av) \qquad \text{(for all } u \text{ and } v\text{)}$$

are said to be *hermitian symmetric* or simply *symmetric.* The condition for this property to be valid is:

$$\sum\sum\sum g_{il}\bar{a}_{ij}\bar{c}_j c_l = \sum\sum\sum g_{jk}\bar{c}_j a_{kl} c_l$$

or

$$\sum_i g_{il}\bar{a}_{ij} = \sum_k g_{jk} a_{kl}$$

or

$$A^\dagger G = GA.$$

In particular, if G is a primitive form, the symmetry condition simply states that

$$A^\dagger = A \quad \text{or} \quad \bar{a}_{ik} = a_{ki},$$

which clarifies the nomenclature "symmetric."

Those linear transformations U which leave invariant the Fundamental Form $G(u, u)$:

$$G(Au, Au) = G(u, u) \quad \text{or} \quad A^\dagger GA = G,$$

are called *unitary* or in the real case *orthogonal.* In this case we obviously have $G(Au, Av) = G(u, v)$. In particular, if $G = E$, which we may always assume in the positive definite case, the condition states

$$A^\dagger A = E \quad \text{or} \quad A^\dagger = A^{-1} \quad \text{or} \quad AA^\dagger = E.$$

When written out we obtain the "orthogonality conditions"

$$\sum \bar{a}_{ik} a_{il} = \delta_{kl} = \begin{cases} 0 & \text{for } k \neq l \\ 1 & \text{for } k = l \end{cases}$$

which are equivalent to

$$\sum a_{ik}\bar{a}_{jk} = \delta_{ij}.$$

A real orthogonal transformation with the determinant 1 is called a *rotation.*

If a symmetric or unitary transformation A transforms a vector u distinct from zero into a multiple of itself:

$$Au = \lambda u, \tag{4}$$

that is, when A leaves invariant the line generated by u, then A also leaves invariant the R_{n-1} perpendicular to u.

PROOF. When v belongs to R_{n-1}, so that $G(u, v) = 0$, then for A symmetric:

$$G(u, Av) = G(Au, v) = G(\lambda u, v) = \lambda G(u, v) = 0$$

and for A unitary:

$$G(u, Av) = G(AA^{-1}u, Av) = G(A^{-1}u, v) = G(\lambda^{-1}u, v) = \lambda^{-1}G(u, v) = 0.$$

A vector $u \neq 0$ with the property (4) is called an *eigenvector* of the transformation A; λ is called the *eigenvalue* belonging to it.

As we have already seen in Section 112, the eigenvalues are found from the "*secular equation*"

$$\chi(\lambda) = \begin{vmatrix} \lambda - \alpha_{11} & -\alpha_{12} & \dots \\ -\alpha_{21} & \lambda - \alpha_{22} & \dots \\ \dots & \dots & \dots \end{vmatrix} = 0 \tag{5}$$

and the corresponding eigenvectors are found from the linear equations

$$\sum \alpha_{ik}c_k = \lambda c_i \tag{6}$$

which are equivalent to (4).

If we now assume that the K is a real closed field (say the field of real numbers) and therefore $K(\theta)$ is algebraically closed (cf. Section 70), then the secular equation (5) always has a root λ_1 in $K(\theta)$, to which also belongs an eigenvector e_1. The R_{n-1} perpendicular to e_1 is transformed into itself by A, and A is symmetric or unitary in R_{n-1} according as A is symmetric or unitary in R_n. Hence by the same reasoning there is in R_{n-1} an eigenvector e_2, whose perpendicular space R_{n-2} inside R_{n-1} is again invariant, etc. *Continuing thus, we can find a complete system of n linearly independent eigenvectors $e_1, \dots, e_n$ perpendicular to one another:*

$$Ae_\nu = \lambda_\nu e_\nu.$$

The matrix A, relative to the new basis $(e_1, \dots, e_n)$, takes on the diagonal form

$$A_1 = P^{-1}AP = \begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}. \tag{7}$$

Let the e_ν be normalized by the condition $G(e_\nu, e_\nu) = 1$; this is always possible if K is a real closed field since the square root of the positive quantity $G(e_\nu, e_\nu)$ is always contained in K. Then G, relative to the e_ν as basis, is equal to the primitive form E. Now, if the matrix A is symmetric, A_1 must also be symmetric, and therefore identical with $A_1^\dagger$. Hence

$$\lambda_\nu = \bar{\lambda}_\nu \quad \text{or} \quad \lambda_\nu \in \mathsf{K}.$$

The characteristic polynomial of the matrix A or A_1 is

$$\chi(x) = \prod_1^n (x - \lambda_n).$$

Hence *the secular equation* $\chi(\lambda) = 0$ *of a symmetric matrix* A *has only real roots.*

Furthermore, if the matrices A and G are real, the eigenvectors e_ν, as solutions of the real equations (6), are also real. Hence *a real symmetric matrix* A *may be transformed by real steps into the diagonal form* (7).

In our proof of this theorem we proceeded from the existence of the roots λ_ν in $\mathsf{K}(\theta)$ and proved only afterwards that the λ_ν must be real. We may prove the theorem in the case of the field of real numbers also in the reals; cf. say R. Courant and D. Hilbert, *Methoden der mathematischen Physik, Vol. I, Section 3, 1924.*

To the symmetric transformation A there is an hermitian form

$$H(u, u) = G(u, Au) = G(Au, u)$$

which is an invariant of the transformation. Its matrix is given by

$$H = GA$$

and the matrix A is determined conversely by

$$A = G^{-1}H.$$

The diagonal transformation of A and G is at the same time one for $H = GA$; the transformed form is

$$H(u, u) = \sum \bar{c}_\nu c_\nu \lambda_\nu.$$

Hence we have proved:

Every pair of hermitian forms G, H, *for which one, say* G, *is positive definite, may be brought at the same time by a single transformation to the form*

$$\begin{cases} G(u, u) = \sum \bar{c}_\nu c_\nu \\ H(u, u) = \sum \bar{c}_\nu c_\nu \lambda_\nu. \end{cases}$$

The λ_ν are the characteristic roots of the matrix $A = G^{-1}H$, in other words, the roots of the secular equation

$$|\lambda g_{jk} - h_{jk}| = 0.$$

Especially, *every pair of real quadratic forms, for which one is positive definite, may be transformed by real steps simultaneously to the sum of squares*

$$G(u, u) = \sum c_\nu^2,$$
$$H(u, u) = \sum c_\nu^2 \lambda_\nu.$$

For a general treatment of the classification of pairs of quadratic forms, see L. E. Dickson: *Modern Algebraic Theories*, Chicago 1926 (also in German by E. Bodewig, Leipzig, 1929).

EXERCISES. 1. When r vectors $v_1, \ldots, v_r$ generate an R_r, the vectors perpendicular to these vectors form an R_{n-r}, and the whole space R_n is the direct sum of $R_r + R_{n-r}$.

2. When a symetric or unitary transformation A of the space R_r is invariant, it is also an invariant for the R_{n-r} that is perpendicular to it.

3. Every system of symmetric or unitary transformations is completely reducible.

4. The determinant D of a unitary transformation has the value 1, that is $D\overline{D} = 1$. The determinant of a real orthogonal transformation is ± 1.

5. The unitary and similarly the real orthogonal transformations of a vector space in itself form a group.

CHAPTER XVI

THEORY OF THE HYPERCOMPLEX QUANTITIES

114. SYSTEMS OF HYPERCOMPLEX QUANTITIES

By a *hypercomplex system* (or, as we say nowadays, an *algebra*) over the commutative field P we understand by Section 14 a ring which is at the same time a finite module of linear forms with respect to P :

$$\mathfrak{o} = b_1\mathsf{P} + \cdots + b_n\mathsf{P},$$

and whose elements are permutable with the elements of P. Hence the elements of $\mathfrak{o}$ have the form

$$a = b_1\lambda_1 + \cdots + b_n\lambda_n = \lambda_1 b_1 + \cdots + \lambda_n b_n. \qquad (\lambda_i \in \mathsf{P}).$$

If the b_i are linearly independent with respect to P, then the number n is the *rank* of the system. For a given P the hypercomplex system $\mathfrak{o}$ is completely determined as soon as the basis elements and their multiplication table are given. When there exists no ambiguity regarding the choice of P, we may simply write $\mathfrak{o} = (b_1, \ldots, b_n)$. The multiplication table is subject to the single condition that the associative law shall be valid for the basis elements:

$$b_\lambda(b_\mu b_\nu) = (b_\lambda b_\mu)b_\nu.$$

EXAMPLES OF HYPERCOMPLEX SYSTEMS, besides those given in Section 14:

a) The *complete matrix ring* over P, of rank n^2, whose basis elements c_{ik} (cf. Section 106, Exer. 4) satisfy the rules

$$c_{ij}c_{jl} = c_{il},$$

$$c_{ij}c_{kl} = 0 \quad \text{for} \quad j \neq k.$$

b) All skew fields of finite rank over P, which contain P in the centrum. The rank is the field degree. For instance, the finite commutative extension fields studied in Chapter V fall in this category.

c) The quaternion ring $\mathfrak{o} = (1, j, k, l)$ of rank 4, which is defined by the following rules:

$$j^2 = k^2 = l^2 = -1,$$

$$jk = -kj = l,$$

$$kl = -lk = j,$$

$$lj = -jl = k.$$

(In Section 14 P was taken as the field of real or rational numbers. This restriction is now abolished.)

d) The residue class ring modulo a zero-dimensional ideal $\mathfrak{a}$ in a polynomial domain $\mathsf{P}[x_1, \ldots, x_n]$ (or, more general, in an order of a function field) is a (commutative) hypercomplex system over P. The rank is called the *degree* of the ideal $\mathfrak{a}$.

e) The residue class ring modulo a rational prime number p in an order of a number field is a commutative hypercomplex system over $\mathsf{P} = C/(p)$, where C designates as usual the ring of ordinary integers. The rank is equal to the degree of the number field.

EXERCISES. 1. A hypercomplex system without zero divisors is a field. [Compare for $a \neq 0$ the rank of the system $a\mathfrak{o}$ with that of the whole system $\mathfrak{o}$.]

2. In a hypercomplex system $\mathfrak{o}$ if there is a non-zero divisor a, then the equations $xa = b$ and $ax = b$ may be solved; in this case there is an identity and every non-zero divisor has an inverse in $\mathfrak{o}$.

3. The quaternion ring is without zero divisors (therefore a field) if and only if in the ground field P the sum of 4 squares vanishes only if all 4 terms vanish individually.

4. An algebraically closed field has no hypercomplex proper extension without zero divisors.

5. If P is a (commutative) field, whose characteristic is distinct from 2, there are only the following three types of hypercomplex systems of rank 2 with an identity (all commutative):

a) $(1, c)$, where c^2 lies in P but is not the square of an element of P. This system is a commutative field over P.

b) $(1, c)$, where c^2 is the square of an element γ of P distinct from zero. The system is the direct sum of two fields: $(c - \gamma)\mathsf{P} = \mathsf{P}_1$ and $(c + \gamma)\mathsf{P} = \mathsf{P}_2$; these fields are both isomorphic to P and mutually annihilate one another: $\mathsf{P}_1\mathsf{P}_2 = (0)$.

c) $(1, c)$, where $c^2 = 0$ (*"system of dual numbers"*).

6. The residue class ring of a hypercomplex system with an identity modulo a two-sided ideal is again a hypercomplex system over the same ground field ("difference algebra").

PRODUCTS OF HYPERCOMPLEX SYSTEMS. Let $\mathfrak{o}_1 = (b_1, \ldots, b_n)$ and $\mathfrak{o}_2 = (c_1, \ldots, c_m)$ be two hypercomplex systems over the ground field P. By the *product* $\mathfrak{o}_1 \times \mathfrak{o}_2$ we understand the system

$$\mathfrak{o}_1 \times \mathfrak{o}_2 = (b_1 c_1, \ldots, b_\nu c_\mu, \ldots, b_n c_m),$$

where b_ν is permutable with c_μ, and the multiplication is defined by

$$b_\gamma c_\mu \cdot b_\varrho c_\sigma = (b_\gamma b_\varrho)(c_\mu c_\sigma).$$

Hence the elements of the product system are the sums

$$\sum\sum\alpha_{\lambda\mu}b_\lambda c_\mu.$$

These sums may be written either as

$$\sum b'_\mu c_\mu,$$

where the b'_μ are arbitrary elements of $\mathfrak{o}_1$, or as

$$\sum b_\lambda c'_\lambda,$$

where the c'_λ are arbitrary elements of $\mathfrak{o}_2$. The first expression shows that the formation of a product is independent of the basis chosen for $\mathfrak{o}_1$; the second shows the independence of the basis chosen for $\mathfrak{o}_2$.

It is easy to show that

$$\mathfrak{o}_1 \times \mathfrak{o}_2 = \mathfrak{o}_2 \times \mathfrak{o}_1,$$

$$\mathfrak{o}_1 \times (\mathfrak{o}_2 \times \mathfrak{o}_3) = (\mathfrak{o}_1 \times \mathfrak{o}_2) \times \mathfrak{o}_3.$$

Of particular importance is the product of a system $\mathfrak{o}$ and a field Λ of finite degree over P. If $\mathfrak{o} = (b_1, \ldots, b_n)$, the elements of such a product may be written in the form

$$\lambda_1 b_1 + \cdots + \lambda_n b_n = b_1\lambda_1 + \cdots + b_n\lambda_n \qquad (\lambda_i \in \Lambda),$$

i.e., the product $\Lambda \times \mathfrak{o}$ is a hypercomplex system with the same basis elements as $\mathfrak{o}$, but with Λ instead of P as the ground field. We also designate the system $\Lambda \times \mathfrak{o}$ by $\mathfrak{o}_\Lambda$. The symbol $\mathfrak{o}_\Lambda$ is also used, in the sense just described, when Λ is an infinite extension field of P. Furthermore, when Λ is a hypercomplex system over P, we will occasionally use the symbol $\mathfrak{o}_\Lambda$ as equivalent to $\Lambda \times \mathfrak{o}$.

In an extension of the ground field essential properties of the system $\mathfrak{o}$ may no longer be valid. For instance, the quaternion field $(1, j, k, l)$ does not remain a field in the extension of the rational number field Γ to $\Gamma(i)$ since zero divisors are thereby introduced:

$$j^2 + 1 = j^2 - i^2 = (j - i)(j + i) = 0,$$

and the system of quaternions over $\Gamma(i)$ becomes isomorphic to a matrix system with the basis elements

$$c_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad c_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad c_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad c_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

by the following correspondence:

$$1 \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = c_{11} + c_{22},$$

$$j \to \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = i(c_{11} - c_{22}),$$

$$k \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = c_{12} - c_{21},$$

$$i \to \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = i(c_{12} + c_{21}).$$

Important product relations are valid for complete matrix rings. Thus, let $\mathfrak{S}_r$ denote the system of all matrices of degree r with coefficients in $\mathfrak{S}$. Then

(1) $$\mathfrak{S}_r \simeq \mathfrak{S} \times \mathsf{P}_r$$

(2) $$\mathsf{P}_r \times \mathsf{P}_s \cong \mathsf{P}_{rs}.$$

Formula (1) is an immediate consequence of the representation of the elements of $\mathfrak{S}_r$ in the form $\sum c_{ij} \varkappa_{ij} = \sum c_{ij} (e \varkappa_{ij})$, where the $\varkappa_{ij} \in \mathfrak{S}$, the c_{ij} are permutable with the $\varkappa_{ij}$, and e is the unit matrix of r-th degree. The $e\varkappa$ form a subring $e\mathfrak{S} \cong \mathfrak{S}$, and the c_{ij} generate a subring $\cong \mathsf{P}_r$.

Formula (2) may be derived as follows: if P_r is generated by the r^2 elements c'_{ik} and P_s by the s^2 elements c''_{jl}, then $\mathsf{P}_r \times \mathsf{P}_s$ is generated by the $r^2 s^2$ elements

$$c_{ij,kl} = c'_{ik} c''_{jl}$$

which satisfy the rules

$$c_{ij,kl} \cdot c_{mn,pq} = \begin{cases} 0, & \text{if } k \neq m \text{ or } l \neq n \\ c_{ij,pq}, & \text{if } k = m,\ l = n. \end{cases}$$

If we number the rs possible pairs of indices ij by an index α which runs from 1 to rs, and similarly the kl indices by an index β, then these rules go over into

$$c_{\alpha\beta} \cdot c_{\gamma\delta} = \begin{cases} 0 & \text{for } \beta \neq \gamma, \\ c_{\alpha\delta} & \text{for } \beta = \gamma, \end{cases}$$

and we recognize the isomorphism to P_{rs}.

From (1) and (2) follows

(3) $$\mathfrak{S}_r \times \mathsf{P}_s \cong \mathfrak{S} \times \mathsf{P}_r \times \mathsf{P}_s \cong \mathfrak{S} \times \mathsf{P}_{rs} \cong \mathfrak{S}_{rs}.$$

115. HYPERCOMPLEX SYSTEMS AS GROUPS WITH OPERATORS. GENERALIZATION

A hypercomplex system $\mathfrak{o}$, considered as an Abelian group with respect to addition, admits two types of operator domains.

First, the field P. For this operator domain all allowable subgroups are *linear systems*, i.e., subsets of $\mathfrak{o}$ which contain λa (every λ in P) for every a and

$a - b$ for every a and b. Every linear system has a rank $\leqq n$, where n is the rank of $\mathfrak{o}$ (Section 33).

Secondly, the system $\mathfrak{o}$ itself, whose elements may be interpreted either as left- or right operators. In this case the allowable subgroups are the *left ideals, right ideals,* and *two-sided ideals.*

We now agree once and for all that in the consideration of (left, right, or two-sided) ideals in hypercomplex systems the field P will always be regarded as an operator domain. This means that an *allowable left ideal* will be a subgroup which besides a contains not only every ra (r in $\mathfrak{o}$) but also every λa (λ in P), and correspondingly for right ideals. Hence allowable ideals are always linear systems. Furthermore, two left ideals are *operator isomorphic* only if an isomorphism exists such that if a is mapped on $\bar{a}$, then every ra is mapped [1] on $r\bar{a}$ and every λa on $\lambda\bar{a}$. Finally, a left ideal is said to be *simple* or *minimal,* when it contains no allowable left ideals besides itself and the null ideal.

With these restrictions imposed on the concepts of ideals, the ideals of a hypercomplex system satisfy the "*maximal- and minimal condition.*"

Every non-empty set of (right, left, or two-sided) ideals contains (at least) one maximal ideal, i.e., an ideal which is contained in no other ideal of the set, and one minimal ideal, i.e., one which contains no other ideal of the set.

Thus, according to the above convention, every ideal is also a linear system and in every non-empty set of linear systems of rank $\leqq n$ there is a system of largest and smallest rank.

In order to develop the Fundamental Theorem of the hypercomplex algebra under as general assumptions as possible we will no longer restrict ourselves to hypercomplex systems in the course of this chapter. Instead, we will assume that $\mathfrak{o}$ is an arbitrary ring which satisfies, say for left ideals, the maximal- and minimal condition formulated above. Occasionally, we shall actually assume only the maximal- or only the minimal condition.[2]

The ring $\mathfrak{o}$ may (though not necessarily) possess an operator domain Ω (which takes over the role of P); its operators $\lambda, \mu, \ldots$ must have the properties

$$\lambda(a + b) = \lambda a + \lambda b,$$
$$\lambda(ab) = (\lambda a)b = a(\lambda b).$$

If such an operator domain exists, the concept of ideal shall be restricted, as above, by the condition that every ideal shall contain besides a also λa (λ in Ω). When we wish to stress this explicitly, we shall speak of *allowable* right- or left ideals. We will impose the maximal- and (or) minimal condition only for these ideals.

[1] This differs from ring isomorphism, whereby ra is not mapped on $r\bar{a}$ but on $\bar{r}\bar{a}$ when r and a both belong to the subring under consideration.

[2] By Section 84 the maximal condition is equivalent to the divisor chain condition.

Since we will be concerned with arbitrary rings which satisfy only the maximal- and minimal condition, the extent of our investigation is considerably expanded; for, there are many rings which satisfy these conditions without being hypercomplex systems. For instance, all finite rings (such as the residue class rings modulo the ideals, distinct from the null ideal, of an order in a number field and especially the residue class rings modulo an integer in the ring C) evidently satisfy the maximal- and minimal condition. For commutative rings which also satisfy this condition, see Exercises 3, 4, and 5, below. Meanwhile, the hypercomplex systems remain the principal object of our investigation.

We now state that the minimal condition is more restrictive than the maximal condition. On the one hand, we have already seen in Section 84 that there is a wide variety of rings with zero divisors and without zero divisors for which the maximal condition is valid (the most interesting rings fall in this category). On the other hand, we will soon show that the minimal condition is valid, for instance, in rings without zero divisors only if the rings are fields.

We must now determine if the ideal-theoretic combining concepts: sum, product, etc., retain their meaning for non-commutative rings with operator domains or without operator domains. First, it is clear (as, in general, for groups with operators) that the *intersection* $\mathfrak{a} \cap \mathfrak{b}$ and the *sum* $(\mathfrak{a}, \mathfrak{b})$ of two allowable right- or left ideals $\mathfrak{a}$ and $\mathfrak{b}$ are also allowable right- or left ideals respectively. Secondly, it is easy to see that a *product* $\mathfrak{a} \cdot \mathfrak{b}$ (the set of all sums $\sum ab$, $a \in \mathfrak{a}$, $b \in \mathfrak{b}$) is an allowable right ideal as soon as the second factor is an allowable right ideal, and an allowable left ideal as soon as the first factor is an allowable left ideal. In each case the other factor may be either an entirely arbitrary set or a single element of $\mathfrak{o}$; for instance, $\mathfrak{p}\mathfrak{r}$, the totality of all products $\mathfrak{p}a (a \in \mathfrak{r})$, is a right ideal as soon as $\mathfrak{r}$ is one.

As usual the associative and distributive laws are valid for modules and especially for ideals in a ring $\mathfrak{o}$:

$$\mathfrak{a} \cdot \mathfrak{b}\mathfrak{c} = \mathfrak{a}\mathfrak{b} \cdot \mathfrak{c},$$

$$\mathfrak{a}(\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a}\mathfrak{b}, \mathfrak{a}\mathfrak{c}),$$

$$(\mathfrak{b}, \mathfrak{c})\mathfrak{a} = (\mathfrak{b}\mathfrak{a}, \mathfrak{c}\mathfrak{a}).$$

In these formulae $\mathfrak{a}$ may be either an arbitrary set or a single element.

In a ring $\mathfrak{o}$ if the minimal condition is valid, say for left ideals, and $\mathfrak{o}$ is not the null ring, then in the set of *all* left ideals distinct from the null ideal there are minimal ideals; we simply call these *minimal left ideals.* They are characterized by the property that they possess no proper subideals distinct from the null ideal. Hence they may also be designated as *simple left ideals.*

If an (one-sided or two-sided) ideal $\mathfrak{a}$ in $\mathfrak{o}$ is the direct sum of one-sided or two-sided ideals respectively, say

$$\mathfrak{a} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n,$$

where $n > 1$ and every $\mathfrak{a}_\nu \neq (0)$, then the ideal $\mathfrak{a}$ is said to be (one-sided or two-sided) *directly decomposable.* If such a decomposition is not possible, $\mathfrak{a}$ is said to be *directly indecomposable.*

In order to show the restrictiveness of the minimal condition we prove the following theorem.

If $\mathfrak{o}$ is a ring satisfying the minimal condition for left ideals and if a is an element of $\mathfrak{o}$ which is not a right zero divisor in $\mathfrak{o}$, then the equation $xa = b$ can be solved in $\mathfrak{o}$ for every b.

PROOF. In the set of left ideals $\mathfrak{o}a^\mu (\mu = 1, 2, \ldots)$ there must be a minimal one, say $\mathfrak{o}a^m$. Since $\mathfrak{o}a^{m+1} \subseteq \mathfrak{o}a^m$ is valid but $\mathfrak{o}a^{m+1} \subset \mathfrak{o}a^m$ is excluded, then $\mathfrak{o}a^{m+1} = \mathfrak{o}a^m$. Hence every product ba^m may also be written in the form ca^{m+1}:

$$ba^m = ca^{m+1}$$

Since the factor a may be cancelled m times on the right and left, this equality may be reduced to

$$b = ca.$$

Hence the equation $xa = b$ has a solution.

Similarly, *if $\mathfrak{o}$ is a ring satisfying the minimal condition for the right ideals and if a is not a left zero divisor, then $ax = b$ can be solved.*

On combining these two theorems we have:

If $\mathfrak{o}$ is a ring without zero divisors satisfying the minimal condition for right- and left ideals, then $\mathfrak{o}$ is a field.

EXERCISES. 1. In the above we have considered only ideals which have P or Ω as operator domains. For a ring with an identity, this restriction is unessential: every ideal allows the multiplication by P or Ω.

2. The left ideals of a domain $\mathfrak{o}$ satisfy the maximal- and minimal condition if and only if there exists a composition series for these left ideals.

3. In a commutative ring satisfying the minimal condition, the residue class ring modulo a prime ideal is always a field and therefore every prime ideal is maximal.

116. NILPOTENT IDEALS

An element a of a ring $\mathfrak{o}$ is said to be *nilpotent* if a power $a^e = 0$. A (left- or right) ideal $\mathfrak{a}$ is said to be *nilpotent* if a power $\mathfrak{a}^e$ is equal to the null ideal (0). The following theorems are valid:

1. *The sum $(\mathfrak{l}_1, \mathfrak{l}_2)$ of two nilpotent left ideals is a nilpotent left ideal.*

PROOF. Let $\mathfrak{l}_1^n = \mathfrak{l}_2^m = (0)$. Then $(\mathfrak{l}_1, \mathfrak{l}_2)^{n+m-1}$ is a left ideal; it is the totality of all sums whose summands are products of $n + m - 1$ factors from $\mathfrak{l}_1$

or $\mathfrak{I}_2$. In each summand there must be at least n factors from $\mathfrak{I}_1$ or m factors from $\mathfrak{I}_2$. If we assume the first case, the term has the form

$$\ldots \mathfrak{I}_1 \ldots \mathfrak{I}_1 \ldots \mathfrak{I}_1 \ldots,$$

where the dots can stand for factors from $\mathfrak{I}_2$ and at least n of the factors are from $\mathfrak{I}_1$. Therefore, since $\mathfrak{o}\mathfrak{I}_1 \subseteq \mathfrak{I}_1$, it follows that $\ldots \mathfrak{I}_1 \ldots \mathfrak{I}_1 \ldots \mathfrak{I}_1 \ldots \subseteq \mathfrak{I}_1^n \ldots = (0)$,

$$(\mathfrak{I}_1, \mathfrak{I}_2)^{n+m-1} = (0).$$

2. *Every nilpotent left ideal (or right ideal) is contained in a nilpotent two-sided ideal.*

PROOF. Let $\mathfrak{I}$ be a nilpotent left ideal: $\mathfrak{I}^\varrho = (0)$. Then $\mathfrak{I}\mathfrak{o}$ is also nilpotent:

$$(\mathfrak{I}\mathfrak{o})^\varrho = \mathfrak{I}(\mathfrak{o}\mathfrak{I})^{\varrho-1}\mathfrak{o} \subseteq \mathfrak{I}\mathfrak{I}^{\varrho-1}\mathfrak{o} = \mathfrak{I}^\varrho\mathfrak{o} = (0).$$

The right ideal $(\mathfrak{I}, \mathfrak{I}\mathfrak{o})$ generated by $\mathfrak{I}$ is accordingly the sum of two nilpotent left ideals and therefore it is itself a nilpotent left ideal. Hence it is a nilpotent two-sided ideal.

If we define a *root element* w as an element of $\mathfrak{o}$ which generates a nilpotent two-sided ideal, then

3. *All elements of a nilpotent left- or right ideal are root elements.*

PROOF. If w is contained in the nilpotent left ideal $\mathfrak{I}$, then by 2. w is also contained in a nilpotent two-sided ideal. Hence the two-sided ideal generated by w is also nilpotent.

By 3. we may also define the root elements as those elements which generate a nilpotent left- or right ideal.

4. *The totality of all root elements is a two-sided ideal which contains all nilpotent right- and left ideals.*

PROOF. Let w_1 and w_2 be root elements and $\mathfrak{w}_1$, $\mathfrak{w}_2$ the two-sided ideals generated by $\mathfrak{w}_1$, $\mathfrak{w}_2$. Then $w_1 - w_2$ is contained in the ideal $(\mathfrak{w}_1, \mathfrak{w}_2)$ which is nilpotent by 1.; therefore $w_1 - w_2$ is also a root element. Similarly, every multiple cw_1 or w_1c is a root element because such multiples belong to $\mathfrak{w}_1$. Hence the totality of root elements is a two-sided ideal. The remaining statements of the theorem follow from 3.

The totality of all root elements is called the *radical* of $\mathfrak{o}$.

DEFINITION. A *ring without radical* is a ring whose radical is the null ideal, in other words, a ring in which the null ideal is the only nilpotent ideal.

In a "ring *with* radical" there is a nilpotent left- or right ideal and consequently by 2. a nilpotent two-sided ideal $\mathfrak{a} \neq (0)$. It is easy to show that in this case there is also a two-sided ideal $\mathfrak{c} \neq (0)$ such that $\mathfrak{c}^2 = (0)$. Thus, if ϱ is the smallest integer such that $\mathfrak{a}^\varrho = (0)$, then $\mathfrak{c} = \mathfrak{a}^{\varrho-1}$ has the desired property.

If the maximal condition for left ideals is valid in $\mathfrak{o}$, there is a maximal nilpotent left ideal $\mathfrak{I}$. This ideal must include all root elements w, since other-

wise there would be a nilpotent left ideal $(\mathfrak{o}\, w, \mathfrak{l})$ which would properly contain $\mathfrak{l}$. Hence $\mathfrak{l}$ is equal to the radical, and it follows that *the radical is itself nilpotent.*

As a consequence we have:

For a ring $\mathfrak{o}$ which satisfies the maximal condition, the ring of the residue classes modulo the radical $\mathfrak{w}$ is always a ring without radical.

PROOF. A left ideal in $\mathfrak{o}/\mathfrak{w}$ may always be considered as a group of residue classes $\mathfrak{l}/\mathfrak{w}$, where $\mathfrak{l}$ is a left ideal in $\mathfrak{o}$. Let us assume that $\mathfrak{l}/\mathfrak{w}$ is nilpotent, say

$$(\mathfrak{l}/\mathfrak{w})^{\varrho} = (0),$$

Then every product of ϱ residue classes of $\mathfrak{l}$ (mod $\mathfrak{w}$) is equal to zero; this means that every product of ϱ elements of $\mathfrak{l}$ is contained in $\mathfrak{w}$:

$$\mathfrak{l}^{\varrho} \subseteq \mathfrak{w},$$
$$\mathfrak{w}^{\sigma} \subseteq (0),$$
$$\mathfrak{l}^{\varrho\sigma} = (\mathfrak{l}^{\varrho})^{\sigma} \subseteq \mathfrak{w}^{\sigma} = (0);$$

therefore $\mathfrak{l}$ is nilpotent and

$$\mathfrak{l} \subseteq \mathfrak{w},$$
$$\mathfrak{l}/\mathfrak{w} = (0).$$

A ring without radical satisfying the minimal condition for left ideals is also called *semi-simple.* This nomenclature is motivated by the fact that semi-simplicity is less restrictive than the concept of *simplicity*, which requires that there be no two-sided ideal in $\mathfrak{o}$ besides (0) and $\mathfrak{o}$ itself. Thus, let us assume that the ring $\mathfrak{o}$ not only satisfies the minimal condition but that there also exists an identity in the ring. Then $\mathfrak{o}$ itself cannot be nilpotent; therefore, the radical of a simple system with an identity can only be the null ideal.

