

Theory of algebraic functions of one variable.

(By Messrs. *R. Dedekind* in Braunschweig and *H. Weber* in Königsberg.)

Introduction.

The investigations communicated below have the aim of founding the theory of the algebraic functions of one variable, which is one of the principal results of *Riemann's* creation, from a simple and at the same time rigorous and completely general point of view. In the investigations on this subject so far, certain restrictive assumptions are as a rule made about the singularities of the functions under consideration, and the so-called exceptional cases are either mentioned in passing as limiting cases or else set aside altogether. Likewise certain principles about continuity and expandability are admitted, whose evidence rests on geometric intuition of various kinds. A secure basis for the fundamental notions, as well as for a general treatment of the theory without exceptions, can be gained if one starts from a generalization of the theory of the rational functions of one variable, in particular of the theorem that every integral rational function of one variable can be decomposed into linear factors. This generalization is simple and well known in the first case, in which the number denoted by *Riemann* by p (the genus according to *Clebsch*) has the value zero. For the general case, which is related to the one just mentioned as the case of the most general algebraic numbers is to that of the rational numbers, the methods applied with the best success in the theory of numbers, which attach to *Kummer's* creation of the ideal numbers, and which are capable of

transfer to the theory of functions, pointed out the right way*).

If, in analogy with the theory of numbers, one understands by a *field of algebraic functions* a system of such functions of such a nature that the application of the four species to functions of the system always leads to functions of the same system, then this notion coincides completely with that of *Riemann's* class of algebraic functions. Among the functions of such a field any one may be regarded as the independent variable and the rest as dependent on it. For each of these “modes of representation” there results a system of functions of the field, to be designated as *integral functions*, whose quotients exhaust the whole field. Among these integral functions one can now again single out groups of functions which possess the characteristic marks of those integral rational functions that have a common divisor. Such a divisor does not, it is true, exist in the general case; but if one attaches the relevant theorems about rational functions not to the divisor itself but to the system of the functions divisible by it, then they admit a complete transfer to the general algebraic functions. In this way one arrives at the notion of the *ideal*, a name that comes from *Kummer's* number-theoretic works, where the non-existent divisors are introduced into the calculation as “ideal divisors”.

Although the present work is by no means concerned with “ideal” functions, but all operations are carried out only on systems of actually existing functions,

it nevertheless seemed expedient to retain the name “ideal”, which is already customary in the theory of numbers.

With these ideals, after a proper explanation of multiplication, one can calculate entirely by the same rules as with rational functions.

*) The ideal numbers were first introduced by *Kummer* in the memoir: *Zur Theorie der complexen Zahlen* (*Crelle's Journal*, vol. 35); a further continuation and a general exposition of the theory of algebraic numbers is to be found in the second and third editions of *Dirichlet's* lectures on the theory of numbers, as well as in the memoir by *Dedekind*: *Sur la théorie des nombres entiers algébriques* (Paris 1877. Reprint from the Bulletin des Sciences math. et astron. of *Darboux* and *Hoüel*). A knowledge of these writings, however, is nowhere presupposed in our work.

From oral communications it has now become known to us that *Kronecker*, years ago already, with reference to the works of *Weierstrass*, undertook investigations which rest on the same foundation as ours.

In particular there results the theorem that every ideal is decomposable in one single way into factors which themselves cannot be decomposed further and are therefore called *prime ideals*. These prime ideals correspond to the linear factors in the theory of integral rational functions. On their basis one arrives at a completely precise and general definition of the “point of the *Riemann* surface”, i.e. of a perfectly determined system of numerical values which can be assigned to the functions of the field without contradiction.

A formal definition of the differential quotient founded on this then leads to the genus number and to a quite general, elegant representation of the differentials of the first kind. To this is attached the proof of the *Riemann-Roch* theorem on the number of arbitrary constants in a function determined by its points of infinity, and the theory of the differentials of the second and third kinds. Up to this point the continuity and expandability of the functions investigated come into consideration in no way whatever. There would, e.g. nowhere remain a gap if one wished to restrict the domain of the numbers used to the system of the algebraic numbers. Thereby a well delimited and fairly comprehensive part of the theory of algebraic functions is treated solely by means belonging to its own sphere.

Admittedly all these results follow with a far smaller expenditure of means, and as special cases of a far-reaching generality, from *Riemann's* theory; but it is known that this theory still offers certain difficulties as regards a rigorous foundation, and until these difficulties have been completely overcome, the way we have taken, or at least a related one, may well be the only one that leads to the goal for the theory of algebraic functions with satisfactory rigour and generality. Thus the theory of ideals itself would be extraordinarily simplified if one were willing to presuppose the notion of the *Riemann* surface, and in particular that of a point of it, together with the intuitions founded on the continuity of algebraic functions. In our work, conversely, the theory of ideals is founded algebraically by a long detour, and from it a perfectly precise and rigorous definition of the “point of the *Riemann* surface” is obtained, which can also serve as a basis for the investigation of continuity and of the questions

connected with it. These questions,

to which those relating to the *Abelian* integrals and the moduli of periodicity also belong, remain excluded from our investigation for the time being. We hope to return to them on another occasion.

Königsberg, 22 October 1880.

Part I.

§ 1. Fields of algebraic functions.

A variable θ is called an *algebraic function* of an independent variable z if it satisfies an irreducible algebraic equation

$$F(\theta, z) = 0 \quad (1.)$$

Here F denotes an expression of the form

$$F(\theta, z) = a_0\theta^n + a_1\theta^{n-1} + \cdots + a_{n-1}\theta + a_n,$$

in which the coefficients $a_0, a_1, \dots, a_n$ are integral rational functions of z without a common divisor. The assumed irreducibility of equation (1.) implies that θ does not satisfy an equation of lower degree with respect to θ , and, as follows from the algorithm of the greatest common divisor, that if

$$G(\theta, z) = b_0\theta^m + b_1\theta^{m-1} + \cdots + b_{m-1}\theta + b_m = 0$$

is a second equation which θ satisfies, $G(\theta, z)$ must be algebraically divisible by $F(\theta, z)$. It can now be shown that $G(\theta, z)$ cannot be of lower degree than $F(\theta, z)$ with respect to z either, and is of the same degree only if a factor independent of z can be split off from $G(\theta, z)$. Let us assume that the coefficients $b_0, b_1, \dots, b_m$ have been freed of common factors, and denote by

$$H(\theta, z) = c_0\theta^{m-n} + c_1\theta^{m-n-1} + \cdots + c_{m-n}$$

the quotient of G by F , freed of its denominator; then

$$kG(\theta, z) = F(\theta, z).H(\theta, z),$$

where k is an integral rational function of z , and comparison of the coefficients gives

$$\begin{aligned} kb_0 &= a_0c_0, \\ kb_1 &= a_0c_1 + a_1c_0, \\ kb_2 &= a_0c_2 + a_1c_1 + a_2c_0, \\ &\dots\dots\dots \end{aligned}$$

where the $c_0, c_1, \dots, c_{m-n}$ may likewise be assumed to be without a common divisor.

From this it follows first that k must be constant and may be set $= 1$; for if $a_0, a_1, \dots, a_{r-1}, c_0, c_1, \dots, c_{s-1}$ are divisible by some linear factor of k , and a_r, c_s are not divisible, then it follows from

$$kb_{r+s} = \dots a_{r-1}c_{s+1} + a_rc_s + a_{r+1}c_{s-1} + \dots$$

the contradiction that a_rc_s would have to be divisible by the same linear factor. But from this it follows further that the degree of $G(\theta, z)$ with respect to z is equal to the sum of the degrees of F and H with respect to z ; for if a_r, c_s are the first among the coefficients a, c whose degree reaches the maximum value, then it follows again from

$$b_{r+s} = \dots a_{r-1}c_{s+1} + a_rc_s + a_{r+1}c_{s-1} + \dots,$$

that the degree of b_{r+s} is equal to the sum of the degrees of a_r and c_s .

If one divides equation (1.) by a_0 , it can also be put in the form

$$f(\theta, z) = \theta^n + b_1\theta^{n-1} + \dots + b_{n-1}\theta + b_n = 0, \quad (2.)$$

where the coefficients $b_1, b_2, \dots, b_n$ may also be fractional rational functions of z .

The system of all rational functions of θ and z , $\Phi(\theta, z)$, has the property that its individuals reproduce themselves under the elementary operations of calculation, addition, subtraction, multiplication and division, and this system is therefore designated as a *field of algebraic functions Ω of degree n* . If first $\varphi(\theta)$ is an *integral* rational function of θ whose coefficients depend rationally on z , then by algebraic division one can determine two functions of the same kind, $q(\theta), r(\theta)$, of which the second does not exceed the degree $n - 1$, such that

$$\varphi(\theta) = q(\theta)f(\theta) + r(\theta)$$

or, because of (2.),

$$\varphi(\theta) = r(\theta).$$

If $\varphi(\theta)$ is not divisible by $f(\theta)$, then these two functions (because of the assumed irreducibility of $f(\theta)$) have no divisor in common, and therefore by the method of the greatest common divisor two functions $f_1(\theta), \varphi_1(\theta)$ can be determined such that

$$f(\theta)f_1(\theta) + \varphi(\theta)\varphi_1(\theta) = 1,$$

hence, because of (2.),

$$\varphi_1(\theta) = \frac{1}{\varphi(\theta)}.$$

From these two remarks, taken together with the assumption of the irreducibility of $f(\theta)$, there results the following

Theorem. Every function ζ of the field Ω can be put in one single way into the form:

$$\zeta = x_0 + x_1\theta + \dots + x_{n-1}\theta^{n-1},$$

where the coefficients $x_0, x_1, \dots, x_{n-1}$ are rational functions of z . Conversely, every function of this form belongs, as a matter of course, to the field Ω .

If one chooses from among the functions of the field Ω n arbitrary ones:

$$\begin{aligned}\eta_1 &= x_0^{(1)} + x_1^{(1)}\theta + \dots + x_{n-1}^{(1)}\theta^{n-1}, \\ \eta_2 &= x_0^{(2)} + x_1^{(2)}\theta + \dots + x_{n-1}^{(2)}\theta^{n-1}, \\ &\dots\dots\dots \\ \eta_n &= x_0^{(n)} + x_1^{(n)}\theta + \dots + x_{n-1}^{(n)}\theta^{n-1},\end{aligned}$$

but in such a way that the determinant

$$\Sigma \pm x_0^{(1)} x_1^{(2)} \dots x_{n-1}^{(n)}$$

is not identically zero, then it follows that every function of the field Ω can also be represented in the form

$$\zeta = y_1\eta_1 + y_2\eta_2 + \dots + y_n\eta_n,$$

whose coefficients $y_1, y_2, \dots, y_n$ are rational functions of z . Such a system of functions $\eta_1, \eta_2, \dots, \eta_n$ shall be called a *basis of the field Ω* .

For a system of functions $\eta_1, \eta_2, \dots, \eta_n$ of the field Ω to form a basis of it, it is necessary and sufficient that there exist among them no equation (identity) of the form

$$y_1\eta_1 + y_2\eta_2 + \dots + y_n\eta_n = 0$$

in which the coefficients $y_1, y_2, \dots, y_n$ do not all vanish. For example, the functions $1, \theta, \theta^2, \dots, \theta^{n-1}$ form a basis of Ω .

§ 2. Norms, traces and discriminants.

If one chooses an arbitrary basis $\eta_1, \eta_2, \dots, \eta_n$ for the representation of the functions of Ω , then, if ζ denotes any function in Ω , one can set:

$$\begin{cases} \zeta\eta_1 = y_{1,1}\eta_1 + y_{1,2}\eta_2 + \dots + y_{1,n}\eta_n, \\ \zeta\eta_2 = y_{2,1}\eta_1 + y_{2,2}\eta_2 + \dots + y_{2,n}\eta_n, \\ \dots\dots\dots \\ \zeta\eta_n = y_{n,1}\eta_1 + y_{n,2}\eta_2 + \dots + y_{n,n}\eta_n, \end{cases} \quad (1.)$$

where the coefficients $y_{i,j}$ are rational functions of z . From this there results the equation

$$\begin{vmatrix} y_{1,1} - \zeta, & y_{1,2}, & \dots & y_{1,n} \\ y_{2,1}, & y_{2,2} - \zeta, & \dots & y_{2,n} \\ \dots & \dots & \dots & \dots \\ y_{n,1}, & y_{n,2}, & \dots & y_{n,n} - \zeta \end{vmatrix} = 0, \quad (2.)$$

which, ordered by powers of ζ , has the shape

$$\varphi(\zeta) = \zeta^n + b_1\zeta^{n-1} + \dots + b_{n-1}\zeta + b_n = 0 \quad (3.)$$

and, as follows without difficulty from the multiplication theorem of determinants, is entirely independent of the choice of the basis $\eta_1, \eta_2, \dots, \eta_n$ taken as foundation. Of the coefficients $b_1, b_2, \dots, b_n$ of the function φ , which are all rational functions of z and are completely determined by the function ζ , two which are of importance in what follows shall be distinguished by special names. The function

$$(-1)^n b_n = \begin{vmatrix} y_{1,1} & y_{1,2} & \dots & y_{1,n} \\ y_{2,1} & y_{2,2} & \dots & y_{2,n} \\ \dots & \dots & \dots & \dots \\ y_{n,1} & y_{n,2} & \dots & y_{n,n} \end{vmatrix} \quad (4.)$$

is called the *norm* of the function ζ , and is denoted by $N(\zeta)$. The following theorems hold for this function.

1. The only function whose norm vanishes identically is the function “zero”; for if one makes the assumption in the system (1.) that $N(\zeta) = 0$, it follows that a system of rational functions of z which do not all vanish, $y_1, y_2, \dots, y_n$, can be determined such that

$$\zeta(y_1\eta_1 + y_2\eta_2 + \dots + y_n\eta_n) = 0,$$

hence, since $\eta_1, \eta_2, \dots, \eta_n$ form a basis of Ω , $\zeta = 0$.

2. The norm of a rational function of z is the n^{th} power of this function. For if ζ is rational, the equations (1.) reduce to the identities $\zeta\eta_h = \zeta\eta_h$, from which $N(\zeta) = \zeta^n$ follows.

3. If ζ' is any second function of the field Ω and the system of equations for this function corresponding to the system (1.) is

$$\zeta'\eta_h = \sum_{\iota} y'_{h,\iota} \eta_{\iota},$$

then it follows:

$$\zeta\zeta'\eta_h = \sum_{\iota, \iota'} y'_{h,\iota} y_{\iota, \iota'} \eta_{\iota'}$$

¹ and from this, by the multiplication theorem of determinants,

$$N(\zeta\zeta') = N(\zeta)N(\zeta').$$

4. From 2. and 3. it follows:

$$N(\zeta)N\left(\frac{1}{\zeta}\right) = 1,$$

hence:

$$N\left(\frac{\zeta}{\zeta'}\right) = \frac{N(\zeta)}{N(\zeta')}.$$

¹ *Editorial note:* Over the second y the print shows a small malformed mark; it is not clear from the print whether it is a prime or stray ink. Set unprimed, as the composition of the two systems requires.

5. Finally there results from the definition of the function φ , (2.), (3.), the important theorem: If t is an arbitrary constant (or also a rational function of z), then

$$\varphi(t) = N(t - \zeta).$$

Next, the function

$$-b_1 = y_{1,1} + y_{2,2} + \cdots + y_{n,n} \quad (5.)$$

shall be called the *trace* of ζ and denoted by $S(\zeta)$. For it the following theorems result immediately from the definition:

$$S(0) = 0, \quad (6.)$$

$$S(1) = n. \quad (7.)$$

And if x denotes a rational function of z , and further ζ, ζ' two functions in Ω :

$$S(x\zeta) = xS(\zeta), \quad (8.)$$

$$S(\zeta + \zeta') = S(\zeta) + S(\zeta'). \quad (9.)$$

It has resulted from this consideration *that every function ζ in Ω satisfies an equation of the n^{th} degree, $\varphi(\zeta) = 0$, whose coefficients depend rationally on z . If this equation is irreducible, the functions $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ form a basis of Ω . In the other case let*

$$\varphi_1(\zeta) = \zeta^e + b'_0\zeta^{e-1} + \cdots + b'_{e-1}\zeta + b'_e = 0 \quad (10.)$$

² be the equation of lowest degree, with coefficients rational in z , which the function ζ satisfies, and consequently $\varphi_1(\zeta) = 0$ irreducible, $e < n$.

Since $\varphi(\zeta)$ nevertheless vanishes, $\varphi(\zeta)$ must be algebraically divisible by $\varphi_1(\zeta)$, and as in § 1 it follows that every rational function η of z and ζ can be represented in the form

$$\eta = x_0 + x_1\zeta + \cdots + x_{e-1}\zeta^{e-1},$$

whose coefficients $x_0, x_1, \dots, x_{e-1}$ depend rationally on z^*). Now if

$$\theta^f + \eta_1\theta^{f-1} + \cdots + \eta_{f-1}\theta + \eta_f = 0$$

is the equation of lowest degree which θ satisfies, with coefficients depending rationally on z and ζ , then between the *e.f* functions

$$\zeta^h \theta^k \quad (h=0, 1, \dots, e-1; k=0, 1, \dots, f-1) \quad (11.)$$

there exists no linear equation with coefficients depending rationally on z , while *every* function in Ω can be represented *linearly* by these functions with coefficients depending rationally on z . It follows from this that they form a basis of Ω , and that accordingly

$$e.f = n,$$

² *Editorial note:* Printed b'_0 as the coefficient of ζ^{e-1} ; the monic equation and the remaining coefficients b'_{e-1}, b'_e require b'_1 . An apparent misprint.

hence e is a divisor of n .

If one applies the basis (11.) to setting up the norm of ζ , one easily recognizes by means of equation (10.) that

$$N(\zeta) = ((-1)^e b'_e)^f = (-1)^n b_e'^f$$

holds. Since further, for an arbitrary constant t , the function $\zeta - t$ satisfies an equation of the same degree as ζ , there results the theorem:

10.³ *The function $\varphi(t)$ (3.) is either irreducible or an integral power of an irreducible function.*

If $\eta_1, \eta_2, \dots, \eta_n$ is an arbitrary system of n functions in Ω , no matter whether it forms a basis or not, we introduce a rational function of z belonging to this system, which we designate as its *discriminant*, $\Delta(\eta_1, \eta_2, \dots, \eta_n)$, and define as follows

$$\Delta(\eta_1, \eta_2, \dots, \eta_n) = \begin{vmatrix} S(\eta_1\eta_1) & S(\eta_1\eta_2) & \dots & S(\eta_1\eta_n) \\ S(\eta_2\eta_1) & S(\eta_2\eta_2) & \dots & S(\eta_2\eta_n) \\ \dots & \dots & \dots & \dots \\ S(\eta_n\eta_1) & S(\eta_n\eta_2) & \dots & S(\eta_n\eta_n) \end{vmatrix}. \quad (12.)$$

The discriminant is not identically zero if and only if the functions $\eta_1, \eta_2, \dots, \eta_n$ form a basis of Ω .