EXERCISES. 1. The first two hypercomplex systems in Section 114, Exercise 5 are semi-simple; on the other hand, the remaining have the linear system (c) as the radical.

2. The hypercomplex system of rank 3 with the multiplication table

	e_1	e_2	u
e_1	e_1	0	u
e_2	0	e_1	0
u	0	u	0

has a radical; what is it? The residue class ring modulo the radical is the direct sum of two fields.

3. The system of all matrices of degree n in a field K is simple.

4. For commutative rings a root element is nothing else than a nilpotent element. Hence show that the residue class ring $C/(m)$ modulo an integer m is a ring without radical if and only if m has no prime factor which is squared.

5. This is also valid for the residue class ring modulo an ideal in the principal order of a number field.

6. The radical of a commutative primary ring is the prime ideal belonging to the null ideal.

7. If $(0) = [q_1, \ldots, q_r]$ is a decomposition of the null ideal of a commutative ring $\mathfrak{o}$ into primary components and if $p_1, \ldots, p_r$ are the prime ideals belonging to the components, then $[p_1, \ldots, p_r]$ is the radical.

117. THE COMPLETE REDUCIBILITY OF THE RINGS WITHOUT RADICAL

All group-theoretic terminology (direct sum, operator isomorphism, etc.) to be used in this section refers to the ring $\mathfrak{o}$ and its left ideals as an Abelian group with $\mathfrak{o}$ (and possibly also P or Ω; cf. Section 115) as a fixed (left) multiplicative domain.

The object of this section is to prove the *Fundamental Theorem of semi-simple rings*:

A ring $\mathfrak{o}$ without radical satisfying the minimal condition for left ideals has an identity and is a direct sum of simple left ideals. Conversely, a ring with identity, which is a direct sum of simple left ideals, is a ring without radical satisfying the minimal condition for left ideals.

The lemmas necessary for the proof of this theorem are also of interest in themselves.

LEMMA. 1. *If $\mathfrak{l}$ is a left ideal, a an element of $\mathfrak{o}$, then $\mathfrak{l}$ is operator-homomorphic to $\mathfrak{l}a$ by the correspondence*

$$x \to xa.$$

PROOF.[3]

$$(x + y)a = xa + ya,$$

$$(rx) \cdot a = r \cdot (xa),$$

$$(\lambda x) \cdot a = \lambda \cdot (xa).$$

LEMMA. 2. *A minimal (= simple) left ideal $\mathfrak{l}$ is mapped by an operator homomorphism either on the null ideal or the homomorphism is an isomorphism.*

PROOF. The totality of the elements a of $\mathfrak{l}$ which are mapped on the zero is a left ideal $\subseteq \mathfrak{l}$. Hence it is either $= (0)$ or $= \mathfrak{l}$. In the first case the correspondence is an isomorphism.

DEFINITION. An element e of $\mathfrak{o}$ is called *idempotent* when $e^2 = e$ (and therefore $e^3 = e$, etc.).

Hence the null element and the unit element are always idempotent.

[3] The proof is also valid when a is in an $\mathfrak{o}$-module instead of $\mathfrak{o}$.

LEMMA. 3. *A minimal left ideal* $\mathfrak{l}$ *is either nilpotent, and then we have* $\mathfrak{l}^2 = (0)$, *or* $\mathfrak{l}$ *contains an idempotent element* e *and is generated by this element:*

$$e^2 = e \quad \text{in } \mathfrak{l}, \qquad \mathfrak{l} = \mathfrak{o}e.$$

PROOF. Let us assume that $\mathfrak{l}^2 \neq (0)$. Then there is in $\mathfrak{l}$ an a such that $\mathfrak{l}a \neq (0)$. The correspondence $x \to xa$ is by Lemma 1 an homomorphism and by Lemma 2 an isomorphism; it carries $\mathfrak{l}$ into $\mathfrak{l}a$ and

$$\mathfrak{l}a \neq (0), \qquad \mathfrak{l}a \subseteq \mathfrak{l}.$$

Hence

$$\mathfrak{l}a = \mathfrak{l}.$$

Accordingly every element of $\mathfrak{l}$ may be represented in the form xa (x in $\mathfrak{l}$); in particular for a itself:

$$a = ea \qquad (e \text{ in } \mathfrak{l}).$$

This implies that $e \neq 0$ and $ea = e^2a$. Hence the elements e and e^2 are mapped, by the isomorphism $x \to xa$, on the same element ea; therefore they are equal to one another:

$$e^2 = e.$$

The ideal $\mathfrak{o}e$ is not the null ideal (since it contains the element $e^2 = e$) and is contained in $\mathfrak{l}$; therefore it is equal to $\mathfrak{l}$. This completes the proof.

LEMMA. 4. *If* e *is idempotent and* $\mathfrak{l} = \mathfrak{o}e$, *then* $\mathfrak{o}$ *is the direct sum of* $\mathfrak{l}$ *and another left ideal* $\mathfrak{l}'$:

$$\mathfrak{o} = \mathfrak{l} + \mathfrak{l}'.$$

Furthermore, for all x *in* $\mathfrak{l}$

$$xe = x$$

for all x' *in* $\mathfrak{l}'$,

$$x'e = 0.$$

PROOF. Every a in $\mathfrak{o}$ may be written as $a = ae + (a - ae)$ (left-sided Peirce decomposition). The elements ae form the left ideal $\mathfrak{o}e = \mathfrak{l}$. The elements $a - ae$ also form a left ideal $\mathfrak{l}'$, since

$$(a - ae) - (b - be) = (a - b) - (a - b)e,$$
$$r(a - ae) = ra - (ra)e,$$
$$\lambda(a - ae) = \lambda a - (\lambda a)e.$$

The elements $a - ae$ are annihilated by e:

$$(a - ae)e = ae - ae^2 = 0;$$

while the elements ae reproduce themselves when multiplied by e:

$$(ae)e = ae^2 = ae.$$

The single element, which is annihilated and reproduced when multiplied by e, is the null element. Hence $\mathfrak{l}$ and $\mathfrak{l}'$ have only the null element in common; i.e., the sum $\mathfrak{o} = \mathfrak{l} + \mathfrak{l}'$ is direct.

We can now prove the first part of the Fundamental Theorem:

THEOREM. 1. *A ring without radical satisfying the minimal condition for left ideals is the direct sum of simple left ideals.*

PROOF. The theorem is obviously valid for the null ring. Let us assume therefore that $\mathfrak{o}$ is distinct from the null ring, and that $\mathfrak{l}_1$ is a minimal left ideal distinct from the null ideal. By Lemmas 3 and 4 we have

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}'.$$

If $\mathfrak{l}'$ is not the null ideal, we seek in $\mathfrak{l}'$ a minimal left ideal $\mathfrak{l}_2$ distinct from the null ideal; then by Lemmas 3 and 4

$$\mathfrak{o} = \mathfrak{l}_2 + \mathfrak{l}^*.$$

But if we apply this sum representation of the elements of $\mathfrak{o}$ to the elements of $\mathfrak{l}'$, we obtain

$$\mathfrak{l}' = \mathfrak{l}_2 + \mathfrak{l}'',$$

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \mathfrak{l}''.$$

Again, if $\mathfrak{l}'' \neq (0)$, we seek in $\mathfrak{l}''$ a minimal left ideal $\mathfrak{l}_3 \neq (0)$ and find as above that

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \mathfrak{l}_3 + \mathfrak{l}''',$$

etc. The series $\mathfrak{o} \supset \mathfrak{l}' \supset \mathfrak{l}'' \supset \mathfrak{l}''' \supset \cdots$ must contain a minimal left ideal by the minimal condition. If we call it $\mathfrak{l}_n$ and continue the decomposition up to $\mathfrak{l}_n$, we obtain

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \cdots + \mathfrak{l}_n,$$

which *proves* Theorem 1.

In our construction every one of the ideals $\mathfrak{l}_i$ is generated by an idempotent element:

$$\mathfrak{l}_i = \mathfrak{o}e_i, \qquad e_i^2 = e_i \in \mathfrak{l}_i$$

Furthermore, since $\mathfrak{l}'$ is annihilated by e_1, we have

$$e_2e_1 = 0, \quad e_3e_1 = 0, \quad \ldots, \quad e_ne_1 = 0,$$

similarly, since $\mathfrak{l}''$ is annihilated by e_2:

$$e_3e_2 = 0, \quad \ldots, \quad e_ne_2 = 0$$

etc.; in general

$$e_ke_i = 0 \quad \text{for} \quad k > i.$$

We will now show that the given assumptions imply the *existence of the identity.* We form

$$e_{12} = e_1 + e_2 - e_1 e_2.$$

Then

$$\begin{aligned} e_1 e_{12} &= e_1^2 + e_1 e_2 - e_1^2 e_2 &&= e_1, \\ e_2 e_{12} &= e_2 e_1 + e_2^2 - e_2 e_1 e_2 &&= e_2, \\ (e_1 e_2) e_{12} &= e_1 (e_2 e_{12}) &&= e_1 e_2. \end{aligned}$$

Hence

$$\begin{aligned} (e_1 + e_2 - e_1 e_2) e_{12} &= e_1 + e_2 - e_1 e_2, \\ e_{12}^2 &= e_{12}. \end{aligned}$$

The element e_{12} is therefore idempotent and is contained in $\mathfrak{l}_1 + \mathfrak{l}_2$. By the above calculations the element e_1 as well as e_2 occurs among the left multiples xe_{12}. Hence every element of $\mathfrak{l}_1 + \mathfrak{l}_2$ is such a multiple and

$$\mathfrak{l}_1 + \mathfrak{l}_2 = \mathfrak{o} e_{12}.$$

Furthermore,

$$e_k e_{12} = 0 \quad \text{for} \quad k > 2.$$

Next, set

$$e_{123} = e_{12} + e_3 - e_{12} e_3;$$

as above. we find that

$$\begin{aligned} e_{123}^2 &= e_{123}, \\ \mathfrak{o} e_{123} &= \mathfrak{o} e_{12} + \mathfrak{l}_3 = \mathfrak{l}_1 + \mathfrak{l}_2 + \mathfrak{l}_3. \end{aligned}$$

Continuing in this manner we finally obtain an idempotent element $e = e_{12\ldots n}$ with the property

$$\mathfrak{o} e = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n = \mathfrak{o}.$$

By Lemma 4 e is a right unit element for $\mathfrak{o} = \mathfrak{o} e$. In order to show that e is also a left unit element, we form a right-sided Peirce decomposition (Lemma 4 with the interchange of right and left). We have

$$\begin{aligned} \mathfrak{o} &= e\mathfrak{o} + \mathfrak{r}, \\ e\mathfrak{r} &= (0), \\ \mathfrak{r} &= \mathfrak{r} e \quad \text{(since } e \text{ is a right unit element)}, \\ \mathfrak{r}^2 &= \mathfrak{r} e \mathfrak{r} = (0); \end{aligned}$$

consequently, since $\mathfrak{o}$ is a ring without radical,

$$\begin{aligned} \mathfrak{r} &= (0), \\ \mathfrak{o} &= e\mathfrak{o}. \end{aligned}$$

Hence e is a left unit element (Lemma 4 with the interchange of right and left).

This *proves* the first part of the Fundamental Theorem.

For the converse we need

LEMMA. 5. *If a ring* $\mathfrak{o}$ *with identity is a direct sum of n left ideals:*

$$\mathfrak{o} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n,$$

and there exists in particular for the identity the representation

$$1 = e_1 + \cdots + e_n, \qquad (e_i \in \mathfrak{l}_i)$$

then

$$\mathfrak{l}_i = \mathfrak{o} e_i,$$
$$e_i^2 = e_i,$$
$$e_i e_k = 0 \quad \textit{for} \quad i \neq k.$$

PROOF. For every a in $\mathfrak{l}_1$ we have

$$a = a \cdot 1 = ae_1 + ae_2 + \cdots + ae_n,$$

and

$$a = a + 0 + \cdots + 0.$$

Hence since the sum is direct,

$$ae_1 = a, \quad ae_2 = 0, \quad \ldots, \quad ae_n = 0.$$

If we apply this in particular to $a = e_1$, then

$$e_1^2 = e_1, \quad e_1 e_2 = 0, \quad \ldots, \quad e_1 e_n = 0.$$

Similarly, since no one index is preferred to another, we have

$$e_i^2 = e_i,$$
$$e_i e_k = 0 \quad \textit{for} \quad i \neq k.$$

Furthermore, the equation $ae_1 = a$ shows that every a of $\mathfrak{l}_1$ may be written in the form ae_1. Hence

$$\mathfrak{l}_1 = \mathfrak{o} e_1$$

and similarly in general

$$\mathfrak{l}_i = \mathfrak{o} e_i \qquad \text{(Q.E.D.)}.$$

In regard to the converse of the Fundamental Theorem we note the following facts.

If a ring $\mathfrak{o}$ is a direct sum of n *simple* left ideals, we say that $\mathfrak{o}$ is *left-sided completely reducible.* From a pure group-theoretic point of view this implies the existence of a composition series (for left ideals) of length n (Section 47). Hence every left ideal also possesses a composition series whose length is at most n. Therefore in every non-empty set of left ideals there is an ideal of smallest length; consequently a minimal left ideal: *The minimal condition is therefore a consequence of the complete reducibility.* (A similar relationship exists for the maximal condi-

tion.) Furthermore, we have the pure group-theoretic fact that every left ideal is a direct summand (Section 47).

If we now assume the existence of an identity, it is very easy to prove that we are dealing with a ring without radical. Thus, if we had a nilpotent left ideal $\mathfrak{l}$, say with $\mathfrak{l}^e = (0)$, then

$$\mathfrak{o} = \mathfrak{l} + \mathfrak{l}'.$$

By Lemma 5 this implies that there is in $\mathfrak{l}$ a generating element e_1 with $e_1^2 = e_1$; therefore $e_1^e = e_1$. But $e_1^e = 0$ since $\mathfrak{l}$ is nilpotent. Hence $e_1 = 0$ and $\mathfrak{l} = (0)$. This means that the only nilpotent left ideal is the null ideal.

This completes the proof of the second part of the Fundamental Theorem.

EXERCISES. 1. Every ring without zero divisors which satisfies the minimal condition for left ideals is a field.

2. Decompose the ring with radical of Section 116, Exer. 2 into directly indecomposable left- or right ideals and verify that these are not simple.

3. The system consisting of all matrices of degree n in a field K is (left- and right-sided) completely reducible.

4. Prove the following converse of Lemma 5:

In a ring $\mathfrak{o}$ with identity if

$$1 = e_1 + \cdots + e_n,$$

$$e_i^2 = e_i, \quad e_i e_k = 0 \quad \text{for} \quad i \neq k,$$

then

$$\mathfrak{o} = \mathfrak{o}e_1 + \cdots + \mathfrak{o}e_n$$

is a decomposition of $\mathfrak{o}$ in left ideals and similarly

$$\mathfrak{o} = e_1\mathfrak{o} + \cdots + e_n\mathfrak{o}$$

is a decomposition of $\mathfrak{o}$ in right ideals.

118. TWO-SIDED DECOMPOSITION AND DECOMPOSITION OF CENTRUM

In Section 117 we investigated the decomposition of a ring $\mathfrak{o}$ as a direct sum of left ideals under certain assumptions; now we shall see what may be said about the decomposition in *two-sided* ideals

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n. \tag{1}$$

First, it is obvious that for a decomposition (1) the summands $\mathfrak{a}_i$ must mutually annihilate one another:

$$\mathfrak{a}_i\mathfrak{a}_k = (0) \quad \text{for} \quad i \neq k,$$

since $\mathfrak{a}_i\mathfrak{a}_k$ is contained both in $\mathfrak{a}_i$ and in $\mathfrak{a}_k$.

The ideals $\mathfrak{a}_i$ may also be considered as rings. The decomposition (1) is therefore a representation of $\mathfrak{o}$ as a sum of rings which mutually annihilate one another.

Conversely, if there exists a representation of $\mathfrak{o}$ as a sum of rings $\mathfrak{a}_i$ which mutually annihilate one another, these rings are necessarily two-sided ideals in $\mathfrak{o}$; for

$$\begin{aligned}\mathfrak{o}\mathfrak{a}_i &= (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)\cdot\mathfrak{a}_i \\ &= (\mathfrak{a}_1\mathfrak{a}_i, \ldots, \mathfrak{a}_n\mathfrak{a}_i) = \mathfrak{a}_i^2 \subseteq \mathfrak{a}_i\end{aligned}$$

and similarly

$$\mathfrak{a}_i\mathfrak{o} \subseteq \mathfrak{a}_i.$$

Furthermore this shows: *every (one-sided or two-sided) ideal in the ring* $\mathfrak{a}_i$ *is at the same time an (one-sided or two-sided) ideal in* $\mathfrak{o}$. Thus, if $\mathfrak{l}$ is, let us say, a left ideal in $\mathfrak{a}_1$, then

$$\begin{aligned}\mathfrak{o}\mathfrak{l} &= (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)\,\mathfrak{l} = (\mathfrak{a}_1\mathfrak{l}, \ldots, \mathfrak{a}_n\mathfrak{l}) \\ &= \mathfrak{a}_1\mathfrak{l} \subseteq \mathfrak{l}\end{aligned}$$

In particular if the ideals $\mathfrak{a}_i$ are two-sided simple, then according to this theorem they are two-sided simple also as rings. A "two-sided simple ring" is usually called a *simple ring*. Hence a simple ring possesses no two-sided ideals except itself and the null ideal.

If a ring $\mathfrak{o}$ *with identity can be represented as a direct sum of directly indecomposable two-sided ideals distinct from the null ideal:*

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n,$$

then the ideals $\mathfrak{a}_i$ *are uniquely determined.*

PROOF. If we had a second decomposition

$$\mathfrak{o} = \mathfrak{c}_1 + \cdots + \mathfrak{c}_m,$$

then

$$\mathfrak{c}_1 = \mathfrak{o}\mathfrak{c}_1 = (\mathfrak{a}_1\mathfrak{c}_1, \mathfrak{a}_2\mathfrak{c}_1, \ldots, \mathfrak{a}_n\mathfrak{c}_1).$$

The sum on the right is direct since

$$\mathfrak{a}_1\mathfrak{c}_1 \subseteq \mathfrak{a}_1, \ldots, \mathfrak{a}_n\mathfrak{c}_1 \subseteq \mathfrak{a}_n.$$

However since $\mathfrak{c}_1$ is directly indecomposable, all products on the right must $= (0)$ with the exception of a single one, say $\mathfrak{a}_1\mathfrak{c}_1$. Then we have

$$\mathfrak{c}_1 = \mathfrak{a}_1\mathfrak{c}_1 \subseteq \mathfrak{a}_1.$$

Similarly, we can show that conversely $\mathfrak{a}_1$ is contained in a $\mathfrak{c}_i$. Therefore

$$\mathfrak{c}_1 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{c}_i;$$

this implies $i = 1$ and $\mathfrak{c}_1 = \mathfrak{a}_1$. Hence every $\mathfrak{c}_i$ is equal to an $\mathfrak{a}_i$.

For the decomposition as a direct sum of one-sided ideals we shall see that this uniqueness is no longer valid.

For *commutative* rings the distinction between one-sided and two-sided ideals is dropped. The Fundamental Theorem of Section 117 together with Lemma 5 implies the existence of a representation for an arbitrary semi-simple commutative ring $\mathfrak{o}$ as a sum of simple rings with unit elements which mutually annihilate one another. But, every simple commutative ring with an identity is a field since the multiples ax of an element $a \neq 0$ form an ideal distinct from the null ideal and therefore the entire ring. Hence (Theorem of Dedekind):

Every commutative ring without radical satisfying the minimal condition is a direct sum of commutative fields which mutually annihilate one another.

In the case of commutative rings $\mathfrak{o}$ *with* radical and with identity we can find a similar sum decomposition, i.e., as direct sum of primary rings, by decomposing (cf. Section 115, Exercise 3), under the assumption of the maximal- and minimal condition, the null ideal by Section 90 into single-primed primary ideals and thereby derive by Section 89, end, a sum representation for $\mathfrak{o}$.

By the *centrum* of a ring $\mathfrak{o}$ we understand the totality of the elements a of $\mathfrak{o}$ which are permutable with all elements of $\mathfrak{o}$:

$$ax = xa \quad \text{for all } x.$$

The centrum is a subring; for if $ax = xa$ and $bx = xb$, then

$$(a - b)x = ax - bx = xa - xb = x(a - b)$$

and

$$ab \cdot x = axb = x \cdot ab.$$

When $\mathfrak{o}$ possesses an operator domain in the sense of Section 115, then the centrum $\mathfrak{Z}$ is also an allowable subring; for if a is any element of the centrum, then for all operators λ and all x we have

$$(\lambda a)x = \lambda(ax) = \lambda(xa) = x \cdot \lambda a,$$

whereupon λa also belongs to the centrum.

The centrum is naturally commutative. If the ring has an identity, this element always belongs to the centrum.

If $\mathfrak{o}$ is a ring without radical, then $\mathfrak{Z}$ is also a ring without radical.

PROOF. Let us assume that the radical of $\mathfrak{Z}$ is distinct from the null ideal. Then the ring $\mathfrak{Z}$ has an ideal $\mathfrak{c} \neq (0)$ such that $\mathfrak{c}^2 = (0)$. $\mathfrak{c}$ generates in $\mathfrak{o}$ a left ideal $\mathfrak{b} = (\mathfrak{c}, \mathfrak{o}\mathfrak{c})$, and since $\mathfrak{c}$ is permutable with $\mathfrak{o}$, then

$$\mathfrak{b}^2 = (\mathfrak{c}, \mathfrak{o}\mathfrak{c})^2 = (\mathfrak{c}^2, \mathfrak{c}\mathfrak{o}\mathfrak{c}, \mathfrak{o}\mathfrak{c}^2, \mathfrak{o}\mathfrak{c}\mathfrak{o}\mathfrak{c})$$
$$= (\mathfrak{c}^2, \mathfrak{o}\mathfrak{c}^2, \mathfrak{o}^2\mathfrak{c}^2) = (0).$$

Hence $\mathfrak{o}$ has a nilpotent ideal $\mathfrak{b} \neq (0)$, which contradicts the hypothesis.

If $\mathfrak{o}$ is a direct sum of two-sided ideals:

(1) $$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n,$$

then the centrum $\mathfrak{Z}$ *of* $\mathfrak{o}$ *is a direct sum of the centrums* $\mathfrak{Z}_i$ *of the rings* $\mathfrak{a}_i$*:*

$$\mathfrak{Z} = \mathfrak{Z}_1 + \cdots + \mathfrak{Z}_n.$$

PROOF. First, the centrums $\mathfrak{Z}_i$ of the rings $\mathfrak{a}_i$ are contained in $\mathfrak{Z}$. Thus, if a_i belongs to $\mathfrak{Z}_i$, then for an arbitrary

$$x = x_1 + \cdots + x_n \qquad (x_j \in \mathfrak{a}_j)$$

from $\mathfrak{o}$:

$$a_i x = a_i x_i = x_i a_i = x a_i;$$

all products $a_i x_k$ and $x_k a_i$ with $i \neq k$ are actually zero.

Moreover by (1) every element a of $\mathfrak{Z}$ admits a decomposition

$$a = a_1 + \cdots + a_n \qquad (a_j \in \mathfrak{a}_j)$$

and for any x_i from $\mathfrak{a}_i$ we have

$$a_i x_i = a x_i = x_i a = x_i a_i;$$

consequently, every a_i is contained in $\mathfrak{Z}_i$. $\mathfrak{Z}$ is therefore the sum of the $\mathfrak{Z}_i$; these summands naturally annihilate one another. From $0 = a_1 + \cdots + a_n (a_i \in \mathfrak{Z}_i)$ it follows that $a_i = 0$ since the sum (1) is direct. Hence the sum of the $\mathfrak{Z}_i$ is direct.

EXERCISES. 1. If $\mathfrak{Z} = \mathfrak{Z}_1 + \cdots + \mathfrak{Z}_n$ is a decomposition of the centrum $\mathfrak{Z}$ of a ring $\mathfrak{o}$ with identity and we set

$$\mathfrak{a}_i = \mathfrak{o}\mathfrak{Z}_i,$$

then the $\mathfrak{a}_i$ are two-sided ideals in $\mathfrak{o}$ and

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n,$$

while $\mathfrak{Z}_i = \mathfrak{a}_i \cap \mathfrak{Z}$ is the centrum of the ring $\mathfrak{a}_i$.

2. If the $\mathfrak{a}_\nu$ in (1) are directly indecomposable, the same is true of the $\mathfrak{Z}_\nu$.

3. The centrum $\mathfrak{Z}$ of a hypercomplex system $\mathfrak{o}$ is again a hypercomplex system; if $\mathfrak{o}$ is a system without radical, $\mathfrak{Z}$ is a direct sum of fields.

4. If $\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n$ is a two-sided decomposition of a ring with identity, every minimal left ideal of $\mathfrak{o}$ is contained in one of the $\mathfrak{a}_\nu$.

5. The centrum of the group ring of a group $\mathfrak{G}$ consists of those sums

$$\sum \lambda_\nu a_\nu$$

in which all elements a_ν of a class of conjugate elements of $\mathfrak{G}$ have the same coefficients λ_ν. There are in $\mathfrak{o}$ as many linearly independent centrum elements as there are classes in $\mathfrak{G}$.

119. THE ENDOMORPHISM RING OF A COMPLETELY REDUCIBLE MODULE

In Section 117 we have seen that a semi-simple ring $\mathfrak{o}$, considered as an $\mathfrak{o}$-left module, is completely reducible. We will now determine the endomorphism ring of this completely reducible module.

The problem of the structure of the endomorphism ring of a completely reducible module $\mathfrak{M}$ is important in itself and for various applications. We will solve the problem from a general point of view and then go over to the special case, from which we started, wherein the module $\mathfrak{M}$ is a ring with itself as multiplicative domain.

Let $\mathfrak{M}$ be a completely reducible module with an arbitrary multiplicative domain. By an endomorphism of $\mathfrak{M}$ we understand by Section 10 an operator homomorphism of $\mathfrak{M}$ into itself. By Section 43 these endomorphisms always form a ring; the structure of this endomorphism ring will now be considered.

If the module $\mathfrak{M}$ is in particular a module of linear forms with respect to a field K (whose elements are written as right operators) and $\mathfrak{M}$ possesses moreover certain left operators $A, B, \ldots$, which satisfy the condition $Am \cdot \varkappa = A \cdot m\varkappa$ and therefore induce linear transformations of the vector space (cf. Section 106), then the endomorphisms of this double module $\mathfrak{M}$ are also linear transformations Θ which are permutable with the transformations A, B,

$$\Theta(Am) = A(\Theta m).$$

Our investigation therefore will contain, as a special case, the determination of the linear transformations permutable with a completely reducible system of linear transformations (cf. Exer. 1, below).

First we consider the homomorphic mappings of a simple module $\mathfrak{M}_1$. The submodule of those elements which are mapped on zero is either $\mathfrak{M}_1$ itself or consists only of the null element. In the latter case the mapping is a 1-isomorphism. *For every homomorphism the simple module $\mathfrak{M}_1$ is mapped either on zero or the mapping is a 1-isomorphism.*

If $\mathfrak{M}_1$ is mapped into itself and the mapping is not the null operator (which maps $\mathfrak{M}_1$ on zero), then the mapping is a 1-isomorphism and takes $\mathfrak{M}_1$ in a submodule distinct from zero, i.e., on $\mathfrak{M}_1$ itself. Such a 1-automorphism always possesses an inverse automorphism. Hence in the endomorphism ring of $\mathfrak{M}_1$ every element distinct from zero has an inverse, i.e., *the endomorphism ring of a simple module is a skew field.*

In the same manner we have: *if $\mathfrak{M}_1$ is mapped homomorphically on another simple module $\mathfrak{M}_2$ and the mapping is not the null operator, then it must be a 1-isomorphism and therefore $\mathfrak{M}_1 \cong \mathfrak{M}_2$.*

We may now determine the endomorphisms of $\mathfrak{M} = \mathfrak{M}_1 + \cdots + \mathfrak{M}_r$, where the $\mathfrak{M}_i$ are simple. First we note: if an element m is decomposed into its components

(1) $$m = m_1 + \ldots + m_r,$$

then every correspondence $m \to m_\nu$ is an homomorphism. We designate it by H_ν. Instead of (1) we may now write:

(2) $$m = \sum_\nu H_\nu m.$$

An arbitrary endomorphism Θ is completely determined as soon as we know its effect on the components $m_\nu = H_\nu m$ since

(3) $$\Theta m = \sum_\nu \Theta m_\nu$$

Decompose the elements Θm_ν into components:

(4) $$\Theta m_\nu = \sum_\mu H_\mu \Theta m_\nu.$$

The operator $H_\mu \Theta$, applied to the elements m_ν of $\mathfrak{M}_\nu$, produces a homomorphism which maps $\mathfrak{M}_\nu$ into $\mathfrak{M}_\mu$. We designate this homomorphism by $\Theta_{\mu\nu}$. The r^2 homomorphisms $\Theta_{\mu\nu}$ may be arranged as a square matrix. If $\mathfrak{M}_\nu$ is not isomorphic to $\mathfrak{M}_\mu$, then $\Theta_{\mu\nu}$ must be the null operator. Instead of (4) we now write

(5) $$\Theta m_\nu = \sum_\mu \Theta_{\mu\nu} m_\nu.$$

Setting this in (3), we obtain

(6) $$\Theta m = \sum_\mu \sum_\nu \Theta_{\mu\nu} m_\nu = \sum_\mu \sum_\nu \Theta_{\mu\nu} H_\nu m \quad \text{or}$$

(7) $$\Theta = \sum_\mu \sum_\nu \Theta_{\mu\nu} H_\nu.$$

Since we may go back from (6) or (7) to (5) by specializing m to m_ν, and since the homomorphisms $\Theta_{\mu\nu}$ are uniquely determined by (5), then every endomorphism Θ is uniquely representable in the form (7) and the $\Theta_{\mu\nu}$ may be arbitrarily chosen.