*) From the equation $\varphi_1(\zeta) = 0$ there arises a field of algebraic functions Ω_1 of degree e , whose functions are all at the same time contained in the field Ω , and which can therefore be designated as a divisor of the field Ω .

To prove the first part of this assertion, we assume that $\Delta(\eta_1, \eta_2, \dots, \eta_n) = 0$. Under this assumption a system of rational functions $y_1, y_2, \dots, y_n$ of z , which do not all vanish identically, can be determined such that

$$y_1 S(\eta_1\eta_k) + y_2 S(\eta_2\eta_k) + \dots + y_n S(\eta_n\eta_k) = S(\eta_k(y_1\eta_1 + y_2\eta_2 + \dots + y_n\eta_n)) = 0. \\ (k=1, 2, \dots, n)$$

If one therefore chooses a system of rational functions $x_1, x_2, \dots, x_n$ of z quite arbitrarily and sets:

$$y_1\eta_1 + y_2\eta_2 + \dots + y_n\eta_n = \eta, \\ x_1\eta_1 + x_2\eta_2 + \dots + x_n\eta_n = \xi,$$

it follows:

$$S(\xi\eta) = 0.$$

But if the functions $\eta_1, \eta_2, \dots, \eta_n$ form a basis of Ω , then ξ can be any function whatever in Ω , hence, since η does not vanish, for example also $\frac{1}{\eta}$. But then the last equation is certainly not satisfied, and therefore under this assumption the discriminant of $\eta_1, \eta_2, \dots, \eta_n$ can *not* vanish identically.

Let us keep to the assumption that $\eta_1, \eta_2, \dots, \eta_n$ is a basis of Ω , and set:

$$\eta'_k = x_{1,k}\eta_1 + x_{2,k}\eta_2 + \dots + x_{n,k}\eta_n, \quad (k=1, 2, \dots, n)$$

³*Editorial note:* Printed 10. although the preceding propositions of this § are numbered 1. to 5.; 6. expected. An apparent misprint.

then the functions $\eta'_1, \eta'_2, \dots, \eta'_n$ form a basis of Ω or not, according as the determinant of the rational functions $x_{h,k}$ of z

$$X = \Sigma \pm x_{1,1}x_{2,2} \dots x_{n,n}$$

is different from zero or not. Now, however,

$$S(\eta'_h \eta'_k) = \sum_{1,n}^{\iota, \iota'} x_{\iota, h} x_{\iota', k} S(\eta_\iota \eta_{\iota'}),$$

and from this, by the multiplication theorem of determinants, there results the *fundamental theorem on discriminants*

$$\Delta(\eta'_1, \eta'_2, \dots, \eta'_n) = X^2 \Delta(\eta_1, \eta_2, \dots, \eta_n), \quad (13.)$$

from which the correctness of the second part of the above assertion also becomes clear, that the discriminant of a system of functions always vanishes identically when it does not form a basis of Ω .

§ 3. The system of integral functions of z in the field Ω .

Definition. A function ω of the field Ω shall be called an *integral* function of z if in the equation of lowest degree which it satisfies according to § 2:

$$\varphi(\omega) = \omega^e + b_1 \omega^{e-1} + \dots + b_{e-1} \omega + b_e = 0, \quad (1.)$$

the coefficients $b_1, b_2, \dots, b_e$ are *integral rational* functions of z ; in the opposite case let it be called a *fractional* function. The totality of all integral functions of z in Ω shall be denoted by $\mathfrak{o}$. Since according to § 2 $N(t - \omega)$ is an integral power of $\varphi(t)$, it follows that for an integral function ω all the coefficients of $N(t - \omega)$ too are integral rational functions of z , hence in particular:

1. The norm and the trace of an integral function are integral rational functions of z .

From the definition of the integral functions there results further:

2. A rational function of z belongs to the system $\mathfrak{o}$ if and only if it is an integral rational function of z .

3. Every function η in Ω can be converted into a function of the system $\mathfrak{o}$ by multiplication by an integral rational function of z different from zero. For according to § 2 η satisfies an equation of lowest degree of the form

$$b_0 \eta^e + b_1 \eta^{e-1} + \dots + b_{e-1} \eta + b_e = 0,$$

whose coefficients are integral rational functions of z , and by the substitution $b_0 \eta = \omega$ this passes over into an equation of the form (1.) for ω .

4. A function ω of the field Ω which satisfies any equation of the form

$$\psi(\omega) = \omega^m + c_1 \omega^{m-1} + \dots + c_{m-1} \omega + c_m = 0,$$

in which the coefficients $c_1, \dots, c_m$ are integral rational functions of z , is an *integral function*. For if

$$\varphi(\omega) = \omega^e + b_1\omega^{e-1} + \dots + b_{e-1}\omega + b_e = 0$$

is the equation of lowest degree which ω satisfies, then $\psi(\omega)$ must be algebraically divisible by $\varphi(\omega)$:

$$\psi(\omega) = \varphi(\omega)\chi(\omega),$$

which, as is easily shown, has the consequence that the coefficients of $\varphi(\omega)$ and $\chi(\omega)$ too are integral rational functions of z (*Gauss*, Disq. Ar. art. 42). From this there results the fundamental theorem on integral functions:

5. *Sum, difference, product of two integral functions are again integral functions.*

For if ω' , ω'' are two integral functions in Ω which satisfy respectively the equations

$$\begin{aligned}\omega'^{n'} + b'_1\omega'^{n'-1} + \dots + b'_{n'-1}\omega' + b'_{n'} &= 0, \\ \omega''^{n''} + b''_1\omega''^{n''-1} + \dots + b''_{n''-1}\omega'' + b''_{n''} &= 0,\end{aligned}$$

then, if one understands by $\omega_1, \omega_2, \dots, \omega_m$ the $m = n'n''$ products

$$\omega'^{h'} \omega''^{h''} \quad (h'=0, 1, \dots, n'-1; h''=0, 1, \dots, n''-1)$$

and by ω one of the three functions $\omega' \pm \omega''$, $\omega'\omega''$, one can set:

$$\begin{aligned}\omega\omega_1 &= x_{1,1}\omega_1 + \dots + x_{1,m}\omega_m, \\ &\dots\dots\dots \\ \omega\omega_m &= x_{m,1}\omega_1 + \dots + x_{m,m}\omega_m,\end{aligned}$$

where the $x_{h,h'}$ are integral rational functions of z , and from this one obtains

$$\begin{vmatrix} x_{1,1} - \omega, & x_{1,2}, & \dots & x_{1,m} \\ x_{2,1}, & x_{2,2} - \omega, & \dots & x_{2,m} \\ \dots & \dots & \dots & \dots \\ x_{m,1}, & x_{m,2}, & \dots & x_{m,m} - \omega \end{vmatrix} = 0,$$

hence an equation for ω whose coefficients are integral rational functions of z .

As a corollary it follows from this that every integral rational function of functions in $\mathfrak{o}$ is itself a function of the system $\mathfrak{o}$.

6. An integral function ω is called *divisible* by another integral function ω' if there exists a third integral function ω'' which satisfies the condition

$$\omega = \omega'\omega''.$$

From this definition there follows at once:

If ω is divisible by ω' , and ω' by ω'' , then ω is also divisible by ω'' .

If ω' and ω'' are divisible by ω , then $\omega' \pm \omega''$ is also divisible by ω , and in general: if $\omega_1, \omega_2, \omega_3, \dots$ are divisible by ω , and $\omega'_1, \omega'_2, \omega'_3, \dots$ are arbitrary functions in $\mathfrak{o}$, then $\omega'_1\omega_1 + \omega'_2\omega_2 + \omega'_3\omega_3 + \dots$ is also divisible by ω .

7. If the functions $\eta_1, \eta_2, \dots, \eta_n$ form a basis of Ω , then (by 3.) one can determine n integral rational functions of z different from zero, $a_1, a_2, \dots, a_n$, in such a way that

$$\omega_1 = a_1\eta_1, \quad \omega_2 = a_2\eta_2, \quad \dots \quad \omega_n = a_n\eta_n$$

are integral functions, and these likewise form a basis of Ω , since

$$\Delta(\omega_1, \omega_2, \dots, \omega_n) = a_1^2 a_2^2 \dots a_n^2 \Delta(\eta_1, \eta_2, \dots, \eta_n)$$

is different from zero. There are therefore bases of Ω , $\omega_1, \omega_2, \dots, \omega_n$, which consist entirely of integral functions, and the discriminant of such a basis, since the $S(\omega_r, \omega_s)$ are integral rational functions of z , is itself an integral rational function of z different from zero. Every function of the form

$$\omega = x_1\omega_1 + x_2\omega_2 + \dots + x_n\omega_n, \quad (2.)$$

in which the $x_1, x_2, \dots, x_n$ are integral rational functions of z , then belongs to the system $\mathfrak{o}$; but it is by no means necessary that, conversely, every function in $\mathfrak{o}$ be representable in this form.

Let us therefore assume that there exist in $\mathfrak{o}$ still other functions than those contained in the form (2.); then a linear function $z - c$ and certain integral rational functions $x_1, x_2, \dots, x_n$, not all divisible by $z - c$, must be capable of being chosen such that

$$\frac{x_1\omega_1 + x_2\omega_2 + \dots + x_n\omega_n}{z - c}$$

is an integral function. The functions $x_1, x_2, \dots, x_n$ can now be reduced to their constant remainders $c_1, c_2, \dots, c_n$ with respect to $z - c$, which do not all vanish, and from this it becomes clear that

$$\omega = \frac{c_1\omega_1 + c_2\omega_2 + \dots + c_n\omega_n}{z - c}$$

is also an integral function. If c_1 is different from zero, then the n integral functions

$$\omega \quad \text{and} \quad \omega_2, \omega_3, \dots, \omega_n$$

also form a basis of Ω , and at the same time, by § 2 (13.),

$$\Delta(\omega, \omega_2, \dots, \omega_n) = \frac{c_1^2}{(z - c)^2} \Delta(\omega_1, \omega_2, \dots, \omega_n),$$

hence of lower degree than $\Delta(\omega_1, \omega_2, \dots, \omega_n)$. Now since these two discriminants are integral rational functions of z , one arrives by repeated application of this procedure finally at a basis of Ω consisting of integral

functions, $\omega'_1, \omega'_2, \dots, \omega'_n$, whose discriminant cannot be lowered further in degree, and which consequently has the property *that every function ω in $\mathfrak{o}$ is contained in the form*

$$\omega = x_1\omega'_1 + x_2\omega'_2 + \dots + x_n\omega'_n$$

with integral rational functions of z as coefficients. Such a system shall be called a basis of $\mathfrak{o}$.

If $\omega_1, \omega_2, \dots, \omega_n$ is a basis of $\mathfrak{o}$ and

$$\omega'_\iota = x_{\iota,1}\omega_1 + x_{\iota,2}\omega_2 + \dots + x_{\iota,n}\omega_n, \quad (\iota=1, 2, \dots, n)$$

then the system $\omega'_1, \omega'_2, \dots, \omega'_n$ will likewise form a basis of $\mathfrak{o}$ if and only if the determinant of the integral rational functions $x_{\iota,\iota'}$

$$X = \Sigma \pm x_{1,1}x_{2,2} \dots x_{n,n}$$

is a *constant* different from zero. For let us assume that this determinant has some linear factor $z - c$; then constants $c_1, c_2, \dots, c_n$, not all vanishing, can be determined such that the n integral rational functions of z

$$c_1x_{1,\iota} + c_2x_{2,\iota} + \dots + c_nx_{n,\iota}$$

become divisible by $z - c$ (i.e. vanish for $z = c$); but then

$$\frac{c_1\omega'_1 + c_2\omega'_2 + \dots + c_n\omega'_n}{z - c}$$

is an integral function and consequently $\omega'_1, \omega'_2, \dots, \omega'_n$ is not a basis of $\mathfrak{o}$.

Now since on the other hand

$$\Delta(\omega'_1, \omega'_2, \dots, \omega'_n) = X^2 \Delta(\omega_1, \omega_2, \dots, \omega_n)$$

it follows that the discriminant of a basis of $\mathfrak{o}$, apart from a constant factor, is independent of the choice of this basis. One therefore obtains a perfectly determined integral rational function of z if in the discriminant of an arbitrary basis of $\mathfrak{o}$ one makes the coefficient of the highest power of $z = 1$ by division. *This function shall be called the discriminant of the field Ω or of the system $\mathfrak{o}$ and denoted by $\Delta(\Omega)$ or $\Delta(\mathfrak{o})$.*

§ 4. The function modules.

In what follows we consider systems of functions which we call *function modules*, or also simply *modules*, and define as follows.

A system of functions (in Ω) is called a module if its functions reproduce themselves under addition, subtraction and multiplication by integral rational functions of z .

If one denotes by $\alpha_1, \alpha_2, \dots, \alpha_m$ any m given functions, and by $x_1, x_2, \dots, x_m$ arbitrary integral rational functions of z , then the totality of all functions of the form

$$\alpha = x_1\alpha_1 + x_2\alpha_2 + \dots + x_m\alpha_m$$

forms a module. Such a one shall be called a *finite module* and denoted by

$$\mathfrak{a} = [\alpha_1, \alpha_2, \dots, \alpha_m]$$

The system of functions $\alpha_1, \alpha_2, \dots, \alpha_m$ is called the basis of this module.

We shall call a system of functions $\alpha_1, \alpha_2, \dots, \alpha_m$ *rationally irreducible*, or the functions $\alpha_1, \alpha_2, \dots, \alpha_p$ ⁴ *rationally independent*, if an equation of the form

$$x_1\alpha_1 + x_2\alpha_2 + \dots + x_m\alpha_m = 0$$

for rational x can hold only if $x_1 = 0, x_2 = 0, \dots, x_m = 0$. A system of functions which forms a basis of the field Ω is therefore always rationally irreducible, and there is no system of more than n rationally independent functions in Ω .

We now prove first the theorem:

1. *Every finite module possesses a rationally irreducible basis.*

Its proof results immediately from the following lemma:

If the integral rational functions $y_{1,1}, y_{2,1}, \dots, y_{m,1}$ are without a common divisor, then other integral rational functions $y_{1,2}, y_{2,2}, \dots, y_{m,m}$ can be determined such that

$$\Sigma \pm y_{1,1}y_{2,2} \dots y_{m,m} = 1^*).$$

*) The theorem is true and known for $m = 2$. Let us therefore assume it proved for $m-1$; then, if ∂ denotes the greatest common divisor of $y_{1,1}, y_{2,1}, \dots, y_{m-1,1}$, we can satisfy the equation

$$\begin{vmatrix} y_{1,1} & y_{2,1} & \dots & y_{m-1,1} \\ y_{1,3} & y_{2,3} & \dots & y_{m-1,3} \\ \dots & \dots & \dots & \dots \\ y_{1,m} & y_{2,m} & \dots & y_{m-1,m} \end{vmatrix} = \partial$$

and if we then determine the integral rational functions x, y such that

$$xy_{m,1} - y\partial = (-1)^{m-1}$$

it follows:

$$\begin{vmatrix} y_{1,1} & y_{2,1} & \dots & y_{m-1,1} & y_{m,1} \\ \frac{xy_{1,1}}{\partial} & \frac{xy_{2,1}}{\partial} & \dots & \frac{xy_{m-1,1}}{\partial} & y \\ y_{1,3} & y_{2,3} & \dots & y_{m-1,3} & 0 \\ \dots & \dots & \dots & \dots & \dots \\ y_{1,m} & y_{2,m} & \dots & y_{m-1,m} & 0 \end{vmatrix} = 1.$$

5

⁴Editorial note: Printed α_p instead of α_m ; an apparent misprint.

⁵Editorial note: Printed a period after $y_{2,1}$ in the first row where a comma is expected; possibly a comma whose tail failed to ink.

Now if the functions $\alpha_1, \alpha_2, \dots, \alpha_m$ satisfy an equation

$$\sum_{1,m}^{\iota} y_{\iota,1} \alpha_{\iota} = 0,$$

in which the integral rational functions $y_{1,1}, \dots, y_{m,1}$ may be assumed to be without a common divisor, set

$$\begin{aligned} \sum_{1,m}^{\iota} y_{\iota,2} \alpha_{\iota} &= \beta_2, \\ &\dots\dots\dots \\ \sum_{1,m}^{\iota} y_{\iota,m} \alpha_{\iota} &= \beta_m; \end{aligned}$$

then the module $[\alpha_1, \alpha_2, \dots, \alpha_m]$ is completely identical with the module $[\beta_2, \beta_3, \dots, \beta_m]$, whose basis contains one function fewer. If the functions β_{ι} are not yet rationally independent, one can reduce them further in the same way, and one finally arrives, provided the functions α_{ι} do not all vanish (a case which we wish to exclude entirely from the notion of a module), at an irreducible basis. In what follows we shall always understand by a basis simply an irreducible basis.

2. Although by the foregoing one can find very different irreducible bases for one and the same module, the number of functions contained in such a basis is nevertheless always the same, since in the opposite case that system of functions which contains more functions could not be rationally irreducible. If therefore $\alpha_1, \alpha_2, \dots, \alpha_m; \beta_1, \beta_2, \dots, \beta_m$ are two irreducible bases of the same module $\mathfrak{a}$, then, since both the α_k and the β_k are contained in $\mathfrak{a}$:

$$\alpha_k = \sum_{1,m}^{\iota} p_k^{(\iota)} \beta_{\iota}; \quad \beta_k = \sum_{1,m}^{\iota} q_k^{(\iota)} \alpha_{\iota},$$

where the coefficients p, q are integral rational functions of z . But from this it follows:

$$\sum_{1,m}^{\iota} q_{\iota}^{(k)} p_{\iota}^{(h)} = 0 \quad \text{or} \quad 1,$$

according as h is different from k or not, and from this:

$$\Sigma \pm p_1^{(1)} p_2^{(2)} \dots p_m^{(m)} \cdot \Sigma \pm q_1^{(1)} q_2^{(2)} \dots q_m^{(m)} = 1,$$

and since both determinants are integral rational functions of z , they must both be *constant*.

3. *Definition.* A module $\mathfrak{a}$ is called *divisible* by a module $\mathfrak{b}$, or $\mathfrak{b}$ a *divisor* of $\mathfrak{a}$, $\mathfrak{a}$ a *multiple* of $\mathfrak{b}$ ($\mathfrak{b}$ goes into $\mathfrak{a}$), if every function in $\mathfrak{a}$ is at the same time contained in $\mathfrak{b}$. $\mathfrak{b}$ shall be called a *proper divisor* of $\mathfrak{a}$ if $\mathfrak{a}$ is divisible by $\mathfrak{b}$ but not identical with $\mathfrak{b}^*$.

From this definition there follows at once:

If $\mathfrak{a}$ is divisible by $\mathfrak{b}$, and $\mathfrak{b}$ divisible by $\mathfrak{c}$, then $\mathfrak{a}$ is also divisible by $\mathfrak{c}$.

4. *Definition.* The totality $\mathfrak{m}$ of all those functions which are contained at the same time in two modules $\mathfrak{a}, \mathfrak{b}$ forms, if it does not consist of the single

function “zero”, a module (by the general definition), which is called the *least common multiple of $\mathfrak{a}$ and $\mathfrak{b}$* , because every module which is a multiple both of $\mathfrak{a}$ and of $\mathfrak{b}$ is also a multiple of $\mathfrak{m}$. The least common multiple of an arbitrary number of modules $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \dots$ is correspondingly the totality of all the functions that are contained at the same time in $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \dots$. One can form it by replacing, at pleasure, any two of the modules $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \dots$ by their least common multiple.

5. *Definition.* If α is an arbitrary function in $\mathfrak{a}$, and β an arbitrary function in $\mathfrak{b}$, then the totality of all functions of the form $\alpha + \beta$ forms a module $\mathfrak{d}$, which is called *the greatest common divisor of the two modules $\mathfrak{a}$ and $\mathfrak{b}$* . It is, if $\mathfrak{a}$ and $\mathfrak{b}$ are finite modules, itself such a one. For if

$$\mathfrak{a} = [\alpha_1, \alpha_2, \dots, \alpha_r], \quad \mathfrak{b} = [\beta_1, \beta_2, \dots, \beta_s],$$

then

$$\mathfrak{d} = [\alpha_1, \alpha_2, \dots, \alpha_r, \beta_1, \beta_2, \dots, \beta_s].$$

By the definition of divisibility $\mathfrak{d}$ is a divisor both of $\mathfrak{a}$ and of $\mathfrak{b}$. If conversely $\mathfrak{d}'$ is a divisor of $\mathfrak{a}$ and of $\mathfrak{b}$, then the functions

*) The notion of divisibility of modules is formed contrary to the intuition familiar from numbers, inasmuch as the divisor has a greater content of functions than the multiple.

α as well as the functions β , and consequently also the functions $\alpha + \beta$, are contained in $\mathfrak{d}'$; therefore $\mathfrak{d}$ is divisible by $\mathfrak{d}'$.

The definition of the greatest common divisor of an arbitrary number of modules now follows of itself.

6. *Definition.* If $\mathfrak{a}$ is a module, α every function in $\mathfrak{a}$, and μ an arbitrary function in Ω , we understand by the product $\mu\mathfrak{a}$ or $\mathfrak{a}\mu$ the totality of all functions $\mu\alpha$, which is again a module. If

$$\mathfrak{a} = [\alpha_1, \alpha_2, \dots, \alpha_r]$$

is a finite module, then

$$\mu\mathfrak{a} = [\mu\alpha_1, \mu\alpha_2, \dots, \mu\alpha_r],$$

hence likewise a finite module, and from $\mu\mathfrak{a} = \mu\mathfrak{b}$ there follows $\mathfrak{a} = \mathfrak{b}$ if μ is different from zero.

7. *Definition.* If $\mathfrak{a}, \mathfrak{b}$ are two modules, and α, β all the functions in $\mathfrak{a}$, resp. in $\mathfrak{b}$, we understand by the *product*

$$\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a} = \mathfrak{c}$$

the totality of all products of a function α and a function β and of all sums of such products, hence of all the functions which can be denoted by the sign

$$\gamma = \Sigma\alpha\beta$$

This system of functions always forms a module, and indeed a finite one if $\mathfrak{a}$ and $\mathfrak{b}$ are such. For if $\mathfrak{a}$ and $\mathfrak{b}$ are defined as in 5., the $r.s$ functions

$\alpha_i \beta_x$ form a basis of $\mathfrak{c}$, albeit a reducible one. A product of arbitrarily many modules $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \dots$ is now explained of itself, and for it the fundamental theorem of multiplication on the interchangeability of the factors holds. If the individual functions of such a product, whose number may be m , are equal to one another and $= \mathfrak{a}$, it is denoted by $\mathfrak{a}^m$, and

$$\mathfrak{a}^{m+m'} = \mathfrak{a}^m \mathfrak{a}^{m'}.$$

In general a product $\mathfrak{a}\mathfrak{b}$ is *not* divisible by $\mathfrak{a}$. On the other hand the theorem holds, whose proof follows immediately from the definition:

If $\mathfrak{a}$ is divisible by $\mathfrak{a}_1$, and $\mathfrak{b}$ by $\mathfrak{b}_1$, then $\mathfrak{a}\mathfrak{b}$ is divisible by $\mathfrak{a}_1\mathfrak{b}_1$.

8. *Definition.* By the quotient $\frac{\mathfrak{b}}{\mathfrak{a}}$ of two modules $\mathfrak{a}, \mathfrak{b}$ shall be understood the totality of all those functions γ which have the property

that $\gamma\mathfrak{a}$ is divisible by $\mathfrak{b}$. This quotient, if it does not consist of the single function “zero”, is a module $\mathfrak{c}$, as becomes clear at once from the definition. The product $\frac{\mathfrak{b}}{\mathfrak{a}} \cdot \mathfrak{a}$ is always divisible by $\mathfrak{b}$, though not always equal to $\mathfrak{b}$.

§ 5. Congruences.

Two functions α, β are called *congruent* with respect to the module $\mathfrak{a}$

$$\alpha \equiv \beta \pmod{\mathfrak{a}},$$

if the difference of the two functions, $\alpha - \beta$, is contained in the module $\mathfrak{a}$.

From this definition the following theorems result immediately:

1. If $\alpha \equiv \beta, \beta \equiv \gamma \pmod{\mathfrak{a}}$, then $\alpha \equiv \gamma \pmod{\mathfrak{a}}$.
2. If $\mathfrak{d}$ is any divisor of $\mathfrak{a}$, it follows from $\alpha \equiv \beta \pmod{\mathfrak{a}}$ that also $\alpha \equiv \beta \pmod{\mathfrak{d}}$.
3. If $\alpha \equiv \beta \pmod{\mathfrak{a}}$, and μ is an arbitrary function in Ω , then $\mu\alpha \equiv \mu\beta \pmod{\mu\mathfrak{a}}$ follows, and conversely the former congruence follows from the latter if μ is different from zero.
4. If $\alpha \equiv \beta, \alpha_1 \equiv \beta_1 \pmod{\mathfrak{a}}$, then also $\alpha \pm \alpha_1 \equiv \beta \pm \beta_1 \pmod{\mathfrak{a}}$.

If $\lambda_1, \lambda_2, \dots, \lambda_m$ are arbitrarily given functions in Ω , and $c_1, c_2, \dots, c_m$ arbitrary constants, then the totality of all functions of the form

$$c_1\lambda_1 + c_2\lambda_2 + \dots + c_m\lambda_m$$

is called a *family* and is denoted by $(\lambda_1, \lambda_2, \dots, \lambda_m)$. The system of functions $\lambda_1, \lambda_2, \dots, \lambda_m$ is called *the basis of the family*. The functions $\lambda_1, \lambda_2, \dots, \lambda_m$ are called *linearly independent*, or their system *linearly irreducible*, if an equation (identity) of the form

$$c_1\lambda_1 + c_2\lambda_2 + \dots + c_m\lambda_m = 0$$

cannot hold otherwise than if the constant coefficients $c_1, c_2, \dots, c_m$ all vanish.

Accordingly the theorem holds *that every family possesses a linearly irreducible basis*. For if $c_1\lambda_1 + c_2\lambda_2 + \dots + c_m\lambda_m = 0$ and c_1 is different from zero, then the family $(\lambda_1, \lambda_2, \dots, \lambda_m)$ is identical with the family $(\lambda_2, \lambda_3, \dots, \lambda_m)$,

whose basis contains one function fewer. If this is not yet linearly irreducible, one can continue the inference in the same way. Here too, in

what follows, a basis shall be understood simply as an irreducible basis. The number of functions contained in an irreducible basis of a family is always the same and is called the *dimension* of the family. If m is the dimension, the family is also called an m -fold one. Any m functions of such a family form an irreducible basis of it if and only if they are linearly independent.

The functions $\lambda_1, \lambda_2, \dots, \lambda_m$ are called *linearly independent with respect to the module $\mathfrak{a}$* if a congruence of the form

$$c_1\lambda_1 + c_2\lambda_2 + \dots + c_m\lambda_m \equiv 0 \pmod{\mathfrak{a}}$$

holds for no constant coefficients $c_1, c_2, \dots, c_m$ other than vanishing ones. Two sums of the form $\sum c_i \lambda_i$ with different values of the constant coefficients c_i are then also always incongruent with respect to the module $\mathfrak{a}$.

Now let $\mathfrak{a}$ and $\mathfrak{b}$ be two modules, and let it *first* be assumed that there exist in $\mathfrak{b}$ only a finite number of functions $\lambda_1, \lambda_2, \dots, \lambda_m$ which are linearly independent with respect to the module $\mathfrak{a}$. Every function β in $\mathfrak{b}$ then satisfies one and only one congruence of the form

$$\beta \equiv c_1\lambda_1 + c_2\lambda_2 + \dots + c_m\lambda_m \pmod{\mathfrak{a}}$$

with constant coefficients $c_1, c_2, \dots, c_m$. The family $(\lambda_1, \lambda_2, \dots, \lambda_m)$ can therefore be called a *complete system of residues of the module $\mathfrak{b}$ with respect to the module $\mathfrak{a}$* , and $\lambda_1, \lambda_2, \dots, \lambda_m$ a *basis* of it, and in symbolic notation one can set:

$$\mathfrak{b} \equiv (\lambda_1, \lambda_2, \dots, \lambda_m) \pmod{\mathfrak{a}}.$$

If one chooses in $\mathfrak{b}$ any system of m functions $\lambda'_1, \lambda'_2, \dots, \lambda'_m$, then m congruences hold

$$\lambda'_h \equiv \sum_{\iota} k_{h,\iota} \lambda_{\iota} \pmod{\mathfrak{a}}$$

with constant $k_{h,\iota}$, and this system forms a basis of a complete system of residues of $\mathfrak{b}$ with respect to $\mathfrak{a}$ if and only if the determinant

$$\Sigma \pm k_{1,1}k_{2,2} \dots k_{m,m}$$

is different from zero.

§ 6. Norm of a module with respect to another.

If $(\lambda_1, \lambda_2, \dots, \lambda_m)$ is an arbitrary complete system of residues of a module $\mathfrak{b}$ with respect to another, $\mathfrak{a}$, then, because $z\mathfrak{b}$ is divisible by $\mathfrak{b}$,

there results a completely determined system of m^2 constants $c_{h,k}$ by which the congruences are satisfied:

$$\left. \begin{aligned} z\lambda_1 &\equiv c_{1,1}\lambda_1 + c_{2,1}\lambda_2 + \dots + c_{m,1}\lambda_m \\ z\lambda_2 &\equiv c_{1,2}\lambda_1 + c_{2,2}\lambda_2 + \dots + c_{m,2}\lambda_m \\ &\dots\dots\dots \\ z\lambda_m &\equiv c_{1,m}\lambda_1 + c_{2,m}\lambda_2 + \dots + c_{m,m}\lambda_m \end{aligned} \right\} \pmod{\mathfrak{a}}$$

and by solving this system one recognizes that every function λ_i , and consequently every function β of the module $\mathfrak{b}$, is converted into a function of the module $\mathfrak{a}$ by multiplication by the integral rational function of z of the m^{th} degree

$$(\mathfrak{b}, \mathfrak{a}) = (-1)^m \begin{vmatrix} c_{1,1} - z, & c_{2,1}, & \dots & c_{m,1} \\ c_{1,2}, & c_{2,2} - z, & \dots & c_{m,2} \\ \dots & \dots & \dots & \dots \\ c_{1,m}, & c_{2,m}, & \dots & c_{m,m} - z \end{vmatrix}$$

This function $(\mathfrak{b}, \mathfrak{a})$ is, as follows easily from the multiplication theorem of determinants, independent of the choice of the basis $\lambda_1, \lambda_2, \dots, \lambda_m$, hence dependent only on the two modules $\mathfrak{a}, \mathfrak{b}$, and shall be called the *norm of $\mathfrak{a}$ with respect to $\mathfrak{b}$* .

If every function in $\mathfrak{b}$ is at the same time contained in $\mathfrak{a}$, hence $\mathfrak{b}$ divisible by $\mathfrak{a}$, then $m = 0$ and $(\mathfrak{b}, \mathfrak{a}) = 1$ is to be set. If on the other hand $\mathfrak{b}$ does *not*, as assumed above, contain a finite number of functions linearly independent with respect to $\mathfrak{a}$, then it shall be stipulated that $(\mathfrak{b}, \mathfrak{a}) = 0$.

1. If $\mathfrak{m}$ is the least common multiple and $\mathfrak{d}$ the greatest common divisor of $\mathfrak{a}$ and $\mathfrak{b}$, then every congruence between functions of the module $\mathfrak{b}$ with respect to the module $\mathfrak{a}$ is completely equivalent to the congruence of the same functions with respect to the module $\mathfrak{m}$; on the other hand every function in $\mathfrak{b}$ is congruent to a function in $\mathfrak{d}$, and conversely every function in $\mathfrak{d}$ to a function in $\mathfrak{b}$, with respect to the module $\mathfrak{a}$. From these remarks there results at once the important theorem:

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{b}, \mathfrak{m}) = (\mathfrak{d}, \mathfrak{a}),$$

which remains true also when $(\mathfrak{b}, \mathfrak{a}) = 0$.

2. If the module $\mathfrak{a}$ is divisible by the module $\mathfrak{b}$, and this by the third module $\mathfrak{c}$, then

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

The theorem is evidently true if of the two norms $(\mathfrak{c}, \mathfrak{b}), (\mathfrak{b}, \mathfrak{a})$ one vanishes. If this is not the case, and

$$\begin{aligned} \mathfrak{c} &\equiv (\varrho_1, \varrho_2, \dots, \varrho_r) \pmod{\mathfrak{b}}, \\ \mathfrak{b} &\equiv (\lambda_1, \lambda_2, \dots, \lambda_s) \pmod{\mathfrak{a}}, \end{aligned}$$

then the functions $\varrho_1, \varrho_2, \dots, \varrho_r, \lambda_1, \lambda_2, \dots, \lambda_s$ taken together are linearly independent with respect to the module $\mathfrak{a}$; for if

$$\sum_i^r c_i \varrho_i + \sum_i^s c'_i \lambda_i \equiv 0 \pmod{\mathfrak{a}},$$

then, since $\mathfrak{a}$ is divisible by $\mathfrak{b}$ and the functions λ_i are contained in $\mathfrak{b}$, it follows

$$\begin{aligned} \sum_i^r c_i \varrho_i &\equiv 0 \pmod{\mathfrak{b}}, \quad \text{hence} \quad c_i = 0, \\ \sum_i^s c'_i \lambda_i &\equiv 0 \pmod{\mathfrak{a}}, \quad \text{hence} \quad c'_i = 0. \end{aligned}$$

Since further every function γ in $\mathfrak{c}$ satisfies a congruence of the form:

$$\gamma \equiv \Sigma c_i \varrho_i + \Sigma c'_i \lambda_i \pmod{\mathfrak{a}},$$

the $(r+s)$ -fold family $(\varrho_1, \varrho_2, \dots, \varrho_r, \lambda_1, \lambda_2, \dots, \lambda_s)$ is a complete system of residues of $\mathfrak{c}$ with respect to $\mathfrak{a}$, or

$$\mathfrak{c} \equiv (\varrho_1, \varrho_2, \dots, \varrho_r, \lambda_1, \lambda_2, \dots, \lambda_s) \pmod{\mathfrak{a}}.$$

If therefore

$$\begin{aligned} z\varrho_1 &= e_{1,1}\varrho_1 + \dots + e_{r,1}\varrho_r + \beta_1 \\ &\dots\dots\dots \end{aligned}$$

$$z\varrho_r = e_{1,r}\varrho_1 + \dots + e_{r,r}\varrho_r + \beta_r,$$

where the $e_{i,\mathfrak{x}}$ are constants and the β_i functions in $\mathfrak{b}$, hence:

$$(\mathfrak{c}, \mathfrak{b}) = (-1)^r \begin{vmatrix} e_{1,1} - z, & \dots & e_{r,1} \\ \dots & \dots & \dots \\ e_{1,r}, & \dots & e_{r,r} - z \end{vmatrix},$$

and further:

$$\left. \begin{aligned} \beta_1 &\equiv h_{1,1}\lambda_1 + \dots + h_{s,1}\lambda_s \\ &\dots\dots\dots \\ \beta_r &\equiv h_{1,r}\lambda_1 + \dots + h_{s,r}\lambda_s \\ z\lambda_1 &\equiv c_{1,1}\lambda_1 + \dots + c_{s,1}\lambda_s \\ &\dots\dots\dots \\ z\lambda_s &\equiv c_{1,s}\lambda_1 + \dots + c_{s,s}\lambda_s \end{aligned} \right\} \pmod{\mathfrak{a}}$$

with constant coefficients $h_{i,\mathfrak{x}}, c_{i,\mathfrak{x}}$, hence

$$(\mathfrak{b}, \mathfrak{a}) = (-1)^s \begin{vmatrix} c_{1,1} - z, & \dots & c_{s,1} \\ \dots & \dots & \dots \\ c_{1,s}, & \dots & c_{s,s} - z \end{vmatrix},$$

then it follows:

$$\left. \begin{aligned} z\varrho_1 &\equiv e_{1,1}\varrho_1 + \dots + e_{r,1}\varrho_r + h_{1,1}\lambda_1 + \dots + h_{s,1}\lambda_s \\ &\dots\dots\dots \\ z\varrho_r &\equiv e_{1,r}\varrho_1 + \dots + e_{r,r}\varrho_r + h_{1,r}\lambda_1 + \dots + h_{s,r}\lambda_s \\ z\lambda_1 &\equiv c_{1,1}\lambda_1 + \dots + c_{s,1}\lambda_s \\ &\dots\dots\dots \\ z\lambda_s &\equiv c_{1,s}\lambda_1 + \dots + c_{s,s}\lambda_s \end{aligned} \right\} \pmod{\mathfrak{a}}$$

and from this

$$(\mathfrak{c}, \mathfrak{a}) = (-1)^{r+s} \begin{vmatrix} e_{1,1} - z, & \dots & e_{r,1}, & h_{1,1}, & \dots & h_{s,1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ e_{1,r}, & \dots & e_{r,r} - z, & h_{1,r}, & \dots & h_{s,r} \\ 0 & \dots & 0 & c_{1,1} - z, & \dots & c_{s,1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & c_{1,s}, & \dots & c_{s,s} - z \end{vmatrix} = (\mathfrak{c}, \mathfrak{b})(\mathfrak{b}, \mathfrak{a}).$$