If η is a second endomorphism:

$$\eta = \sum_\mu \sum_\nu \eta_{\mu\nu} H_\nu,$$

the sum and product of η and Θ is given by:

$$\eta + \Theta = \sum_\mu \sum_\nu (\eta_{\mu\nu} + \Theta_{\mu\nu}) H_\nu,$$

$$\eta\Theta = \sum_\lambda \sum_\mu \eta_{\lambda\mu} H_\mu \sum_{\mu'} \sum_\nu \Theta_{\mu'\nu} H_\nu$$

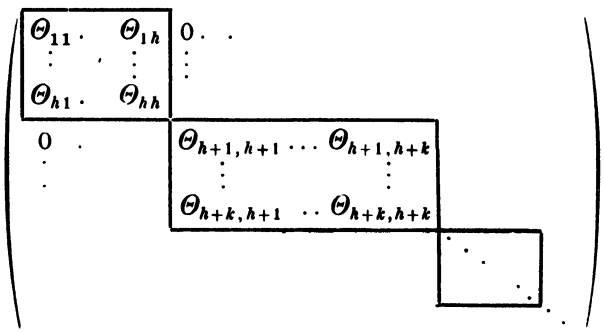
$$- \sum_\lambda \sum_\mu \eta_{\lambda\mu} \sum_\nu \Theta_{\mu\nu} H_\nu \,^4$$

$$= \sum_\lambda \sum_\nu (\sum_\mu \eta_{\lambda\mu} \Theta_{\mu\nu}) H_\nu.$$

[4] For $\mu \neq \mu'$ we have $H_\mu \Theta_{\mu'\nu} = 0$, since every element of $\mathfrak{M}_{\mu'}$ is annihilated by H_μ. On the contrary if $\mu = \mu'$, we have $H_\mu \Theta_{\mu'\nu} = \Theta_{\mu\nu}$, since every element of $\mathfrak{M}_\mu$ is reproduced by H_μ.

Hence every Θ corresponds to a matrix $(\Theta_{\mu\nu})$ and the sum and product correspond to the sum and product of the corresponding matrices. The matrix elements $\Theta_{\mu\nu}$ are zero when the indices μ and ν belong to non-isomorphic modules $\mathfrak{M}_\mu$ and $\mathfrak{M}_\nu$; they are arbitrary homomorphisms of $\mathfrak{M}_\nu$ into $\mathfrak{M}_\mu$ when $\mathfrak{M}_\mu$ and $\mathfrak{M}_\nu$ are isomorphic.

Now let us divide the module $\mathfrak{M}_\lambda$ into isomorphic classes and number them so that, for instance, $\mathfrak{M}_1, \ldots, \mathfrak{M}_h$ are isomorphic to one another, $\mathfrak{M}_{h+1}, \ldots, \mathfrak{M}_{h+k}$ are isomorphic to one another, etc. Then the matrix $(\Theta_{\mu\nu})$ is "decomposed" into square blocks of $h, k, \ldots$ rows and columns such that only zeros appear outside of these blocks:



If we write in the first block arbitrary elements and in all other blocks only zeros, we obtain a matrix ring $\mathfrak{A}_1$ which is a subring of the original matrix ring $\mathfrak{A}$. Similarly, if we write zero everywhere except in the second block, we obtain a ring $\mathfrak{A}_2 \subseteq \mathfrak{A}$, etc. It is clear that every element of $\mathfrak{A}$ is uniquely representable as a sum of elements from $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ and that the elements of $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ mutually annihilate one another. This implies: *the ring $\mathfrak{A}$ is a direct sum of the rings $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ which mutually annihilate one another.*

In order to know the structure of $\mathfrak{A}$ we therefore have only to investigate the structure of one of the $\mathfrak{A}_\lambda$, for instance, that of $\mathfrak{A}_1$. The elements of $\mathfrak{A}_1$ are mapped on the h-rowed matrices

$$\begin{pmatrix} \Theta_{11} \ldots \Theta_{1h} \\ \vdots \quad\quad \vdots \\ \Theta_{h1} \ldots \Theta_{hh} \end{pmatrix}$$

of the first "block."

Θ_{11} is an element of the endomorphism field K_1 of $\mathfrak{M}_1$. The remaining elements $\Theta_{\mu\nu}$ do not belong to this skew field but represent homomorphisms of $\mathfrak{M}_\nu$ into $\mathfrak{M}_\mu$. However they may be uniquely mapped on the elements of K_1 by means of h fixed 1-isomorphisms

$$\Gamma_1, \ldots, \Gamma_h,$$

which map $\mathfrak{M}_1, \ldots, \mathfrak{M}_h$ on $\mathfrak{M}_1$. Let Γ_1 be chosen as the identity automorphism. Set up the correspondence whereby each $\Theta_{\mu\nu}$ is mapped on the element

$$\Theta'_{\mu\nu} = \Gamma_\mu \Theta_{\mu\nu} \Gamma_\nu^{-1} \tag{8}$$

which belongs to K_1 (since Γ_ν^{-1} maps $\mathfrak{M}_1$ on $\mathfrak{M}_\nu$, $\Theta_{\mu\nu}$ maps $\mathfrak{M}_\nu$ on $\mathfrak{M}_\mu$, and Γ_μ maps $\mathfrak{M}_\mu$ again on $\mathfrak{M}_1$). For this correspondence the sum $\eta_{\mu\nu} + \Theta_{\mu\nu}$ is mapped on the sum $\eta'_{\mu\nu} + \Theta'_{\mu\nu}$ and the product $\eta_{\lambda\mu}\Theta_{\mu\nu}$[5], when it has a sense, is mapped on the product

$$\eta'_{\lambda\mu}\Theta'_{\mu\nu} = \Gamma_\lambda \eta_{\lambda\mu} \Gamma_\mu^{-1} \Gamma_\mu \Theta_{\mu\nu} \Gamma_\nu^{-1} = \Gamma_\lambda (\eta_{\lambda\mu}\Theta_{\mu\nu}) \Gamma_\nu^{-1}.$$

Hence the correspondence is one-to-one between the matrices $(\Theta_{\mu\nu})$ and the matrices $(\Theta'_{\mu\nu})$ whose elements are in K_1, and the sum- and product matrix defined by

$$\begin{cases} \sigma_{\mu\nu} = \eta_{\mu\nu} + \Theta_{\mu\nu}, \\ \pi_{\lambda\nu} = \sum \eta_{\lambda\mu}\Theta_{\mu\nu} \end{cases}$$

corresponds to the sum- and product matrix. Furthermore, for fixed μ, ν and fixed Γ_μ, Γ_ν *every* element of K_1 may be written in the form $\Theta'_{\mu\nu}$ of (8). *Hence* $\mathfrak{A}_1$ *is isomorphic to the ring of all h-rowed matrices with elements in the skew field* K_1, *the automorphism field of the simple module* $\mathfrak{M}_1$.

EXERCISE. 1. If a completely reducible system of matrices

$$A = \begin{pmatrix} A_1 & & & \\ & A_1 & & \\ & & \ddots & \\ & & & A_1 \end{pmatrix} \quad \begin{matrix} & & \\ & & \\ & & \\ & & \end{matrix} \quad \begin{pmatrix} A_2 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_2 \end{pmatrix} \quad \begin{matrix} & & \\ & & \\ & & \\ & & \end{matrix} \quad \begin{pmatrix} \ddots & & \\ & \ddots & \\ & & \ddots \end{pmatrix}$$

is given, where the matrices A_1 in the first block run over h irreducible systems equivalent to one another, similarly the A_2 in the second block over k equivalent systems which are however not equivalent to the system determining the A_1, etc., then the matrices permutable with this system have the form

[5] A product $\eta_{\lambda\mu}\Theta_{\mu'\nu}$ has a sense only if $\mu' = \mu$. Thus $\Theta_{\mu'\nu}$ maps $\mathfrak{M}_\nu$ on $\mathfrak{M}_{\mu'}$, and $\eta_{\lambda\mu}$ must therefore map $\mathfrak{M}_{\mu'}$ on any other if the product is to have a meaning.

$$T = \begin{pmatrix} \begin{matrix} T_{11} & \cdots & T_{1k} \\ \vdots & & \vdots \\ T_{k1} & \cdots & T_{kk} \end{matrix} & & \\ & \begin{matrix} T_{k+1,k+1} & \cdots & T_{k+1,k+k} \\ \vdots & & \\ T_{k+k,k+1} & \cdots & T_{k+k,k+k} \end{matrix} & \\ & & \ddots \end{pmatrix},$$

where the T_{ik} in the first block are permutable with the system of the A_1, those in the second block with the system of the A_2, etc. The matrices T_{11}, which are permutable with the irreducible system of the A_1, form a skew field of finite degree over the ground field K.

2. If the ground field K is algebraically closed, the matrices T_{11} of Exer. 1, which are permutable with an irreducible matrix system, must be multiples λE of the unit matrix E.

120. STRUCTURE OF THE COMPLETELY REDUCIBLE RINGS WITH IDENTITY

Let $\mathfrak{o}$ be a semi-simple ring or a left-sided completely reducible ring with identity; in Section 117 the equivalence of these two concepts was established. As a module, with $\mathfrak{o}$ itself as the left multiplication domain, $\mathfrak{o}$ is a direct sum of simple modules (left ideals):

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \ldots + \mathfrak{l}_r.$$

We now form the endomorphism ring of this module. If Γ is an operator endomorphism which maps the identity on the element c:

$$\Gamma 1 = c,$$

then Γ maps an arbitrary element a on

$$\Gamma a = \Gamma(a \cdot 1) = a \cdot \Gamma 1 = ac.$$

On the other hand, if we choose c arbitrarily and every a of $\mathfrak{o}$ is mapped on ac, then the correspondence is an operator endomorphism since

$$(a + b)c = ac + bc,$$
$$ab \cdot c = a \cdot bc.$$

In this manner a one-to-one correspondence is set up between each element c and an endomorphism Γ. Furthermore, the sum $c + d$ corresponds to the sum $\Gamma + \Delta$, while the product cd corresponds to the reverse product $\Delta\Gamma$, since

$$a \cdot cd = ac \cdot d = \Delta(ac) = \Delta\Gamma a.$$

Two rings $\mathfrak{o}$ and $\mathfrak{o}'$ are said to be *inverse-isomorphic* or, simply, *inverse* of one another, if there exists a one-to-one correspondence between the rings such that the sum $a + b$ corresponds to the sum $a' + b'$ and the product $a \cdot b$ to the reverse product $b' \cdot a'$. Hence the ring $\mathfrak{o}$ is inverse-isomorphic to its endomorphism ring.

On the other hand by Section 119 the endomorphism ring of a completely reducible module is isomorphic to a direct sum of matrix rings that mutually annihilate one another, and whose matrix elements are taken from a skew field (the endomorphism field of a simple module).

The ring $\mathfrak{o}$ is therefore inverse-isomorphic to a direct sum of matrix rings which mutually annihilate one another.

For every ring we can construct, uniquely except for ring isomorphism, an inverse ring by mapping every ring element a on a new symbol a' and defining the sum and product by $a' + b' = (a + b)'$ and $a' \cdot b' = (b \cdot a)'$. Obviously the inverse ring of a skew field is also a skew field. The inverse ring of a matrix ring over a skew field K can be constructed by replacing K by the inverse skew field K' and every matrix $(a'_{\lambda\mu})$ by the transpose matrix $(a'_{\mu\lambda})$. Finally, the inverse ring of a direct sum of rings is the direct sum of the inverse rings of the summands. Consequently:

The ring $\mathfrak{o}$ is a direct sum of rings $\mathfrak{a}_\nu$, each of which is isomorphic to a complete matrix ring with respect to a skew field $\mathsf{K}^{(\nu)}$ and which mutually annihilate one another. There are as many $\mathfrak{a}_\nu$ as there are non-isomorphic left ideals $\mathfrak{l}_i$ in the decomposition as a direct sum.

Thereby the structure of the semi-simple rings is completely cleared up.

If the $\mathfrak{a}_\nu$ mutually annihilate one another, they are ideals in $\mathfrak{o}$. Hence if the ring $\mathfrak{o}$ is two-sided simple, we can only have one $\mathfrak{a}_\nu = \mathfrak{a}_1$: *a left-sided completely reducible ring with an identity which is two-sided simple is isomorphic to a complete matrix ring over a skew field. All minimal left ideals are operator isomorphic.*

Conversely we have:

The ring $\mathfrak{o}$ of matrices of n-th degree over a skew field K is (two-sided) simple and left-sided completely reducible, and the endomorphism ring of the minimal left ideals of $\mathfrak{o}$ is inverse-isomorphic to K.

PROOF. Let $c_{11}, \ldots, c_{1n}, \ldots; c_{n1}, \ldots, c_{nn}$ be the basis elements of the matrix ring (Section 114, *a*). Further, let $\mathfrak{a}$ be a two-sided ideal $\neq (0)$ and

$$a = \sum \gamma_{ik} c_{ik}$$

an element of $\mathfrak{a}$ distinct from 0. One of the coefficients γ_{ik} must be distinct from 0; let us say that $\gamma_{23} \neq 0$. Then the element

$$\gamma_{23}^{-1} c_{\lambda 2} a c_{3\mu} = \gamma_{23}^{-1} \sum_{i,k} \gamma_{ik} c_{\lambda 2} c_{ik} c_{3\mu}$$

$$= \gamma_{23}^{-1} \gamma_{23} c_{\lambda 2} c_{23} c_{3\mu} = c_{\lambda\mu}$$

belongs to $\mathfrak{a}$ (for all λ and μ), i.e., $\mathfrak{a}$ contains all basis elements of $\mathfrak{o}$. Hence $\mathfrak{a} = \mathfrak{o}$ and $\mathfrak{o}$ is a simple ring with identity.

The K-module $\mathfrak{l} = (c_{11}, c_{21}, \ldots, c_{n1})$ is a minimal left ideal in $\mathfrak{o}$. This can be seen as follows: first, the product of any basis elements c_{ik} of $\mathfrak{o}$ by an arbitrary basis element c_{l1} of $\mathfrak{l}$ is equal either to 0 or to c_{i1}; therefore it is always an element of $\mathfrak{l}$. Secondly, that $\mathfrak{l}$ is minimal will be proved by showing that an arbitrary element $\alpha \neq 0$ of $\mathfrak{l}$ always generates the whole ideal $\mathfrak{l}$. Thus, if

$$a = \sum \alpha_k c_{k1}$$

and let us say $\alpha_2 \neq 0$, then the left multiples of a include the elements

$$\alpha_2^{-1} c_{j2} a = \alpha_2^{-1} \alpha_2 c_{j2} c_{21} = c_{j1} \qquad (j = 1, \ldots, n).$$

Similarly, it follows that every $\mathfrak{l}_\nu = (c_{1\nu}, c_{2\nu}, \ldots, c_{n\nu})$ is a simple left ideal in $\mathfrak{o}$. Since $\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \ldots + \mathfrak{l}_n$ then $\mathfrak{o}$ is left-sided completely reducible.

Finally, let us determine the endomorphism field of $\mathfrak{l}$. An operator endomorphism which maps. let us say, c_{11} on

$$a = \sum \alpha_k c_{k1} \tag{1}$$

must map every $x \cdot c_{11}$ on $x \cdot a$, in particular $c_{11}^2 (= c_{11})$ on

$$c_{11} a = \sum \alpha_k c_{11} c_{k1} = \alpha_1 c_{11}.$$

But this must be the element a. Hence in (1) all terms are missing except $\alpha_1 c_{11}$, and the automorphism maps $x \cdot c_{11}$ on $x \cdot \alpha_1 c_{11} = x c_{11} \cdot \alpha_1$. This endomorphism has therefore the effect of multiplying the elements of $\mathfrak{l}$ (all of which have the form $x c_{11}$) on the right by α_1. The elements α_1 of the skew field are inverse-isomorphic to their associated automorphisms; therefore. the automorphism field of the minimal left ideals is inverse-isomorphic to K.

In the same manner we can also prove that the complete matrix ring over a skew field K is a right-sided completely reducible ring. The automorphism field of the minimal right ideals is directly isomorphic to K. In connection with the theorems of Section 118 it follows further that a direct sum of matrix rings which mutually annihilate one another is also (left and right) completely reducible. The concepts:

a) ring without radical satisfying the minimal condition for left (or right) ideals;

b) left-sided or right-sided completely reducible ring with identity;

c) direct sum of two-sided simple ideals each of which is ring isomorphic to a complete matrix ring over a skew field;

are therefore *completely equivalent.*

From here on we designate the ring of matrices of degree n over the skew field K by K_n; the unit matrix, by E. We state: *if* Z *is the centrum of* K, *then* $\mathsf{Z} \cdot E$ *is the centrum of* K_n.

PROOF. When a matrix

$$a = (\alpha_{ik}) = \sum \alpha_{ik} c_{ik}$$

belongs to the centrum of K_n, it must be permutable in particular with $c_{1\mu}$. This means that

$$c_{1\mu} \cdot \sum_{i,k} \alpha_{ik} c_{ik} = \sum_{i,k} \alpha_{ik} c_{ik} \cdot c_{1\mu},$$

$$\sum_{k} \alpha_{\mu k} c_{1k} = \sum_{i} \alpha_{i1} c_{i\mu}.$$

On equating the coefficients of the left and right members we obtain

$$\alpha_{\mu k} = 0 \quad \text{for} \quad \mu \neq k,$$

$$\alpha_{\mu\mu} = \alpha_{11}.$$

Hence

$$a = \begin{pmatrix} \alpha_{11} & & 0 \\ & \alpha_{11} & \\ & \ddots & \\ 0 & & \alpha_{11} \end{pmatrix} = \alpha_{11} \cdot E = \alpha \cdot E.$$

Furthermore, if $a = \alpha \cdot E$ is permutable with every $\beta \cdot E$, α must belong to the centrum of K. Q.E.D.

If we bring this result together with the results of Section 118 and take into consideration that the centrums of two inverse-isomorphic rings are obviously isomorphic in the usual sense, then:

The centrum of a semi-simple ring $\mathfrak{o}$ *is a direct sum of fields which are contained in the individual two-sided components of* $\mathfrak{o}$, *and is represented by* $\mathsf{Z} \cdot E$ *in the matrix representation, where* Z *is the centrum of the skew field* K.

EXERCISES. 1. A semi-simple hypercomplex system $\mathfrak{o}$ over an algebraically closed field Ω is the direct sum of matrix rings in Ω.

2. The quaternion ring $(1, i, k, l)$ over a field P of characteristic $\neq 2$ is always two-sided simple and therefore always either a field or isomorphic to the ring of all two-rowed matrices in P.

121. THE BEHAVIOR OF THE SEMI-SIMPLE HYPERCOMPLEX SYSTEMS IN THE EXTENSION OF THE GROUND FIELD

Let $\mathfrak{S}$ be a semi-simple system over the ground field P. We will investigate how $\mathfrak{S}$ behaves in the extension of the ground field to an extension field Λ; especially, what properties of $\mathfrak{S}$ remain unchanged, and which are lost. We will proceed as follows: first, $\mathfrak{S}$ will be taken as a commutative field, then as a skew field, next as a simple system, and finally as a semi-simple system; each case will be handled by means of the less complicated preceding one. The theorems to be proved

under 2. have a more general significance since for them Λ need not be commutative.

1. *If $\mathfrak{S}$ is a separable finite extension field of P, then $\mathfrak{S}_\Lambda$ is without radical no matter how the field Λ is chosen; on the contrary, if $\mathfrak{S}$ is inseparable, then $\mathfrak{S}_\Lambda$ has a radical for a suitable choice of Λ.*

PROOF. Let $\mathfrak{S}$ be separable, ϑ a primitive element of $\mathfrak{S}$ (Section 40), and $\varphi(z)$ the irreducible polynomial satisfied by ϑ. If n is the degree of $\varphi(z)$, then by Section 32

$$\mathfrak{S} = \mathsf{P}(\vartheta) = \mathsf{P} + \mathsf{P}\vartheta + \cdots + \mathsf{P}\vartheta^{n-1} \cong \mathsf{P}[z]/(\varphi(z))$$

and after the extension of the ground field

$$\mathfrak{S}_\Lambda = \Lambda + \Lambda\vartheta + \cdots + \Lambda\vartheta^{n-1} \cong \Lambda[z]/(\varphi(z)).$$

But $\varphi(z)$ is without multiple factors also in $\Lambda[z]$. Hence a polynomial $f(z)$ must be $\equiv 0(\varphi(z))$ if one of its powers is $\equiv 0(\varphi(z))$, i.e., there is in $\Lambda[z]/\varphi(z)$ no nilpotent element except the null element. This means that $\mathfrak{S}_\Lambda$ is a (commutative) ring without radical; therefore, by Section 118 (Theorem of Dedekind) it is a direct sum of fields. By an investigation based on the propositions at the end of Section 89 it may be easily shown that these fields correspond to the irreducible factors $\varphi_\nu(z)$ in which $\varphi(z)$ factors in $\Lambda[z]$, and that each field is isomorphic to a residue class field $\Lambda[z]/(\varphi_\nu(z))$. Here we need only the fact that $\mathfrak{S}_\Lambda$ has no radical.

On the contrary, if $\mathfrak{S}$ is inseparable and ϑ an inseparable element of $\mathfrak{S}$, then $\mathfrak{S}$ has a subfield $\mathsf{P}(\vartheta)$ and $\mathfrak{S}_\Lambda$ has the subring $\Lambda(\vartheta)$ which is isomorphic to $\Lambda[z]/(\varphi(z))$, as above. For a suitable choice of Λ, $\varphi(z)$ has multiple roots in Λ, and there is in $\Lambda[z]$ a polynomial $f(z)$ which is itself not divisible by $\varphi(z)$ but has a power which is divisible by $\varphi(z)$. This means that there is a non-vanishing nilpotent element in $\Lambda[z]/(\varphi(z))$; therefore, there is one in $\Lambda(\vartheta)$ and this element generates a nilpotent ideal in $\mathfrak{S}_\Lambda$, since in a commutative ring every nilpotent element generates a nilpotent ideal. This completes the proof of the theorem.

Since the roles of $\mathfrak{S}$ and Λ may be interchanged, the first part of the theorem may be formulated as follows: if at least one of the fields $\mathfrak{S}$ and Λ is finite and separable over P, then $\mathfrak{S} \times \Lambda$ is semi-simple. Furthermore, since $\mathfrak{S} \times \Lambda$ is commutative, by Section 118 it follows: *$\mathfrak{S} \times \Lambda$ is the direct sum of fields.*

2. Next, we go over to the case: $\mathfrak{S}$ is a skew field K. This case may be reduced to the commutative one by means of the following *Reduction Theorem:*

Let K be a skew field over P with centrum $\mathsf{Z} \supseteq \mathsf{P}$, and Λ a hypercomplex system over P (in the applications it is usually a finite extension field or skew field over P). Then for $\mathfrak{R} = \mathsf{K} \times \Lambda$ and $\mathfrak{Z} = \mathsf{Z} \times \Lambda$ every two-sided ideal $\mathfrak{a}$ in $\mathfrak{R}$ is generated by a two-sided ideal of $\mathfrak{Z}$.

The Reduction Theorem is best understood when it is expressed in a more general form as a *Module Theorem:*

Let K be a skew field which admits the fixed automorphisms σ. Let $\mathfrak{M}$ be a K-module of finite rank:

$$\mathfrak{M} = z_1\mathsf{K} + \cdots + z_q\mathsf{K}.$$

The automorphisms σ of K induce automorphisms in $\mathfrak{M}$ by the following definition:

$$\sigma(z_1\varkappa_1 + \cdots + z_q\varkappa_q) = z_1(\sigma\varkappa_1) + \cdots + z_q(\sigma\varkappa_q).$$

We now state: *every submodule* $\mathfrak{a}$ *of* $\mathfrak{M}$, *which admits the automorphisms* σ, *possesses a* K-*basis whose elements are carried individually into themselves by the automorphisms.*

PROOF. If $(u_1, \ldots, u_r)$ is a K-basis for $\mathfrak{a}$, by Section 28 we may expand it to a K-basis for $\mathfrak{M}$ by the addition of some of the z_i, say $z_{r+1}, \ldots, z_q$. Every element of $\mathfrak{M}$ is then congruent modulo $\mathfrak{a}$ to a linear form in $z_{r+1}, \ldots, z_q$ with coefficients in K. In particular for $i = 1, 2, \ldots, r$ we have

$$z_i \equiv \sum_{k=r+1}^{q} z_k\gamma_{ki} \pmod{\mathfrak{a}}.$$

If we set

$$l_i = z_i - \sum_{k=r+1}^{q} z_k\gamma_{ki},$$

then the l_i are linearly independent elements of $\mathfrak{a}$. This follows from the fact that every linear relation between the l_i gives rise to the same linear relation between $z_1, \ldots, z_r$; these latter elements are linearly independent. Hence $l_1, \ldots, l_r$ form a K-basis for $\mathfrak{a}$. Now if we apply one of the automorphisms σ to l_i, we obtain

$$\sigma l_i = z_i - \sum_{r+1}^{q} z_k(\sigma\gamma_{ik}). \tag{1}$$

As σl_i must again belong to $\mathfrak{a}$, it must be equal to a linear combination of the original l_i:

$$\sigma l_i = \sum l_j\alpha_j = \sum_{1}^{r} z_j\alpha_j - \sum_{r+1}^{q} z_k \sum_{j} \gamma_{kj}\alpha_j. \tag{2}$$

On equating (1) and (2) we see that all $\alpha_j = 0$ with the exception of $\alpha_i = 1$. Hence $\sigma l_i = l_i$ which proves the theorem.

In order to obtain the Reduction Theorem from the Module Theorem, we need only to assume that the automorphism used in the Module Theorem is the inner automorphism $\varkappa \to \beta\varkappa\beta^{-1}$ of K. The transformation by β operates on a sum $z_1\varkappa_1 + \cdots + z_q\varkappa_q$ as follows: it leaves the z_i unchanged and carries the $\varkappa_i$ over to $\beta\varkappa_i\beta^{-1}$. A two-sided ideal $\mathfrak{a}$ in $\mathsf{K} \times \Lambda$ is also a two-sided K-module and therefore permits the automorphism $\mathfrak{a} \to \beta\mathfrak{a}\beta^{-1}$. Hence $\mathfrak{a}$ has a basis consisting

of elements $\sum z_i \varkappa_i$ which are mapped into themselves by the transformation with β, i.e., the coefficients $\varkappa_i$ belong to the centrum Z of K. These basis elements belong therefore to $\mathfrak{Z} = \mathsf{Z} \times \Lambda$, whereby the Reduction Theorem is proved.

COROLLARY. The Reduction Theorem is also valid when Λ is replaced by an infinite extension field or skew field Ω provided that K has finite rank over P. Thus, if $\mathfrak{a}$ is a two-sided ideal of $\mathfrak{R} = \mathsf{K} \times \Omega$, then $\mathfrak{a}$, just as $\mathfrak{R}$, has finite rank over Ω, and therefore a finite Ω-basis $(a_1, \ldots, a_s)$. The basis elements, expressed in the form $\sum \omega_i \varkappa_i$, contain altogether only finitely many ω_i; these generate a finite submodule Λ of Ω. To the product $\mathfrak{M} = \mathsf{K} \times \Lambda$ and its submodule $\mathfrak{a} \cap \mathfrak{M}$ we can then apply the Module Theorem and thus find a module basis for $\mathfrak{a} \cap \mathfrak{M}$. This means that there is an ideal basis for $\mathfrak{a}$ which is invariant with respect to the inner automorphisms of K and therefore belongs to $\mathsf{Z} \times \Omega$.

From the Reduction Theorem it follows immediately: *if $\mathsf{Z} \times \Lambda$ decomposes into simple two-sided ideals, then $\mathsf{K} \times \Lambda$ decomposes into exactly as many simple two-sided ideals; these latter ideals are generated by the former. Hence if $\mathsf{Z} \times \Lambda$ is semi-simple, $\mathsf{K} \times \Lambda$ is also.* We have already verified this proposition in the case where Z and Λ are both commutative fields and at least one of the two is finite and separable over P.

A simple hypercomplex system $\mathfrak{S}$ or especially a finite extension field K of P is called *normal* over the ground field P when the centrum $\mathsf{Z} = \mathsf{P}$. The normal case is the one to which all others are brought when Z itself is chosen as the ground field. In this case $\mathsf{Z} \times \Lambda = \Lambda$ cannot be decomposed in general and we obtain as an important special case:

If K is a normal skew field over P and Λ is a simple hypercomplex system or an arbitrary skew field over P, then $\mathsf{K} \times \Lambda$ is again simple.

3. We now go from skew fields to the simple systems with identity, i.e., to complete matrix rings $\mathfrak{S} = \mathsf{K}_r$. If Λ is an arbitrary skew field over P, we have

$$\mathfrak{S}_\Lambda = \mathfrak{S} \times \Lambda \cong \mathsf{K}_r \times \Lambda \cong \mathsf{K} \times \mathsf{P}_r \times \Lambda \cong \mathsf{K} \times \Lambda \times \mathsf{P}_r = \mathsf{K}_\Lambda \times \mathsf{P}_r .$$

$\mathfrak{S}_\Lambda$ is a complete matrix ring of degree r over K_Λ. When the centrum Z of K is separable or when Λ is commutative, separable and finite over P, then K_Λ is semi-simple and therefore decomposes into complete matrix rings, say:

$$\mathsf{K}_\Lambda \cong \mathsf{K}'_{r'} + \mathsf{K}''_{r''} + \cdots \cong \mathsf{K}' \times \mathsf{P}_{r'} + \mathsf{K}'' \times \mathsf{P}_{r''} + \cdots \tag{3}$$

$$\begin{aligned} \mathfrak{S}_\Lambda &\cong (\mathsf{K}' \times \mathsf{P}_{r'} + \mathsf{K}'' \times \mathsf{P}_{r''} + \cdots) \times \mathsf{P}_r \\ &\cong \mathsf{K}' \times \mathsf{P}_{r'} \times \mathsf{P}_r + \mathsf{K}'' \times \mathsf{P}_{r''} \times \mathsf{P}_r + \cdots \\ &\cong \mathsf{K}' \times \mathsf{P}_{r'r} + \mathsf{K}'' \times \mathsf{P}_{r''r} + \cdots \cong \mathsf{K}'_{r'r} + \mathsf{K}''_{r''r} + \cdots \end{aligned} \tag{4}$$

Consequently $\mathfrak{S}_\Lambda$ is again a ring without radical; it decomposes in exactly as many matrix rings as K_Λ with the degrees of the matrices all multiplied by r. By this theorem the simple systems $\mathfrak{S}$ are lead back to the skew field K.

In particular, if $\mathfrak{S}$ is normal over P, i.e., $\mathsf{Z} = \mathsf{P}$, then $\mathfrak{S}_\Lambda \cong \mathsf{K}'_{r',r''}$ is again a simple system. Moreover if Λ is commutative, it is easy to show that the centrum of $\mathfrak{S} \times \Lambda$ is equal to $\mathsf{Z} \times \Lambda = \mathsf{P} \times \Lambda = \Lambda$; consequently $\mathfrak{S} \times \Lambda$ is normal over Λ. Hence *a normal simple system* $\mathfrak{S}$ *remains normal and simple in an arbitrary commutative extension of the ground field.*

4. The preceding theorems give a complete survey of the behavior of simple hypercomplex systems in the extension of the ground field. The semi-simple systems may be studied by simple systems since they are direct sums of simple systems. Thus, if

$$\mathfrak{S} = \mathfrak{S}' + \mathfrak{S}'' + \cdots$$

is a semi-simple system which is the direct sum of the simple systems $\mathfrak{S}'$, $\mathfrak{S}''$, ..., then

$$\mathfrak{S}_\Lambda = \mathfrak{S}'_\Lambda + \mathfrak{S}''_\Lambda + \cdots.$$

In particular we have: *a semi-simple hypercomplex system remains semi-simple in every finite separable extension of the ground field. If the centrums of the simple systems* $\mathfrak{S}'$, $\mathfrak{S}''$, ..., *in which the semi-simple system decomposes, are all separable over* P, *then the semi-simplicity remains valid in every arbitrary extension of the ground field.*

5. We have seen that the behavior of a simple hypercomplex system in the extension of the ground field depends entirely on the behavior of the skew field underlying the simple system. Hence we will investigate further the behavior of normal skew fields.

We proved in 3. that a normal skew field remains normal and simple in every extension of the ground field. However, the skew field need not remain a skew field. Instead it may become a matrix ring over a skew field. If this is the case we say that the extension of the ground field produces a *splitting* of the skew field (namely, a decomposition into simple left ideals).

We now show: *if* $\mathsf{K} \neq \mathsf{P}$ *is a normal skew field, then there is always an extension field which produces a splitting of the skew field.*

Thus, let β be an element of K which does not belong to P. β is a zero of a irreducible polynomial $\varphi(x)$ in $\mathsf{P}[x]$. The polynomial $\varphi(x)$ is factorable in a suitably chosen field Λ; we can choose, for instance, $\Lambda \cong \mathsf{P}(\beta)$ since $\varphi(x)$ splits off a linear factor in Λ. As proved earlier, $\Lambda \times \mathsf{P}(\beta) \cong \Lambda[x]/(\varphi(x))$; therefore $\Lambda \times \mathsf{P}(\beta)$ has zero divisors, so that the comprehending ring $\Lambda \times \mathsf{K}$ also has zero divisors. Accordingly, this ring is no longer a skew field; instead it must be a matrix ring $\mathsf{K}'_{r'}$ with $r' > 1$.

Let the symbol $(\mathsf{K}:\mathsf{P})$ represent the rank of K over P. On equating the rank over Λ of the left and right members of $\mathsf{K} \times \Lambda = \mathsf{K}'_{r'}$, we obtain

$$(\mathsf{K}:\mathsf{P}) = r'^2 \cdot (\mathsf{K}':\Lambda).$$

Consequently, in every case the rank of K' over Λ is smaller than that of K over P. If $\mathsf{K}' \neq \Lambda$, we may also split the skew field K' by a further extension of the field Λ. Then $\mathsf{K}'_{r'}$ goes over to a matrix ring of degree $r'r''$. This process cannot be continued indefinitely since the ranks of the skew fields always become smaller. Hence we will eventually arrive at a *complete splitting*, whereby the skew field K becomes a matrix ring over Λ:

$$\mathsf{K} \times \Lambda \cong \Lambda_m .$$

A field Λ, which has this property, is called a *splitting field* of the skew field K. The above proof shows that there is always a splitting field of finite degree over P. The relation between the orders given above now becomes

$$(\mathsf{K} : \mathsf{P}) = m^2 .$$

The rank of a skew field K over its centrum P is accordingly *always a square number* m^2. The number m, i.e., the degree of the matrices resulting from the complete splitting, is called the *degree* (or also the *index*) of the skew field K. Hence the degree is not, as in the case of commutative fields, the same as the rank.

A splitting field of K is at the same time also a splitting field of all complete matrix rings K_r and conversely. For, by the above remarks, $\mathsf{K} \times \Lambda$ and $\mathsf{K}_r \times \Lambda$ are complete matrix rings over one and the same skew field K'; Λ is the splitting field only if K' turns out to be equal to Λ.

More generally we call Λ a splitting field of the arbitrary hypercomplex system $\mathfrak{S}$ when $\mathfrak{S} \times \Lambda$ is semi-simple and a direct sum of complete matrix rings over Λ, or still more general, when $\mathfrak{S}$ has a radical $\mathfrak{c}$ and the residue class ring modulo $\mathfrak{c}$ is a direct sum of complete matrix rings over Λ. Of course with the existence of a radical we can no longer speak of a splitting since in this case the system $\mathfrak{S} \times \Lambda$ is no longer completely reducible.

EXERCISES. 1. A product of two skew fields over P is semi-simple when one of the skew fields has finite rank over P, while the centrum of the other is finite and separable over P.

2. A product of two simple systems over P is simple provided that one of the systems is normal over P. If both are normal, so also is the product.

3. An algebraically closed field Ω over P is the splitting field of all skew fields of finite rank over P.

CHAPTER XVII

REPRESENTATION THEORY OF GROUPS AND HYPERCOMPLEX SYSTEMS

122. STATEMENT OF THE PROBLEM

Let $\mathfrak{G}$ be a group. A *representation of* $\mathfrak{G}$ *by linear transformations in the field* K is defined to be a group homomorphism which maps every element a on a linear transformation A with coefficients in K. The representation is said to be *faithful* or *unfaithful* according as it is an isomorphism or not.

Similarly, a *representation of a ring* $\mathfrak{o}$ *by linear transformations in* K is defined to be a ring homomorphism $a \to A$ (therefore not only are products mapped into products but also sums into sums). Finally, if the ring $\mathfrak{o}$ is a *hypercomplex system over a field* P, we also require that a *representation* satisfy the following conditions: the ground field P is contained in the centrum of the representation field K and the ring homomorphism is an operator homomorphism with respect to P, i.e., if $a \to A$, then $a\varrho \to A\varrho$ for all elements ϱ of P. In terms of the representation module $\mathfrak{M}$ which is adapted to the representation by Section 110 this means that

$$a\varrho \cdot m = am \cdot \varrho \quad \text{for} \quad m \in \mathfrak{M}.$$

In the following we will usually limit ourselves, when considering the representations of groups, to finite groups $\mathfrak{G} = \{a_1, a_2, \ldots, a_h\}$ and, in the case of rings. to hypercomplex systems. Our problem is to find all representations and (if possible) to split them up into irreducible components. We note that the representation problem for *groups* may be stated as one for *hypercomplex systems* by forming out of the group $\mathfrak{G}$ the *group ring*

$$\mathfrak{o} = a_1\mathsf{K} + \cdots + a_h\mathsf{K},$$

whose basis elements are the elements of $\mathfrak{G}$. Thus, if the representation of the group is given by $a_i \to A_i$, then

$$\sum a_i x_i \to \sum A_i x_i$$

is a representation of the system $\mathfrak{o}$ as soon as we assume that the representation field K is commutative. It is obvious that sums correspond to sums, the product

$$(\sum a_i \varkappa_i)(\sum a_k \lambda_k) = \sum a_i a_k \varkappa_i \lambda_k$$

corresponds to the matrix

$$\sum\sum A_i A_k \varkappa_i \lambda_k = (\sum A_i \varkappa_i)(\sum A_k \lambda_k),$$

and, the product $(\sum a_i \varkappa_i) \cdot \varrho$ corresponds to $(\sum A_i \varkappa_i) \cdot \varrho$. Conversely every representation of the group ring $\mathfrak{o}$ in the field K maps in particular the basis elements $a_1, \ldots, a_h$ on certain linear transformations; this totality produces a representation of the group $\mathfrak{G}$. Hence:

Every representation of a finite group $\mathfrak{G}$ in a commutative field K may be obtained from a representation of the group ring $\mathfrak{o} = a_1\mathsf{K} + \cdots + a_h\mathsf{K}$.

Among the representations of hypercomplex systems we are particularly interested in those for which the representation field K coincides with the ground field P. The general case (at least for commutative K) can be reduced to this case if we extend the ground field P to K and therefore extend the hypercomplex system $\mathfrak{o}$ to $\mathfrak{o}_\mathsf{K}$ (Section 121). Thus, if in the original representation the basis elements $b_1, \ldots, b_n$ of $\mathfrak{o}$ are mapped on the matrices $B_1, \ldots, B_n$ of K, then on mapping an element $\sum b_l \varkappa_l (\varkappa_l \in \mathsf{K})$ of $\mathfrak{o}_\mathsf{K}$ on the matrix $\sum B_l \varkappa_l$ the representation of $\mathfrak{o}$ is extended to a representation of $\mathfrak{o}_\mathsf{K}$. *Consequently every representation of $\mathfrak{o}$ in a commutative field K can be obtained from a representation of $\mathfrak{o}_\mathsf{K}$.*

A further limitation is imposed on the problem stated above when we assume that the ring $\mathfrak{o}$ has a unit element. Thereupon we can always assume that the unit element 1 is also a unity operator for the representation module, i.e., the identity is mapped on the unit matrix in the representation. Otherwise, as in Section 106, the representation module becomes a direct sum $\mathfrak{M}_0 + \mathfrak{M}_1$, where $\mathfrak{M}_0$ is annihilated by $\mathfrak{o}$, while $\mathfrak{M}_1$ has 1 as a unity operator. Hence the representation decomposes completely into two components such that the first contains only the null matrices, and so is of no interest, while the second produces a representation which has the unit element as a unity operator.

A particularly important representation of a hypercomplex system $\mathfrak{o}$ is the so-called *regular representation*, which we obtain when we take $\mathfrak{o}$ itself as the representation module ($\mathfrak{o}$-left and P-right module). The submodules are the left ideals, and the reduced form of the representation may be obtained from a composition series of the left ideals. The regular representation is completely reducible when the ring $\mathfrak{o}$ is itself completely reducible.

In all considerations of this chapter we must always keep clearly in mind the connection, explained in Section 110, between representations and representation modules; only thus will the proofs be intelligible.

*

123. REPRESENTATION OF HYPERCOMPLEX SYSTEMS

The representation theory of hypercomplex systems depends on the following two theorems:

THEOREM. 1. *Let* $\mathfrak{o}$ *be a (left-sided) completely reducible ring with a unit element and* $\mathfrak{M}$ *a finite* $\mathfrak{o}$*-(left) module. Let the submodule* $\mathfrak{M}_0$*, which is annihilated by* $\mathfrak{o}$*, be zero or completely reducible. Then* $\mathfrak{M}$ *is completely reducible, and the irreducible components are either annihilated by* $\mathfrak{o}$ *or are isomorphic to minimal left ideals of* $\mathfrak{o}$*. This is also valid when* $\mathfrak{M}$ *and* $\mathfrak{o}$ *have in addition a right multiplicative domain* Ω *with the usual properties*

$$am \cdot \varrho = a \cdot m\varrho = a\varrho \cdot m \quad \text{for} \quad a \in \mathfrak{o},\ m \in \mathfrak{M},\ \varrho \in \Omega.$$

PROOF. We have already seen that we can limit ourselves to the case where the unit element of $\mathfrak{o}$ is a unity operator. Now, if

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \cdots + \mathfrak{l}_r, \tag{1}$$

$$\mathfrak{M} = (m_1, \ldots, m_s) = (\mathfrak{o}m_1, \ldots, \mathfrak{o}m_s), \tag{2}$$

we obtain after (1) is substituted in (2)

$$\mathfrak{M} = (\ldots, \mathfrak{l}_i m_k, \ldots). \tag{3}$$

The modules $\mathfrak{l}_i m_k$, which are distinct from the null module, are isomorphic to the corresponding $\mathfrak{l}_i$ (cf. Section 117, Lemmas 1 and 2) and therefore are minimal $\mathfrak{o}$-modules. Hence each module either has only the zero in common with the sum of the preceding ones or is entirely contained therein. Consequently, if we leave out of the sum (3) those $\mathfrak{l}_i m_k$ which are already contained in the sum of the preceding ones, the sum becomes direct.

For the *application to the representation theory* of hypercomplex systems, Ω is the coefficient field P and at the same time the representation field, while $\mathfrak{M}$ is a representation module. Now every representation module is finite with respect to P; therefore, if $\mathfrak{o}$ has a unit element e, it is also finite with respect to $e\mathsf{P} \subseteq \mathfrak{o}$.[1] Hence *all representations of a semi-simple hypercomplex system are completely reducible.*

The left ideals $\mathfrak{l}_1, \ldots, \mathfrak{l}_r$ of $\mathfrak{o}$ may be obtained by first decomposing $\mathfrak{o}$ into two-sided ideals:

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s,$$

and then splitting up the simple rings $\mathfrak{a}_\nu$ into left ideals. The $\mathfrak{l}_i$ contained in an $\mathfrak{a}_\nu$ will be annihilated by every $\mathfrak{a}_\mu$ with $\mu \neq \nu$. Consequently in the representation adapted to $\mathfrak{l}_i$ all $\mathfrak{a}_\mu$ with the exception of the single ideal $\mathfrak{a}_\nu$ are represented by

[1] The module $\mathfrak{M}_0$ which is annihilated by $\mathfrak{o}$ is automatically completely reducible since it is a finite P-module.

zero. The ideal $\mathfrak{a}_\nu$ has only one irreducible representation except for equivalence, since all minimal left ideals of $\mathfrak{a}_\nu$ are operator isomorphic. Furthermore, the representation of $\mathfrak{a}_\nu$ itself is *faithful* since $\mathfrak{a}_\nu$ is two-sided simple. The representation will be constructed explicitly later on.

The converse of Theorem 1 is trivial: if every finite $\mathfrak{o}$-module is completely reducible, $\mathfrak{o}$ itself is completely reducible; for $\mathfrak{o}$ is a finite $\mathfrak{o}$-module with the basis 1. Hence we have the theorem:

If $\mathfrak{o}$ is a hypercomplex system with identity and if all representations of the system $\mathfrak{o}$ are completely reducible, then $\mathfrak{o}$ itself is completely reducible.

While Theorem 1 gives us a complete survey of all representations of a system without radical, Theorem 2 will refer only to the *irreducible* representations of a system *with* radical. This means that we will not be concerned with the matrix elements that can appear in a *reducible* representation outside of the irreducible diagonal blocks.

THEOREM. 2. *If $\mathfrak{o}$ is a ring satisfying the maximal- and minimal condition for left ideals and $\mathfrak{c}$ is the radical of $\mathfrak{o}$, then every irreducible $\mathfrak{o}$-module $\mathfrak{M}$ is either annihilated by $\mathfrak{o}$ or isomorphic to a simple left ideal of the ring without radical $\mathfrak{o}/\mathfrak{c}$. This is also true if there exists a multiplicative domain Ω as in Theorem* 1.

PROOF. We must have $\mathfrak{c}\mathfrak{M} = (0)$; otherwise $\mathfrak{c}\mathfrak{M} = \mathfrak{M}$, and

$$\mathfrak{M} = \mathfrak{c}\mathfrak{M} = \mathfrak{c}^2\mathfrak{M} = \cdots = (0).$$

Hence we may think of $\mathfrak{M}$ as an $\mathfrak{o}/\mathfrak{c}$-module since all elements of a residue class modulo $\mathfrak{c}$ yield the same product when multiplied by an element of $\mathfrak{M}$. As $\mathfrak{o}/\mathfrak{c}$ is a ring without radical, it has an identity and is completely reducible. The theorem now follows from Theorem 1.

In particular Theorem 2 shows that the simple composition factors of $\mathfrak{o}$ already appear in the composition series of $\mathfrak{o}/\mathfrak{c}$ (or of $\mathfrak{o}$ modulo $\mathfrak{c}$).

When applied to representations, Theorem 2 states that *all irreducible representations of a hypercomplex system $\mathfrak{o}$ are already contained in the regular representation (and actually in the regular representation of $\mathfrak{o}/\mathfrak{c}$)*. Furthermore, all two-sided simple components of $\mathfrak{o}/\mathfrak{c}$ are represented by zero except at most a single one, which is represented faithfully. Hence an *irreducible* representation of an entirely arbitrary hypercomplex system is essentially a representation of a *simple* system (provided it is not the null representation which can happen, on account of the irreducibility, only in the case of representations of the first degree).

The irreducible representations appearing in Theorem 1 and Theorem 2 may be obtained through the left ideals of simple rings. We will now explicitly construct these irreducible representations for simple hypercomplex systems.

A simple hypercomplex system $\mathfrak{o}$ with identity is by Section 120 always isomorphic to a complete matrix ring over a skew field Δ; therefore

$$\mathfrak{o} = c_{11}\Delta + c_{12}\Delta + \cdots + c_{nn}\Delta.$$

A minimal left ideal $\mathfrak{l}$ is given by

$$\mathfrak{l} = c_{11}\Delta + c_{21}\Delta + \cdots + c_{n1}\Delta.$$

The ground field P, which could also be the representation field, is contained in Δ, and Δ has finite rank over P. Obviously the rank of $\mathfrak{o}$ is n^2-times the rank of Δ.

We consider first the case $\Delta = \mathsf{P}$. This case must occur, for instance, whenever P is algebraically closed. The basis $(c_{11}, c_{21}, \ldots, c_{n1})$ of $\mathfrak{l}$ may then be used to set up explicitly the matrices of the representation. If $a = \sum_{i,k=1}^{n} c_{ik}\alpha_{ik}$ is an element of $\mathfrak{o}$, then

$$ac_{k1} = \sum_{i=1}^{n} c_{ik}c_{k1}\alpha_{ik} = \sum_{i=1}^{n} c_{i1}\alpha_{ik};$$

consequently in the representation adapted to $\mathfrak{l}$ *the element* a *is mapped on the matrix* (α_{ik}). Hence the isomorphism of $\mathfrak{o}$ to the complete matrix ring of the matrices (α_{ik}) is precisely the irreducible representation which is adapted to a minimal left ideal $\mathfrak{l}$. This is to be expected since we have already proved that except for equivalence there can be only *one* irreducible representation.

It is important to note that in the case under investigation $\Delta = \mathsf{P}$ the matrices of the representation always form the *complete* matrix ring of degree n. We can also state this result by saying that there are exactly n^2 linearly independent matrices among the matrices of the representation.

Secondly, if Δ is a proper extension field of P:

$$\Delta = \lambda_1\mathsf{P} + \cdots + \lambda_r\mathsf{P},$$

we first form the regular representation of Δ in P, whereby every β of Δ is mapped on the matrix B defined by

$$\beta\lambda_j = \sum \lambda_i\beta_{ij}, \qquad B = (\beta_{ij}).$$

Next, when $\mathfrak{o}$ is simple, we form

$$\mathfrak{l} = c_{11}\Delta + \cdots + c_{n1}\Delta \tag{4}$$
$$= (c_{11}\lambda_1\mathsf{P} + \cdots + c_{11}\lambda_r\mathsf{P}) + \cdots + (c_{n1}\lambda_1\mathsf{P} + \cdots + c_{n1}\lambda_r\mathsf{P}).$$

If we represent an element $\beta \cdot c_{ik}$ of $\mathfrak{o}$ by means of this basis, then

$$\beta c_{ik} \to \begin{pmatrix} 0 & \ldots & 0 & \ldots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \ldots & B & \ldots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \ldots & 0 & \ldots & 0 \end{pmatrix},$$

where the zeros represent r-rowed null matrices and the matrix B stands in the k-th position of the i-th row of matrices. Hence on summing we obtain

$$(5) \qquad \sum_{i,k=1}^{n} \alpha_{ik} c_{ik} \to \begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \cdots & A_{nn} \end{pmatrix},$$

where the A_{ik} are the matrices which correspond to the α_{ik} in the regular representation of $\mathfrak{A}$.

From the form of the irreducible representation adapted to $\mathfrak{l}$ we can also determine how such representations decompose in an extension of the ground field P to a commutative extension field Ω. For this extension $\mathfrak{A}$ goes over into a system $\mathfrak{A}_\Omega = \mathfrak{A} \times \Omega$ and the left ideal $\mathfrak{l} = c_{11}\mathfrak{A} + \cdots + c_{n1}\mathfrak{A}$ into

$$\mathfrak{l}_\Omega = c_{11}\mathfrak{A}_\Omega + \cdots + c_{n1}\mathfrak{A}_\Omega.$$

Now if $\mathfrak{A}_\Omega$ is reducible, so that it has a proper left ideal $\mathfrak{l}'$, then $\mathfrak{l}_\Omega$ also has a proper subideal

$$\mathfrak{L}' = c_{11}\mathfrak{l}' + \cdots + c_{n1}\mathfrak{l}'.$$

Similarly, if $\mathfrak{A}_\Omega$ decomposes into irreducible left ideals $\mathfrak{l}'$, then $\mathfrak{l}_\Omega$ decomposes into the same number of irreducible left ideals $\mathfrak{L}'$. *The irreducible representation of* $\mathfrak{G}$ *adapted to* $\mathfrak{l}$ *becomes reducible or decomposable in an extension of* P *to* Ω *according as the system* $\mathfrak{A}_\Omega$ *is reducible or decomposable respectively into left* ideals.

If $\mathfrak{A} \neq \mathsf{P}$, we can always choose, by Section 121, the field Ω so that $\mathfrak{A}_\Omega$ has zero divisors; therefore it is no longer a field and contains at least one proper subideal. This means that the representation which is irreducible in P and adapted to $\mathfrak{l}$ becomes reducible in Ω. On the other hand, if $\mathfrak{A} = \mathsf{P}$, the representation adapted to $\mathfrak{l}$ is *absolutely irreducible*, i.e., it remains irreducible for every extension of the ground field. *Consequently* $\mathfrak{A} = \mathsf{P}$ *is the necessary and sufficient condition that a representation irreducible in* P *be absolutely irreducible.*

We will return in Section 130 to the splitting of an irreducible representation in the extension of the ground field.

Let the system $\mathfrak{o}$, which is being represented, be semi-simple instead of simple; therefore it is a direct sum of simple rings $\mathfrak{a}_1 + \cdots + \mathfrak{a}_s$. Let the left ideal $\mathfrak{l}$, which gives rise to an irreducible representation, be a left ideal in $\mathfrak{a}_\nu$. In order to find the representation adapted to $\mathfrak{l}$ we first write a as a sum $a_1 + \cdots + a_s$, then take out of this representation the component a_ν, and form the matrix belonging to the a_ν by formula (5). The remaining components $a_1, \ldots, a_{\nu-1}, a_{\nu+1}, \ldots, a_s$ annihilate the ideal $\mathfrak{l}$ and will therefore be represented by zero.

Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ be complete matrix rings of degrees $n_1, \ldots, n_s$ over the skew fields $\mathfrak{A}_1, \ldots, \mathfrak{A}_s$, let r_ν be the rank of $\mathfrak{A}_\nu$, and $\mathfrak{D}_\nu$ the irreducible representation adapted to a left ideal of $\mathfrak{a}_\nu$. Then the rank h of $\mathfrak{o}$ is equal to the sum of the ranks of $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$; therefore

(6) $$h = \sum_1^s n_\nu^2 r_\nu .$$

Furthermore, by (4) or (5) the degree of the representation $\mathfrak{D}_\nu$ is equal to

(7) $$g_\nu = n_\nu r_\nu .$$

Finally, $\mathfrak{a}_\nu$ splits into n_ν equivalent left ideals $\mathfrak{l}_\nu$; therefore the regular representation—adapted to $\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s$—contains the representation $\mathfrak{D}_\nu$ exactly n_ν times as a component.

In particular if all $\mathfrak{D}_\nu$ are absolutely irreducible, then all $r_\nu = 1$; in this case (6) and (7) simplify to

$$h = \sum_1^s n_\nu^2 ; \quad g_\nu = n_\nu .$$

EXERCISES. 1. Determine all irreducible representations of the hypercomplex system given in Section 116, Exer. 2.

2. Determine all irreducible representations of the quaternion system: a) over the rational number field Γ; b) over the field $\Gamma(i)$; c) over the field $\Gamma(\sqrt{2})$; d) over the prime field of characteristic 2.

3. If P is algebraically closed and $\mathfrak{o}$ is a system with radical, then the regular representation contains each and every irreducible representation at least as often as the degree of the representation. The rank of $\mathfrak{o}$ is greater than the sum of the squares of the degrees of the representations. [This sum is of course equal to the rank of $\mathfrak{o}/\mathfrak{c}$.]

4. Let the basis elements $a_1, \ldots, a_n$ of a hypercomplex system $\mathfrak{o}$ be mapped by a representation onto the matrices $A_1, \ldots, A_n$ and by means of the indeterminates $x_1, \ldots, x_n$ (which are adjoined to the ground field Ω) let us form the "generic element" $x_1 a_1 + \cdots + x_n a_n$ and its representation $A_x = x_1 A_1 + \cdots + x_n A_n$, then the determinant of the matrix A_x is a function of $x_1, \ldots, x_n$, which

a) is irreducible for an absolutely irreducible representation;

b) is equal to the determinant arising from an irreducible representation equivalent to the given representation, but is not equal to that arising from a non-equivalent representation;

c) splits into irreducible factors which correspond to the irreducible components of the representation.

[We choose the c_{ik}, together with a basis of the radical, as new basis elements and transform A_x correspondingly.]

124. THE REPRESENTATIONS OF THE CENTRUM

The centrum of a hypercomplex system $\mathfrak{o}$ must be mapped by an irreducible representation on a set of matrices each of which is permutable with all matrices of the representation. If the ground field is algebraically closed, the ring formed by the matrices of the representation is a complete matrix ring. Since the centrum of a complete matrix ring contains only multiples of the unit matrix: λE_n, the centrum of $\mathfrak{o}$ is represented by matrices of the form λE_n. This is also valid for absolutely irreducible representations since for these the ground field can always be extended to an algebraically closed field without destroying the irreducibility. Hence *for an absolutely irreducible representation of a hypercomplex system* $\mathfrak{o}$ *the centrum elements are represented by multiples of the unit matrix.*

If the system $\mathfrak{o}$ is commutative, which means that it is its own centrum, then all matrices obtained from an absolutely irreducible representation have the form λE_n. But the irreducibility implies that the representation must be of the first degree. Hence *the absolutely irreducible representations of a commutative hypercomplex system are of the first degree.*

A representation of first degree of $\mathfrak{o}$ is a homomorphic mapping of $\mathfrak{o}$ in the representation field K. If K is commutative, two equivalent representations of first degree are equal; for if A is a matrix of the representation, λ an element of K, then

$$\lambda^{-1} A \lambda = A.$$

Hence a commutative hypercomplex system $\mathfrak{o}$ *has as many inequivalent representations of first degree in the commutative field* K *as there are distinct homomorphisms of* $\mathfrak{o}$ *in* K.

We return now to the non-commutative systems and assume that $\mathfrak{o}$ is a system without radical. Then $\mathfrak{o}$ is a direct sum of simple systems:

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s,$$

and the centrum $\mathfrak{Z}$ of $\mathfrak{o}$ is the sum of exactly as many fields:

$$\mathfrak{Z} = \mathfrak{Z}_1 + \cdots + \mathfrak{Z}_s \qquad (\mathfrak{Z}_\nu \text{ centrum of } \mathfrak{a}_\nu).$$

The number of inequivalent irreducible representations of $\mathfrak{o}$, and so of $\mathfrak{Z}$, is equal to the number s of two-sided components of $\mathfrak{o}$, or $\mathfrak{Z}$; thus, each of these representations $\mathfrak{D}_\nu$ of $\mathfrak{o}$ may be obtained from a left ideal of $\mathfrak{a}_\nu$, and similarly each representation $\mathfrak{D}'_\nu$ of $\mathfrak{Z}$ may be obtained from an $\mathfrak{Z}_\nu$. *Hence there are exactly as many inequivalent irreducible representations of* $\mathfrak{o}$ *as of* $\mathfrak{Z}$, *and every irreducible representation* $\mathfrak{D}_\nu$ *of* $\mathfrak{o}$, *for which all* $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ *with the exception of* $\mathfrak{a}_\nu$ *are represented by zero, may be associated with a representation* $\mathfrak{D}'_\nu$ *of* $\mathfrak{Z}$, *for which all* $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_s$ *with the exception of* $\mathfrak{Z}_\nu$ *are represented by zero.*

In particular, if the ground field P is a splitting field of $\mathfrak{o}$, which means that $\mathfrak{o}$ is the sum of complete matrix rings over P, then the fields $\mathfrak{Z}_\nu$ have rank 1 and are isomorphic to P; consequently, in this case, the number s of the irreducible representations of $\mathfrak{o}$ is equal to the rank of the centrum $\mathfrak{Z}$. From the fact that the $\mathfrak{Z}_\nu$ are P-modules of rank 1 it again follows that the irreducible representations of $\mathfrak{Z}$ are of the first degree.

The relations existing between the irreducible representations $\mathfrak{D}_\nu$ of $\mathfrak{o}$ and the irreducible representations (of first degree) of $\mathfrak{Z}$ are in this case quite simple. Thus, for the representation $\mathfrak{D}_\nu$ each centrum element a is represented by a matrix of the form αE_{n_ν}, where E_{n_ν} designates the unit matrix of n_ν-th degree. This means that each a corresponds (for a given ν) to a fixed α, and we can write:

$$\alpha = \Theta_\nu(a).$$

The function Θ_ν gives rise to a homomorphism of the centrum, since

$$\Theta_\nu(a+b) = \Theta_\nu(a) + \Theta_\nu(b),$$
$$\Theta_\nu(ab) = \Theta_\nu(a)\,\Theta_\nu(b),$$
$$\Theta_\nu(a\lambda) = \Theta_\nu(a)\lambda.$$

For this homomorphism all $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_s$ with the exception of $\mathfrak{Z}_\nu$ are represented by zero; i.e., the homomorphism Θ_ν is exactly the representation of first degree of the centrum designated earlier by $\mathfrak{D}_\nu$.

The representation Θ_ν is known as soon as a P-basis is given for the module $\mathfrak{Z}_\nu$; for this purpose we can choose the unit element e_ν of the field $\mathfrak{Z}_\nu$. If we write every element a of $\mathfrak{Z}$ in the form

$$a = \sum_{\nu=1}^{s} e_\nu \lambda_\nu, \tag{1}$$

then

$$a e_\nu = e_\nu^2 \lambda_\nu = e_\nu \lambda_\nu;$$

consequently, $\lambda_\nu E_{n_\nu}$ is the matrix representing a:

$$\Theta_\nu(a) = \lambda_\nu.$$

(1) may now be written as

$$a = \sum_{\nu=1}^{s} e_\nu \Theta_\nu(a). \tag{2}$$

This means: *the coefficients $\Theta_\nu(a)$ in the expansion of the centrum element a according to the idempotent elements e_ν of the centrum give rise at the same time to the homomorphisms or representations of first degree of the centrum.*

EXERCISES. 1. The number of representations of the first degree of a commutative hypercomplex system $\mathfrak{o}$ in the algebraically closed extension field Ω of P is equal to the rank of $\mathfrak{o}_\Omega/\mathfrak{c}$, where $\mathfrak{c}$ is the radical of $\mathfrak{o}_\Omega$.

2. If K is a commutative field over P, the number of representations of first degree of K in Ω is equal to the reduced field degree of K over P. We have $\mathfrak{c} = (0)$ if and only if K is separable over P.

3. The degree of the irreducible representation $\mathfrak{D}'_\nu$ of $\mathfrak{Z}$ is equal to the rank of $\mathfrak{Z}_\nu$ over P. In the representation $\mathfrak{D}_\nu$ of $\mathfrak{Z}$ the representation $\mathfrak{D}'_\nu$ is contained exactly $n_\nu t_\nu$ times, where n_ν and t_ν are determined as follows: $\mathfrak{a}_\nu$ is a complete matrix ring of n_ν-th degree with matrix elements in a skew field K_ν, and t_ν is the rank of K_ν with respect to its centrum $\mathfrak{Z}_\nu$.