3. If the basis functions $\beta_1, \beta_2, \dots, \beta_s$ of a finite module $\mathfrak{b} = [\beta_1, \beta_2, \dots, \beta_s]$ can be converted into functions of a module $\mathfrak{a}$ by multiplication by integral rational functions of z different from zero, then the norm of $\mathfrak{a}$ with respect to $\mathfrak{b}$, $(\mathfrak{b}, \mathfrak{a})$, is different from zero. At the same time the least common multiple of $\mathfrak{a}$ and $\mathfrak{b}$ is a finite module $\mathfrak{m}$, of which an irreducible basis may be assumed in the form:

$$\begin{aligned}\mu_1 &= a_{1,1}\beta_1, \\ \mu_2 &= a_{1,2}\beta_1 + a_{2,2}\beta_2, \\ &\dots\dots\dots \\ \mu_s &= a_{1,s}\beta_1 + a_{2,s}\beta_2 + \dots + a_{s,s}\beta_s,\end{aligned}$$

where the coefficients $a_{l,\kappa}$ are integral rational functions of z , and indeed such that

$$(\mathfrak{b}, \mathfrak{a}) = a_{1,1}a_{2,2} \dots a_{s,s}.$$

To prove this important theorem, let us assume that $\mathfrak{a}_1$ is the greatest common divisor of $\mathfrak{a}$ and $[\beta_1]$, $\mathfrak{a}_2$ that of $\mathfrak{a}_1$ and $[\beta_2]$, and so on, so that $\mathfrak{a}_r$ is the totality of all functions of the form

$$\alpha_r = \alpha + y_1\beta_1 + \dots + y_r\beta_r$$

where α is a function in $\mathfrak{a}$ and $y_1, \dots, y_r$ are integral rational functions of z . Then $\mathfrak{a}_s$ is the greatest common divisor of $\mathfrak{a}$ and $\mathfrak{b}$. Now since every module $\mathfrak{a}_r$ is divisible by the following one $\mathfrak{a}_{r+1}$, it follows from

1. and 2.

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{a}_s, \mathfrak{a}) = (\mathfrak{a}_s, \mathfrak{a}_{s-1})(\mathfrak{a}_{s-1}, \mathfrak{a}_{s-2}) \dots (\mathfrak{a}_1, \mathfrak{a}),$$

and it is therefore still a matter of determining $(\mathfrak{a}_r, \mathfrak{a}_{r-1})$. But

$$\alpha_r = \alpha_{r-1} + y_r\beta_r \equiv y_r\beta_r \pmod{\mathfrak{a}_{r-1}},$$

and by the assumption there is an integral rational function x_r of z , different from zero, for which

$$x_r\beta_r \equiv 0 \pmod{\mathfrak{a}},$$

hence also

$$x_r\beta_r \equiv 0 \pmod{\mathfrak{a}_{r-1}}.$$

Now if $a_{r,r}$ is, among all the functions x_r satisfying the latter congruence, one of the lowest possible degree m_r , which at the same time is assumed such that the coefficient of the highest power of $z = 1$, then all the other functions x_r satisfying this congruence are divisible by $a_{r,r}$; for, for an arbitrary integral rational q ,

$$(x_r - qa_{r,r})\beta_r \equiv 0 \pmod{\mathfrak{a}_{r-1}},$$

and if x_r is not divisible by $a_{r,r}$, then q can be chosen such that $x_r - qa_{r,r}$ becomes of lower degree than $a_{r,r}$, contrary to the assumption.

If one therefore sets

$$y_r = qa_{r,r} + b_{r,r}$$

and determines q such that the degree of $b_{r,r}$ becomes smaller than m_r , it follows:

$$\alpha_r \equiv b_{r,r}\beta_r \pmod{\mathfrak{a}_{r-1}}$$

and from this

$$\mathfrak{a}_r \equiv (\beta_r, z\beta_r, \dots, z^{m_r-1}\beta_r) \pmod{\mathfrak{a}_{r-1}}.$$

If one therefore sets for the moment:

$$\begin{aligned} a_{r,r} &= c_0 + c_1z + \dots + c_{m_r-1}z^{m_r-1} + z^{m_r}, \\ \lambda_k &= z^{k-1}\beta_r, \end{aligned}$$

it follows:

$$\begin{aligned} z\lambda_1 &= \lambda_2, \quad z\lambda_2 = \lambda_3, \quad \dots \\ z\lambda_{m_r} &\equiv -c_0\lambda_1 - c_1\lambda_2 - \dots - c_{m_r-1}\lambda_{m_r} \pmod{\mathfrak{a}_{r-1}} \end{aligned}$$

hence:

$$(\mathfrak{a}_r, \mathfrak{a}_{r-1}) = (-1)^{m_r} \begin{vmatrix} -z, & 1, & 0, & \dots & 0 \\ 0, & -z, & 1, & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0, & 0, & 0, & \dots & 1 \\ -c_0, & -c_1, & -c_2, & \dots & -c_{m_r-1} - z \end{vmatrix} = a_{r,r}.$$

From this it follows, as in 2., that the system of functions

$$\begin{aligned} &\beta_1, \quad z\beta_1, \quad \dots \quad z^{m_1-1}\beta_1, \\ &\beta_2, \quad z\beta_2, \quad \dots \quad z^{m_2-1}\beta_2, \\ &\dots\dots\dots \\ &\beta_s, \quad z\beta_s, \quad \dots \quad z^{m_s-1}\beta_s, \end{aligned}$$

forms a basis of a complete system of residues of $\mathfrak{b}$ with respect to $\mathfrak{a}$, and that

$$(\mathfrak{b}, \mathfrak{a}) = a_{1,1}a_{2,2} \dots a_{s,s}$$

is of degree

$$m = m_1 + m_2 + \dots + m_s$$

Now since $a_{r,r}\beta_r \equiv 0 \pmod{\mathfrak{a}_{r-1}}$, a function μ_r in $\mathfrak{a}$ and integral rational functions $a_{k,r}$ can be determined such that

$$\mu_r = a_{1,r}\beta_1 + a_{2,r}\beta_2 + \dots + a_{r,r}\beta_r$$

⁶ holds; the functions determined in this way

$$\begin{aligned}\mu_1 &= a_{1,1}\beta_1, \\ \mu_2 &= a_{1,2}\beta_1 + a_{2,2}\beta_2, \\ &\dots\dots\dots \\ \mu_s &= a_{1,s}\beta_1 + a_{2,s}\beta_2 + \dots + a_{s,s}\beta_s\end{aligned}$$

are, since none of the functions $a_{1,1}, \dots, a_{s,s}$ vanishes, rationally independent, and are all contained at the same time in $\mathfrak{a}$ and in $\mathfrak{b}$, hence also in the least common multiple $\mathfrak{m}$ of these two modules. It remains to be shown that they form a basis of $\mathfrak{m}$.

Let $\mathfrak{m}_r$ be the least common multiple of $\mathfrak{a}$ and $[\beta_1, \beta_2, \dots, \beta_r]$, $\mathfrak{m}_s = \mathfrak{m}$, so that among the modules $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_s$ each is divisible by all the following ones, hence also by $\mathfrak{m}$, and let

$$\nu_r = z_1\beta_1 + z_2\beta_2 + \dots + z_r\beta_r$$

be a function in $\mathfrak{m}_r$, hence also in $\mathfrak{a}$.

Accordingly

$$z_r\beta_r \equiv 0 \pmod{\mathfrak{a}_{r-1}},$$

hence

$$z_r = x_r a_{r,r},$$

where x_r denotes an integral rational function. Therefore

$$\nu_r - x_r\mu_r \equiv 0 \pmod{\mathfrak{m}_{r-1}}, \quad \nu_1 - x_1\mu_1 = 0,$$

from which it follows:

$$\nu_r = x_1\mu_1 + x_2\mu_2 + \dots + x_r\mu_r,$$

hence:

$$\begin{aligned}\mathfrak{m}_r &= [\mu_1, \mu_2, \dots, \mu_r], \\ \mathfrak{m} &= [\mu_1, \mu_2, \dots, \mu_s],\end{aligned}$$

q. e. d.

Accordingly an irreducible basis of the module $\mathfrak{m}$ contains exactly as many functions as an irreducible basis of $\mathfrak{b}$. If instead of the basis $\mu_1, \mu_2, \dots, \mu_s$ one chooses another one $\mu'_1, \mu'_2, \dots, \mu'_s$, then $\mu'_1, \mu'_2, \dots, \mu'_s$ can be expressed in the form

$$\mu'_k = a'_{1,k}\beta_1 + a'_{2,k}\beta_2 + \dots + a'_{s,k}\beta_s$$

with integral rational coefficients $a'_{\iota,k}$, and from § 4, 2. there results

$$(\mathfrak{b}, \mathfrak{a}) = \text{const. } \Sigma \pm a'_{1,1}a'_{2,2} \dots a'_{s,s}.$$

⁶*Editorial note:* Printed a_{rr} without the comma between the two indices; the notation throughout requires $a_{r,r}$. An apparent dropped sort.

4. If we make in particular the assumption that $\mathfrak{a}$ is likewise a finite module possessing an irreducible basis of just as many functions as $\mathfrak{b}$, and that moreover $\mathfrak{a}$ is divisible by $\mathfrak{b}$, then, if

$$\mathfrak{a} = [\alpha_1, \alpha_2, \dots, \alpha_s]$$

the integral rational functions $b_{l,k}$ of z can be determined such that

$$\alpha_k = b_{1,k}\beta_1 + b_{2,k}\beta_2 + \dots + b_{s,k}\beta_s,$$

and the assumption of 3., that the functions β_l can be converted into functions of the module $\mathfrak{a}$ by multiplication by integral rational functions of z , is fulfilled, as one recognizes by solving this system of equations. At the same time $\mathfrak{a}$ itself is here the least common multiple of $\mathfrak{a}$ and $\mathfrak{b}$, and from this there results

$$(\mathfrak{b}, \mathfrak{a}) = \text{const. } \Sigma \pm b_{1,1}b_{2,2} \dots b_{n,n}.$$

7

5. If $\mathfrak{m}$ is the least common multiple of two modules $\mathfrak{a}$, $\mathfrak{b}$, and ν an arbitrary function in Ω , then, as follows without difficulty from the definition, $\nu\mathfrak{m}$ is the least common multiple of $\nu\mathfrak{a}$ and $\nu\mathfrak{b}$. If $(\mathfrak{b}, \mathfrak{a}) = 0$, then also $(\nu\mathfrak{b}, \nu\mathfrak{a}) = 0$. But if $(\mathfrak{b}, \mathfrak{a})$ and ν are different from zero, there results

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

if in 3. one replaces the basis functions μ_l, β_l of $\mathfrak{m}$ and $\mathfrak{b}$ by $\nu\mu_l, \nu\beta_l$.

§ 7. The ideals in $\mathfrak{o}$.

A system $\mathfrak{a}$ of *integral* functions of z in the field Ω is called an *ideal* if it fulfils the two following conditions:

- I. The sum and difference of any two functions in $\mathfrak{a}$ again yield a function in $\mathfrak{a}$.
- II. The product of each function in $\mathfrak{a}$ with each function in $\mathfrak{o}$ (§ 3) is again a function in $\mathfrak{a}$.

Every ideal is thus at the same time a module, and all the notions and notations explained for modules can be applied to ideals.

The module $\mathfrak{o}$ (the system of all integral functions of z) is itself an ideal, and *every ideal is divisible by $\mathfrak{o}$* . Likewise, if μ denotes an arbitrary function in $\mathfrak{o}$ different from zero, the module $\mathfrak{o}\mu$ (the system of all integral functions divisible by μ) is an ideal. Such an ideal shall be called a *principal ideal*. If $\omega_1, \omega_2, \dots, \omega_n$ is a basis of $\mathfrak{o}$, then

$$\mathfrak{o}\mu = [\omega_1\mu, \omega_2\mu, \dots, \omega_n\mu]$$

and $\mathfrak{o}\mu$ is the least common multiple of $\mathfrak{o}$ and $\mathfrak{o}\mu$. Therefore, by § 6, 4. and by the definition (4.) in § 2:

$$(\mathfrak{o}, \mathfrak{o}\mu) = \text{const. } N(\mu) \tag{1.}$$

⁷ *Editorial note:* Printed $b_{n,n}$ as the last diagonal term; the bases here have s members and the coefficients run to $b_{s,k}$, so $b_{s,s}$ is expected. An apparent misprint.

and consequently different from zero.

If $\mathfrak{a}$ is any ideal and α an arbitrary function in $\mathfrak{a}$, then (because of II.) the principal ideal $\mathfrak{o}\alpha$ is divisible by $\mathfrak{a}$, and consequently, by § 6, 2.:

$$(\mathfrak{o}, \mathfrak{o}\alpha) = (\mathfrak{o}, \mathfrak{a})(\mathfrak{a}, \mathfrak{o}\alpha), \quad (2.)$$

consequently $(\mathfrak{o}, \mathfrak{a})$ too is different from zero. Now since again $\mathfrak{a}$ is the least common multiple of $\mathfrak{a}$ and $\mathfrak{o}$, $\mathfrak{a}$ possesses, by § 6, 3., an irreducible basis consisting of n integral functions $\alpha_1, \alpha_2, \dots, \alpha_n$, which accordingly also form a basis of the field Ω .

The norm of $\mathfrak{a}$ with respect to $\mathfrak{o}$, i.e. the integral rational function $(\mathfrak{o}, \mathfrak{a})$ of z , shall be called the *norm of the ideal* $\mathfrak{a}$ and denoted by $N(\mathfrak{a})$. The degree of this integral rational function is at the same time called the *degree of the ideal* $\mathfrak{a}$.

If

$$\mathfrak{a} = [\alpha_1, \alpha_2, \dots, \alpha_n], \quad \mathfrak{o} = [\omega_1, \omega_2, \dots, \omega_n]$$

and

$$\alpha_1 = a_{1,1}\omega_1 + a_{2,1}\omega_2 + \dots + a_{n,1}\omega_n,$$

$$\alpha_2 = a_{1,2}\omega_1 + a_{2,2}\omega_2 + \dots + a_{n,2}\omega_n,$$

$$\dots\dots\dots$$

$$\alpha_n = a_{1,n}\omega_1 + a_{2,n}\omega_2 + \dots + a_{n,n}\omega_n$$

with integral rational coefficients $a_{i,j}$, then there results from § 6, 4.:

$$N(\mathfrak{a}) = \text{const.} \Sigma \pm a_{1,1}a_{2,2} \dots a_{n,n}. \quad (3.)$$

Since every function in $\mathfrak{o}$, hence also the function “1”, is converted into a function of the ideal $\mathfrak{a}$ by multiplication by $N(\mathfrak{a})$, $N(\mathfrak{a})$ is always a function in $\mathfrak{a}$.

The norm of the ideal $\mathfrak{o}$ is equal to 1, and conversely $\mathfrak{o}$ is the only ideal which has this property. Also $\mathfrak{o}$ is the only ideal which contains the function “1” (or a constant).

If α is a function in $\mathfrak{a}$, it follows from (1.), (2.), (3.):

$$N(\alpha) = \text{const.} N(\mathfrak{a})(\mathfrak{a}, \mathfrak{o}\alpha), \quad (4.)$$

i.e. the norm of every function contained in $\mathfrak{a}$ is divisible by the norm of $\mathfrak{a}$.

For congruences with respect to an ideal modulus the following theorem holds, which essentially distinguishes ideals from general modules.

If μ, μ_1, ν, ν_1 are functions in $\mathfrak{o}$ which satisfy the congruences

$$\mu \equiv \mu_1, \quad \nu \equiv \nu_1 \pmod{\mathfrak{a}},$$

then also

$$\mu\nu \equiv \mu_1\nu_1 \pmod{\mathfrak{a}}.$$

§ 8. Multiplication and division of ideals.

From the fundamental properties I., II. of ideals and from the definitions in § 4 there results first:

1. The least common multiple, the greatest common divisor, and the product of two (and hence also of arbitrarily many) ideals are themselves ideals. Likewise, if ν is a function in $\mathfrak{o}$ and $\mathfrak{a}$ an ideal, the product $\mathfrak{a}\nu$ is an ideal.

2. The product of several ideals is divisible by each of its factors, and for every ideal $\mathfrak{a}$

$$\mathfrak{a}\mathfrak{o} = \mathfrak{a};$$

for by I., II. every function in $\mathfrak{a}\mathfrak{o}$ is at the same time a function in $\mathfrak{a}$, and, since $\mathfrak{o}$ contains the function “1”, conversely every function in $\mathfrak{a}$ is at the same time a function in $\mathfrak{a}\mathfrak{o}$.

3. A principal ideal $\mathfrak{o}\mu$ is divisible by a principal ideal $\mathfrak{o}\nu$ if and only if the integral function μ is divisible by the integral function ν .

We add the following definitions:

4. *Definition.* A function α in $\mathfrak{o}$ shall be called *divisible* by the ideal $\mathfrak{a}$ if the principal ideal $\mathfrak{o}\alpha$ is divisible by $\mathfrak{a}$, or, what says the same thing, if α is a function in $\mathfrak{a}$.

5. *Definition.* Two ideals $\mathfrak{a}$, $\mathfrak{b}$ are called *relatively prime* if their greatest common divisor is $\mathfrak{o}$. The necessary and sufficient condition for this is that there exist in $\mathfrak{a}$ a function α , and in $\mathfrak{b}$ a function β , such that

$$\alpha + \beta = 1,$$

or, expressed otherwise, that there exists in $\mathfrak{a}$ a function satisfying the congruence $\alpha \equiv 1 \pmod{\mathfrak{b}}$, or in $\mathfrak{b}$ one satisfying the congruence $\beta \equiv 1 \pmod{\mathfrak{a}}$.

6. *Definition.* An ideal $\mathfrak{p}$ different from $\mathfrak{o}$ is called a *prime ideal* if no other ideal besides $\mathfrak{p}$ and $\mathfrak{o}$ goes into $\mathfrak{p}$.

On the basis of these definitions the following theorems on the divisibility of ideals now result.

7. If $\mathfrak{a}$, $\mathfrak{b}$ are two ideals with the least common multiple $\mathfrak{m}$ and the greatest common divisor $\mathfrak{d}$, then it follows from § 6, 1., 2.

$$\begin{aligned} N(\mathfrak{m}) &= N(\mathfrak{b})(\mathfrak{b}, \mathfrak{m}) = N(\mathfrak{b})(\mathfrak{b}, \mathfrak{a}), \\ N(\mathfrak{a}) &= N(\mathfrak{d})(\mathfrak{d}, \mathfrak{a}) = N(\mathfrak{d})(\mathfrak{b}, \mathfrak{a}), \end{aligned}$$

consequently $(\mathfrak{b}, \mathfrak{a})$ is different from zero and

$$N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{m})N(\mathfrak{d}).$$

8. If the ideal $\mathfrak{a}$ is divisible by the ideal $\mathfrak{b}$, then, by § 6, 2.

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

hence $N(\mathfrak{a})$ is divisible by $N(\mathfrak{b})$.

If in particular $(\mathfrak{b}, \mathfrak{a}) = 1$, then $\mathfrak{b}$ too is divisible by $\mathfrak{a}$, and it follows:

9. If $\mathfrak{a}$ is divisible by $\mathfrak{b}$ and at the same time $N(\mathfrak{a}) = N(\mathfrak{b})$, then $\mathfrak{a} = \mathfrak{b}$, i.e. the two ideals are identical.

10. If $\mathfrak{a}$ is divisible by $\mathfrak{a}_1$, and $\mathfrak{b}$ by $\mathfrak{b}_1$, then $\mathfrak{a}\mathfrak{b}$ is divisible by $\mathfrak{a}_1\mathfrak{b}_1$ (§ 4, 7.).

11. If an ideal $\mathfrak{a}$ is divisible by a principal ideal $\mathfrak{o}\mu$, then all functions in $\mathfrak{a}$ are of the form $\beta\mu$, and the totality of the functions β is again an ideal $\mathfrak{b}$, so that one can set

$$\mathfrak{a} = \mu\mathfrak{b}.$$

12. If μ is an arbitrary function in $\mathfrak{o}$ different from zero, and the ideal $\mathfrak{a}\mu$ divisible by the ideal $\mathfrak{b}\mu$, then $\mathfrak{a}$ is divisible by $\mathfrak{b}$, and from $\mathfrak{a}\mu = \mathfrak{b}\mu$ follows $\mathfrak{a} = \mathfrak{b}$.

13. The least common multiple of two ideals $\mathfrak{a}, \mathfrak{o}\nu$, of which one is a principal ideal, has by 11. the form $\mathfrak{r}\nu$, where $\mathfrak{r}$ is an ideal. Since on the other hand $\mathfrak{a}\nu$ is a common multiple of $\mathfrak{a}$ and $\mathfrak{o}\nu$, hence divisible by $\mathfrak{r}\nu$, $\mathfrak{r}$ is by 12. a divisor of $\mathfrak{a}$.

14. If $\mathfrak{a}$ is an ideal and ν a function in $\mathfrak{o}$, then by § 6, 2., 5.:

$$(\mathfrak{o}, \mathfrak{a}\nu) = (\mathfrak{o}, \mathfrak{o}\nu)(\mathfrak{o}\nu, \mathfrak{a}\nu) = (\mathfrak{o}, \mathfrak{o}\nu)(\mathfrak{o}, \mathfrak{a}),$$

hence

$$N(\mathfrak{a}\nu) = \text{const. } N(\mathfrak{a})N(\nu).$$

If therefore $\mathfrak{r}\nu$ is the least common multiple and $\mathfrak{d}$ the greatest common divisor of the two ideals $\mathfrak{a}, \mathfrak{o}\nu$, there results from 7.

$$N(\mathfrak{a}) = N(\mathfrak{r})N(\mathfrak{d}).$$

15. Every ideal $\mathfrak{a}$ different from $\mathfrak{o}$ is divisible by a prime ideal $\mathfrak{p}$.

For if $\mathfrak{a}$ is not a prime ideal, it has at least one proper divisor different from $\mathfrak{o}$, and among these let $\mathfrak{p}$ be one whose norm is of the lowest possible degree. This cannot have a proper divisor $\mathfrak{p}'$ different from $\mathfrak{o}$, for then $\mathfrak{p}'$ too would be a divisor of $\mathfrak{a}$, and at the same time (by 8.) $N(\mathfrak{p}')$ of lower degree than $N(\mathfrak{p})$. This contradicts the assumption about $\mathfrak{p}$, and consequently $\mathfrak{p}$ is a prime ideal.

16. If $\mathfrak{a}$ is relatively prime to $\mathfrak{b}$, then $\mathfrak{a}\mathfrak{b}$ is the least common multiple of $\mathfrak{a}$ and $\mathfrak{b}$, and consequently every ideal divisible by $\mathfrak{a}$ and by $\mathfrak{b}$ is also divisible by the product $\mathfrak{a}\mathfrak{b}$.

For by assumption there are in $\mathfrak{a}, \mathfrak{b}$ two functions α_1, β_1 such that

$$\alpha_1 + \beta_1 = 1$$

(5.). If on the other hand $\alpha = \beta$ is a function of the least common multiple $\mathfrak{m}$ of $\mathfrak{a}$ and $\mathfrak{b}$, then accordingly

$$\alpha = \beta = \alpha_1\beta + \alpha\beta_1,$$

hence a function in $\mathfrak{a}\mathfrak{b}$. Accordingly $\mathfrak{m}$ is divisible by $\mathfrak{a}\mathfrak{b}$, and since conversely (in consequence of 2.) $\mathfrak{a}\mathfrak{b}$ is divisible by $\mathfrak{m}$, $\mathfrak{m}$ is identical with $\mathfrak{a}\mathfrak{b}$, and from 7. it further follows for this case

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

17. If $\mathfrak{a}$ is an arbitrary ideal and $\mathfrak{p}$ a prime ideal, then either $\mathfrak{a}$ is divisible by $\mathfrak{p}$ or $\mathfrak{a}$ is relatively prime to $\mathfrak{p}$; for since $\mathfrak{p}$ has no other divisor than $\mathfrak{o}$ and $\mathfrak{p}$, the greatest common divisor of $\mathfrak{a}$ and $\mathfrak{p}$ too can be none other than $\mathfrak{o}$ or $\mathfrak{p}$.

18. If $\mathfrak{a}$ is relatively prime to $\mathfrak{b}$ and to $\mathfrak{c}$, then $\mathfrak{a}$ is also relatively prime to $\mathfrak{bc}$.

By assumption (5.) there are in $\mathfrak{b}, \mathfrak{c}$ two functions satisfying the congruences

$$\beta \equiv 1, \quad \gamma \equiv 1 \pmod{\mathfrak{a}}$$

consequently, by § 7,

$$\beta\gamma \equiv 1 \pmod{\mathfrak{a}}.$$

Since $\beta\gamma$ is contained in $\mathfrak{bc}$, the assertion is hereby proved.

It further follows from this that, if the product $\mathfrak{ab}$ is divisible by a prime ideal, at least one of the two factors $\mathfrak{a}, \mathfrak{b}$ must be divisible by $\mathfrak{p}$, and, applied to principal ideals, that if the product of two integral functions, $\mu\nu$, is contained in $\mathfrak{p}$, at least one of the two factors μ, ν must be contained in $\mathfrak{p}$.

19. If $\mathfrak{a}$ is relatively prime to $\mathfrak{c}$ and $\mathfrak{ab}$ divisible by $\mathfrak{c}$, then $\mathfrak{b}$ is divisible by $\mathfrak{c}$. By assumption there is in $\mathfrak{a}$ a function α which satisfies the congruence

$$\alpha \equiv 1 \pmod{\mathfrak{c}}.$$

Now if β is an arbitrary function in $\mathfrak{b}$, then accordingly

$$\beta \equiv \alpha\beta \quad \text{and by hyp.} \quad \equiv 0 \pmod{\mathfrak{c}},$$

consequently β is contained in $\mathfrak{c}$, hence $\mathfrak{b}$ divisible by $\mathfrak{c}$.

§ 9. Laws of divisibility of ideals.

All these theorems, which for the most part followed immediately from the definition of ideals, do not suffice to prove the complete analogy which prevails between the laws of divisibility of ideals and those of integral rational functions. In this proof we rely on the following theorem:

1. *If $\mathfrak{a}$ is an ideal and k an arbitrary integral rational function of z , then a function α can be selected in $\mathfrak{a}$ such that $(\mathfrak{a}, \mathfrak{o}\alpha)$ has no divisor in common with k^* .*

For if

$$\begin{aligned} \mathfrak{a} &= [\alpha_1, \alpha_2, \dots, \alpha_n], \\ \mathfrak{o} &= [\omega_1, \omega_2, \dots, \omega_n], \end{aligned}$$

and α is an arbitrary function in $\mathfrak{a}$, then the integral rational functions $x_{h,k}$ can be determined such that

$$\begin{aligned} \alpha\omega_1 &= x_{1,1}\alpha_1 + x_{2,1}\alpha_2 + \dots + x_{n,1}\alpha_n, \\ \alpha\omega_2 &= x_{1,2}\alpha_1 + x_{2,2}\alpha_2 + \dots + x_{n,2}\alpha_n, \\ &\dots\dots\dots \\ \alpha\omega_n &= x_{1,n}\alpha_1 + x_{2,n}\alpha_2 + \dots + x_{n,n}\alpha_n, \end{aligned}$$

and (§ 6, 4.)

$$(\mathfrak{a}, \mathfrak{o}\alpha) = \text{const. } \Sigma \pm x_{1,1}x_{2,2} \dots x_{n,n}.$$

Now if $\Sigma \pm x_{1,1}x_{2,2} \dots x_{n,n}$ is divisible by a linear factor $z - c$ of k , then a function ω in $\mathfrak{o}$ not divisible by $z - c$ and a function α' in $\mathfrak{a}$ can be determined such that

$$\alpha\omega = (z - c)\alpha'^{**}).$$

If one now sets, understanding by t an indeterminate constant:

$$t(z - c) - \omega = \omega',$$

then

$$N(\omega') = t^n(z - c)^n + a_1 t^{n-1}(z - c)^{n-1} + \dots + a_{n-1}t(z - c) + a_n,$$

where the coefficients $a_1, a_2, \dots, a_n$, independent of t , are integral rational functions of z . Now it cannot be that at the same time a_1 is divisible by $z - c$, a_2 by $(z - c)^2$, $\dots$, a_n by $(z - c)^n$, because otherwise, contrary to the assumption, $\frac{\omega}{z - c}$ would be an integral function (§ 2, 5., § 3, 4.). Therefore not

*) The possibility of proving this theorem already at this point essentially distinguishes the theory of algebraic functions from that of algebraic numbers, and permits in the former a not inconsiderable simplification in comparison with the latter.

**) For if the determinant $\Sigma \pm x_{1,1}x_{2,2} \dots x_{n,n}$ is divisible by $z - c$, i.e. vanishes for $z = c$, then one can determine a system of constants $c_1, c_2, \dots, c_n$, not all vanishing, such that the integral rational functions

$$c_1 x_{k,1} + c_2 x_{k,2} + \dots + c_k x_{k,n} \quad (k=1, 2 \dots n)$$

⁸ vanish for $z = c$, hence are divisible by $z - c$, and one then has to set

$$\omega = c_1 \omega_1 + c_2 \omega_2 + \dots + c_n \omega_n$$

all the terms of $N(\omega')$ can be divided by $(z - c)^n$, and if therefore $(z - c)^{n-r}$ is the highest power of $z - c$ by which they are divisible, then $r \geq 0$ and

$$\frac{N(\omega')}{(z - c)^{n-r}} = t^n(z - c)^r + b_1 t^{n-1} + \dots + b_{n-1}t + b_n = f(t),$$

where the integral rational functions $b_1, b_2, \dots, b_n$ do not all vanish for $z = c$. There is therefore only a finite number of constant values t for which $f(t)$ is divisible by $z - c$. If $z - c'$ is a linear factor of k different from $z - c$, then $f(t)$ likewise becomes divisible by $z - c'$ only for a finite number of values t . From this it follows that one can dispose of t in such a way that $N(\omega')$ becomes

⁸ Editorial note: Printed $c_k x_{k,n}$ as the last term; the sum runs over $c_1, c_2, \dots, c_n$, so $c_n x_{k,n}$ is expected. An apparent misprint.

divisible neither by $(z - c)^n$ nor at the same time by any other linear factor of k^*). If, when this has been done, one sets

$$t\alpha - \alpha' = \alpha'',$$

which is likewise a function in $\mathfrak{a}$, it follows

$$\begin{aligned}\alpha\omega' &= (z - c)\alpha'', \\ N(\alpha'') &= \frac{N(\alpha)N(\omega')}{(z - c)^n}\end{aligned}$$

and consequently, since by § 7, (4.)

$$(\mathfrak{a}, \mathfrak{o}\alpha) = \text{const.} \frac{N(\alpha)}{N(\mathfrak{a})}$$

holds:

$$(\mathfrak{a}, \mathfrak{o}\alpha'') = \text{const.} \frac{(\mathfrak{a}, \mathfrak{o}\alpha)N(\omega')}{(z - c)^n}.$$

The function $(\mathfrak{a}, \mathfrak{o}\alpha'')$ therefore contains the factor $z - c$ at least once fewer than $(\mathfrak{a}, \mathfrak{o}\alpha)$, while at the same time it contains no other linear factor of k more often than $(\mathfrak{a}, \mathfrak{o}\alpha)$. By repeated application of this procedure the correctness of the stated theorem results.

2. Every ideal $\mathfrak{a}$ can be represented as the greatest common divisor of two principal ideals $\mathfrak{o}\mu$, $\mathfrak{o}\nu$, of which one may be assumed quite arbitrarily, only divisible by $\mathfrak{a}$.

Proof. Choose at pleasure in $\mathfrak{a}$ a function ν different from zero, and a second function μ such that the two functions $(\mathfrak{a}, \mathfrak{o}\nu)$ and $(\mathfrak{a}, \mathfrak{o}\mu)$ have no common divisor (by 1). Now if α is an arbitrary function in $\mathfrak{a}$, then by § 6 $(\mathfrak{a}, \mathfrak{o}\mu)\alpha$ is contained in $\mathfrak{o}\mu$ and $(\mathfrak{a}, \mathfrak{o}\nu)\alpha$ in $\mathfrak{o}\nu$, so that there are two functions ω , ω' in $\mathfrak{o}$ for which

$$(\mathfrak{a}, \mathfrak{o}\mu)\alpha = \mu\omega, \quad (\mathfrak{a}, \mathfrak{o}\nu)\alpha = \nu\omega'.$$

*) These inferences no longer hold in the analogous question of the theory of numbers.

If therefore one chooses, as is possible by the assumption about $(\mathfrak{a}, \mathfrak{o}\mu)$, $(\mathfrak{a}, \mathfrak{o}\nu)$, two integral rational functions g , h of z which satisfy the condition

$$g(\mathfrak{a}, \mathfrak{o}\mu) + h(\mathfrak{a}, \mathfrak{o}\nu) = 1,$$

it follows

$$\alpha = g\mu\omega + h\nu\omega',$$

i.e. $\mathfrak{a}$ is divisible by the greatest common divisor of $\mathfrak{o}\mu$ and $\mathfrak{o}\nu$. And since the latter conversely is divisible by $\mathfrak{a}$ (because $\mathfrak{o}\mu$ and $\mathfrak{o}\nu$ are divisible by $\mathfrak{a}$), it is equal to $\mathfrak{a}$, q. e. d.

3. Every ideal $\mathfrak{a}$ can be converted by multiplication by an ideal $\mathfrak{m}$ into a principal ideal $\mathfrak{o}\mu = \mathfrak{a}\mathfrak{m}$.

Proof. Choose (by 1.) in $\mathfrak{a}$ a function μ such that $(\mathfrak{a}, \mathfrak{o}\mu)$ has no divisor in common with $N(\mathfrak{a})$, and thereupon a second function ν such that $(\mathfrak{a}, \mathfrak{o}\nu)$ has no divisor in common with $(\mathfrak{a}, \mathfrak{o}\mu)$. Then (by 2.) $\mathfrak{a}$ is the greatest common divisor of $\mathfrak{o}\mu$ and $\mathfrak{o}\nu$. The least common multiple of $\mathfrak{o}\mu$ and $\mathfrak{o}\nu$ is (by § 8, 13) of the form $\mathfrak{m}\nu$, where $\mathfrak{m}$ is a divisor of $\mathfrak{o}\mu$. By § 8, 14 we then have

$$N(\mathfrak{m}) = \frac{N(\mathfrak{o}\mu)}{N(\mathfrak{a})} = (\mathfrak{a}, \mathfrak{o}\mu),$$

hence, by assumption, without a common divisor with $N(\mathfrak{a})$. If therefore one again determines two integral rational functions g, h of z such that

$$gN(\mathfrak{m}) + hN(\mathfrak{a}) = 1,$$

then it follows from § 8, 5, since $N(\mathfrak{m})$ is contained in $\mathfrak{m}$ and $N(\mathfrak{a})$ in $\mathfrak{a}$, that $\mathfrak{m}$ and $\mathfrak{a}$ are relatively prime ideals, and from this, by § 8, 16.

$$N(\mathfrak{m}\mathfrak{a}) = N(\mathfrak{m})N(\mathfrak{a}) = N(\mathfrak{o}\mu).$$

Now since $\mathfrak{o}\mu$ is divisible by $\mathfrak{m}$ and by $\mathfrak{a}$, hence also by $\mathfrak{m}\mathfrak{a}$ (§ 8, 16.), by § 8, 9.

$$\mathfrak{m}\mathfrak{a} = \mathfrak{o}\mu,$$

q. e. d.*)

4. If an ideal $\mathfrak{c}$ is divisible by an ideal $\mathfrak{a}$, there is one and *only* one ideal $\mathfrak{b}$ which satisfies the condition

$$\mathfrak{a}\mathfrak{b} = \mathfrak{c}$$

and which is called the *quotient of $\mathfrak{c}$ by $\mathfrak{a}$* .