125. TRACES AND CHARACTERS

By the *trace of the element a in the representation* $\mathfrak{D}$, written

$$S_{\mathfrak{D}}(a) \quad \text{or simply} \quad S(a),$$

we understand the trace $S(A)$ of the matrix A corresponding to a in the representation $\mathfrak{D}$. The trace $S_{\mathfrak{D}}$, which for fixed $\mathfrak{D}$ may be considered as a function of the element a, is also called the *trace of the representation* $\mathfrak{D}$.

In view of the relation

$$S(P^{-1}AP) = S(A)$$

equivalent representations have the same traces.

The traces are *linear functions*, i.e.,

$$S(a + b) = S(a) + S(b),$$
$$S(a\lambda) = S(a)\lambda.$$

The traces of the absolutely irreducible representations (in other words, the traces of the irreducible representations in the algebraically closed field Ω) are called *characters*.[2] The character of an element a in the ν-th irreducible representation ϑ_ν is designated by

$$\chi_\nu(a).$$

The index ν, when we are dealing with a fixed representation, will occasionally be omitted.

For an absolutely irreducible representation $\mathfrak{D}_\nu$ of degree n_ν the centrum element z is mapped, by Section 124, on the diagonal matrix $E_{n_\nu} \cdot \Theta_\nu(z)$, where Θ_ν is a homomorphism of the centrum in the field Ω. The trace of the matrix $E_{n_\nu} \cdot \Theta_\nu(z)$ is

[2] Nowadays authors also use the word character for reducible representations and then speak of "compound characters." This designation is avoided here since in the special case of the Abelian groups it does not give to the word "character" the meaning usually attached to it in the past (cf. Section 126), and besides the word "trace" (of the representation) designates the meaning just as clearly.

(1) $$\chi_\nu(z) = n_\nu \cdot \Theta_\nu(z).$$

In particular the identity of $\mathfrak{o}$ is represented by the unit matrix E_{n_ν} whose trace is equal to n_ν:

$$\chi_\nu(1) = n_\nu.$$

We assume in the following that the degrees n_ν of the absolutely irreducible representations are not divisible by the characteristic of the field Ω. Then we can divide (1) by n_ν and obtain

(2) $$\Theta_\nu(z) = \frac{\chi_\nu(z)}{n_\nu}.$$

In this manner the homomorphisms of the centrum are expressed in terms of the characters.

THEOREM. *A completely reducible representation of a hypercomplex system* $\mathfrak{o}$ *in the field* Ω *of characteristic* 0 *is uniquely determined except for equivalence by the traces of the matrices of the representation.*

PROOF. If $\mathfrak{c}$ is the radical of $\mathfrak{o}$, every completely reducible representation of $\mathfrak{o}$ is at the same time one of $\mathfrak{o}/\mathfrak{c}$. By assumption the traces of the matrices which represent the elements of $\mathfrak{o}/\mathfrak{c}$ are known. Let

$$\mathfrak{o}/\mathfrak{c} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n$$

and $e_1, \ldots, e_n$ be the unit elements of $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$. Then in the irreducible representation $\mathfrak{D}_\nu$ the element e_ν is represented by the n_ν-rowed unit matrix; consequently the pertaining trace is

$$S_\nu(e_\nu) = n_\nu,$$

while

$$S_\nu(e_\mu) = 0 \quad \text{for} \quad \mu \neq \nu.$$

Now a completely reducible representation is known as soon as we know how often every irreducible representation $\mathfrak{D}_\nu$ occurs in it. If the representation $\mathfrak{D}_\nu$ occurs, let us say, q_ν-times, then the representation consists of q_1 blocks $\mathfrak{D}_1$, q_2 blocks $\mathfrak{D}_2$, etc. Hence the trace of e_ν in this representation is

(3) $$S(e_\nu) = q_\nu n_\nu.$$

From (3) the q_ν may be calculated as soon as all traces $S(e_\nu)$ are known. Thereby the theorem is proved.

REMARK. The traces of all elements of $\mathfrak{o}$ are known as soon as the traces of the basis elements of $\mathfrak{o}$ are known. Hence if $\mathfrak{o}$ is the group ring of a finite group, we need to know only the traces of the group elements in order to determine the representation. Therefore:

A completely reducible representation of a finite group is completely determined except for equivalence by the traces of the group elements.

If $a_1, \ldots, a_n$ are the basis elements of a system $\mathfrak{o}$ and $\chi_\nu(a_i)$ their traces for the irreducible representations, then for an arbitrary representation we have

$$S(a_i) = \sum_{\nu=1}^{g} q_\nu \chi_\nu(a_i). \tag{4}$$

These equations uniquely determine the numbers q_ν as a consequence of the above theorem. Furthermore, the equations (4) yield a computational procedure for breaking up a given completely reducible representation into irreducible components by means of calculations on the traces alone. This assumes, of course, that the characters of the irreducible components are known beforehand.

EXERCISES. 1. For a representation which is not completely reducible the representation itself is not uniquely determined by the traces alone, though the irreducible diagonal blocks appearing in it (composition factors of the representation module) are so determined.

2. A completely reducible representation of an infinite group is uniquely determined except for equivalence by the traces alone. [If any two representations of finite degree with equal traces are given, then we may follow one by the other for a representation and extend the system of the representation matrices to a ring. This ring is then hypercomplex, and we have before us two representations of a hypercomplex system.]

126. REPRESENTATION OF ABELIAN GROUPS

The finite Abelian groups form an excellent as well as simple example for the representation theory.

Let the group $\mathfrak{G}$ of order h be a direct product of cyclic groups of orders $h_1, \ldots, h_r$; then every element a of $\mathfrak{G}$ may be uniquely represented in the form

$$a = c_1^{\lambda_1} c_2^{\lambda_2} \ldots c_r^{\lambda_r} \qquad (0 \leqq \lambda_1 < h_1,\ 0 \leqq \lambda_2 < h_2, \ldots, 0 \leqq \lambda_r < h_r).$$

We seek the irreducible representations of the group in an algebraically closed field Ω whose characteristic is zero or at least does not divide $h = h_1 h_2 \ldots h_r$.

First, the irreducible representations are *linear* (i.e., of degree 1). Hence we are concerned with the problem of associating to each group element a a number $\chi(a)$ of Ω such that the relation of homomorphism

$$\chi(ab) = \chi(a)\chi(b) \tag{1}$$

is satisfied. Such a function χ is called a *character* of the group. (This definition is in accord with the more general one given in Section 125, since the trace of the matrix (χ) is equal to χ.)

We exclude the null representation

$$\chi(a) = 0 \qquad \text{for all } a.$$

Then we must have $\chi(1) = 1$. Furthermore,

$$\chi(c_1^{\lambda_1} \dots c_r^{\lambda_r}) = \chi(c_1)^{\lambda_1} \dots \chi(c_r)^{\lambda_r},$$

$$\chi(c_\nu)^{h_\nu} = \chi(c_\nu^{h_\nu}) = \chi(1) = 1;$$

consequently, $\chi(c_\nu)$ is an h_ν-th root of unity ζ_ν and the representation has the form

$$\chi(c_1^{\lambda_1} \dots c_r^{\lambda_r}) = \zeta_1^{\lambda_1} \dots \zeta_r^{\lambda_r}. \tag{2}$$

Conversely, the equation (2) for an arbitrary choice of the roots of unity $\zeta_1, \dots, \zeta_r$ always represents a homomorphism of the group $\mathfrak{G}$. For every root of unity ζ_ν we have h_ν values at our disposal; *altogether there are therefore*

$$h = h_1 h_2 \dots h_r$$

distinct characters, which admit just as many inequivalent representations of first degree.

If we choose all $\zeta_\nu = 1$, we obtain the *principal character* χ_0:

$$\chi_0(a) = 1.$$

We can very easily carry out the details to show how all representations arise from the reduction of the regular representation (cf. Section 123). First, we take a single cyclic group $\mathfrak{G}$ with generating element c; $c^h = 1$. Then the regular representation of c is given by the linear transformation

$$c \cdot c^\lambda = c^{\lambda+1}, \quad \text{in the vector space } (1, c, c^2, \dots, c^{h-1}).$$

In order to reduce the representation we introduce the new basis elements

$$(\zeta, c) = 1 + \zeta c + \zeta^2 c^2 + \dots + \zeta^{h-1} c^{h-1} \tag{3}$$

(cf. the Lagrange resolvent in Section 55), where ζ runs through the h h-th roots of unity. These actually form a basis since the c^λ may be expressed in terms of (ζ, c). Thus if we multiply (3) by ζ^{-r} and sum over all ζ, we obtain

$$\sum \zeta^{-r}(\zeta, c) = h c^r. \tag{4}$$

Furthermore, an easy computation shows that

$$c \cdot (\zeta, c) = \zeta^{-1} \cdot (\zeta, c), \tag{5}$$

consequently, each individual basis element (ζ, c) defines an invariant subspace: *the representation is completely reducible*, and the matrix representing c in a single subspace is

$$(\chi(c)) = (\zeta^{-1}).$$

ζ^{-1}, as well as ζ, runs through all h-th roots of unity.

For a direct product of cyclic groups we introduce in place of the products $c_1^{\lambda_1} c_2^{\lambda_2} \dots c_r^{\lambda_r}$ the new basis elements

$$(\zeta_1, \dots, \zeta_r; c_1, \dots, c_r) = (\zeta_1, c_1)(\zeta_2, c_2) \dots (\zeta_r, c_r)$$

and find in a completely reduced form the representation

$$c_\mu \cdot (\zeta_1, \ldots, \zeta_r; c_1, \ldots, c_r) = \zeta_\mu^{-1}(\zeta_1, \ldots, \zeta_r; c_1, \ldots, c_r);$$

therefore as irreducible representations we have:

$$\chi(c_\mu) = \zeta_\mu^{-1},$$
$$\chi(c_1^{\lambda_1} c_2^{\lambda_2} \ldots c_r^{\lambda_r}) = \zeta_1^{-\lambda_1} \zeta_2^{-\lambda_2} \ldots \zeta_r^{-\lambda_r}.$$

Hence

The group ring of an Abelian group formed with the help of an algebraically closed field is completely reducible and the direct sum of h fields $\mathfrak{Z}_\nu$, *which are generated by the new basis vectors* $(\zeta_1, \ldots, \zeta_r; c_1, \ldots, c_r)$, *provided that we assume throughout that the characteristic of the field does not divide the order h of the group.*

The $(\zeta_1, \ldots, \zeta_r; c_1, \ldots, c_r)$ must therefore be idempotent except for a factor. In fact it easily follows that

$$(\zeta_\nu, c_\nu)^2 = h_\nu(\zeta_\nu, c_\nu),$$

consequently

$$(\zeta_1, \ldots, \zeta_r; c_1, \ldots, c_r)^2 = h(\zeta_1, \ldots, \zeta_r; c_1, \ldots, c_r),$$

i.e., the element

$$\frac{1}{h}(\zeta_1, \ldots, \zeta_r; c_1, \ldots, c_r)$$

is idempotent (and the unit element of the field $\mathfrak{Z}_\nu$).

In view of the proof just given it follows, by Section 123, Theorem 1, that *every representation of the group* $\mathfrak{G}$ *is completely reducible.*

Between the characters there exists a series of relations which are found as follows: first, the product of two characters is again a character:

$$\chi(a)\chi'(a) = \chi''(a), \tag{6}$$

and similarly the inverse of a character is a character. Consequently *the characters form a group* $\mathfrak{H}$.

If ζ_ν is a primitive h_ν-th root of unity, the character

$$\chi(c_1^{\lambda_1} \ldots c_r^{\lambda_r}) = \zeta_\nu^{\lambda_\nu}$$

generates a cyclic subgroup $\mathfrak{H}_\nu$ of order h_ν in the group $\mathfrak{H}$. We can easily show that the whole group $\mathfrak{H}$ is the direct product of the subgroups $\mathfrak{H}_\nu$. Consequently, just as in the case of $\mathfrak{G}$, the group $\mathfrak{H}$ is a direct product of cyclic groups of orders $h_1, \ldots, h_r$; *therefore the group* $\mathfrak{H}$ *of the characters is isomorphic to the given group* $\mathfrak{G}$.

The reciprocity expressed by equations (1), (6) between the groups $\mathfrak{G}$, $\mathfrak{H}$ is reversible. Thus, the number $\chi(a)$ depends on the character χ and on the group element a and for fixed a may be interpreted as a function of the character χ; by (6) this function is a homomorphism of the character group $\mathfrak{H}$. The number of

these homomorphisms is again h; therefore all homomorphisms of the group $\mathfrak{H}$ are given by the group $\mathfrak{G}$.

From (2) we obtain through summation over all $\lambda_1, \ldots, \lambda_r$:

$$\sum_a \chi(a) = (\sum \zeta_1^{\lambda_1})(\sum \zeta_2^{\lambda_2}) \ldots (\sum \zeta_r^{\lambda_r}) = \begin{cases} h \text{ when all } \zeta_\nu = 1 \\ 0 \text{ otherwise.} \end{cases}$$

Therefore we have

$$\sum_a \chi(a) = \begin{cases} h & \text{for } \chi = \chi_0, \\ 0 & \text{for } \chi \neq \chi_0. \end{cases} \tag{7}$$

Similarly the reciprocal relation is valid

$$\sum_\chi \chi(a) = \begin{cases} h & \text{for } a = 1, \\ 0 & \text{for } a \neq 1. \end{cases} \tag{8}$$

If we set in (8) $a = a'a''$, then

$$\sum_\chi \chi(a')\chi(a'') = \begin{cases} h & \text{for } a' = a''^{-1}, \\ 0 & \text{for } a' \neq a''^{-1}. \end{cases} \tag{9}$$

Similarly we have reciprocally

$$\sum_a \chi'(a)\chi''(a) = \begin{cases} h & \text{for } \chi' = \chi''^{-1}, \\ 0 & \text{for } \chi' \neq \chi''^{-1}. \end{cases} \tag{10}$$

The character χ^{-1} is said to be *conjugate* to χ and is designated by $\bar{\chi}$. (In the case of number fields ζ^{-1} is conjugate complex to ζ, and therefore χ^{-1} is conjugate complex to χ.) Since we obviously have $\chi(a^{-1}) = \bar{\chi}(a)$ we may write instead of (9) and (10):

$$\sum_\chi \chi(a')\bar{\chi}(a'') = \begin{cases} h & \text{for } a' = a'', \\ 0 & \text{for } a' \neq a'', \end{cases} \tag{11}$$

$$\sum_a \chi'(a)\overline{\chi''}(a) = \begin{cases} h & \text{for } \chi' = \chi'', \\ 0 & \text{for } \chi' \neq \chi''. \end{cases} \tag{12}$$

Each of these two equations says that the matrix of the h^2 numbers $\chi(a)$ (where χ is the row index and a the column index) is the inverse of the transpose of the matrix with elements $\frac{1}{h}\bar{\chi}(a)$ ($\bar{\chi}$ the row index, a the column index). We call (11) the *orthogonality relation of the characters.*

The characters of Abelian groups are frequently used in the theory of numbers. Let n be a natural number. For $\mathfrak{G}$ we take the multiplicative group of the residue classes mod n which have as a representative the natural numbers $\leqq n$ that are relatively prime to n. (h is therefore Euler's function $\varphi(n)$.) By a *residue character*

$\chi(m)$ *of a number* m *modulo* n *relatively prime to* n we understand a character of the residue class of m in the residue class group. Furthermore, set $\chi(m) = 0$ whenever the natural number m is not relatively prime to n. By this convention the summation in (7) or (10) may be extended over a complete residue system modulo n, while (1), (6), and (9) are valid for all numbers a, b or a', a''.

EXERCISE. 1. Write all characters of the numbers 1 to 11 modulo 12; similarly for modulo 11.

For generalizations of the theory of characters to infinite Abelian groups we refer to the works of Pontrjagin, Alexander, and Van Kampen in *Ann. of Math. Vols. 35 and 36 (1934/35).*

127. REPRESENTATIONS OF FINITE GROUPS

In Section 122 we stated the problem of the representation of a finite group $\mathfrak{G}$ in terms of the same problem regarding the group ring $\mathfrak{o} = (a_1, \ldots, a_h)$. The determination of all representations will be based on Theorem 1 of Section 123 as soon as we have proved that the group ring is completely reducible. For this purpose it is sufficient to prove the following *Theorem of Maschke:*

Every representation of a finite group $\mathfrak{G}$ *in a field* P, *whose characteristic does not divide the order* h *of the group, is completely reducible.*

PROOF. Let the representation module $\mathfrak{M}$ be reducible, and let $\mathfrak{N}$ be a minimal (or irreducible) submodule. We will show that $\mathfrak{M}$ may be represented as a direct sum $\mathfrak{N} + \mathfrak{N}''$, where $\mathfrak{N}''$ is again a representation module.

Since $\mathfrak{M}$ is a vector space it decomposes according to the scheme $\mathfrak{N} + \mathfrak{N}'$; however, $\mathfrak{N}'$ is not necessarily invariant relative to $\mathfrak{o}$, and so it is not necessarily a representation module. If y is an element of $\mathfrak{N}'$ and a is one of $\mathfrak{G}$, then ay may be uniquely represented as the sum of an element of $\mathfrak{N}$ and an element y' of $\mathfrak{N}'$; therefore

$$ay \equiv y' \,(\mathrm{mod}\, \mathfrak{N}).$$

The element y' for fixed a is uniquely determined by y and depends linearly on y: if $ay \equiv y'$ and $az \equiv z'$, then $a(y + z) \equiv y' + z'$ and $ay\lambda \equiv y'\lambda$ for $\lambda \in \mathsf{P}$. We can therefore write

$$y' = A'y; \qquad A'y \equiv ay \,(\mathrm{mod}\, \mathfrak{N}),$$

where A' is[3] a linear operator (i.e., a linear transformation) in $\mathfrak{N}'$ and depends on a. Actually, the operators A' form a representation of the group $\mathfrak{G}$, since if $a \to A'$ and $b \to B'$, then $ab \to A'B'$.

[3] If we represent all linear transformations by matrices, as in Section 110, formula (4), then A' is the matrix standing on the right and designated there by T.

We now set

$$\frac{1}{h}\sum_a a^{-1}A'y = Qy = y'';$$

then y'' also depends linearly on y and consequently the y'' form a linear subsystem $\mathfrak{N}'' = Q\mathfrak{N}'$. Furthermore, it follows modulo $\mathfrak{N}$ that

$$y'' \equiv \frac{1}{h}\sum_a a^{-1}ay = y.$$

Hence every element of $\mathfrak{M}$ is congruent modulo $\mathfrak{N}$ not only to an element y of $\mathfrak{N}'$ but also to a uniquely determined element y'' of $\mathfrak{N}''$; i.e., there exists the representation as a direct sum

$$\mathfrak{M} = \mathfrak{N} + \mathfrak{N}''.$$

Finally, for every element b of $\mathfrak{G}$ we have

$$\begin{aligned} by'' &= \frac{1}{h}\sum_a ba^{-1}A'y \\ &= \frac{1}{h}\sum_a (ab^{-1})^{-1}(A'B'^{-1})B'y \\ &= QB'y \in Q\mathfrak{N}' = \mathfrak{N}''; \end{aligned}$$

consequently, $\mathfrak{N}''$ is transformed into itself by the operators b of $\mathfrak{G}$, i.e., $\mathfrak{N}''$ is a representation module.

If $\mathfrak{N}''$ is also reducible, we can handle $\mathfrak{N}''$ in the same manner by splitting off a minimal submodule, etc. Continuing thus we finally arrive at the complete decomposition of the module $\mathfrak{M}$ and thereby of the representation.

If we wish to set up all representations of a group, it is sufficient, by the theorem just proved, to find the irreducible ones; these we can find by means of the minimal left ideals of the group ring (in other words, by the reduction of the regular representation). In a reducible representation every irreducible one can be repeated arbitrarily often.

The number of absolutely irreducible representations is by Section 124 equal to the rank of the centrum, and the centrum of the group ring consists, as we see without difficulty, of all those sums

$$\sum_\lambda a_\lambda \varrho_\lambda \qquad (a_\lambda \in \mathfrak{G},\ \varrho_\lambda \in \mathsf{P}), \tag{1}$$

in which conjugate group elements have the same coefficients. The elements conjugate to an element a form a "*class.*" If k_a is the sum of the elements of this class, then (1) is a sum of such sums k_a with coefficients in P. Consequently we have the theorem: *the centrum of the group ring is generated by the class sums* k_a. Hence the rank of the centrum is equal to the number of classes. This implies:

The number of inequivalent absolutely irreducible representations of a group is equal to the number of classes of conjugate elements.

The degrees $n_1, \ldots, n_s$ of the irreducible representations satisfy the relation

$$n_1^2 + n_2^2 + \cdots + n_s^2 = h,$$

since the group ring of rank h is the direct sum of matrix rings of ranks $n_1^2, n_2^2, \ldots, n_s^2$.

A representation of first degree, which always exists, is the "identical representation" whereby every group element is mapped on the element 1.

If there are other representations of first degree there must exist a proper normal divisor with an Abelian factor group; for the transformations of the representations of first degree are permutable with one another and form an Abelian group homomorphic to the group. Conversely, if a proper normal divisor with an Abelian factor group exists, then the characters of this Abelian group always give rise to representations of first degree. All remaining representations are of higher degree.

EXAMPLES. 1. *The symmetric group* $\mathfrak{S}_3$. Class number is 3; therefore 3 representations. The alternating group has 2 cosets $\mathfrak{R}_0$, $\mathfrak{R}_1$: those of even and odd substitutions. The 2 characters of this group of two elements:

$$\chi(\mathfrak{R}_0) = 1, \qquad \chi(\mathfrak{R}_1) = \pm 1,$$

determine the representations of first degree. Since

$$n_1^2 + n_2^2 + n_3^2 = 6$$

the third representation must have degree 2. If we take three vectors e_1, e_2, e_3 in a plane, whose sum is zero, then the permutations of these three vectors produces a faithful representation of this permutation group; the representation can be easily shown to be irreducible. If we take e_1 and e_2 as basis vectors, the representation takes on the following form:

$$\begin{cases}(1\ 2)e_1 = e_2,\\ (1\ 2)e_2 = e_1,\end{cases} \quad \begin{cases}(1\ 3)e_1 = -e_1 - e_2,\\ (1\ 3)e_2 = e_2,\end{cases} \quad \begin{cases}(2\ 3)e_1 = e_1,\\ (2\ 3)e_2 = -e_1 - e_2,\end{cases}$$

$$\begin{cases}(1\ 2\ 3)e_1 = e_2,\\ (1\ 2\ 3)e_2 = -e_1 - e_2,\end{cases} \quad \begin{cases}(1\ 3\ 2)e_1 = -e_1 - e_2,\\ (1\ 3\ 2)e_2 = e_1.\end{cases}$$

2. *The quaternion group* $\mathfrak{Q}_8$:

$$j^4 = 1, \qquad k^2 = j^2, \qquad kj = j^3k.$$

Class number is 5; therefore there are 5 representations. The normal divisor $\{1, j^2\}$ has as factor group the Klein four-group, whose 4 characters give rise to 4 linear representations. The remaining representation must have degree 2 since

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 8.$$

If we map the group elements $1, j, j^2, j^3, k, jk, j^2k, j^3k$ on the quaternions $1, j, -1, -j, k, l, -k, -l$, we obtain a homomorphic mapping of the group

ring $\mathfrak{o}$ on the quaternion field; therefore the quaternion field must occur among the two-sided composition factors of $\mathfrak{o}$. Hence the decomposition of $\mathfrak{o}$ in the rational ground field Γ is given by

$$\mathfrak{o} = \mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3 + \mathfrak{a}_4 + \mathfrak{a}_5,$$

where $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4$ are isomorphic to Γ and $\mathfrak{a}_5$ is isomorphic to the quaternion field. If we go over to an algebraically closed ground field (it is sufficient in this case to adjoin $i = \sqrt{-1}$), then the quaternion field splits and we obtain the matrix representation

$$j \to \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad k \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad l \to \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

3. *The alternating group* $\mathfrak{A}_4$ may be handled in the same way as the symmetric group $\mathfrak{S}_3$ and so we will leave it to the reader. There are 4 representations of degrees 1, 1, 1, 3.

4. *The symmetric group.* $\mathfrak{S}_4$. The class number is 5; therefore there are 5 representations. The Klein four-group $\{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ has a factor group isomorphic to $\mathfrak{S}_3$, for which we have already found 3 irreducible representations of degrees 1, 1, 2; they also produce representations of degrees 1, 1, 2 of $\mathfrak{S}_4$. Let these degrees be designated by n_1, n_2, n_3. Then from

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 24,$$

follows

$$n_4^2 + n_5^2 = 18$$

which is valid only for $n_4 = 3$, $n_5 = 3$. If we introduce 4 vectors e_1, e_2, e_3, e_4 whose sum is zero, then the permutations of these 4 vectors generate a faithful representation of third degree of $\mathfrak{S}_4$. If we choose e_1, e_2, e_3 as basis vectors, the representation takes on the following form:

$$\begin{cases} (1\ 2)e_1 = e_2, \\ (1\ 2)e_2 = e_1, \\ (1\ 2)e_3 = e_3, \end{cases} \quad \begin{cases} (1\ 3)e_1 = e_3, \\ (1\ 3)e_2 = e_2, \\ (1\ 3)e_3 = e_1, \end{cases} \quad \begin{cases} (1\ 4)e_1 = -e_1 - e_2 - e_3, \\ (1\ 4)e_2 = e_2, \\ (1\ 4)e_3 = e_3, \end{cases}$$

$$\begin{cases} (1\ 2\ 3)e_1 = e_2, \\ (1\ 2\ 3)e_2 = e_3, \\ (1\ 2\ 3)e_3 = e_1, \end{cases} \quad \text{etc.}$$

Since the representation is faithful, it can not be reduced to the representations of first and second degree; therefore it is irreducible. If we multiply the matrices representing the odd substitutions by -1, we obtain another representation of third degree. This representation is also faithful and therefore irreducible; moreover, it is not equivalent to the previous one since the traces are different. Hence we have found all representations.

EXERCISES. 1. The element $s = \sum_{a \in \mathfrak{G}} a$ of the group ring $\mathfrak{o}$ satisfies the equations

$$bs = s \quad \text{for} \quad b \in \mathfrak{B}.$$

What left ideals are generated by s? What representation belongs to this ideal? What idempotent element is contained in this ideal?

2. If the number h of group elements is divisible by the characteristic of the field, the ideal given in Exercise 1 is nilpotent. Using this fact show that the condition: the characteristic should not divide h, is also necessary for the Theorem of Maschke.

128. GROUP CHARACTERS

The Kronecker Product Transformation

Let two linear transformations A', A'' be given such that one operates in the vector space $(u_1, \ldots, u_n)$, and the other in the vector space $(v_1, \ldots, v_m)$, where the u and v are understood to be indeterminates. Hence let us say that

$$A'u_k = \sum_i u_i \alpha'_{ik},$$
$$A''v_l = \sum_j v_j \alpha''_{jl}.$$

On applying these transformations to the u and v at the same time, the products $u_k v_l$ are transformed as follows: [4]

$$A\, u_k v_l = \sum_i \sum_j u_i v_j \alpha'_{ik} \alpha''_{jl}. \tag{1}$$

The transformation A, which is thereby generated, operates in the vector space with the $n \cdot m$ linearly independent elements $u_k v_l$; A is called the *Kronecker product transformation*, and is designated by $A' \times A''$. The matrix elements of A are by (1) the products $\alpha'_{ik}\alpha''_{jl}$. The trace of A is

$$\sum_i \sum_j \alpha'_{ii}\alpha''_{jj} = \sum_i \alpha'_{ii} \cdot \sum_j \alpha''_{jj} = S(A') \cdot S(A'');$$

consequently: *the trace of the product transformation $A' \times A''$ is the product of the traces of the transformations A' and A''.*

If we apply to the u the two transformations B', A' one after the other and to the v the two transformations B'', A'' one after the other, then the products $u_k v_l$ undergo one after the other the transformations $B' \times B''$ and $A' \times A''$; i.e.,

$$(A' \times A'') \cdot (B' \times B'') = A'B' \times A''B''. \tag{2}$$

If the matrices $A', B', \ldots$ form a representation $\mathfrak{D}'$ of a group $\mathfrak{G}$ and matrices $A'', B'', \ldots$ another representation $\mathfrak{D}''$ of the same group, it follows from

[4] The indeterminates are assumed to be permutable with one another and with the coefficients.

(2) that the product transformations $A = A' \times A''$, $B = B' \times B''$, ... again form a representation. This *product representation* of the representations $\mathfrak{D}'$, $\mathfrak{D}''$ is designated by $\mathfrak{D}' \times \mathfrak{D}''$.

Let $\mathfrak{D}' + \mathfrak{D}''$ designate a reducible representation which decomposes completely into $\mathfrak{D}'$ and $\mathfrak{D}''$, and let equivalent representations be considered as not distinct. We can easily show that the sums and products of representations satisfy the following rules:

$$\mathfrak{D}' + \mathfrak{D}'' = \mathfrak{D}'' + \mathfrak{D}', \qquad \mathfrak{D}' \times \mathfrak{D}'' = \mathfrak{D}'' \times \mathfrak{D}',$$

$$\mathfrak{D}' + (\mathfrak{D}'' + \mathfrak{D}''') = (\mathfrak{D}' + \mathfrak{D}'') + \mathfrak{D}''', \quad \mathfrak{D}' \times (\mathfrak{D}'' \times \mathfrak{D}''') = (\mathfrak{D}' \times \mathfrak{D}'') \times \mathfrak{D}''',$$

$$\mathfrak{D}' \times (\mathfrak{D}'' + \mathfrak{D}''') = \mathfrak{D}' \times \mathfrak{D}'' + \mathfrak{D}' \times \mathfrak{D}''', \quad (\mathfrak{D}'' + \mathfrak{D}''') \times \mathfrak{D}' = \mathfrak{D}'' \times \mathfrak{D}' + \mathfrak{D}''' \times \mathfrak{D}'.$$

In particular if $\mathfrak{G}$ is a finite group, every representation decomposes completely into irreducible representations $\mathfrak{D}_\nu$; therefore

$$\mathfrak{D}_\lambda \times \mathfrak{D}_\mu = \sum_\nu c_{\lambda\mu}^\nu \mathfrak{D}_\nu, \tag{3}$$

where the $c_{\lambda\mu}^\nu$ are integers $\geqq 0$. Hence we can interpret the representations $\mathfrak{D}_\nu$ as generators of a commutative hypercomplex system $\mathfrak{H}$.

In regard to the traces it follows from (3) that

$$S_\lambda(a) \cdot S_\mu(a) = \sum_\nu c_{\lambda\mu}^\nu S_\nu(a).$$

If the representations are absolutely irreducible, the traces become characters, and we can write:

$$\chi_\lambda(a) \cdot \chi_\mu(a) = \sum_\nu c_{\lambda\mu}^\nu \chi_\nu(a) \quad (\textit{first character-relation}). \tag{4}$$

The Characters As Class Functions

If a and a' are conjugate group elements:

$$a' = bab^{-1},$$

then for the corresponding matrices we have

$$A' = BAB^{-1}.$$

Consequently A and A' have the same traces: i.e.,

$$S(bab^{-1}) = S(a),$$

in particular

$$\chi(bab^{-1}) = \chi(a).$$

If we put, as before, all group elements conjugate to a in a *class* $\mathfrak{K}_a$, then the character of any one element of a class has the same value as that of any other element of the class.

If h_a is the number of elements of the class $\mathfrak{K}_a$ and k_a is the sum of the elements of this class (in the group ring $\mathfrak{o}$), then the character of k_a is the sum of the characters of the elements of the class; therefore

$$\chi(k_a) = h_a \cdot \chi(a).$$

As we saw in Section 127, the quantities k_a generate the centrum $\mathfrak{Z}$ of the group ring $\mathfrak{o}$. By Section 125 the homomorphisms Θ_ν of $\mathfrak{Z}$ are related to the characters χ_ν by the relations [5]

$$\Theta_\nu(z) = \frac{\chi_\nu(z)}{n_\nu},$$

where $n_\nu = \chi_\nu(1)$ is the degree of the absolutely irreducible representation $\mathfrak{D}_\nu$; in particular

$$\Theta_\nu(k_a) = \frac{\chi_\nu(k_a)}{n_\nu} = \frac{h_a}{n_\nu}\chi_\nu(a). \tag{5}$$

The product $k_a k_b$ is a sum of group elements which again belong to $\mathfrak{Z}$ and therefore can be expressed in terms of the class sums k_a with integer coefficients:

$$k_a \cdot k_b = \sum_c{}' g_{ab}^c k_c. \tag{6}$$

The homomorphism property of the Θ_ν yields the equations

$$\Theta_\nu(k_a) \cdot \Theta_\nu(k_b) = \sum_c{}' g_{ab}^c \Theta_\nu(k_c), \tag{7}$$

which by (5) can be rewritten as

$$h_a h_b \chi_\nu(a)\chi_\nu(b) = n_\nu \sum_c{}' g_{ab}^c h_c \chi_\nu(c) \quad (\textit{second character-relation}). \tag{8}$$

In the sums (6), (7), and (8) c runs through a system of representatives of all classes. If we let c run through all group elements, then in (8) the factor h_c on the right-hand side is omitted. Since the Θ_ν are the only homomorphisms of $\mathfrak{Z}$, the characters χ_ν are the only solutions of the equation (8).

Now (7) together with (6) implies that $\Theta_\nu(k_a)$ for fixed ν is a homomorphism of the centrum $\mathfrak{Z}$. Similarly, (4) together with (3) implies that $\chi_\nu(a)$ for fixed a, i.e., considered as a function of $\mathfrak{D}_\nu$, is a homomorphism of the ring $\mathfrak{H}$ in the field Ω: to the product of two representations corresponds the product of the characters, to the sum corresponds the sum. The two commutative rings $\mathfrak{Z}$, $\mathfrak{H}$ are therefore reciprocal to one another: every basis element k_a of $\mathfrak{Z}$ determines a homomorphism $\chi_\nu(a)$ of $\mathfrak{H}$, and every basis element $\mathfrak{D}_\nu$ of $\mathfrak{H}$ determines a homomorphism $\Theta_\nu(k_a)$ of $\mathfrak{Z}$. Between the Θ_ν and the χ_ν there exists the simple

[5] We assume again that neither the order h of the group nor the degrees n_ν of the representations are divisible by the characteristic of the field.

relation (5). The number of homomorphisms of $\mathfrak{H}$ is equal to the number of classes and therefore equal to the rank of $\mathfrak{H}$. Hence $\mathfrak{H}$ is a system without radical; for if $\mathfrak{H}$ had a radical $\mathfrak{c}$, then the number of possible homomorphisms or representations of first degree of $\mathfrak{H}$ would only be equal to the rank of $\mathfrak{H}/\mathfrak{c}$. At the same time we have shown that the $\chi_\nu(a)$ give rise to the *totality* of homomorphisms of $\mathfrak{H}$ in Ω.

The Conjugate Characters

To every representation $a \to A$ there is a "*conjugate* (or *contragradient*) *representation*" $a \to A'^{-1}$, where A' is the matrix transpose to A. For this correspondence we have

$$ab \to (AB)'^{-1} = (B'A')^{-1} = A'^{-1}B'^{-1}.$$

The conjugate of a conjugate representation is the original representation. If the representation $a \to A$ is reducible, so also is its conjugate, and conversely. Hence the conjugate of an irreducible representation is also irreducible.

If we go from A to an equivalent representation $P^{-1}AP$, the conjugate representation goes into

$$(P^{-1}AP)'^{-1} = P'A'^{-1}P'^{-1},$$

therefore in every case to an equivalent one.

If we designate by $\mathfrak{D}_{\nu'}$ the irreducible representation conjugate to $\mathfrak{D}_\nu$ and $\mathfrak{D}_\nu(a) = A$, then

$$\mathfrak{D}_{\nu'}(a^{-1}) = A',$$

and since the trace of A' is equal to that of A we have

$$\chi_{\nu'}(a^{-1}) = \chi_\nu(a).$$

We denote the *character conjugate to* χ_ν not only by $\chi_{\nu'}$ but also by $\bar{\chi}_\nu$.

Every character is a sum of roots of unity. Thus, every element a of $\mathfrak{G}$ generates a cyclic subgroup $\mathfrak{C}$, whose order m is a divisor of h, and every irreducible representation $\mathfrak{D}_\nu$ of $\mathfrak{G}$ gives rise to a representation of $\mathfrak{C}$; by Section 126 this decomposes completely into representations of first degree whose matrix elements are m-th roots of unity. The trace of the corresponding matrix is the sum of the diagonal elements, and therefore a sum of m-th roots of unity, say

$$\chi(a) = \zeta^{\nu_1} + \zeta^{\nu_2} + \cdots + \zeta^{\nu_n}, \tag{9}$$

where ζ is a primitive m-th root of unity.

The transpose matrix A', when A is written in the diagonal form given above, is equal to A itself, and A'^{-1} is generated by substituting ζ^{-1} for ζ. Hence

$$\bar{\chi}(a) = \zeta^{-\nu_1} + \zeta^{-\nu_2} + \cdots + \zeta^{-\nu_n}.$$

In the case of number fields $\bar{\chi}$ is conjugate complex to χ.

The substitution of ζ^{-1} for ζ is an automorphism of the field of m-th roots of unity, and this automorphism takes χ into $\bar{\chi}$. In an analogous manner an arbitrary field automorphism will take every character χ into an algebraically conjugate character χ^*, which also belongs to an algebraically conjugate representation since every isomorphism of the field of the characters may be extended to an isomorphism of the field of the representation. χ^* is conjugate to χ in the wider field-theoretic sense.

Further Character-Relations

If $S(c)$ is the trace of the group element c in the regular representation, then

$$S(c) = \sum_{\nu} n_\nu \chi_\nu(c),$$

since the regular representation actually contains the irreducible representation $\mathfrak{D}_\nu$ exactly n_ν times. The trace $S(c)$ can also be computed directly. Thus the group elements $a_1, \ldots, a_h$ form a basis of the vector space $\mathfrak{o}$ of the regular representation and

$$c a_i = a_k.$$

Terms with $i = k$ can occur only when c is equal to the unit element 1 of the group; in this case each i is equal to the corresponding k. Hence

$$S(1) = h; \qquad S(c) = 0 \quad \text{for } c \neq 1,$$

consequently

$$\sum_{\nu} n_\nu \chi_\nu(c) = \begin{cases} h & \text{for } c = 1, \\ 0 & \text{for } c \neq 1. \end{cases} \tag{10}$$

If we now sum (8) over all ν and bear in mind (10), we obtain

$$h_a h_b \sum_{\nu} \chi_\nu(a)\chi_\nu(b) = g^1_{ab} \cdot h. \tag{11}$$

The number g^1_{ab}, whenever it occurs, states that a product $a'b'$ is equal to 1, where a' belongs to the class $\mathfrak{K}_a$ and b' to the class $\mathfrak{K}_b$. Hence this number is zero whenever $\mathfrak{K}_a$ and $\mathfrak{K}_b$ contain no two elements which are inverse to one another. However, whenever such a pair occurs, say $b = a^{-1}$, then to each element $a' = cac^{-1}$ of $\mathfrak{K}_a$ there is an element $b' = a'^{-1} = cbc^{-1}$ of $\mathfrak{K}_b$ which is inverse to it. Hence

$$g^1_{ab} = h_a = h_b.$$

Consequently, on dividing by h_b (11) becomes

$$h_a \sum_{\nu} \chi_\nu(a)\chi_\nu(b) = \begin{cases} h & \text{for } \mathfrak{K}_b = \mathfrak{K}_{a^{-1}}, \\ 0 & \text{for } \mathfrak{K}_b \neq \mathfrak{K}_{a^{-1}} \end{cases} \quad (\textit{third character-relation}). \tag{12}$$

For the special case $a = 1$ we get back (10).

Now let $a_1, \ldots, a_s$ be a system of representatives of all classes. If we set

$$\chi_{\nu\mu} = \chi_\nu(a_\mu),$$
$$\eta_{\mu\nu} = \frac{h_\mu}{h}\bar{\chi}_\nu(a_\mu) = \frac{h_\mu}{h}\chi_\nu(a_\mu^{-1}),$$

then the relation (12) says that the matrices $\Xi = (\chi_{\mu\nu})$ and $\Upsilon = (\eta_{\mu\nu})$ are inverse to one another:

$$\Upsilon\Xi = E \quad \text{or} \quad \Upsilon = \Xi^{-1}. \tag{13}$$

From (13) follows

$$\Xi\Upsilon = E$$

or, written out,

$$\frac{1}{h}\sum_{\mathfrak{K}_a} h_a \chi_\nu(a)\bar{\chi}_\mu(a) = \begin{cases} 1 & \text{for } \nu = \mu, \\ 0 & \text{for } \nu \neq \mu. \end{cases} \tag{14}$$

Here a runs through a system of representatives of all classes. If we let a run through all group elements we must omit the factor h_a. From this follows the *orthogonality of the characters*

$$\sum_{a \in \mathfrak{G}} \bar{\chi}_\mu(a)\chi_\nu(a) = \begin{cases} h & \text{for } \nu = \mu, \\ 0 & \text{for } \nu \neq \mu. \end{cases} \quad (\textit{fourth character-relation}). \tag{15}$$

In particular if $\mu = 0$, i.e., if χ_μ is the character χ_0 of the identical representation, (15) implies that

$$\sum_a \chi_\nu(a) = \begin{cases} h & \text{for } \nu = 0, \\ 0 & \text{for } \nu \neq 0. \end{cases} \tag{16}$$

The relation (15) may be used to determine the coefficients $c_{\lambda\mu}^\nu$ in (4) provided we multiply (4) by $\bar{\chi}_\varkappa(a)$ and sum over all a. This gives:

$$\sum_a \bar{\chi}_\varkappa(a)\chi_\lambda(a)\chi_\mu(a) = hc_{\lambda\mu}^\varkappa.$$

If we replace $\varkappa$ by $\varkappa'$, where $\mathfrak{D}_{\varkappa'}$ is the representation conjugate to $\mathfrak{D}_\varkappa$, we obtain:

$$\sum_a \chi_\varkappa(a)\chi_\lambda(a)\chi_\mu(a) = hc_{\lambda\mu}^{\varkappa'}.$$

Hence *the coefficient* $c_{\lambda\mu}^{\varkappa'}$ *is symmetric in the indices* $\lambda, \mu, \varkappa$. *This coefficient occurs whenever the representation conjugate to* $\mathfrak{D}_\varkappa$ *is contained in the product* $\mathfrak{D}_\lambda \times \mathfrak{D}_\mu$.

We can use the fact that the matrices Ξ and Υ are inverse to one another to compute the idempotent centrum elements $e_1, \ldots, e_s$ which generate the two-sided simple ideals in $\mathfrak{o}$. Thus, by Section 124 the basis elements k_a of the centrum $\mathfrak{Z}$ have the form

$$k_a = \sum_\nu e_\nu \Theta_\nu(k_a) = \sum_\nu e_\nu \frac{h_a}{n_\nu} \chi_\nu(a). \tag{17}$$

On multiplying by $\bar{\chi}_\mu(a)$ and summing over all classes $\mathfrak{K}_a$, we obtain

$$\sum_{\mathfrak{K}_a} k_a \bar{\chi}_\mu(a) = e_\mu \cdot \frac{h}{n_\mu}$$

or

$$e_\nu = \sum_{\mathfrak{K}_a} k_a \frac{n_\nu}{h} \chi_\nu(a^{-1}).$$

THEOREM. *The degrees of the irreducible representations of a finite group in the field of all algebraic numbers are divisors of the order of the group.*

PROOF. In (7) let the element b run through a system of representatives of all classes and assume that the $\Theta_\nu(k_a)$ on the left-hand side are known. Thereby we obtain a system of homogeneous linear equations in the $\Theta_\nu(k_c)$. On eliminating these quantities we obtain the relation

$$|\delta_b^c \Theta_\nu(k_a) - g_{ab}^c| = 0$$

(a is held fixed, b and c are the row- and column indices respectively) where

$$\delta_b^c = \begin{cases} 1 & \text{for} \quad b = c, \\ 0 & \text{for} \quad b \neq c. \end{cases}$$

Therefore $\Theta_\nu(k_a)$ is an integral algebraic number since it is the root of an equation with integral rational coefficients and leading coefficient 1. In the same manner it follows from (4) that the characters $\chi_\nu(a)$ are integral algebraic numbers; this fact also follows from (9). But the first half of (14) may be written as follows:

$$\frac{n_\nu}{h} \sum_{\mathfrak{K}_a} \Theta_\nu(k_a) \bar{\chi}_\mu(a) = 1 \quad \text{for} \quad \mu = \nu$$

or

$$\sum_{\mathfrak{K}_a} \Theta_\nu(k_a) \chi_\nu(a^{-1}) = \frac{h}{n_\nu}.$$

Since the left side of this equality is an integral algebraic number, h/n_ν is integral and at the same time rational; therefore, it is integral rational. Q.E.D.

LITERATURE. The representation theory of finite groups is developed independently of the theory of hypercomplex numbers by I. Schur, "Neue Begründung der Theorie der Gruppencharaktere," *Sitzungsber. Berlin 1905, p. 406.* The generalization of this theory to infinite groups is given by J. v. Neumann: "Almost periodic functions in groups." *Trans. Amer. Math. Soc. Vol. 36 (1934).* For further literature see B. L. v. d. Waerden: *Gruppen von linearen Transformationen.* Ergebn. Math. IV 2, Berlin 1935.

EXERCISES. 1. Set up a character table for the symmetric groups of 3 and 4 elements and compute the idempotent elements of the centrum of the group ring.

2. Show that the relation (8) may also be written as

$$h\chi_\kappa(a)\chi_\nu(b) = n_\nu \sum_d \chi_\nu(adbd^{-1}).$$

3. The product representation $\mathfrak{D}_\lambda \times \mathfrak{D}_\mu$ contains the identical representation if and only if, and actually exactly once, the representations $\mathfrak{D}_\lambda$ and $\mathfrak{D}_\mu$ are conjugate to one another.

4. In the field of complex numbers the representation conjugate complex to a representation is equivalent to the conjugate one.

129. THE REPRESENTATIONS OF THE SYMMETRIC GROUPS[6]

We consider the group $\mathfrak{S}_n$ of the permutations of the n numerals $1, 2, \ldots, n$ and seek its absolutely irreducible representations, for instance, in the field Ω of all algebraic numbers. It will also be shown that these representations are rational, i.e., are found in the field Γ of the rational numbers.

We start with the group ring $\mathfrak{o} = s_1\Omega + \cdots + s_{n!}\Omega$ and consider its left ideals. Each such left ideal is a direct sum of minimal left ideals; the latter give rise to the irreducible representations. Since every left ideal is generated by an idempotent element, we will now look for the idempotent elements.

We write the numerals $1, 2, \ldots, n$ in any order and in h rows (h arbitrary) one under another so that the ν-th row contains α_ν numerals and the conditions

$$\begin{cases} \alpha_1 \geqq \alpha_2 \geqq \cdots \geqq \alpha_h, \\ \sum_{\nu=1}^{h} \alpha_\nu = n \end{cases}$$

are satisfied. We write the first elements of the h rows all under one another, similarly for the second, etc., say as in the following scheme where points represent numerals:

$$(\alpha_1, \alpha_2, \alpha_3) = (3, 2, 2), \qquad n = 7$$

Such an ordering of the numerals $1, 2, \ldots, n$ we call a *scheme* Σ_α. The index α designates the numeral sequence $(\alpha_1, \alpha_2, \ldots, \alpha_h)$. The possible indices α are ordered by the following condition: $\alpha > \beta$ when the first non-vanishing difference $\alpha_\nu - \beta_\nu$ is positive. For instance for $n = 5$ we have

$$(5) > (4, 1) > (3, 2) > (3, 1, 1) > (2, 2, 1) > (2, 1, 1, 1) > (1, 1, 1, 1, 1)$$

If a scheme Σ_α is given, we designate by p all those permutations which permute only the numerals within the rows of the scheme, leaving the rows themselves invariant; while by q those permutations which only permute the numerals inside the columns of the scheme. For every fixed q we understand by σ_q the number $+1$ or -1, according as q is an even or an odd permutation. If s is an arbitrary permutation, we designate by $s\Sigma_\alpha$ the scheme into which Σ_α is transformed by the permutation s. It is easy to show that if q leaves invariant the columns of Σ_α, then sqs^{-1} leaves invariant the columns of $s\Sigma_\alpha$, and conversely. Finally we set (in the group ring $\mathfrak{o}$) for each fixed Σ_α

---

[6] For the simplified proofs given in this section of the Frobenian theory (*Sitzungsber. Berlin 1903, p. 328*) I am obliged to an oral communication with J. von Neumann.

$$S_\alpha = \sum_p p,$$

$$A_\alpha = \sum_q q\sigma_q.$$

We easily verify the rules:

(2) $$pS_\alpha = S_\alpha p = S_\alpha.$$

(3) $$A_\alpha q\sigma_q = qA_\alpha\sigma_q = A_\alpha.$$

From (2) and (3) it follows that S_α and A_α are idempotent except for a factor f_α. The additional algebraic properties of the S_α and A_α result from the following *combinatorial lemma.*

Let Σ_α and Σ_β be two schemes as described above and let $\alpha \geqq \beta$. If two numerals, which lie in the same column in Σ_β, are never both contained in a row of Σ_α, then $\alpha = \beta$, and the scheme Σ_α is transformed into the scheme Σ_β by a permutation of the form pq :

$$pq\Sigma_\alpha = \Sigma_\beta.$$

(The designation p and q refers to Σ_α, i.e., p leaves the rows and q the columns of Σ_α invariant.)

PROOF. From $\alpha \geqq \beta$ follows $\alpha_1 \geqq \beta_1$. The first row of Σ_α contains α_1 numerals. If these numerals are all to lie in distinct columns of Σ_β, then Σ_β must have at least α_1 columns, so that $\alpha_1 \leqq \beta_1$; therefore $\alpha_1 = \beta_1$. By a permutation q_1', which leaves invariant the columns of Σ_β, these numerals can all be brought to the first row of Σ_β.

Next, from $\alpha \geqq \beta$ follows $\alpha_2 \geqq \beta_2$. The second row of Σ_α contains α_2 numerals. If these are all to lie in distinct columns of $q_1'\Sigma_\beta$, then $q_1'\Sigma_\beta$, except for the first row which is already filled up, must have at least α_2 columns. This means that $\alpha_2 \leqq \beta_2$; therefore $\alpha_2 = \beta_2$. By a permutation q_2', which leaves invariant the columns of $q_1'\Sigma_\beta$ and also the first row, the numerals under consideration can all be brought to the second row of Σ_β.

Continuing thus, we finally obtain a scheme $q'\Sigma_\beta = q_h' \ldots q_2'q_1'\Sigma_\beta$ whose rows are determined by those of Σ_α. Hence Σ_α can be transformed by a permutation p into $q'\Sigma_\beta$:

$$q'\Sigma_\beta = p\Sigma_\alpha.$$

The permutation $q' = q_h' \ldots q_2'q_1'$ leaves invariant the columns of Σ_β and therefore also those of $q'\Sigma_\beta = p\Sigma_\alpha$. Hence we can find a q such that

$$q' = pq^{-1}p^{-1}$$

and therefore

$$pq^{-1}p^{-1}\Sigma_\beta = p\Sigma_\alpha,$$

$$\Sigma_\beta = pq\Sigma_\alpha. \qquad \text{Q.E.D.}$$

From this combinatorial lemma it follows that

(4) $$A_\beta S_\alpha = 0 \quad \text{for} \quad \alpha > \beta.$$

For by the lemma if $\alpha > \beta$ there must be a pair of numerals which in Σ_α lie in a row and in Σ_β lie in a column. If t is a transposition which permutes this pair of numerals, then by (2) and (3)

$$A_\beta S_\alpha = A_\beta t t^{-1} S_\alpha = -A_\beta S_\alpha,$$

whereupon (4) follows.

Similarly, we prove

$$S_\alpha A_\beta = 0 \quad \text{for} \quad \alpha > \beta.$$

This also means that all transforms of A_β will be annihilated by S_α:

$$S_\alpha s A_\beta s^{-1} = 0 \quad \text{for} \quad \alpha > \beta;$$

since $sA_\beta s^{-1}$ is again an A_β, only to the permuted scheme $s\Sigma_\beta$. From this result it follows on multiplying by $s\Omega$ and summing over all s of $\mathfrak{G}$ that

or
$$S_\alpha(\sum s\Omega)A_\beta = (0)$$

(5) $$S_\alpha \mathfrak{o} A_\beta = (0) \qquad (\alpha > \beta).$$

The left ideals $\mathfrak{o}A_\beta$ with $\beta < \alpha$ are therefore annihilated by S_α, in other words, S_α is represented by zero in the representation adapted to $\mathfrak{o}A_\beta$. On the contrary, $S_\alpha A_\alpha \neq 0$, since the coefficient of the unit element in the product $S_\alpha A_\alpha$ does not vanish. Hence S_α is not represented by zero in the representation adapted to $\mathfrak{o}A_\alpha$; consequently this representation contains at least one irreducible component which occurs in no $\mathfrak{o}A_\beta$ with $\beta < \alpha$. These irreducible components will now be determined in detail.

The element $S_\alpha A_\alpha = \sum_p \sum_q pq\sigma_q$ has by (2) and (3) the property

$$pS_\alpha A_\alpha q\sigma_q = S_\alpha A_\alpha.$$

We prove now that $S_\alpha A_\alpha$ is the single element with this property except for a factor; i.e., we prove: *if an element a of* $\mathfrak{o}$ *has the property*

(6) $$paq\sigma_q = a$$

for all p and q, then a must have the form $(S_\alpha A_\alpha)\cdot\lambda$.

PROOF. We set

(7) $$a = \sum_s s\gamma_s \qquad (\gamma_s \in \Omega).$$

Substituting (7) in (6) we obtain

(8) $$\sum_s s\gamma_s = \sum_s psq\sigma_q\gamma_s.$$

On the left side there occurs only one term with pq, namely $pq\gamma_{pq}$; on the right side there is also only one, namely the term with $s = 1$. On equating the coefficients we obtain:

$$\gamma_{pq} = \sigma_q\gamma_1.$$

We now take an s which does not have the form pq. Then $s\Sigma_\alpha$ is distinct from all $pq\Sigma_\alpha$, and by the combinatorial lemma there are two numerals j, k which in Σ_α lie in a row and in $s\Sigma_\alpha$ lie in a column. If t is the transposition of these numerals: $t = (jk)$, then $t' = s^{-1}ts$ permutes only the numerals $s^{-1}j$ and $s^{-1}k$ which lie in a column of $s^{-1}s\Sigma_\alpha = \Sigma_\alpha$. Hence t is a permutation p and t' a permutation q, and in (8) we can set $p = t$ and $q = t'$; therefore for our special s we have

$$psq = tss^{-1}ts = s,$$
$$\sigma_q = -1,$$

consequently, on equating the terms with s on the left and right in (8):

$$\gamma_s = -\gamma_s, \qquad \gamma_s = 0.$$

This implies that in (7) there occur only the terms with $s = pq, \gamma_s = \sigma_q\gamma_1$, and it becomes

$$a = \sum_{p,q} pq\sigma_q\gamma_1 = (S_\alpha A_\alpha)\gamma_1, \qquad \text{Q.E.D.}$$

From the above proof it follows immediately that for every element b of $\mathfrak{o}$ the element $S_\alpha bA_\alpha$ has the form $(S_\alpha A_\alpha)\lambda$; thus, for every p and every q we have

$$pS_\alpha bA_\alpha q\sigma_q = S_\alpha bA_\alpha.$$

Hence

$$S_\alpha \mathfrak{o} A_\alpha \subseteq (S_\alpha A_\alpha)\Omega.$$

If we set $S_\alpha A_\alpha = I_\alpha$, then

(9) $$I_\alpha \mathfrak{o} I_\alpha \subseteq S_\alpha \mathfrak{o} A_\alpha \subseteq I_\alpha\Omega.$$

We now state that $\mathfrak{o}I_\alpha$ is a minimal left ideal. For, if $\mathfrak{l}$ is a subideal of $\mathfrak{o}I_\alpha$, then by (9) we have

$$I_\alpha \mathfrak{l} \subseteq I_\alpha\Omega,$$

therefore, since $I_\alpha\Omega$ is a Ω-module of rank one, and so minimal, either

$$I_\alpha\mathfrak{I} = I_\lambda\Omega \quad \text{or} \quad I_\lambda\mathfrak{I} = (0).$$

In the first case $\mathfrak{o}I_\alpha = \mathfrak{o}I_\alpha\Omega \subseteq \mathfrak{o}I_\alpha\mathfrak{I} \subseteq \mathfrak{I}$; consequently $\mathfrak{I} = \mathfrak{o}I_\alpha$. In the second case $\mathfrak{I}^2 \subseteq \mathfrak{o}I_\alpha\mathfrak{I} = (0)$; consequently, since there is no nilpotent ideal except (0), $\mathfrak{I} = (0)$.

The minimal left ideals $\mathfrak{o}I_\alpha$ and $\mathfrak{o}I_\beta$ are for $\alpha > \beta$ not operator isomorphic. Thus, by (5) if $\varkappa > \beta$ we have

$$S_\varkappa\mathfrak{o}I_\beta = S_\varkappa\mathfrak{o}S_\beta A_\beta \subseteq S_\alpha\mathfrak{o}A_\beta = (0),$$

therefore for every a' from $\mathfrak{o}I_\beta$:

$$S_\varkappa a' = 0.$$

Now if it were true that $\mathfrak{o}I_\varkappa \cong \mathfrak{o}I_\beta$, then for every a of $\mathfrak{o}I_\alpha$ we would have

$$S_\varkappa a = 0.$$

However this can not happen for $a = I_\varkappa = S_\varkappa A_\varkappa$, since $S_\alpha^i A_\alpha = f_\alpha S_\alpha A_\alpha \neq 0$.

Every left ideal $\mathfrak{o}I_\alpha$ admits an irreducible representation $\mathfrak{D}_\alpha$, and by the above remarks these representations are inequivalent for distinct α.

The number of these representations $\mathfrak{D}_\alpha$ is equal to the number of the solutions of (1).[7] This number however is at the same time the number of classes of conjugate permutations; for, each of these classes consists of all elements which decompose in cycles of fixed lengths $\alpha_1, \alpha_2, \ldots, \alpha_h$, and these lengths can again be ordered according to the conditions (1). However, since the number of *all* inequivalent irreducible representations is given by the number of classes of conjugate permutations, this shows that *the representations* $\mathfrak{D}_\alpha$ *exhaust except for equivalence all irreducible representations of the symmetric group* $\mathfrak{S}_n$.

The minimal left ideals $\mathfrak{o}I_\alpha$ have been rationally determined in the preceding. Hence we have shown the *rationality of the irreducible representations* (as well as of the characters).

For the explicit computation of the characters and degrees of the representations we refer to the works of Frobenius,[8] Weyl,[9] and Schur.[10]

130. SEMIGROUPS OF LINEAR TRANSFORMATIONS AND THEIR BEHAVIOR IN THE EXTENSION OF THE GROUND FIELD

We start with a ground field P and consider systems of linear transformations (or matrices) whose matrix elements belong either to P or to a commutative extension field Λ of P. Such a system is called a *semigroup* when it contains the product of every pair of matrices that belong to the system. The *linear closure* of a system of matrices with respect to P consists of all linear combinations of matrices

[7] To every solution of (1) there actually belong distinct schemes which can differ only in the ordering of the numerals and can give rise to distinct p_α; it is sufficient however to choose for every α a single $p_\varkappa$.

[8] Frobenius: *Sitzungsber. Berlin 1900, p. 516.*

[9] Weyl, H.: *Math. Z. 23 (1925), p. 271.*

[10] Schur, I.: *Sitzungsber. Berlin 1927, p. 58.*

of the system with coefficients in P. In the following we will consider only systems which contain only a finite number of linearly independent matrices with respect to P: the linear closure has finite rank over P. This is always the case when Λ is a finite extension field of P. Under these assumptions the linear closure of a semigroup is a *hypercomplex system* over P.

In the following we will be concerned only with those properties of semigroups of linear transformations which remain valid in the transition to the linear closure. Such properties are: irreducibility, complete reducibility, decomposition into equivalent or inequivalent components (always with respect to Λ). By the transition to the linear closure $\mathfrak{S}$ all properties of this kind can be interpreted as properties of the hypercomplex system $\mathfrak{S}$, in fact as properties of a faithful representation $\mathfrak{D}$ of $\mathfrak{S}$. We will be primarily concerned with the question: *how does an irreducible representation $\mathfrak{D}$ decompose in the extension of the field Λ, especially in the extension of P to Λ?*

We will always assume that the representation $\mathfrak{D}$ does not contain the null representation as a component.

The following two theorems are fundamental for the theory:

1. *If the representation $\mathfrak{D}$ is completely reducible, then the system $\mathfrak{S}$ is semi-simple.*

2. *If the representation $\mathfrak{D}$ is irreducible or decomposable into equivalent irreducible components, then $\mathfrak{S}$ is simple.*

PROOF OF 1. If $\mathfrak{c}$ is the radical of $\mathfrak{S}$, the elements of $\mathfrak{c}$ by Section 123, Theorem 2. are represented by zero in every irreducible representation. Since $\mathfrak{D}$ is a faithful representation, then $\mathfrak{c} = 0$.

PROOF OF 2. In each case the system $\mathfrak{S}$ is semi-simple and therefore a direct sum of complete matrix rings: $\mathfrak{S} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s$. By section 121 in an irreducible representation all $\mathfrak{a}_\mu$ are represented by zero except for one $\mathfrak{a}$. This fact is also valid when the representation is repeated. Hence if the representation is faithful, there can be only one $\mathfrak{a}_1$; i.e., $\mathfrak{S}$ is a complete matrix ring and so a simple system.