*) One can at the same time choose the ideal $\mathfrak{m}$ such that it becomes relatively prime to an arbitrary ideal $\mathfrak{b}$. This is achieved if one takes the function μ such that $(\mathfrak{a}, \mathfrak{o}\mu) = N(\mathfrak{m})$ has no divisor in common with $N(\mathfrak{a})N(\mathfrak{b})$ (§ 8, 8.).

If $\mathfrak{a}\mathfrak{b}$ is divisible by $\mathfrak{a}\mathfrak{b}'$, then $\mathfrak{b}$ is divisible by $\mathfrak{b}'$, and from $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}'$ follows $\mathfrak{b} = \mathfrak{b}'$.

Proof. Let $\mathfrak{c}$ be divisible by $\mathfrak{a}$ and (by 3.) $\mathfrak{a}\mathfrak{m} = \mathfrak{o}\mu$. Then $\mathfrak{c}\mathfrak{m}$ too is divisible by $\mathfrak{a}\mathfrak{m} = \mathfrak{o}\mu$, and consequently $\mathfrak{c}\mathfrak{m} = \mathfrak{b}\mu$ (§ 8, 10., 11.); hence, by multiplication of the last equation by $\mathfrak{a}$,

$$\mathfrak{c}\mu = \mathfrak{a}\mathfrak{b}\mu$$

and by § 8, 12.

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

whereby the first part of the theorem is proved*).

Further, if $\mathfrak{a}\mathfrak{b}$ is divisible by $\mathfrak{a}\mathfrak{b}'$, then (§ 8, 10.) $\mu\mathfrak{b}$ is divisible by $\mu\mathfrak{b}'$, hence $\mathfrak{b}$ by $\mathfrak{b}'$. — If $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}'$, then $\mu\mathfrak{b} = \mu\mathfrak{b}'$ follows, and consequently $\mathfrak{b} = \mathfrak{b}'$ (§ 8, 12.).

5. Every ideal different from $\mathfrak{o}$ is either a prime ideal, or it can be represented, and in only one way, as a product of prime ideals alone.

Proof. If the ideal $\mathfrak{a}$ is different from $\mathfrak{o}$, it is (§ 8, 15.) divisible by a prime ideal $\mathfrak{p}_1$, and consequently (by 4.) $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1$, where $\mathfrak{a}_1$ is a *proper* divisor of $\mathfrak{a}$ (for

from $\mathfrak{a}_1 = \mathfrak{a}$ it would follow by 4. that $\mathfrak{p}_1 = \mathfrak{o}$). Hence the degree of $N(\mathfrak{a}_1)$ is lower than that of $N(\mathfrak{a})$. If $\mathfrak{a}_1$ is different from $\mathfrak{o}$, one infers in the same way that $\mathfrak{a}_1 = \mathfrak{p}_2 \mathfrak{a}_2$ must hold, where the degree of $N(\mathfrak{a}_2)$ is again lower than that of $N(\mathfrak{a}_1)$. Continuing in this way, one finally arrives, after a finite number of decompositions, at an ideal $\mathfrak{a}_{r-1} = \mathfrak{p}_r \mathfrak{a}_r$ such that $N(\mathfrak{a}_r) = 1$, hence $\mathfrak{a}_r = \mathfrak{o}$. Therefore

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r.$$

If such a decomposition were possible in a second way, say

$$\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_1 \mathfrak{q}_2 \dots \mathfrak{q}_s,$$

then (§ 8, 18.) of the prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$ at least one, say $\mathfrak{p}_1$, would have to be divisible by $\mathfrak{q}_1$ and hence $= \mathfrak{q}_1$, hence by 4.

$$\mathfrak{p}_2 \mathfrak{p}_3 \dots \mathfrak{p}_r = \mathfrak{q}_2 \mathfrak{q}_3 \dots \mathfrak{q}_s.$$

From this one infers in the same way $\mathfrak{p}_2 = \mathfrak{q}_2$, and so on.

If in the decomposition thus obtained one combines the prime ideals equal to one another into powers, one can set

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_r^{e_r}.$$

*) This definition of the quotient of two ideals agrees completely with the one given in § 4, 8.

Any divisor $\mathfrak{a}_l$ of $\mathfrak{a}$ can then be divisible by no prime ideal different from $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$, and by none more often than $\mathfrak{a}$. One therefore obtains all the divisors of $\mathfrak{a}$, whose number is finite and $= (e_1 + 1)(e_2 + 1) \dots (e_r + 1)$, if in

$$\mathfrak{p}_1^{h_1} \mathfrak{p}_2^{h_2} \dots \mathfrak{p}_r^{h_r}$$

one lets the exponents h_i run through the series of numbers $0, 1, 2, \dots, e_i$ (where by $\mathfrak{p}^0$ the ideal $\mathfrak{o}$ is to be understood). If $\mathfrak{a}, \mathfrak{b}$ are two ideals

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_r^{e_r}; \quad \mathfrak{b} = \mathfrak{p}_1^{f_1} \mathfrak{p}_2^{f_2} \dots \mathfrak{p}_r^{f_r}$$

(where some of the exponents e, f may also be zero), then one obtains the greatest common divisor and the least common multiple of $\mathfrak{a}$ and $\mathfrak{b}$ in the form

$$\mathfrak{p}_1^{g_1} \mathfrak{p}_2^{g_2} \dots \mathfrak{p}_r^{g_r},$$

if for $g_1, g_2, \dots, g_r$ one takes, for the former the smallest, for the latter the greatest, among the numbers $e_1, f_1; e_2, f_2; \dots, e_r, f_r$.

6. If $\mathfrak{a}, \mathfrak{b}$ are any two ideals, then in general

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

Proof. Let, as in 5., $\mathfrak{a} = \mathfrak{p}_1 \mathfrak{a}_1$; then, because $\mathfrak{a}_1$ is a proper divisor of $\mathfrak{a}$, there is in $\mathfrak{a}_1$ a function η not divisible by $\mathfrak{a}$. The least common multiple and the

greatest common divisor of $\mathfrak{a}$ and $\mathfrak{o}\eta$ are respectively $\mathfrak{p}_1\eta$ and $\mathfrak{a}_1$, as follows at once (by 5.) from the decomposition of $\mathfrak{a}$ and $\mathfrak{o}\eta$ into their prime factors. But from this it follows by § 8, 14.

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)N(\mathfrak{a}_1).$$

By repetition of the same inference for $\mathfrak{a}_1$, and so on, there results, if $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$:

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)N(\mathfrak{p}_2) \dots N(\mathfrak{p}_r)$$

and from this

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

7. Every prime ideal is an ideal *of the first degree* (§ 7), and conversely, every ideal of the first degree is a prime ideal^{*)}.

Proof. If $\mathfrak{p}$ is a prime ideal, then $N(\mathfrak{p})$ is divisible by $\mathfrak{p}$, and therefore at least one of the linear factors of $N(\mathfrak{p})$, say $z - c$, is divisible by $\mathfrak{p}$

^{*)} By this theorem the theory of algebraic functions differs essentially from the analogous theory of algebraic numbers.

(§ 8, 18.). If ω is an arbitrary function in $\mathfrak{o}$ which satisfies the equation:

$$\omega^n + a_1\omega^{n-1} + \dots + a_{n-1}\omega + a_n = 0,$$

then one obtains from it, by reducing the integral rational functions $a_1, a_2, \dots, a_n$ to their constant remainders $a_1^{(0)}, a_2^{(0)}, \dots, a_n^{(0)}$ with respect to $z - c$, and decomposing the integral function

$$\omega^n + a_1^{(0)}\omega^{n-1} + \dots + a_{n-1}^{(0)}\omega + a_n^{(0)}$$

into its linear factors $(\omega - b_1), (\omega - b_2), \dots, (\omega - b_n)$:

$$(\omega - b_1)(\omega - b_2) \dots (\omega - b_n) = (z - c)\omega' \equiv 0 \pmod{\mathfrak{p}}.$$

Hence at least one of the factors $\omega - b_1, \omega - b_2, \dots$ must be divisible by $\mathfrak{p}$, i.e.

$$\omega \equiv b \pmod{\mathfrak{p}},$$

where b denotes a constant. Since accordingly every function in $\mathfrak{o}$ is congruent to a constant $\pmod{\mathfrak{p}}$, by § 6 $(\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p}) = z - c$ is a *linear* function of z , whereby the first part of the assertion is proved.

Conversely: if $\mathfrak{q}$ is an ideal of the first degree, and

$$N(\mathfrak{q}) = z - c,$$

then $\mathfrak{q}$ is certainly divisible by a prime ideal $\mathfrak{p}$, and since $N(\mathfrak{q})$ is divisible by $N(\mathfrak{p})$, $N(\mathfrak{p}) = N(\mathfrak{q}) = z - c$, hence (§ 8, 9.)

$$\mathfrak{p} = \mathfrak{q}.$$

It follows from this that the degree of an ideal is equal to the number of prime factors into which it can be decomposed. If therefore

$$\mathfrak{o}(z - c) = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \mathfrak{p}_3^{e_3} \dots,$$

then

$$e_1 + e_2 + e_3 + \dots = n.$$

It follows further that an integral *rational* function of z is divisible by a prime ideal $\mathfrak{p}$ if and only if it is divisible by the norm of $\mathfrak{p}$.

§ 10. The complementary bases of the field Ω .

1. *Definition.* If the functions $\alpha_1, \alpha_2, \dots, \alpha_n$ form a basis of Ω , and one sets for brevity

$$S(\alpha_r \alpha_s) = a_{r,s} = a_{s,r},$$

$$\Delta(\alpha_1, \alpha_2, \dots, \alpha_n) = \Sigma \pm a_{1,1} a_{2,2} \dots a_{n,n} = a \quad (\S 2),$$

then, since a is different from zero, a completely determined system of functions $\alpha'_1, \alpha'_2, \dots, \alpha'_n$ can be determined from the linear equations

$$\alpha_r = \sum_{1,n}^l a_{r,l} \alpha'_l, \quad (1.)$$

and since

$$\Delta(\alpha'_1, \alpha'_2, \dots, \alpha'_n) = \frac{1}{a}$$

is different from zero, the functions $\alpha'_1, \alpha'_2, \dots, \alpha'_n$ likewise form a basis of Ω . This shall be called the *complementary basis* to $\alpha_1, \alpha_2, \dots, \alpha_n$.

2. If, when the indices r, s belong to the series of numbers $1, 2, \dots, n$, one denotes by (r, s) the number 1 or 0 according as r, s are equal or different, then

$$S(\alpha_r \alpha'_s) = (r, s), \quad (2.)$$

for by solving the equations (1.) it follows

$$\alpha'_s = \sum_{1,n}^l a'_{l,s} \alpha_l;$$

$$a'_{r,s} = a'_{s,r}; \quad \sum_{1,n}^l a_{r,l} a'_{l,s} = (r, s),$$

and from this:

$$\alpha_r \alpha'_s = \sum_{1,n}^l a'_{l,s} \alpha_l \alpha_r; \quad S(\alpha_r \alpha'_s) = \sum_{1,n}^l a'_{l,s} a_{l,r} = (r, s).$$

If conversely a system of functions β_s satisfies the conditions $S(\alpha_r \beta_s) = (r, s)$, then $\beta_s = \alpha'_s$; for if one sets $\beta_s = \sum_{1,n}^l b_{l,s} \alpha'_l$, it follows because of (2.)

$$b_{r,s} = S(\beta_s \alpha_r) = (r, s).$$

From this it follows immediately that the relation of the α_i to the α'_i is a reciprocal one, i.e. that the basis $\alpha_1, \alpha_2, \dots, \alpha_n$ is complementary to $\alpha'_1, \alpha'_2, \dots, \alpha'_n$.

3. If η is an arbitrary function in Ω , one can always set

$$\eta = \sum x_i \alpha_i = \sum x'_i \alpha'_i,$$

and by application of (2.) it follows:

$$x_i = S(\eta \alpha'_i), \quad x' = S(\eta \alpha_i),$$

⁹ hence:

$$\eta = \sum \alpha_i S(\eta \alpha'_i) = \sum \alpha'_i S(\eta \alpha_i). \quad (3.)$$

4. If η is an arbitrary function in Ω different from zero, then

$$\frac{\alpha'_1}{\eta}, \frac{\alpha'_2}{\eta}, \dots, \frac{\alpha'_n}{\eta}$$

is the complementary basis to $\eta \alpha_1, \eta \alpha_2, \dots, \eta \alpha_n$. This follows from 2. because of

$$S\left(\eta \alpha_r \cdot \frac{\alpha'_s}{\eta}\right) = S(\alpha_r \alpha'_s) = (r, s).$$

5. If two bases of Ω , $\alpha_1, \alpha_2, \dots, \alpha_n$ and $\beta_1, \beta_2, \dots, \beta_n$, are connected by the n equations

$$\beta_s = \sum x_{i,s} \alpha_i$$

with rational coefficients $x_{i,s}$, then the bases complementary to them are connected by the n equations

$$\alpha'_r = \sum x_{r,i} \beta'_i$$

(transposed substitution). This is an immediate consequence of 3. because of

$$x_{r,s} = S(\alpha'_r \beta_s).$$

6. We have

$$\sum \alpha_i \alpha'_i = 1,$$

hence:

$$\sum_{i,i'} a_{i,i'} \alpha'_i \alpha'_{i'} = \sum_{i,i'} a'_{i,i'} \alpha_i \alpha_{i'} = 1.$$

For if one first sets

$$\sum \alpha_i \alpha_{i'} = \sigma,$$

¹⁰ then it follows from 3. (applied to the functions $\eta \alpha_r$),

$$\eta \alpha_r = \sum \alpha_i S(\eta \alpha_r \alpha'_i),$$

⁹ Editorial note: Printed x' without a subscript; x'_i is meant, as in the line above.

¹⁰ Editorial note: Printed $\alpha_i \alpha_{i'}$; the argument requires $\alpha_i \alpha'_i$, as in the first formula of 6. The prime appears to have been set on the subscript.

consequently, by the definition of the trace in § 2, (5.)

$$S(\eta) = \overset{\iota}{\Sigma} S(\eta \alpha_{\iota} \alpha'_{\iota}) = S(\Sigma \eta \alpha_{\iota} \alpha'_{\iota}),$$

hence:

$$S(\eta \sigma) = S(\eta),$$

and from this, if in 3. one sets first $\eta = \sigma$, then $\eta = 1$:

$$\sigma = \overset{\iota}{\Sigma} \alpha_{\iota} S(\sigma \alpha'_{\iota}) = \overset{\iota}{\Sigma} \alpha_{\iota} S(\alpha'_{\iota}) = 1.$$

We go somewhat more closely into the formation of the complementary bases in two special cases:

7. Let $\omega_1, \omega_2, \dots \omega_n$ be a basis of $\mathfrak{o}$ and $\varepsilon_1, \varepsilon_2, \dots \varepsilon_n$ the complementary basis (of Ω). Let

$$e_{r,s} = e_{s,r} = S(\omega_r \omega_s),$$

which are *integral* rational functions, and

$$D = \text{const. } \Sigma \pm e_{1,1} e_{2,2} \dots e_{n,n}$$

the discriminant of Ω ; then by 2.

$$\varepsilon_r = \frac{1}{D} \overset{\iota}{\Sigma} \frac{\partial D}{\partial e_{\iota,r}} \omega_{\iota},$$

from which it emerges that the functions $D \varepsilon_r$ belong to the *integral functions*. But from 6. it follows further

$$D = \overset{\iota, \iota'}{\Sigma} \frac{\partial D}{\partial e_{\iota, \iota'}} \omega_{\iota} \omega_{\iota'}$$

and from this

$$\begin{aligned} \varepsilon_r \varepsilon_s &= \frac{1}{D^2} \overset{\iota, \iota'}{\Sigma} \frac{\partial D}{\partial e_{r, \iota}} \frac{\partial D}{\partial e_{s, \iota'}} \omega_{\iota} \omega_{\iota'} \\ &= \frac{1}{D} \frac{\partial D}{\partial e_{r,s}} + \frac{1}{D^2} \overset{\iota, \iota'}{\Sigma} \left(\frac{\partial D}{\partial e_{r, \iota}} \frac{\partial D}{\partial e_{s, \iota'}} - \frac{\partial D}{\partial e_{r,s}} \frac{\partial D}{\partial e_{\iota, \iota'}} \right) \omega_{\iota} \omega_{\iota'} \end{aligned}$$

and from this, by a known theorem on determinants:

$$\varepsilon_r \varepsilon_s = \frac{1}{D} \frac{\partial D}{\partial e_{r,s}} + \frac{1}{D} \overset{\iota, \iota'}{\Sigma} \frac{\partial^2 D}{\partial e_{r, \iota} \partial e_{s, \iota'}} \omega_{\iota} \omega_{\iota'},$$

from which follows the important result that the functions $D \varepsilon_r \varepsilon_s$ too belong to the *integral functions*.