From Theorems 1. and 2. immediately follows a Theorem of Burnside and its generalization due to Frobenius and Schur which played a fundamental role in the older developments of the theory of representations.

THEOREM OF BURNSIDE. *In an absolutely irreducible semigroup of matrices of n-th degree there are exactly n^2 linearly independent matrices.*

GENERALIZATION. *If a semigroup of matrices in the field Λ decomposes into absolutely irreducible components among which occur s inequivalent ones of degrees $n_1, \ldots, n_s$, then the semigroup contains exactly*

$$n_1^2 + n_2^2 + \cdots + n_s^2$$

linearly independent matrices (with respect to Λ, or in the case for which the matrix elements all lie in P, with respect to P).

PROOF OF THE GENERALIZATION. The linear closure of the given semigroup, formed with respect to Λ, is the sum of s complete matrix rings of degrees $n_1, n_2, \ldots, n_s$ over Λ and therefore has the rank $n_1^2 + n_2^2 + \cdots + n_s^2$.

In fields of characteristic zero we also have the *trace theorem*:

If two semigroups can be set into a one-to-one correspondence such that products go into products (or, still more general, when each of these can be interpreted as a representation of a single abstract semigroup) and if the traces of the corresponding matrices are equal, then the two semigroups (or the two representations) are equivalent.

PROOF. On writing one after the other the corresponding matrices A and B of the two semigroups:

$$(1) \qquad \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

we obtain a completely reducible semigroup $\mathfrak{g}$ whose linear closure is a hypercomplex system $\mathfrak{S}$. The elements of $\mathfrak{S}$ are linear combinations of the matrices (1) and therefore decompose in the same manner into two conponents each of which produces by itself a representation of $\mathfrak{S}$. The traces of these two representations are determinable linear combinations of the traces of the original matrices A and B and so must coincide for the two representations. Hence (Section 125) the two representations of $\mathfrak{S}$ are equivalent. From this follows the proposition.

If $\Lambda = P$, then by Section 123 Theorems 1. and 2. can be stated conversely without further ado. However. if Λ is a proper extension of P, we must proceed with caution.

1a. *If $\mathfrak{S}$ is semi-simple and Λ is separable over P, then every representation $\mathfrak{D}$ of $\mathfrak{S}$ in Λ is completely reducible.*

2a. *If $\mathfrak{S}$ is simple and normal over P, then every representation of $\mathfrak{S}$ in Λ decomposes into only equivalent irreducible components.*

PROOF. By Section 122 every representation of $\mathfrak{S}$ in Λ can be obtained through a representation of $\mathfrak{S} \times \Lambda$. If $\mathfrak{S}$ is semi-simple and Λ is separable over P, then by Section 121 $\mathfrak{S} \times \Lambda$ is also semi-simple and therefore every representation of $\mathfrak{S} \times \Lambda$ in Λ is completely reducible. If $\mathfrak{S}$ is normal and simple over P, then $\mathfrak{S} \times \Lambda$ is at the same time simple; furthermore by Section 121 every representation of $\mathfrak{S} \times \Lambda$ in Λ decomposes into equivalent irreducible components. Thereby both statements are proved.

We call a semigroup *normal* over P when the linear closure is normal, and therefore the centrum of the linear closure is equal to the ground field P. For an absolutely irreducible semigroup, where all elements of the centrum have the form λI (λ in Λ), the assumption of normality means that all these λ lie in P.

When we take into consideration 1. and 2. we can formulate 1a. and 2a. as follows:

1b. *A completely reducible semigroup of linear transformations in* P *remains completely reducible for every separable extension of the ground field* P.

2b. *A normal irreducible semigroup of linear transformations in* P *remains irreducible or decomposes into only equivalent irreducible components for every extension of the ground field.*

Just as in 1b. we can also prove:

1c. *A completely reducible semigroup remains completely reducible for every extension of the ground field, provided that the centrum of the linear closure is a direct sum of separable fields over* P. In this case we also say that the semigroup is *absolutely completely reducible.*

In the following we will be concerned only with *normal irreducible* semigroups, in other words, with representations of normal simple hypercomplex systems. We start with the (single) irreducible representation $\mathfrak{D}_{\mathsf{P}}$ of $\mathfrak{S}$ in the ground field P. By Section 121 there is at least one splitting field Ω, i.e., a field such that $\mathfrak{S}_{\Omega}$ is a complete matrix ring over Ω. The irreducible representation $\mathfrak{D}_{\Omega}$ of $\mathfrak{S}$ in Ω can be obtained through the representation of $\mathfrak{S}_{\Omega}$ as a complete matrix ring over Ω. $\mathfrak{D}_{\Omega}$ is by Section 123 absolutely irreducible. $\mathfrak{D}_{\mathsf{P}}$ becomes completely reducible in Ω, and the irreducible components can only be equivalent to $\mathfrak{D}_{\Omega}$. If the representation $\mathfrak{D}_{\Omega}$ occurs say m-times in the decomposition of $\mathfrak{D}_{\mathsf{P}}$, then the number m is said to be the *index* of $\mathfrak{D}_{\Omega}$ with respect to P, or the index of the system $\mathfrak{S}$ over P.

The hypercomplex significance of the index becomes clear by the following consideration. Let the system $\mathfrak{S}$ be a complete matrix ring over a field Δ. In Section 123 we have seen that the number of irreducible components in which the irreducible representation $\mathfrak{D}_{\mathsf{P}}$ of $\mathfrak{S}$ decomposes in the transition of P to Ω is equal to the number of irreducible left ideals in which the system Δ_{Ω} decomposes. In Section 121 we called this number the *degree* of the skew field Δ. Hence

The index m of the absolutely irreducible representation $\mathfrak{D}_{\Omega}$ *of* $\mathfrak{S}$ *with respect to* P *is equal to the degree of the skew field over* P *belonging to* $\mathfrak{S}$.

If $\mathfrak{S}$ is a complete matrix ring of degree q over Δ, then $\mathfrak{S}_{\Omega}$ is a complete matrix ring of degree q over Δ_{Ω}, and therefore a complete matrix ring of degree mq over Ω. The degree n of the absolutely irreducible representation $\mathfrak{D}_{\Omega}$ is therefore

$$n = qd.$$

Consequently we have: *the index of the representation* $\mathfrak{D}_{\Omega}$ *with respect to* P *is a divisor of the degree n of this representation.*

Every representation of $\mathfrak{S}$ in P decomposes into only irreducible components which are equivalent to $\mathfrak{D}_{\mathsf{P}}$; these in turn decompose in Ω into the m representations equivalent to $\mathfrak{D}_{\Omega}$. *Therefore the number of absolutely irreducible components* $\mathfrak{D}_{\Omega}$, *which are contained in a representation rational in* P, *is divisible by the index of* $\mathfrak{D}_{\Omega}$.

Such a rational representation, where Ω is a finite extension field of P, may be obtained as follows: replace in the representation $\mathfrak{D}_\Omega$ each of the elements of Ω (the matrix elements of the representation) by the matrix which corresponds to it in the regular representation of Ω. Then from the representation $\mathfrak{D}_\Omega$ of degree n we obtain a representation in P of degree gn, where g is the field degree $(\Omega:\mathsf{P})$. The number of absolutely irreducible components $\mathfrak{D}_\Omega$ of degree n in which this representation decomposes in Ω is therefore equal to g. According to the theorem last formulated, g is divisible by m. Hence *the rank* $(\Omega:\mathsf{P})$ *of every splitting field* Ω *of finite rank is always divisible by the index* m, *in other words, by the degree of the decomposed skew field.*

We will later on give another proof of this theorem. It will be based on a more profound characterization of the splitting field.

131. APPLICATIONS OF THE REPRESENTATION THEORY TO THE THEORY OF THE SKEW FIELD

We have already noticed in Section 122 that every representation of a hypercomplex system $\mathfrak{S}$ in a commutative field K, which includes the ground field P, may be obtained from a representation of the extended system $\mathfrak{S}_\mathsf{K}$. In the language of the representation modules this says that every module which has $\mathfrak{S}$ as left- and K as right multiplicative domain may also be interpreted as a $\mathfrak{S}_\mathsf{K}$-left module. The proof rests on the fact that if we set $\mathfrak{S} = a_1\mathsf{P} + \cdots + a_n\mathsf{P}$, so that $\mathfrak{S}_\mathsf{K} = a_1\mathsf{K} + \cdots + a_n\mathsf{K}$, the left multiplication of the element m of the module by an element of $\mathfrak{S}_\mathsf{K}$ is defined by

$$(a_1\varkappa_1 + \cdots + a_n\varkappa_n)m = a_1m\varkappa_1 + \cdots + a_nm\varkappa_n.$$

The verification of the rules for the $\mathfrak{S}_\mathsf{K}$-module presents no difficulties; only in the proof of the associative law

$$(bc)m = b(cm)$$

is the commutativity essentially used; if say $b = a_1\varkappa_1$, $c = a_2\varkappa_2$ (it is obviously sufficient to consider this special case), then the associative law follows from the relations

$$(a_1\varkappa_1 \cdot a_2\varkappa_2)m = (a_1a_2\varkappa_1\varkappa_2)m = (a_1a_2)m(\varkappa_1\varkappa_2),$$

$$a_1\varkappa_1(a_2\varkappa_2 \cdot m) = a_1\varkappa_1(a_2m\varkappa_2) = a_1(a_2m\varkappa_2)\varkappa_1 = (a_1a_2)m(\varkappa_2\varkappa_1).$$

These two expressions are actually equal to one another since $\varkappa_1\varkappa_2 = \varkappa_2\varkappa_1$.

This situation can be carried over to the case in which K is not commutative by the introduction of the concept of *inverse ring* (or, *skew field*) by Section 120. We designate, as a rule, the inverse ring to $\mathfrak{R}$ by $\mathfrak{R}'$, and note at the outset that when $\mathfrak{R}$ is hypercomplex over the commutative field P, $\mathfrak{R}'$ may also be interpreted as a hypercomplex system over P.

Every module which has $\mathfrak{S}$ *as left- and* K *as right multiplicative domain, where* $\mathfrak{S}$ *and* K *are* [11] *hypercomplex systems over the same ground field* P, *may be interpreted as a* $(\mathfrak{S} \times \mathsf{K}')$*-left module* [12] [*or as a* $(\mathfrak{S}' \times \mathsf{K})$*-right module*].

PROOF as above. Let $\mathfrak{S} = a_1\mathsf{P} + \cdots + a_n\mathsf{P}$ and therefore $\mathfrak{S} \times \mathsf{K}' = a_1\mathsf{K}' + \cdots + a_n\mathsf{K}'$; then we define

$$(1) \qquad (a_1\varkappa'_1 + \cdots + a_n\varkappa'_n)m = a_1 m\varkappa_1 + \cdots + a_n m\varkappa_n.$$

All rules can now be easily verified. The associative law $(bc)m = b(cm)$ follows from

$$(a_1\varkappa'_1 \cdot a_2\varkappa'_2)m = (a_1a_2\varkappa'_1\varkappa'_2)m = (a_1a_2)m(\varkappa_2\varkappa_1),$$
$$a_1\varkappa'_1(a_2\varkappa'_2 \cdot m) = a_1\varkappa'_1(a_2 m\varkappa_2) = a_1(a_2 m\varkappa_2)\varkappa_1 = (a_1a_2)m(\varkappa_2\varkappa_1).$$

In the same manner we may interpret conversely a $(\mathfrak{S} \times \mathsf{K}')$-left module also as a $\mathfrak{S}$-left and $\bar{\mathsf{K}}$-right module by means of the definition $m\varkappa = \varkappa' m$. This is obviously a consequence only of the fact that the module isomorphisms which are generated on multiplying the module elements by the elements of K' may be written on the right instead of the left, provided that the order of the multiplication is reversed: to multiply m on the right by $\varkappa_1\varkappa_2$ means to multiply on the right first by $\varkappa_1$ and then by $\varkappa_2$, while to multiply m on the left by $\varkappa'_1\varkappa'_2$ means to multiply on the left first by $\varkappa'_2$ and then by $\varkappa'_1$. Isomorphic $(\mathfrak{S} \times \mathsf{K}')$-modules generate isomorphic $\mathfrak{S}$-left and K-right modules, and conversely.

These facts have many applications, especially when K and $\mathfrak{S}$ are both simple hypercomplex systems [13] or skew fields of finite rank over P. We assume that one of the two systems, $\mathfrak{S}$ or K, is normal over P, i.e., that P is the centrum of $\mathfrak{S}$ or K. For this case we have proved in Section 121 that the product $\mathfrak{S} \times \mathsf{K}'$ is also a simple system. Hence by Section 123 all irreducible $(\mathfrak{S} \times \mathsf{K}')$-left modules are isomorphic to one another and to the minimal left ideals of $\mathfrak{S} \times \mathsf{K}'$. Therefore all irreducible ($\mathfrak{S}$ left-, K right) double modules are also isomorphic to one another.

If K is a skew field, these double modules are representation modules in the sense of Section 110, and the isomorphism of all representation modules indicates the *equivalence of all irreducible representations of* $\mathfrak{S}$ *in* K. Hence since $\mathfrak{S}$ is simple, we are concerned only with faithful representations, that is, with isomorphisms $\mathfrak{S} \cong \Sigma$, where Σ is a system of matrices of r-th degree over K, and therefore a subring of the complete matrix ring K_r. By the proof, two such repre-

[11] K may also be an arbitrary extension ring of P which contains P in its centrum.

[12] This means that the operators of $\mathfrak{S} \times \mathsf{K}'$ are to be written on the left of the module elements.

[13] By a "simple system" we will always understand in the following a simple hypercomplex system with identity.

sentations $\mathfrak{S} \cong \Sigma_1$ and $\mathfrak{S} \cong \Sigma_2$ are equivalent, i.e., there exists a non-singular matrix Q in K_r such that, when σ_1 and σ_2 are representations in Σ_1 and Σ_2 of the same element of $\mathfrak{S}$, the relation

$$\sigma_1 = Q\sigma_2 Q^{-1} \tag{2}$$

is valid. From this follows the FIRST FUNDAMENTAL THEOREM OF THE THEORY OF SKEW FIELDS.

If Σ_1 and Σ_2 are two simple subsystems of the normal simple hypercomplex system K_r which are isomorphic to one another, then every isomorphism between Σ_1 and Σ_2 which leaves the elements of the ground field P invariant can be obtained from an inner automorphism of K_r according to (2).

Two such isomorphic systems Σ_1 and Σ_2 may always be interpreted as representations of a single system $\mathfrak{S}$. If these representations are reducible, the number of irreducible representations into which they can be decomposed is equal to their degrees (this means r in both cases). Since the irreducible representations are equivalent, the decomposable ones are also.

As a special case we have that *every automorphism of K_r, which leaves invariant the elements of P, is an inner one.*

Hitherto we have been concerned with isomorphisms between two double modules; now we investigate the endomorphisms of a representation module. The two representations $\mathfrak{S} \cong \Sigma_1$ and $\mathfrak{S} \cong \Sigma_2$ now fall together into a representation $\mathfrak{S} \cong \Sigma$. The endomorphisms of the representation module are, according to a remark in Section 119 (small type), linear transformations of the module into itself which are permutable with all transformations of the representation. Hence if Q is the matrix of such a linear transformation, then

$$\sigma Q = Q\sigma, \tag{3}$$

i.e., Q is permutable with all elements of Σ. Since the representation module may be represented as a $(\mathfrak{S} \times \mathsf{K}')$-left module in a unique manner, then endomorphisms of the representation module correspond biuniquely to the endomorphisms of the $(\mathfrak{S} \times \mathsf{K}')$-left module such that the sum of two endomorphisms corresponds to the sum. the product corresponds to the product, and the ϱ-multiple corresponds to the ϱ-multiple (ϱ in P). In case the representation is irreducible, the $(\mathfrak{S} \times \mathsf{K}')$-left module is also irreducible and isomorphic to a minimal left ideal $\mathfrak{l}$ of $\mathfrak{S} \times \mathsf{K}'$. By Section 120 the endomorphism ring Δ' of such a left ideal is inverse-isomorphic to the skew field Δ, in which the ring $\mathfrak{S} \times \mathsf{K}'$ may be represented as a complete matrix ring Δ_t. However, if the representation module is reducible, then it decomposes into s representation modules isomorphic to one another, and the endomorphism ring is by Section 119 isomorphic to a complete matrix ring Δ'_s over Δ'. We have thereby proved the *Second Fundamental Theorem.*

If $\mathfrak{S} \times \mathsf{K}'$ is isomorphic to the complete matrix ring Δ_t of degree t and if Σ

is a subring of K_r, *isomorphic to* $\mathfrak{S}$, *then the elements of* K_r *permutable with all elements of* Σ *form a subring* T *in* K_r, *which is isomorphic to a complete matrix ring* Δ'_s, *where* Δ' *is inverse-isomorphic to* Δ *and* s *is the number of irreducible components into which the* r*-rowed matrices of the system* Σ *decompose.*

In general the rank of a module $\mathfrak{M}$ with respect to a field K is designated by $(\mathfrak{M}:\mathsf{K})$. Let the single irreducible representation of $\mathfrak{S}$ in K be of degree g; then g is the rank of the representation module over K, in other words, equal to the rank of an irreducible $(\mathfrak{S}\times\mathsf{K}')$-left module over K'. As such we can choose a minimal left ideal $\mathfrak{l}$ of $\mathfrak{S}\times\mathsf{K}'$. The following rank relations are valid:

$$(4)\qquad (\Sigma:\mathsf{P}) = (\mathfrak{S}:\mathsf{P}) = (\mathfrak{S}\times\mathsf{K}':\mathsf{K}') = t\cdot(\mathfrak{l}:\mathsf{K}') = tg,$$

$$(5)\qquad g(\mathsf{K}':\mathsf{P}) = (\mathfrak{l}:\mathsf{K}')(\mathsf{K}':\mathsf{P}) = (\mathfrak{l}:\mathsf{P}) = (\mathfrak{l}:\Delta)(\Delta:\mathsf{P}) = t(\Delta:\mathsf{P}).$$

If we multiply (4) by $(\Delta:\mathsf{P})$ and (5) by g, and equate, we obtain

$$(6)\qquad (\Sigma:\mathsf{P})(\Delta:\mathsf{P}) = g^2(\mathsf{K}:\mathsf{P}).$$

By assumption the reducible representation $\mathfrak{S}\to\Sigma$ of degree r contains the irreducible representation of degree g s-times; therefore

$$r = sg.$$

Hence if we multiply (6) by s^2, we obtain

$$(\Sigma:\mathsf{P})\,s^2(\Delta:\mathsf{P}) = r^2(\mathsf{K}:\mathsf{P})$$

or, since $s^2(\Delta:\mathsf{P})$ is the rank of the matrix ring Δ_s isomorphic to T and similarly $r^2(\mathsf{K}:\mathsf{P})$ is the rank of K_r:

$$(7)\qquad (\Sigma:\mathsf{P})(\mathsf{T}:\mathsf{P}) = (\mathsf{K}_r:\mathsf{P}).$$

The second fundamental theorem may be formulated more simply if we start with Σ instead of $\mathfrak{S}$ and instead of $\mathfrak{S}\times\mathsf{K}'$ consider the isomorphic system $\Sigma\times\mathsf{K}'$. Then:

SECOND FUNDAMENTAL THEOREM OF THE THEORY OF SKEW FIELDS. *Let* K *be a skew field of finite rank over* P, *and* Σ *a simple system which is contained in the complete matrix ring* K_r *and decomposes into* s *irreducible components. Let the product system* $\Sigma\times\mathsf{K}'$ *be simple and therefore isomorphic to a complete matrix ring* Δ_t. *Then the elements of* K_r *permutable with all elements of* Σ *form a simple ring* T, *isomorphic to a complete matrix ring* Δ'_s, *where* Δ' *is inverse-isomorphic to* Δ. *In the special case* $s=1$ T *is itself inverse-isomorphic to* Δ.

With the help of the rank relation (7) we may now prove the following COMMUTATIVITY THEOREM:

Let Σ *be a simple subring including* P *of the complete matrix ring* K_r, *whose centrum is* P. *Let* T *be the totality of the elements of* K_r, *which are permutable with all elements of* Σ. *Then conversely* Σ *is the totality of the elements of* K_r *which are permutable with all elements of* T.

PROOF. The totality Σ^* of the elements permutable with all elements of T includes Σ and by (7)

$$(\Sigma : \mathsf{P})\,(\mathsf{T} : \mathsf{P}) = (\mathsf{T} : \mathsf{P})\,(\Sigma^* : \mathsf{P}) = (\mathsf{K}_r : \mathsf{P});$$

therefore

$$(\Sigma : \mathsf{P}) = (\Sigma^* : \mathsf{P})$$
$$\Sigma^* = \Sigma$$

as stated.

Now let $r = 1$, and let Σ be a maximal commutative subfield of K. The totality of the elements of K, which are permutable with all elements of Σ, is Σ itself. Thus, if ϑ is permutable with all elements of Σ, then $\Sigma(\vartheta)$ is commutative and without zero divisors; therefore it is a field and, since Σ is to be maximal, ϑ must be contained in Σ. Consequently $\mathsf{T} = \Sigma$, and from (7) we have

$$(\Sigma : \mathsf{P})^2 = (\mathsf{K} : \mathsf{P}).$$

Hence we have proved anew that the rank of K over P is a square number m^2. The number m was called in Section 121 the *degree* of the skew field K. Hence

The degree $(\Sigma : \mathsf{P})$ *of a maximal commutative subfield of* K *is equal to the degree of the normal skew field* K.

From the fundamental theorem it follows further that $\Sigma \times \mathsf{K}'$ is a complete matrix ring over Δ', where Δ' is isomorphic to $\mathsf{T} = \Sigma$. However, the field Δ' includes Σ, since Σ lies in the centrum of $\Sigma \times \mathsf{K}'$. Hence $\Delta' = \Sigma$, i.e., K'_Σ is a complete matrix ring over Σ. Therefore:

The maximal commutative subfields of K *are at the same time splitting fields of* K.

Further applications of the Second Fundamental Theorem will be given in the next section.

We will now consider some applications of these theorems to questions regarding special skew fields.

1. *Determination of all non-commutative skew fields of finite degree over the field of real numbers as ground field.*

If P is the field of real numbers, K the skew field of index m which is to be determined, Z the centrum of K, and Σ a maximal commutative subfield, then

$$\mathsf{P} \subseteq \mathsf{Z} \subseteq \Sigma \subset \mathsf{K}; \qquad (\Sigma : \mathsf{Z}) = m; \qquad (\mathsf{K} : \mathsf{Z}) = m^2.$$

Since K is non-commutative, then $m > 1$. For the fields Z and Σ we can only have P and $\mathsf{P}(i)$, the field of complex numbers, since P has no other commutative finite extensions. Since $m > 1$ we have $\Sigma \neq \mathsf{Z}$; therefore

$$\Sigma = \mathsf{P}(i), \qquad \mathsf{Z} = \mathsf{P}, \qquad m = 2.$$

Hence the field K to be determined can only have the degree $m^2 = 4$.

The isomorphism of $\mathsf{P}(i)$ which takes i into $-i$ must be obtained, according to the First Fundamental Theorem of the theory of skew fields, by a transformation

with an element k of K, i.e., there must be a k with the property

$$kik^{-1} = -i. \tag{8}$$

Since k is not contained in $\Sigma = \mathsf{P}(i)$, then $\Sigma(k) = \mathsf{K}$; therefore $\mathsf{K} = \mathsf{P}(i, k)$. From (8) follows that

$$k^2ik^{-2} = i;$$

i.e., k^2 is permutable with i. Since k^2 is also permutable with k, then k^2 lies in the centrum: $k^2 = a \in \mathsf{P}$.

If we had $a \geqq 0$, then we would have $a = b^2$,

$$k^2 - b^2 = (k - b)(k + b) = 0,$$

$$k - b = 0 \quad \text{or} \quad k + b = 0,$$

therefore $k \in \mathsf{P}$, which is not true. Hence we must have $a < 0$: $a = -b^2$ $(b \neq 0)$. On multiplying k by the real factor b^{-1} we obtain $k^2 = -1$ without losing the previous properties of k. Hence for i and k the relations

$$ki = -ik,$$

$$i^2 = k^2 = -1$$

are valid. But this characterizes the quaternion field. *Consequently the quaternion field is the only possible non-commutative skew field of finite degree over the field of real numbers as ground field.*

2. *Determination of all finite skew fields* (skew fields with a finite number of elements).

If K is a finite skew field, Z its centrum, m^2 the rank of K over Z, then every element of K is contained in a maximal commutative subfield Σ of degree m over Z. Now all commutative extensions Σ of m-th degree of a Galois field Z of p^n elements are equivalent to one another (they are generated by the adjunction of all roots of the equation $x^q = x$, $q = p^{nm}$; cf. Section 37). Hence these fields all arise from one of them, Σ_0, by transformations with elements $\varkappa$ of K:

$$\Sigma = \varkappa\Sigma_0\varkappa^{-1}.$$

If we omit the null element of K, then K becomes a group $\mathfrak{G}$, Σ_0 a subgroup $\mathfrak{H}$, Σ a conjugate subgroup $\varkappa\mathfrak{H}\varkappa^{-1}$, and these conjugate subgroups together fill up the entire group $\mathfrak{G}$ (since every element of K is contained in an Σ). However, in the theory of groups we have the following

LEMMA. *A proper subgroup $\mathfrak{H}$ of a finite group $\mathfrak{G}$ along with its conjugates $s\mathfrak{H}s^{-1}$ can not possibly fill up the entire group $\mathfrak{G}$.*

PROOF. Let n and N be the orders of $\mathfrak{H}$ and $\mathfrak{G}$, and j the index of $\mathfrak{H}$ so that $N = j \cdot n$. If s and s' belong to the same coset $s\mathfrak{H}$, say that $s' = sh (h \in \mathrm{A})$, then

$$s'\mathfrak{H}s'^{-1} = sh\mathfrak{H}h^{-1}s^{-1} = s\mathfrak{H}s^{-1}.$$

Hence the number of distinct $s\mathfrak{H}s^{-1}$ is at most equal to the number of cosets, i.e., at most j. If these $s\mathfrak{H}s^{-1}$ ($\mathfrak{H}$ also belongs to these) together were to fill up the group $\mathfrak{G}$, then they would have no elements in common; for otherwise we would not have the required $N = j \cdot n$ elements. However, since every pair of distinct $s\mathfrak{H}s^{-1}$ have the unit element in common, they always have common elements, and we have a contradiction.

For our case it follows from the lemma that $\mathfrak{H}$ can not possibly be a *proper* subgroup of $\mathfrak{G}$. Hence $\mathfrak{H} = \mathfrak{G}$ and $\mathsf{K} = \Sigma_0$. Consequently K is commutative. Hence we have proved

Every skew field with a finite number of elements is commutative, and therefore a Galois field.

For an other elementary proof of this theorem due to MacLagan-Wedderburn see E. Witt: *Abh. Math. Sem. Hamburg Vol. 8 (1931) p. 413*

EXERCISES. 1. If under the assumptions of the Commutativity Theorem Σ is normal over P, then $\mathsf{K}_r = \Sigma \times \mathsf{T}$ (MacLagan-Wedderburn). [The product $\Sigma\mathsf{T}$ is in each case a representation of the direct product $\Sigma \times \mathsf{T}$. If the latter is simple, then the representation is faithful. We now equate the rank of this product to that of K.]

2. Determine all fields of index 2 over the rational number field Γ as centrum ("generalized quaternion field").

132. THE BRAUER CLASSES OF ALGEBRAS. CHARACTERIZATION OF THE SPLITTING FIELD

In this section and the following we will be concerned exclusively with *normal* skew fields K and *normal* simple algebras K_r over the fixed ground field P.

In the Second Fundamental Theorem of the previous section if we set $\Sigma = \mathsf{K}$, $r = 1$, then T becomes the centrum of K so that $\mathsf{T} = \mathsf{P}$. Hence $\Sigma \times \mathsf{K}'$ is a complete matrix ring over P. Consequently

If K is a skew field of finite rank over its centrum P, and K' is the inverse skew field, then $\mathsf{K} \times \mathsf{K}'$ is a complete matrix ring over P.

As an example we have that the direct product of the quaternion field with itself is the complete matrix ring P_4.

Let us now partition the simple normal hypercomplex systems over P into classes by assigning to the class (K) all systems K_r which are isomorphic to complete matrix rings over the skew field K.

If K and Δ are skew fields, then $\mathsf{K} \times \Delta$ is again normal and simple (Section 121); therefore

$$\mathsf{K} \times \Delta = \Delta_t. \tag{1}$$

From (1) follows

$$\mathsf{K}_r \times \Delta_s = \mathsf{K} \times \mathsf{P}_r \times \Delta \times \mathsf{P}_s = \Delta_t \times \mathsf{P}_{rs} = \Delta \times \mathsf{P}_t \times \mathsf{P}_{rs} = \Delta \times \mathsf{P}_{trs} = \Delta_{trs},$$

therefore all products $\mathsf{K}_r \times \Delta_s$ of systems of the classes (K) and (Δ) belong to a class (Δ). This is called the *product* of the classes (K) and (Δ). Furthermore, since

$$\mathsf{K} \times \Delta \cong \Delta \times \mathsf{K},$$

$$\mathsf{K} \times (\Delta \times \Gamma) = (\mathsf{K} \times \Delta) \times \Gamma,$$

the product of classes is a commutative and associative operation. There is also a unit class: the class (P) of the ground field. Finally by the theorem just proved, every class (K) has an inverse class, namely, the class (K') where K' is the system inverse-isomorphic to K. Hence *the classes of normal simple hypercomplex systems over* P *form an Abelian group.* This is called the *Brauer group of classes of algebras.*

A subgroup of the Brauer group is always formed by those classes of algebras which possess a given commutative field Σ over P as a splitting field. By Section 121 a splitting field of K is at the same time a splitting field of the entire class (K); it is also a splitting field of the inverse class (K'), since K' is inverse-isomorphic to K and therefore $\mathsf{K}' \times \Sigma$ is inverse-isomorphic to $\mathsf{K} \times \Sigma$. Furthermore, if K and Δ both have Σ as a splitting field, namely,

$$\mathsf{K} \times \Sigma \cong \Sigma_s, \quad \Delta \times \Sigma \cong \Sigma_t,$$

then

$$(\mathsf{K} \times \Delta) \times \Sigma \cong \mathsf{K} \times \Sigma_t \cong \mathsf{K} \times \Sigma \times \mathsf{P}_t \cong \Sigma_s \times \mathsf{P}_t \cong \Sigma \times \mathsf{P}_s \times \mathsf{P}_t \cong \Sigma_{st}.$$

In this case Σ is also a splitting field of the product $\mathsf{K} \times \Delta$ and so of the entire product class $(\mathsf{K} \times \Delta)$.

We will now investigate further the problem of determining which finite extension fields $\mathfrak{S}$ of P can be splitting fields of a given skew field K (or, in other words, of its inverse skew field K'). Our investigation will be based on the Second Fundamental Theorem of Section 131. This theorem implies that the structure of $\mathfrak{S} \times \mathsf{K}'$ is determined by that of the ring T of the matrices in K_r permutable with all elements of Σ, where Σ is a representation of $\mathfrak{S}$ by matrices in K_r. Among these representations there is a single irreducible one; we start our investigation with this representation. In the fundamental theorem, set $s = 1$; thereby the ring T becomes a skew field. Since Σ is commutative, it is permutable with itself, $\mathsf{T} \supseteq \Sigma$, and Σ must be contained in the centrum of T.

Our problem is to investigate the condition $\mathsf{T} = \Sigma$. In this case by the Second Fundamental Theorem $\mathfrak{S} \times \mathsf{K}'$ is isomorphic to a complete matrix ring over $\mathsf{T}' \cong \mathsf{T} = \Sigma \cong \mathfrak{S}$; therefore $\mathfrak{S}$ is a splitting field of K'.

If $\mathsf{T} = \Sigma$, then the elements of K_r which are permutable elementwise with Σ must all belong to Σ; therefore Σ is a maximal commutative subfield as well as a maximal commutative subring of K_r. On the contrary if $\mathsf{T} \supset \Sigma$, then T contains elements τ which do not belong to Σ, but are still permutable with Σ. When such an element τ is adjoined to Σ, it generates a commutative field $\Sigma(\tau)$ which is a proper extension field of Σ. The property $\mathsf{T} = \Sigma$ is accordingly equivalent to the property that Σ is a maximal commutative subfield of K_r.

Consequently we have found the following characterization of the splitting field:

Splitting fields of the normal skew field K *over* P *are those commutative fields* $\mathfrak{S}$ *over* P, *whose irreducible representation by matrices over* K *generates a maximal commutative subfield* (*and at the same time a maximal commutative subring*) *of the matrix ring* K_r.

For every r there are maximal commutative subfields in K_r; however these need not be always irreducible. If Σ is such a maximal commutative subfield and the matrices of Σ decompose into s equivalent irreducible components of degree g, then each of these irreducible components defines a representation Σ_1 of degree g of Σ. Since Σ is a field, Σ_1 is a field isomorphic to Σ. Furthermore, Σ_1 is a maximal commutative subfield of K_g; for if we could extend Σ_1 to a larger subfield, then we could do the same with all equivalent irreducible components, and we would then have an extension of Σ inside K_r. Hence Σ_1 is a splitting field and, since $\Sigma \cong \Sigma_1$, Σ is also a splitting field. Consequently without considering the irreducibility we have the theorem:

Every maximal commutative subfield of a complete matrix ring K_r *is a splitting field of* K, *and conversely, every splitting field can be represented as such a maximal subfield* (*actually irreducible*).

For an irreducible representation it follows from equation (6), Section 131, that the degree of a splitting field (since $\Sigma = \mathsf{T}$) satisfies

$$(\Sigma : \mathsf{P})^2 = r^2(\mathsf{K} : \mathsf{P}). \tag{2}$$

If we set by Section 121 $(\mathsf{K}:\mathsf{P}) = m^2$, where m is the so-called *degree* of K, then from (2) follows

$$\begin{cases} (\Sigma : \mathsf{P})^2 = r^2 m^2, \\ (\Sigma : \mathsf{P}) = rm. \end{cases} \tag{3}$$

These relations could be obtained directly from equation (4), Section 131: the number t, given there, i.e., the degree of the matrix ring $\mathfrak{S} \times \mathsf{K}'$, is equal to our m, and g, i.e., the degree of the irreducible representation of $\mathfrak{S}$ in K, is equal to r. Moreover from (3) follows:

The rank of a splitting field of K *is a multiple of the degree* m *of* K. *The maximal commutative subfields of* K, *and only these, are splitting fields of smallest possible ranks* m.

Finally we prove the theorem:

Every normal skew field K *has at least one separable splitting field.*

For the proof we need the *lemma:* In a field of characteristic p every p^f-rowed matrix A, which satisfies an equation of the form

$$A^{p^e} = \zeta I \quad (\mathrm{I} = \text{unit matrix}), \tag{4}$$

has a characteristic polynomial (cf. Section 112) of the form

$$\chi(x) = x^{p^f} - \beta$$

and therefore in case $p^f > 1$, the trace zero.

Proof of lemma. We can adjoin the p^e-th roots of ζ to the ground field, and therefore take $\zeta = \eta^{p^e}$. If we interpret the matrix A as the matrix of a linear transformation of a vector space, then for every vector v we have

$$0 = (A^{p^e} - \zeta)\, v = (A^{p^e} - \eta^{p^e})\, v = (A - \eta)^{p^e} v.$$

In this case the elementary divisors $f_\nu(x)$ of the matrix A are, according to their definition (Section 111), divisors of $(x - \eta)^{p^e}$, and therefore powers of $(x - \eta)$. The characteristic polynomial $\chi(x)$ is the product of the elementary divisors; therefore in each case it is a power of $(x - \eta)$. Since $\chi(x)$ is a polynomial of degree p^f, then

$$\chi(x) = (x - \eta)^{p^f} = x^{p^f} - \eta^{p^f} = x^{p^f} - \beta.$$

Proof of the existence of a separable splitting field.

Let Z be a maximal separable subfield of K and Δ the set of the elements of K permutable with all elements of Z. The set of the elements of K permutable with all elements of Δ is again Z; i.e., Δ is normal over Z. (This also follows directly from the Second Fundamental Theorem of Section 131, since if $\mathfrak{S} \times \mathsf{K}' = \Delta'_i$ is normal so also is Δ'.)

Now if ϑ is an element of Δ which does not belong to Z, then $\mathsf{Z}(\vartheta)$ is inseparable; furthermore, its reduced degree is one, since otherwise $\mathsf{Z}(\vartheta)$ would contain a separable subfield $\supset \mathsf{Z}$. Hence ϑ satisfies an irreducible equation of the form

$$\vartheta^{p^e} = \zeta, \quad \zeta \text{ in } \mathsf{Z}. \tag{5}$$

This is also true (with $p^e = 1$) when ϑ itself lies in Z.

If Σ is a maximal commutative subfield of Δ, then Σ has in every case the reduced degree one, and therefore a field degree (= rank) p^f. Σ is a splitting field of Δ, i.e., $\Delta \times \Sigma$ is a complete matrix ring over Σ, and actually of degree p^f. In this matrix representation all elements of Δ have, by the lemma, the trace zero whenever $p^f > 1$; for if A is the matrix representing ϑ, the matrix equation (4) follows from (5). All matrices of $\Delta \times \Sigma$ are linear combinations of the matrices of Δ with coefficients from Σ, the ground field of the matrix ring. Hence all these matrices have for $p^f > 1$ the trace zero. However this contradicts the fact

that we are dealing with a *complete* matrix ring. Consequently $p' = 1$, $Z = \Sigma$ remains as the only possibility. In this case Z is itself a maximal commutative subfield of K, and therefore a splitting field.

133. CROSS PRODUCTS. FACTOR SETS

Let K again be a skew field of finite rank over the centrum P. We will describe explicitly the structure of K or, if this can not be done directly, that of a suitable complete matrix ring K_r. Towards this end we take a separable splitting field and extend it to a separable normal splitting field Σ. This can be irreducibly represented by Section 132 as a maximal commutative subfield of a suitable complete matrix ring K_r belonging to K. Hence we assume that $\Sigma \subset K_r$; by Section 132 this implies that every element of K_r permutable with all elements of Σ belongs to Σ.

The Galois group of Σ (Section 50) consists of the automorphisms $S, T, \ldots$ of Σ which leave fixed all elements of the ground field P. The product of the automorphisms S and T (first S, then T) is designated at this time by ST; therefore, if β^S is the field element arising from applying the automorphism S on the field element β, then $\beta^{ST} = (\beta^S)^T$. The order of the Galois group is by Section 50 equal to the field degree $n = (\Sigma : P)$.

By the First Fundamental Theorem of the theory of skew fields the automorphisms S are generated by inner automorphisms of K_r. Hence to every S there is an invertible element u_S in K_r such that for all β of Σ we have

$$u_S^{-1} \beta u_S = \beta^S,$$

or

$$\beta u_S = u_S \beta^S. \tag{1}$$

The element $u_S^{-1} u_S u_T$ is permutable by (1) with all elements of Σ, and therefore it is itself an element of Σ. Hence on setting

$$u_{ST}^{-1} u_S u_T = a_{S,T},$$

we obtain the multiplication rule

$$u_S u_T = u_{ST} a_{S,T}. \tag{2}$$

Since $a_{S,T}$ has an inverse $u_T^{-1} u_S^{-1} u_{ST}$, then $a_{S,T} \neq 0$.

From the relations (1) it follows that the n elements u_S are linearly independent with respect to Σ. Thus, if a u_S were linearly dependent on certain other linearly independent u_T, we would then have

$$u_S = \sum_T u_T \gamma_T. \tag{3}$$

If we multiply this relation first on the left by β and use the permutability

rule (1), second on the right by β^S, we obtain

$$u_S\beta^S = \sum_T u_T\beta^T\gamma_T = \sum_T u_T\gamma_T\beta^S,$$

therefore on equating the coefficients,

$$\beta^T\gamma_T = \gamma_T\beta^S. \tag{4}$$

At least one γ_T must be $\neq 0$, since otherwise by (3) $u_S = 0$. Hence in (4) we can cancel the factor γ_T:

$$\beta^T = \beta^S.$$

As this must be valid for all β, then $T = S$. This is a contradiction; therefore the u_S are linearly independent.

By Section 131 we have

$$(\mathsf{K}_r : \mathsf{P}) = (\Sigma : \mathsf{P})^2 = n^2, \text{ therefore } (\mathsf{K}_r : \Sigma) = n.$$

Hence the n linearly independent u_S form a Σ-basis for K_r.

To sum up we have:

There are n invertible elements u_S in K_r corresponding to the elements of the Galois group which form a Σ-basis for K_r and for which the rules

$$\beta u_S = u_S\beta^S, \tag{1}$$

$$u_S u_T = u_{ST}a_{S,T} \tag{2}$$

are valid.

By these rules the structure of the algebra K_r is completely determined, as soon as the n^2 constants $a_{S,T}$ distinct from zero in the field Σ are known. They form the *Noether factor set* of the algebra K_r for the splitting field Σ.

By the associative law

$$u_S(u_T u_R) = (u_S u_T)u_R,$$

the constants $a_{S,T}$ must satisfy the *associative relations*

$$a_{S,TR}a_{T,R} = a_{ST,R}a_{S,T}^R. \tag{5}$$

Conversely, if n^2 arbitrary constants $a_{S,T}$ distinct from zero are given in Σ, which satisfy the conditions (5), we can form a module of linear forms

$$u_{S_1}\Sigma + u_{S_2}\Sigma + \cdots + u_{S_n}\Sigma$$

and by the rules (1), (2) make this module into an algebra over P. We prove without difficulty that all rules for algebras are satisfied. The algebra thus defined was called by E. Noether the *cross product* of the field Σ with its Galois group pertaining to the factor set $a_{S,T}$.

The cross product is a *simple* algebra. Thus if $\mathfrak{b}$ were a two-sided ideal distinct from the null ideal, then any suitable linear combination $\Sigma u_S\gamma_S$ must be congruent to zero modulo $\mathfrak{b}$, in other words: the u_S would be linearly dependent modulo

$\mathfrak{b}$. We may prove however, just as we would prove the linear independence of the u_S by means of (1), that the u_S modulo $\mathfrak{b}$ are also linearly independent provided that $\mathfrak{b}$ is not the unit ideal. Consequently the algebra is simple.

There is also a unit element, namely $e = u_1 a_{11}^{-1}$. Hence our algebra is a complete matrix ring K_r over a skew field K.

When an element $c = \Sigma u_S \gamma_S$ is permutable with all elements β of Σ,

Then
$$\beta c = c\beta,$$
$$\Sigma u_S \beta^S \gamma_S = \Sigma u_S \gamma_S \beta,$$
$$(\beta^S - \beta)\gamma_S = 0.$$

therefore $\gamma_S = 0$ except for $S = 1$. Consequently $c = u_1\gamma_1 = ea_{11}\gamma_1$ belongs to Σ. It follows that Σ is a maximal commutative subfield of K_r.

Furthermore, K_r is normal over P. For, if c should belong to the centrum of K_r, c must first belong to Σ by the above proofs, secondly must also be permutable with all u_S, and therefore admits all automorphisms of the Galois group of Σ. This implies by Section 50 that c belongs to the ground field P.

To sum up we have:

The n^2 elements $a_{S,T}$ distinct from zero from the normal field Σ, which satisfy the relation (5), form the factor set of a normal simple algebra K_r, defined by the relations (1), (2), with the maximal commutative subfield Σ.

In a given simple normal algebra K_r with the maximal commutative subfield Σ the u_S are not determined uniquely. If v_S is an element which as u_S generates the automorphism S of Σ by the transformation:
$$v_S^{-1}\beta v_S = \beta^S,$$
then $u_S^{-1} v_S$ is permutable with all elements of Σ, and therefore equals an element c_S of Σ:
$$v_S = u_S c_S.$$
It follows that
$$v_S v_T = u_S u_T c_S^T c_T = u_{ST} a_{S,T} c_S^T c_T = v_{ST} a_{S,T} c_{ST}^{-1} c_S^T c_T.$$

Consequently the factor set $b_{S,T}$ belonging to the v_S is given by

$$b_{S,T} = \frac{c_S^T c_T}{c_{ST}} a_{S,T} \tag{6}$$

The factor set $b_{S,T}$ is to be considered as not essentially distinct from the original $a_{S,T}$ and defines the same algebra K_r. We say that it is *associated* to $a_{S,T}$.

Up to now we have always started from a normal splitting field. We can however also define a factor set of a simple algebra K_r, as done by R. Brauer, with respect to a non-normal splitting field.

Let Δ be a finite separable splitting field which need not be normal. Let $\vartheta = \vartheta_1$ be a primitive element of Δ, so that $\Delta = \mathsf{P}(\vartheta)$; let ϑ_α $(\alpha = 1, 2, \ldots, n)$ be the elements conjugate to ϑ in a suitable normal extension field Σ.

There is except for equivalence only one absolutely irreducible representation of K_r by matrices in Δ. Let $a \to A$ be this representation, and let $a \to A_\alpha$ be the representations which are generated from the first by transforming the matrix elements of the representation according to the field isomorphisms $\vartheta \to \vartheta_\alpha$. Since these representations are all equivalent to one another (there is also in Σ only one irreducible representation except for equivalence), then there are matrices $P_{\alpha\beta}$, which transform the representation A_α into A_β :

$$A_\alpha = P_{\alpha\beta} A_\beta P_{\alpha\beta}^{-1}.$$

The matrix $P_{\alpha\beta}$ can be assumed to be in the field $\mathsf{P}(\vartheta_\alpha, \vartheta_\beta)$, since the two representations are already equivalent in this field. We can also choose the $P_{\alpha\beta}$ so that every isomorphism of $\mathsf{P}(\vartheta_\alpha, \vartheta_\beta)$, which takes $\vartheta_\alpha, \vartheta_\beta$ into a conjugate pair $\vartheta_\gamma, \vartheta_\delta$, also takes $P_{\alpha\beta}$ into $P_{\gamma\delta}$. We need for this purpose only to choose a pair α, β from every class of conjugate pairs in order to determine a $P_{\alpha\beta}$ and to derive the remaining $P_{\gamma\delta}$ by the respective isomorphism on $P_{\alpha\beta}$.

We now have

$$A_\alpha = P_{\alpha\beta} A_\beta P_{\alpha\beta}^{-1} = P_{\alpha\beta} P_{\beta\gamma} A_\gamma P_{\beta\gamma}^{-1} P_{\alpha\beta}^{-1} = P_{\alpha\beta} P_{\beta\gamma} P_{\alpha\gamma}^{-1} A_\alpha P_{\alpha\gamma} P_{\beta\gamma}^{-1} P_{\alpha\beta}^{-1}.$$

Hence the matrix $P_{\alpha\beta} P_{\beta\gamma} P_{\alpha\gamma}^{-1}$ is permutable with all matrices A_α of an absolutely irreducible representation; therefore it is a multiple of the unit matrix:

$$\text{(7)} \qquad \begin{cases} P_{\alpha\beta} P_{\beta\gamma} P_{\alpha\gamma}^{-1} = c_{\alpha\beta\gamma} I \\ P_{\alpha\beta} P_{\beta\gamma} = c_{\alpha\beta\gamma} P_{\alpha\gamma}. \end{cases}$$

The *Brauer factor set* $c_{\alpha\beta\gamma}$ is defined by (7). It has the following properties:

a) $c_{\alpha\beta\gamma}$ belongs to the field $\mathsf{P}(\vartheta_\alpha, \vartheta_\beta, \vartheta_\gamma)$;

b) $c_{\alpha\beta\gamma} c_{\alpha\gamma\delta} = c_{\alpha\beta\delta} c_{\beta\gamma\delta}$;

c) $c_{\alpha\beta\gamma}^S = c_{\alpha'\beta'\gamma'}$, when S is an isomorphism of the field $\mathsf{P}(\vartheta_\alpha, \vartheta_\beta, \vartheta_\gamma)$ which takes the $\vartheta_\alpha, \vartheta_\beta, \vartheta_\gamma$ into $\vartheta_{\alpha'}, \vartheta_{\beta'}, \vartheta_{\gamma'}$.

The property a) follows immediately from the definition of the $c_{\alpha\beta\gamma}$, the property b) from the associative law for the matrices $P_{\alpha\beta}$, and the property c) from the behavior of the $P_{\alpha\beta}$ for the isomorphism S.

If we replace $P_{\alpha\beta}$ by $k_{\alpha\beta} P_{\alpha\beta}$, whereby the field elements $k_{\alpha\beta}$ distinct from zero have to satisfy the same conjugate conditions as the $P_{\alpha\beta}$, then the system of the $c_{\alpha\beta\gamma}$ goes over into an *associated factor set*

$$\text{(8)} \qquad c'_{\alpha\beta\gamma} = \frac{k_{\alpha\beta} k_{\beta\gamma}}{k_{\alpha\gamma}} c_{\alpha\beta\gamma}.$$

On the other hand if we replace the representation $a \to A$ by an equivalent representation $a \to QAQ^{-1}$, then the P_α are replaced by $Q_\alpha P_\alpha Q_\alpha^{-1}$; by a computation

we can readily show that the factor set $c_{\alpha\beta\gamma}$ has not been changed. Hence the factor set except for associatedness is uniquely determined by K_r and Δ alone.

The entire theory could be constructed either only from the Noether or only from the Brauer factor sets. However, the proofs become clearer and simpler if we use both types of factor sets side by side and prove their equivalence. Thus some properties can be proved more easily for the Noether while others more easily for the Brauer factor sets. We begin with the fundamental properties of the Brauer factor sets.

If K_r is a complete matrix ring over the ground field P, therefore $\mathsf{K}_r = \mathsf{P}_r$, we can choose all $P_{\alpha\beta} = I$. All $c_{\alpha\beta\gamma}$ then become equal to one, and it follows: *the factor set of an algebra which splits in the ground field is associated to the unit system* $c_{\alpha\beta\gamma} = 1$.

We now seek the factor set of a direct product $\mathsf{K}_r \times \Lambda_S$. If $a \to A$ is the irreducible representation of K_r in the field Δ and $b \to B$ that of Λ_S in the same field, then we obtain a representation of the product system $\mathsf{K}_r \times \Lambda_S$, on representing ab by the Kronecker product $A \times B$ (cf. Section 128). This representation is absolutely irreducible; for the proof we need only to compute its degree. Thus, if the absolutely irreducible representation of K_r had the degree n and that of Λ_s the degree m, then K_r has (for instance, by Burnside's Theorem) the rank n^2 and Λ_s the rank m^2; therefore $\mathsf{K}_r \times \Lambda_s$ has the rank n^2m^2, while the degree of the product representation comes to mn and therefore coincides with the degree of the absolutely irreducible representation of $\mathsf{K}_r \times \Lambda_s$.

We can now compute the factor set of the product representation. From $A_\alpha = P_{\alpha\beta}^{-1} A_\beta P_{\alpha\beta}$ and $B_\alpha = Q_{\alpha\beta}^{-1} B_\beta Q_{\alpha\beta}$ follows

$$A_\alpha \times B_\beta = (P_{\alpha\beta} \times Q_{\alpha\beta})^{-1} (A_\beta \times B_\beta)(P_{\alpha\beta} \times Q_{\alpha\beta}),$$

therefore $P_{\alpha\beta} \times Q_{\alpha\beta}$ are the transformation matrices of the product representation. Similarly it follows from

$$P_{\alpha\beta} P_{\beta\gamma} = c_{\alpha\beta\gamma} P_{\alpha\gamma} \text{ and } Q_{\alpha\beta} Q_{\beta\gamma} = d_{\alpha\beta\gamma} Q_{\alpha\gamma}$$
$$(P_{\alpha\beta} \times Q_{\alpha\beta})(P_{\beta\gamma} \times Q_{\beta\gamma}) = c_{\alpha\beta\gamma} d_{\alpha\beta\gamma} (P_{\alpha\gamma} \times Q_{\alpha\gamma}).$$

Hence $c_{\alpha\beta\gamma} d_{\alpha\beta\gamma}$ *is a factor set of the product algebra* $\mathsf{K}_r \times \Lambda_s$.

On applying this result to the case $\mathsf{K} \times \mathsf{P}_r = \mathsf{K}_r$, which means that the $d_{\alpha\beta\gamma}$ are all equal to one, it follows that *the matrix ring* K_r *has the same factor set as the skew field* K. Consequently every Brauer class of algebras corresponds to a single factor set except for the associated sets.

To sum up we have: *To every element of the Brauer group of classes of algebras with the splitting field* Δ *there corresponds a uniquely determined factor set* $c_{\alpha\beta\gamma}$ *except for associated sets such that to the unit element corresponds the unit set and to the product of two group elements the product of the factor sets.*

We will now investigate the behavior of the Brauer factor set of an algebra in an extension of the splitting field. Hence let $\Delta' = \mathsf{P}(\vartheta')$ be a finite extension field of ${}_{\prime}\Delta = \mathsf{P}(\vartheta)$. Every isomorphism $\vartheta' \to \vartheta'_{\alpha'}$ of the field Δ' also induces an isomorphism $\vartheta \to \vartheta_\alpha$ of the field Δ; therefore every subscript α' corresponds to a subscript α. The proposed representation $a \to A$ of K_r in Δ can be left unchanged by the transition to Δ'. In this case the conjugate representations A_α also remain unchanged, i.e., $A'_{\alpha'} = A_\alpha$, where the subscript α' corresponds to the subscript α. For the transformation matrix $P_{\alpha\beta}$ a corresponding rule is valid: $P'_{\alpha'\beta'} = P_{\alpha\beta}$, where the subscripts α', β' correspond to the subscripts α, β. Finally, for the factor set the same simple rule is valid: $c'_{\alpha'\beta'\gamma'} = c_{\alpha\beta\gamma}$, *when the subscripts* α', β', γ' *correspond to the subscripts* α, β, γ, *therefore when the isomorphisms* $\vartheta' \to \vartheta'_{\alpha'}, \vartheta' \to \vartheta'_{\beta'}, \vartheta' \to \vartheta'_{\gamma'}$ *of the field* Δ' *induces the isomorphisms* $\vartheta \to \vartheta_\alpha, \vartheta \to \vartheta_\beta, \vartheta \to \vartheta_\gamma$ *of the field* Δ.

By these rules we can always go over from an arbitrary separable splitting field Δ to a comprehending normal field Σ. The isomorphisms $\vartheta \to \vartheta_\alpha$ of Σ are then the elements $S, T, \ldots$ of the Galois group: $\vartheta_\alpha = \vartheta^S, \vartheta_\beta = \vartheta^T$, etc. Consequently we can use in this case the elements S, T, R as indices instead of α, β, γ which were used up to now; thereby we may write $c_{S,T,R}$ instead of $c_{\alpha,\beta,\gamma}$. The rule c) states in this new notation

$$c^{Q}_{S,T,R} = c_{SQ,TQ,RQ}. \tag{9}$$

Moreover we can derive the connection to the Noether factor set. We will compute the Brauer factor set for the cross product K_r defined at the beginning of this section and show that it is identical to the Noetherian one except for designation.

An irreducible representation of K_r in Σ is obtained when we interpret K_r itself as a representation module. The basis elements of K_r, as Σ-right module, are exactly the u_S. The matrix representing an element $a = u_S\beta$ (it suffices to limit ourselves to these elements since all others are sums of such elements) is obtained by multiplying this element by all basis elements u_T and developing the product according to the u_T:

$$(u_S\beta)\, u_T = u_S u_T \beta^T = u_{ST}\, a_{S,T}\beta^T.$$

Hence the representation matrix A has the element $a_{S,T}\beta^T$ in the column T and row ST and zero in all other columns. Consequently the conjugate matrix A^R has in the column T and row ST the element

$$(a_{S,T}\beta^T)^R = a^R_{S,T}\beta^{TR}.$$

We seek now to determine the matrix $P_{1,R}$ which transforms A into A^R:

$$A P_{1,R} = P_{1,R} A^R. \tag{10}$$

We choose for $P_{1,R}$ the matrix which has in the column Y and row YR the element $a_{Y,R}$ and zero in every other column. The relation (10) is then satisfied; for in the column T and row STR we find on the left-hand side the element $a_{S,TR}\beta^{TR}a_{T,R}$, while on the right-hand side the element $a_{ST,R}a^{R}_{S,T}\beta^{TR}$, which by (5) are the same. Thereby $P_{1,R}$ is found. The remaining $P_{S,T}$ are obtained (according to the restriction made in the definition of the $P_{\alpha\beta}$) by applying the automorphisms S to $P_{1,R}$:

$$P^{S}_{1,R} = P_{S,RS}.$$

The relation $P_{S,T}P_{T,R} = c_{S,T,R}P_{S,R}$ has to be constructed only for the case $S = 1$ since we can always transform the index 1 into S by applying the isomorphism S; cf. (9). Accordingly we have only to consider

$$P_{1,R}P_{R,TR} = c_{1,R,TR}P_{1,TR}$$

or

$$P_{1,R}P^{R}_{1,T} = c_{1,R,TR}P_{1,TR}.$$

The left side has in the column S and STR the element

$$a_{ST,R}a^{R}_{S,T} = a_{S,TR}a_{T,R},$$

while the right side, the element $c_{1,R,TR}a_{S,TR}$. Therefore we have to set

$$c_{1,R,TR} = a_{T,R}. \tag{11}$$

In view of formula (11) the Noether factor set $a_{S,T}$ is known as soon as the Brauer factor set is known. But the structure of the algebra K_r is determined by the Noether factor set. Hence

A Brauer class of algebras is uniquely determined by the splitting field Δ and the factor set $c_{\alpha\beta\gamma}$.

In the earlier considerations devoted to the factor set of the product algebras we found an homomorphism of the group of the Brauer class of algebras with a given splitting field Δ to the group of its classes of associated factor sets. This homomorphism now becomes an *isomorphism* by the uniqueness proved above.

We may easily show that the relations (5) are consequences of the properties a), b), c) assumed for the $c_{\alpha\beta\gamma}$. *Hence to every set of field elements $c_{\alpha\beta\gamma}$ satisfying the properties a), b), c) there belongs a class of algebras, represented by a cross product with the factor set $a_{S,T}$ defined by* (11).

In view of (11) the fundamental properties of the Brauer factor sets are valid in the Noether factor sets. In particular it is also true that an isomorphism of the group of the classes of algebras with fixed (normal) splitting field gives rise to the group of the classes of its associated (Noether) factor sets. We stress especially:

The cross product K_r is a complete matrix ring over the ground field P if and only if its factor set $a_{S,T}$ is associated to the unit set:

$$a_{S,T} = \frac{c_S^T c_T}{c_{ST}} .$$

EXERCISES. 1. For an extension of the ground field P to an extension field Λ the skew field K goes over into the simple algebra K_Λ. To prove that the Brauer factor set is "shortened" (verkurzt) in the following manner: embed the fields Δ and Λ in a common extension field and seek out among the elements ϑ_α conjugate to ϑ those which are still conjugate to ϑ_1 with respect to the new ground field Λ. The $c_{\alpha\beta\gamma}$ belonging to three of the ϑ_α are retained, all others omitted. In the language of the Noether factor sets this states that only those $a_{S,T}$ are retained for which S and T belong to a fixed subgroup (which?) of the Galois group.

2. With the help of Exercise 1 answer the question: what subfields of Σ are splitting fields of an algebra with the factor set $a_{S,T}$?

For given fields P and Σ (or Δ) in order to set up all decomposable classes of algebras of Σ (or Δ respectively), we have to set up, by the previous remarks, all possible factor sets $a_{S,T}$ (or $c_{\alpha\beta\gamma}$) and to divide them into classes associated to one another. In general the problem is a very difficult one. It is considerably simplified when Σ is a cyclic field. In this case all elements T of the Galois group are powers of a single element S, and we may also choose the pertaining u_T as powers of a single u_S (with exponents $0, 1, \ldots, n-1$). If we set $u_S^n = a$, then a is permutable with all elements of Σ; therefore it is itself an element of the field Σ, and we have

$$u_S^i u_S^j = u_S^{i+j}, \quad \text{if} \quad i + j < n,$$
$$u_S^i u_S^j = a\, u_S^{i+j-n}, \quad \text{if} \quad i + j \geqq n.$$

Consequently the entire factor set, and thereby also the algebra K_r, is determined by the choice of a single element a.

However a can not be chosen arbitrarily. Thus $u_S^n = a$ is permutable with u_S; therefore $a^S = a$ must be valid. By Section 50 this implies, since a admits all automorphisms of the Galois group, that a belongs to P However if this is the case, then the associative law

$$(u_S^i u_S^j)\, u_S^k = u_S^i (u_S^j u_S^k)$$

is always satisfied. Consequently a has no further condition to satisfy than to belong to P and to be distinct from zero.

The cross product defined by a, Σ, and S is called a *cyclic algebra* and is designated according to Hasse by (a, Σ, S).

Instead of u_S we write from now on simply u. If we replace u by $v = uc$, then u^2 is replaced by $(uc)^2 = u^2 c^S c$, similarly u^3 by $(uc)^3 = u^3 c^{S^2} c^S c$, etc., finally $u^n = a$ by

$$u^n c^{S^{n-1}} c^{S^{n-2}} \dots c^S c = a \cdot N(c),$$

where the norm is to be formed in Σ. Now since the replacement of u by uc is the only freedom which we have after the choice of Σ and S, it follows that

Two cyclic algebras (a, Σ, S) *and* (b, Σ, S) *are isomorphic if and only if* a *differs from* b *by a single factor which is a norm. In particular* (a, Σ, S) *is a complete matrix ring over* P *if and only if* a *is the norm of an element of* Σ.

EXERCISES. 3. Determine anew all skew fields of finite rank over the field of real numbers.

4. Let Σ be a Galois field and P a subfield of Σ. Show that every element of P is the norm of an element of Σ and derive from this a new proof of the Wedderburn Theorem regarding the finite skew fields (Section 131).

INDEX

(The numbers refer to the pages on which the expressions appear for the first time.)