8. Let θ be a function in Ω such that $1, \theta, \theta^2, \dots \theta^{n-1}$ form a basis of Ω , and let therefore

$$f(\theta) = \theta^n + a_1 \theta^{n-1} + \dots + a_{n-1} \theta + a_n = 0 \quad (4.)$$

be irreducible, with rational coefficients a . The complementary basis to $1, \theta, \theta^2, \dots, \theta^{n-1}$ is to be found. Let us set, where t denotes an indeterminate constant,

$$\frac{f(t)}{t - \theta} = \eta_0 + \eta_1 t + \eta_2 t^2 + \dots + \eta_{n-1} t^{n-1},$$

hence:

$$\begin{cases} \eta_0 = a_{n-1} + a_{n-2}\theta + \dots + a_1\theta^{n-2} + \theta^{n-1}, \\ \eta_1 = a_{n-2} + a_{n-3}\theta + \dots + \theta^{n-2}, \\ \dots\dots\dots \\ \eta_{n-2} = a_1 + \theta, \\ \eta_{n-1} = 1, \end{cases} \quad (5.)$$

then the functions $\eta_0, \eta_1, \dots, \eta_{n-1}$ likewise form a basis of Ω , since the determinant of the equations (5.) is $(-1)^{\frac{1}{2}n(n-1)}$, hence different from zero. Every function ζ in Ω can therefore be represented in the form

$$\zeta = y_0\eta_0 + y_1\eta_1 + \dots + y_{n-1}\eta_{n-1}.$$

We now continue the series of rational functions $y_0, y_1, \dots, y_{n-1}$ by determining the functions $y_n, y_{n+1}, \dots$ through the recursion

$$a_n y_r + a_{n-1} y_{r+1} + \dots + a_2 y_{r+n-2} + a_1 y_{r+n-1} + y_{r+n} = 0. \quad (6.)$$

Now by (5.)

$$\begin{cases} \theta\eta_0 = -a_n\eta_{n-1}, \\ \theta\eta_1 = \eta_0 - a_{n-1}\eta_{n-1}, \\ \theta\eta_2 = \eta_1 - a_{n-2}\eta_{n-1}, \\ \dots\dots\dots \\ \theta\eta_{n-1} = \eta_{n-2} - a_1\eta_{n-1}, \end{cases} \quad (7.)$$

hence

$$\zeta\theta = y_1\eta_0 + y_2\eta_1 + \dots + y_{n-1}\eta_{n-2} + y_n\eta_{n-1},$$

and likewise in general for every positive integer r :

$$\zeta\theta^r = y_r\eta_0 + y_{r+1}\eta_1 + \dots + y_{r+n-2}\eta_{n-2} + y_{r+n-1}\eta_{n-1},$$

or, if one expresses $\eta_0, \eta_1, \dots, \eta_{n-1}$ by $1, \theta, \theta^2, \dots, \theta^{n-1}$:

$$\zeta\theta^r = x_0^{(r)} + x_1^{(r)}\theta + x_2^{(r)}\theta^2 + \dots + x_{n-1}^{(r)}\theta^{n-1},$$

where

$$\begin{aligned} x_0^{(r)} &= y_r a_{n-1} + y_{r+1} a_{n-2} + \dots + y_{r+n-2} a_1 + y_{r+n-1}, \\ x_1^{(r)} &= y_r a_{n-2} + y_{r+1} a_{n-3} + \dots + y_{r+n-2}, \\ &\dots\dots\dots \\ x_{n-2}^{(r)} &= y_r a_1 + y_{r+1}, \\ x_{n-1}^{(r)} &= y_r. \end{aligned}$$

Consequently (by the definition of S , § 2 (5.))

$$\begin{aligned} S(\zeta) &= x_0^{(0)} + x_1^{(1)} + x_2^{(2)} + \cdots + x_{n-1}^{(n-1)} \\ &= y_0 a_{n-1} + 2y_1 a_{n-2} + \cdots + (n-1)y_{n-2} a_1 + n y_{n-1}, \end{aligned}$$

hence, applied to $\zeta = \eta_r$:

$$S(\eta_r) = (r+1)a_{n-1-r}; \quad S(\eta_{n-1-r}) = (n-r)a_r,$$

where $a_0 = 1$ is to be set.

If one therefore sets for brevity

$$S(\theta^r) = s_r,$$

it follows, as long as $r \leq n$, by means of (5.)

$$(n-r)a_r = a_r s_0 + a_{r-1} s_1 + \cdots + a_1 s_{r-1} + s_r \quad (8.)$$

and by (4.) in general

$$0 = a_n s_r + a_{n-1} s_{r+1} + \cdots + a_1 s_{r+n-1} + s_{r+n}. \quad (9.)$$

But from these formulae it follows further:

$$\begin{cases} f'(\theta) = n\theta^{n-1} + (n-1)a_1\theta^{n-1} + \cdots + 2a_{n-2}\theta + a_{n-1} \\ \quad = s_0\eta_0 + s_1\eta_1 + \cdots + s_{n-1}\eta_{n-1}, \\ \theta^r f'(\theta) = s_r\eta_0 + s_{r+1}\eta_1 + \cdots + s_{r+n-2}\eta_{n-2} + s_{r+n-1}\eta_{n-1}. \end{cases} \quad (10.)$$

11

If one now takes into account the value of the determinant of the system of equations (5.), then from this, with regard to the definition of the norm and of the discriminant in § 2 (4.) and (12.), there follows the important formula

$$Nf'(\theta) = (-1)^{\frac{1}{2}n(n-1)} \begin{vmatrix} s_0, & s_1, & \cdots & s_{n-1} \\ s_1, & s_2, & \cdots & s_n \\ \cdots & \cdots & \cdots & \cdots \\ s_{n-1}, & s_n, & \cdots & s_{2n-2} \end{vmatrix} = (-1)^{\frac{1}{2}n(n-1)} \Delta(1, \theta, \theta^2, \dots, \theta^{n-1}). \quad (11.)$$

But the equations (10.), with regard to the definition 1., also yield the complementary basis to $1, \theta, \theta^2, \dots, \theta^{n-1}$:

$$\frac{\eta_0}{f'(\theta)}, \frac{\eta_1}{f'(\theta)}, \dots, \frac{\eta_{n-1}}{f'(\theta)}.$$

9. If $\mathfrak{a} = [\alpha_1, \alpha_2, \dots, \alpha_n]$ denotes a module whose basis is at the same time a basis of Ω , then from the basis of Ω complementary to $\alpha_1, \alpha_2, \dots, \alpha_n$,

¹¹ *Editorial note:* In the first line of (10.) the print sets $(n-1)a_1\theta^{n-1}$; the derivative requires θ^{n-2} . An apparent misprint.

$\alpha'_1, \alpha'_2, \dots, \alpha'_n$, one obtains another module $\mathfrak{a}' = [\alpha'_1, \alpha'_2, \dots, \alpha'_n]$, which is called the *complementary module* to $\mathfrak{a}$. It is, as follows at once from 5. in connection with § 4, 2., independent of the choice of the basis of $\mathfrak{a}$.

10. We consider in particular the module $\mathfrak{e} = [\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n]$ complementary to $\mathfrak{o} = [\omega_1, \omega_2, \dots, \omega_n]$. If we set

$$\omega_r \omega_s = \sum_{\iota}^{\iota} e_{r,s}^{(\iota)} \omega_{\iota},$$

then by 3.

$$e_{r,s}^{(\iota)} = e_{s,r}^{(\iota)} = S(\omega_r \omega_s \varepsilon_{\iota})$$

is an integral rational function of z , and it follows:

$$\omega_r \varepsilon_s = \sum_{\iota}^{\iota} e_{r,\iota}^{(s)} \varepsilon_{\iota}.$$

From this it results that the module $\mathfrak{o}\mathfrak{e}$ (§ 4, 7.) is divisible by $\mathfrak{e}$; on the other hand, because $\mathfrak{o}$ contains the function 1, $\mathfrak{e}$ is divisible by $\mathfrak{o}\mathfrak{e}$, hence

$$\mathfrak{o}\mathfrak{e} = \mathfrak{e},$$

i.e. the module $\mathfrak{e}$, which, it is true, does not contain merely integral functions, possesses the characteristic property II. § 7 of ideals. The same consequently holds also of the module $\mathfrak{e}^2$. Since the two modules $D\mathfrak{e}$, $D\mathfrak{e}^2$ contain by 7. only integral functions, they are ideals, and from 7. there further results

$$N(D\mathfrak{e}) = D^{n-1}.$$

11. If θ is a function in $\mathfrak{o}$ of such a kind that $1, \theta, \theta^2, \dots, \theta^{n-1}$ forms a basis of Ω , so that in the irreducible equation

$$f(\theta) = \theta^n + a_1 \theta^{n-1} + \dots + a_{n-1} \theta + a_n = 0$$

the coefficients are *integral* rational functions of z , then for $r = 0, 1, 2, \dots, n-1$ one can determine the integral rational functions $k_{\iota}^{(r)}$ such that

$$\theta^r = \sum_{1,n}^{\iota} k_{\iota}^{(r)} \omega_{\iota}$$

holds. If one applies to this the theorems 5. and 8., it follows:

$$f'(\theta) \varepsilon_s = k_s^{(0)} \eta_0 + k_s^{(1)} \eta_1 + \dots + k_s^{(n-1)} \eta_{n-1},$$

and from this it results that the module

$$f'(\theta) \mathfrak{e} = \mathfrak{k}$$

contains only *integral* functions. From 10. one infers that it is an *ideal*.

§ 11. The ramification ideal.

1. *Lemma.* If any two of the ideals $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \dots$ are relatively prime, there always exists a function which with respect to each of them is congruent to a given function in $\mathfrak{o}$.

Proof. Set

$$\mathfrak{m} = \mathfrak{a}\mathfrak{b}\mathfrak{c}\dots = \mathfrak{a}\mathfrak{a}_1 = \mathfrak{b}\mathfrak{b}_1 = \mathfrak{c}\mathfrak{c}_1 = \dots;$$

the greatest common divisor of $\mathfrak{a}_1 = \mathfrak{b}\mathfrak{c}\dots$, $\mathfrak{b}_1 = \mathfrak{a}\mathfrak{c}\dots$, $\mathfrak{c}_1 = \mathfrak{a}\mathfrak{b}\dots$ is then equal to $\mathfrak{o}$, since no prime ideal can go into $\mathfrak{a}_1, \mathfrak{b}_1, \mathfrak{c}_1, \dots$ at the same time. Consequently (§ 4, 5.) one can select α_1 from $\mathfrak{a}_1$, β_1 from $\mathfrak{b}_1$, γ_1 from $\mathfrak{c}_1$, ... such that

$$\alpha_1 + \beta_1 + \gamma_1 + \dots = 1,$$

hence:

$$\begin{aligned} \alpha_1 &\equiv 1, & \beta_1 &\equiv 0, & \gamma_1 &\equiv 0, & \dots & \pmod{\mathfrak{a}}, \\ \alpha_1 &\equiv 0, & \beta_1 &\equiv 1, & \gamma_1 &\equiv 0, & \dots & \pmod{\mathfrak{b}}, \\ \alpha_1 &\equiv 0, & \beta_1 &\equiv 0, & \gamma_1 &\equiv 1, & \dots & \pmod{\mathfrak{c}}, \\ &\dots\dots\dots \end{aligned}$$

If therefore $\lambda, \mu, \nu, \dots$ are given functions in $\mathfrak{o}$, then

$$\omega \equiv \lambda\alpha_1 + \mu\beta_1 + \nu\gamma_1 + \dots \pmod{\mathfrak{m}}$$

satisfies the conditions

$$\omega \equiv \lambda \pmod{\mathfrak{a}}, \quad \omega \equiv \mu \pmod{\mathfrak{b}}, \quad \omega \equiv \nu \pmod{\mathfrak{c}}, \quad \dots$$

2. Let $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \dots$ be all the mutually different prime ideals going into an arbitrary linear function $z - c$, and

$$\mathfrak{o}(z - c) = \mathfrak{p}^e \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots, \quad e + e_1 + e_2 + \dots = n \quad (\S 9, 7.).$$

Choose the functions $\lambda, \lambda_1, \lambda_2, \dots$ divisible respectively by $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \dots$, but not by $\mathfrak{p}^2, \mathfrak{p}_1^2, \mathfrak{p}_2^2, \dots$, and let $b, b_1, b_2, \dots$ denote arbitrary but mutually different constants. By 1. a function ζ can then be determined which satisfies the congruences

$$\zeta \equiv b + \lambda \pmod{\mathfrak{p}^2}, \quad \zeta \equiv b_1 + \lambda_1 \pmod{\mathfrak{p}_1^2}, \quad \zeta \equiv b_2 + \lambda_2 \pmod{\mathfrak{p}_2^2}, \quad \dots,$$

hence

$$\zeta \equiv b \pmod{\mathfrak{p}}, \quad \zeta \equiv b_1 \pmod{\mathfrak{p}_1}, \quad \zeta \equiv b_2 \pmod{\mathfrak{p}_2}, \quad \dots,$$

so that, if a denotes any constant, $\zeta - a$ is divisible by at most one of the prime ideals $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \dots$ and never by one of their squares. If therefore $\varphi(t) = \Pi(t - a)$ is an integral function of the variable t with constant coefficients, then $\varphi(\zeta) = \Pi(\zeta - a)$ is divisible by $\mathfrak{p}^m$ always and only when $\varphi(t)$ is algebraically divisible by $(t - b)^m$, and if $\mathfrak{p}^m$ is the highest power of $\mathfrak{p}$ going into $\varphi(\zeta)$, then

consequently $\mathfrak{p}^{m-1}$ is the highest power of $\mathfrak{p}$ going into $\varphi'(\zeta)$. If therefore $\varphi(\zeta)$ is to be divisible by $z - c$, then $\varphi(t)$ must be divisible by the function of the n^{th} degree

$$\psi(t) = (t - b)^e (t - b_1)^{e_1} (t - b_2)^{e_2} \dots$$

Consequently the congruence

$$x_0 + x_1 \zeta + x_2 \zeta^2 + \dots + x_{n-1} \zeta^{n-1} \equiv 0 \pmod{z - c}$$

can be satisfied only by such integral rational x as are all divisible by $z - c$. If therefore one sets, denoting by $k_1^{(0)}, k_1^{(1)}, \dots$ integral rational functions of z and by $\omega_1, \omega_2, \dots, \omega_n$ a basis of $\mathfrak{o}$:

$$\begin{aligned} 1 &= k_1^{(0)} \omega_1 + k_2^{(0)} \omega_2 + \dots + k_n^{(0)} \omega_n, \\ \zeta &= k_1^{(1)} \omega_1 + k_2^{(1)} \omega_2 + \dots + k_n^{(1)} \omega_n, \\ \zeta^2 &= k_1^{(2)} \omega_1 + k_2^{(2)} \omega_2 + \dots + k_n^{(2)} \omega_n, \\ &\dots\dots\dots \\ \zeta^{n-1} &= k_1^{(n-1)} \omega_1 + k_2^{(n-1)} \omega_2 + \dots + k_n^{(n-1)} \omega_n, \end{aligned}$$

then the determinant

$$k = \Sigma \pm k_1^{(0)} k_2^{(1)} \dots k_n^{(n-1)}$$

can neither vanish identically nor be divisible by $z - c$ (cf. the note to § 9, 1.).

It follows therefore that

$$N(t - \zeta) = f(t, z)$$

is irreducible. Now since $f(\zeta, z) = 0$, and hence $f(\zeta, c)$ is divisible by $z - c$, $f(t, c)$ must be divisible by $\psi(t)$, and hence, since both functions are of the same degree,

$$f(t, c) = \psi(t)$$

from which one further infers, for a later application:

$$S(\zeta) \equiv eb + e_1 b_1 + e_2 b_2 + \dots \pmod{z - c},$$

and, by applying the same consideration to the functions $\zeta^2, \zeta^3, \dots$, which is certainly permitted if none of the constants b vanishes:

$$\begin{aligned} S(\zeta^2) &\equiv eb^2 + e_1 b_1^2 + e_2 b_2^2 + \dots \pmod{z - c}, \\ S(\zeta^3) &\equiv eb^3 + e_1 b_1^3 + e_2 b_2^3 + \dots \pmod{z - c}. \\ &\dots\dots\dots \end{aligned}$$

Thus $\mathfrak{p}^e$ is the highest power of $\mathfrak{p}$ going into $f(\zeta, c)$, hence $\mathfrak{p}^{e-1}$ the highest going into $f'(\zeta, c)$, and since

$$f'(\zeta, c) \equiv f'(\zeta, z) \pmod{\mathfrak{p}^e},$$

$\mathfrak{p}^{e-1}$ is also the highest power of $\mathfrak{p}$ going into $f'(\zeta, z)$. From this there results

$$\mathfrak{o}f'(\zeta, z) = \mathfrak{m}\mathfrak{p}^{e-1}\mathfrak{p}_1^{e_1-1} \dots,$$

where $\mathfrak{m}$, and consequently also $N(\mathfrak{m})$, is relatively prime to $z - c$.

Now if D is the discriminant of Ω , then accordingly, and by § 10, (11.) and § 2, (13.) (apart from constant factors)

$$Nf'(\zeta, z) = \Delta(1, \zeta, \zeta^2, \dots, \zeta^{n-1}) = Dk^2 = (z - c)^{n-s}N(\mathfrak{m}),$$

if s denotes the number of the different prime ideals $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \dots$ going into $z - c$; and since k and $N(\mathfrak{m})$ are not divisible by $z - c$, $(z - c)^{n-s}$ is the highest power of $z - c$ going into D . Consequently:

$$D = \Pi(z - c)^{n-s}, \quad (1.)$$

where the product sign Π refers to all such linear expressions $z - c$ into which fewer than n *different* prime factors go, which are therefore divisible by the second or a higher power of a prime ideal.

There is therefore only a finite number of linear functions $z - c$ which are divisible by the square of a prime ideal.

We now set

$$\mathfrak{z} = \Pi\mathfrak{p}^{e-1}, \quad (2.)$$

where the product sign Π refers to all those prime ideals $\mathfrak{p}$

of which a higher power than the first, namely the e^{th} , goes into their norm, and we call this ideal $\mathfrak{z}$ the *ramification ideal*. From (1.) and (2.) there follows at once

$$N(\mathfrak{z}) = D. \quad (3.)$$

Since further $n - s \geq e - 1$, hence $e(n - s) - 2(e - 1) \geq (e - 1)(e - 2) \geq 0$, D is divisible by $\mathfrak{p}^{2(e-1)}$, hence also by $\mathfrak{z}^2$, and one can set, denoting by $\mathfrak{d}$ likewise an ideal:

$$\mathfrak{o}D = \mathfrak{d}\mathfrak{z}^2, \quad N(\mathfrak{d}) = D^{n-2}. \quad (4.)$$

3. If a function ϱ in $\mathfrak{o}$ is divisible by every prime ideal going into $z - c$, then $S(\varrho)$ is divisible by $z - c$.

Proof. Let ζ be the same function as in 2., so that one can set:

$$x\varrho = x_0 + x_1\zeta + x_2\zeta^2 + \dots + x_{n-1}\zeta^{n-1},$$

where the coefficients $x, x_0, x_1, \dots, x_{n-1}$ are integral rational functions of z without a common divisor, of which the first is not divisible by $z - c$ (cf. 2.). From our assumption about the function ϱ it follows, if the constants b have the same meaning as in 2.,

$$\begin{aligned} x_0 + x_1b + x_2b^2 + \dots + x_{n-1}b^{n-1} &\equiv 0 \pmod{z - c}, \\ x_0 + x_1b_1 + x_2b_1^2 + \dots + x_{n-1}b_1^{n-1} &\equiv 0 \pmod{z - c}, \\ x_0 + x_1b_2 + x_2b_2^2 + \dots + x_{n-1}b_2^{n-1} &\equiv 0 \pmod{z - c}, \\ &\dots\dots\dots \end{aligned}$$

and from this, by multiplying the congruences by $e, e_1, e_2, \dots$ and adding:

$$x_0n + x_1S(\zeta) + x_2S(\zeta^2) + \dots + x_{n-1}S(\zeta^{n-1}) = xS(\varrho) \equiv 0 \pmod{z-c},$$

hence, since x is not divisible by $z-c$,

$$S(\varrho) \equiv 0 \pmod{z-c}$$

q. e. d.

4. Now let

$$r = (z-c)(z-c_1)(z-c_2) \dots$$

be the product of all the mutually different linear factors of D , and

$$\mathfrak{r} = \mathfrak{p}\mathfrak{p}_1\mathfrak{p}_2 \dots$$

the product of all the mutually different prime ideals going into r . If, as above, $\mathfrak{z}$ is the ramification ideal, then

$$\mathfrak{r}\mathfrak{z} = \Pi \mathfrak{p}^e = \mathfrak{o}r \quad (5.)$$

and consequently

$$N(\mathfrak{r}) = \frac{r^n}{D}.$$

Every function ϱ in $\mathfrak{r}$ has by 3. the property that $S(\varrho)$ is divisible by r . Now if, as in § 10,

$$\mathfrak{e} = [\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n]$$

is the module complementary to $\mathfrak{o}$, and ϱ an arbitrary function in $\mathfrak{r}$, one can set

$$\varrho = x_1\varepsilon_1 + x_2\varepsilon_2 + \dots + x_n\varepsilon_n,$$

where by § 10, 3.

$$x_i = S(\varrho\omega_i),$$

hence, since $\varrho\omega_i$ is a function in $\mathfrak{r}$, x_i is an integral rational function of z divisible by r . From this it follows that the ideal $\mathfrak{r}$ is divisible by the module $r\mathfrak{e}$. Hence the ideal $D\mathfrak{r}$ too is divisible by the ideal $rD\mathfrak{e}$. At the same time

$$N(D\mathfrak{r}) = r^n D^{n-1}, \quad N(rD\mathfrak{e}) = r^n D^{n-1} \quad (\S 10, 10.);$$

consequently, by § 8, 9.

$$D\mathfrak{r} = rD\mathfrak{e}$$

or

$$\mathfrak{r} = r\mathfrak{e}. \quad (6.)$$

From which, by means of the above remark about ϱ , it follows that, if ε denotes an arbitrary function in $\mathfrak{e}$, $S(\varepsilon)$ is an *integral* rational function of z . From the formula (6.) there follows, by multiplication by $\mathfrak{z}$, by (5.)

$$\mathfrak{r}\mathfrak{z} = r\mathfrak{e}\mathfrak{z} = \mathfrak{o}r$$

and consequently

$$\mathfrak{e}\mathfrak{z} = \mathfrak{o}. \quad (7.)$$

If one multiplies the last equation by D , there results from (4.)

$$\mathfrak{e}D\mathfrak{z} = \mathfrak{z}^2\mathfrak{d},$$

consequently

$$D\mathfrak{e} = \mathfrak{z}\mathfrak{d} \quad (8.)$$

and by multiplication of this equation by $\mathfrak{e}$, by (7.)

$$D\mathfrak{e}^2 = \mathfrak{d}. \quad (9.)$$

4.¹² If θ is an integral function of z in Ω and $N(t - \theta) = f(t)$, then $f'(\theta)$ is divisible by the ramification ideal $\mathfrak{z}$.

Proof. If $f(t)$ is reducible, then $f'(\theta) = 0$, hence certainly divisible by $\mathfrak{z}$. In the other case, by § 10, 11.,

$$\mathfrak{e}f'(\theta) = \mathfrak{k}$$

is an ideal, consequently, by multiplication by $\mathfrak{z}$, by (7.)

$$\mathfrak{o}f'(\theta) = \mathfrak{k}\mathfrak{z}. \quad (10.)$$

At the same time it follows, if as in § 10, 11. we set

$$\begin{aligned} \theta^r &= \sum k_l^{(r)} \omega_l, \\ k &= \sum \pm k_1^{(0)} k_2^{(1)} \dots k_n^{(n-1)} \end{aligned}$$

that

$$\begin{aligned} Nf'(\theta) &= N(\mathfrak{k})N(\mathfrak{z}) = DN(\mathfrak{k}) \\ &= \text{const. } k^2 D \quad (\text{§ 10, (11.) and § 2, (13.)}), \end{aligned}$$

hence:

$$N(\mathfrak{k}) = \text{const. } k^2 \quad (11.)$$

a perfect square.

§ 12. The fractional functions of z in the field Ω .

1. Every function η whatever in Ω can, by § 3, 3., be represented in infinitely many ways as the quotient of two integral functions of z (the denominator can even be an integral rational function of z). Let therefore

$$\eta = \frac{\nu}{\mu}$$

¹²*Editorial note:* The print numbers this item 4. a second time, after item 4. on p. 226; 5. would be expected.

and μ, ν integral functions of z (functions in $\mathfrak{o}$). Now if $\mathfrak{m}$ is the greatest common divisor of the two principal ideals $\mathfrak{o}\mu, \mathfrak{o}\nu$, hence, if $\mathfrak{a}, \mathfrak{b}$ are relatively prime ideals,

$$\mathfrak{o}\mu = \mathfrak{a}\mathfrak{m}, \quad \mathfrak{o}\nu = \mathfrak{b}\mathfrak{m}, \quad (1.)$$

then it follows (§ 4, 6.)

$$\mathfrak{a}\nu = \mathfrak{b}\mu \quad \text{or} \quad \mathfrak{a}\eta = \mathfrak{b}. \quad (2.)$$

If therefore α is an arbitrary function in $\mathfrak{a}$, then $\alpha\eta$ is contained in $\mathfrak{b}$, hence in any case an integral function of z . If conversely α is an integral function of z which has the property that $\alpha\eta = \beta$ is an integral function, it follows

$$\alpha\nu = \beta\mu,$$

hence by (1.)

$$\alpha\mathfrak{b} = \beta\mathfrak{a};$$

now since $\mathfrak{a}, \mathfrak{b}$ are relatively prime, α must be divisible by $\mathfrak{a}$ and β by $\mathfrak{b}$, and from this it follows:

$\mathfrak{a}$ is the totality of all those integral functions α which have the property that $\alpha\eta$ is an integral function, and the totality of all these integral functions $\alpha\eta$ is the ideal $\mathfrak{b}$; or, expressed otherwise:

$\mathfrak{b}$ is the least common multiple of $\mathfrak{o}\eta$ and $\mathfrak{o}$, and likewise $\mathfrak{a}$ the least common multiple of $\frac{\mathfrak{o}}{\eta}$ and $\mathfrak{o}$. Accordingly, if $\mathfrak{a}', \mathfrak{b}'$ are two ideals satisfying the condition

$$\mathfrak{a}'\eta = \mathfrak{b}'$$

$\mathfrak{a}'$ must be divisible by $\mathfrak{a}$. Let therefore

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

then it follows:

$$\mathfrak{b}' = \mathfrak{n}\mathfrak{a}\eta = \mathfrak{n}\mathfrak{b}.$$

Conversely, for an arbitrary ideal $\mathfrak{n}$ too,

$$\mathfrak{n}\mathfrak{a}\eta = \mathfrak{n}\mathfrak{b}.$$

2. Now let $\mathfrak{a}, \mathfrak{b}$ be two ideals satisfying the condition

$$\mathfrak{a}\eta = \mathfrak{b}$$

no matter whether relatively prime or not. The quotient $\frac{\mathfrak{b}}{\mathfrak{a}}$ is by § 4, 8. the totality of all those functions γ which have the property that $\mathfrak{a}\gamma$ is divisible by $\mathfrak{b}$. To these functions certainly belong all functions of the form $\omega\eta$, if ω denotes an arbitrary function in $\mathfrak{o}$. But conversely, too, every function γ is of this form; for since $\mathfrak{a}\gamma$ is divisible by $\mathfrak{b}$, hence also by $\mathfrak{o}$, it is an ideal (since it possesses the properties I., II. § 7), hence, if $\mathfrak{c}$ is likewise an ideal:

$$\mathfrak{a}\gamma = \mathfrak{c}\mathfrak{b}$$

and by multiplication by η

$$\mathfrak{b}\gamma = \mathfrak{c}\mathfrak{b}\eta.$$

Now if, as above, $\eta = \frac{\nu}{\mu}$, and, if ϱ, σ are integral functions, $\gamma = \frac{\varrho}{\sigma}$, it follows from this

$$\mathfrak{b}\varrho\mu = \mathfrak{c}\mathfrak{b}\nu\sigma,$$

hence:

$$\mathfrak{o}\varrho\mu = \mathfrak{c}\nu\sigma, \quad \mathfrak{o}\gamma = \mathfrak{c}\eta.$$

Both together yield the theorem

$$\mathfrak{o}\eta = \frac{\mathfrak{b}}{\mathfrak{a}}. \quad (3.)$$

If in this representation $\mathfrak{b}, \mathfrak{a}$ are relatively prime, which by 1. can always be assumed, and in only one way, then $\mathfrak{b}$ shall be called the *upper ideal* and $\mathfrak{a}$ the *lower ideal* of the function η .

3. If again in general

$$\mathfrak{a}\eta = \mathfrak{b}, \quad \text{hence} \quad \mathfrak{o}\eta = \frac{\mathfrak{b}}{\mathfrak{a}}$$

and α is an arbitrary function in $\mathfrak{a}$, and β a corresponding function in $\mathfrak{b}$, then

$$\eta = \frac{\beta}{\alpha} \quad \text{and} \quad \mathfrak{a}\beta = \mathfrak{b}\alpha.$$

From this it follows, by forming the norms,

$$N(\eta) = \text{const.} \frac{N(\mathfrak{a})}{N(\mathfrak{b})}.$$

¹³

4. If η, η' are two functions in Ω and, as in 1.,

$$\mathfrak{a}\eta = \mathfrak{b}; \quad \mathfrak{a}'\eta' = \mathfrak{b}',$$

no matter whether $\mathfrak{a}, \mathfrak{b}; \mathfrak{a}', \mathfrak{b}'$ are relatively prime or not, it follows

$$\mathfrak{a}\mathfrak{a}'\eta\eta' = \mathfrak{b}\mathfrak{b}'.$$

Thus from

$$\mathfrak{o}\eta = \frac{\mathfrak{b}}{\mathfrak{a}}, \quad \mathfrak{o}\eta' = \frac{\mathfrak{b}'}{\mathfrak{a}'}$$

there follow the equations

$$\mathfrak{o}\eta\eta' = \frac{\mathfrak{b}\mathfrak{b}'}{\mathfrak{a}\mathfrak{a}'}, \quad \mathfrak{o}\frac{1}{\eta} = \frac{\mathfrak{a}}{\mathfrak{b}}, \quad \mathfrak{o}\frac{\eta}{\eta'} = \frac{\mathfrak{b}\mathfrak{a}'}{\mathfrak{a}\mathfrak{b}'}$$

¹³*Editorial note:* As printed, with $N(\mathfrak{a})$ in the numerator. Since $\mathfrak{a}\eta = \mathfrak{b}$, the quotient $N(\mathfrak{b})$ over $N(\mathfrak{a})$ would be expected; this appears to be a misprint.

5. If $\mathfrak{a}\eta = \mathfrak{b}$, $\mathfrak{a}\eta' = \mathfrak{b}'$, then also

$$\mathfrak{a}(\eta \pm \eta') = \mathfrak{b}''$$

will be an ideal, because, if $\alpha\eta$, $\alpha\eta'$ are integral functions, $\alpha(\eta \pm \eta')$ is always one too. If therefore

$$\mathfrak{o}\eta = \frac{\mathfrak{b}}{\mathfrak{a}}, \quad \mathfrak{o}\eta' = \frac{\mathfrak{b}'}{\mathfrak{a}},$$

it follows

$$\mathfrak{o}(\eta \pm \eta') = \frac{\mathfrak{b}''}{\mathfrak{a}};$$

if the two ideals $\mathfrak{b}$, $\mathfrak{b}'$ have a common divisor, it is also a divisor of $\mathfrak{b}''$.

6. Now let ϱ be a function in Ω whose upper ideal is divisible by an arbitrarily given prime ideal $\mathfrak{p}$, but not by $\mathfrak{p}^2$ (such functions always exist; they can even be integral functions of z), hence

$$\mathfrak{o}\varrho = \frac{\mathfrak{m}\mathfrak{p}}{\mathfrak{n}},$$

where $\mathfrak{m}$, $\mathfrak{n}$ are ideals not divisible by $\mathfrak{p}$. Let further η be an arbitrary function in Ω whose lower ideal is not divisible by $\mathfrak{p}$, hence

$$\mathfrak{o}\eta = \frac{\mathfrak{b}}{\mathfrak{a}}$$

and $\mathfrak{a}$ not divisible by $\mathfrak{p}$. Choose an arbitrary function α in $\mathfrak{a}$ which is not divisible by $\mathfrak{p}$, and a corresponding function β in $\mathfrak{b}$, so that

$$\eta = \frac{\beta}{\alpha}$$

holds. Let

$$\alpha \equiv \alpha_0, \quad \beta \equiv \beta_0 \pmod{\mathfrak{p}}, \quad c_0 = \frac{\beta_0}{\alpha_0},$$

where α_0 , β_0 , c_0 are constants, of which the first is different from zero. By 5.

$$\mathfrak{o}(\eta - c_0) = \mathfrak{o}\frac{\beta - c_0\alpha}{\alpha} = \frac{\mathfrak{b}_1}{\mathfrak{a}},$$

and from

$$\mathfrak{a}(\beta - c_0\alpha) = \mathfrak{b}_1\alpha, \quad \beta - c_0\alpha \equiv 0 \pmod{\mathfrak{p}}$$

it follows, since α is not divisible by $\mathfrak{p}$, that $\mathfrak{b}_1$ must be divisible by $\mathfrak{p}$. If therefore one sets

$$\eta - c_0 = \varrho\eta_1,$$

then the lower ideal of η_1 too is not divisible by $\mathfrak{p}$. In this way a completely determined series of constants $c_0, c_1, \dots, c_{r-1}, \dots$ can be found such that

$$\begin{aligned} \eta &= c_0 + \varrho\eta_1, \\ \eta_1 &= c_1 + \varrho\eta_2, \\ &\dots\dots\dots \\ \eta_{r-1} &= c_{r-1} + \varrho\eta_r, \quad \dots, \end{aligned}$$

where the $\eta_1, \eta_2, \dots, \eta_r, \dots$ denote functions whose lower ideals can have no other prime factors than the lower ideal of η and the upper ideal of ϱ , with the exclusion of $\mathfrak{p}$. Accordingly, for every positive integer r ,

$$\eta = c_0 + c_1\varrho + \dots + c_{r-1}\varrho^{r-1} + \eta_r\varrho^r.$$

If the lower ideal of ζ is divisible by $\mathfrak{p}^s$, not by $\mathfrak{p}^{s+1}$, then one can apply the same consideration to the function $\eta = \zeta\varrho^s$ and obtains

$$\zeta = c_0\varrho^{-s} + c_1\varrho^{-s+1} + \dots + c_{r-1}\varrho^{-s+r} + \eta_r\varrho^{-s+r}.$$

14

§ 13. The rational transformations of the functions of the field Ω .

If z_1 is an arbitrary, non-constant function of the field Ω (a *variable* in Ω), then, as shown in § 2, there exists between z_1 and z an irreducible algebraic equation which, freed of denominators, may be of degree e with respect to z_1 and of degree e_1 with respect to z . As was shown in that same place, e is a divisor of n , $n = ef$. Let this equation be

$$G(z_1^{(e)}, z^{(e_1)}) = 0. \quad (1.)$$

Every rational function ζ of z and z_1 can (§ 1), with the help of this equation, be brought into the two forms

$$\begin{cases} \zeta = x_0 + x_1z_1 + \dots + x_{e-1}z_1^{e-1}, \\ \zeta = x_0^{(1)} + x_1^{(1)}z + \dots + x_{e_1-1}^{(1)}z^{e_1-1} \end{cases} \quad (2.)$$

and indeed in only one way such that $x_0, x_1, \dots, x_{e-1}$ are rational functions of z , and $x_0^{(1)}, x_1^{(1)}, \dots, x_{e_1-1}^{(1)}$ rational functions of z_1 .

Now if θ is a function such that $1, \theta, \theta^2, \dots, \theta^{n-1}$ form a basis^{*)} of Ω (with respect to z), then by § 2 the n functions

$$\begin{pmatrix} 1, & z_1, & z_1^2, & \dots & z_1^{e-1}, \\ \theta, & \theta z_1, & \theta z_1^2, & \dots & \theta z_1^{e-1}, \\ \dots & \dots & \dots & \dots & \dots \\ \theta^{f-1}, & \theta^{f-1}z_1, & \theta^{f-1}z_1^2, & \dots & \theta^{f-1}z_1^{e-1} \end{pmatrix} \quad (3.)$$

likewise form such a basis, and from this it follows by (2.) that between the $e_1f = n_1$ functions

$$\begin{pmatrix} 1, & z, & z^2, & \dots & z^{e_1-1}, \\ \theta, & \theta z, & \theta z^2, & \dots & \theta z^{e_1-1}, \\ \dots & \dots & \dots & \dots & \dots \\ \theta^{f-1}, & \theta^{f-1}z, & \theta^{f-1}z^2, & \dots & \theta^{f-1}z^{e_1-1}, \end{pmatrix} \quad (4.)$$

¹⁴Editorial note: Printed $c_{r-1}\varrho^{-s+r}$; by the preceding expansion $c_{r-1}\varrho^{-s+r-1}$ is expected, an apparent misprint.

which for brevity may be denoted by

$$\eta_1^{(1)}, \quad \eta_2^{(1)}, \quad \dots \quad \eta_{n_1}^{(1)}$$

an equation of the form

$$x_1^{(1)}\eta_1^{(1)} + x_2^{(1)}\eta_2^{(1)} + \dots + x_{n_1}^{(1)}\eta_{n_1}^{(1)} = 0$$

*) Instead of the basis $1, \theta, \dots, \theta^{n-1}$ one could also take any other basis of Ω as the foundation of this consideration. For our purpose, however, it suffices to choose just this one.

holds only if the rational functions $x_1^{(1)}, x_2^{(1)}, \dots, x_{n_1}^{(1)}$ of z_1 all vanish. From this it follows by (2.) that every function η in Ω can be represented, and indeed in only one single way, in the form:

$$\eta = x_1^{(1)}\eta_1^{(1)} + x_2^{(1)}\eta_2^{(1)} + \dots + x_{n_1}^{(1)}\eta_{n_1}^{(1)},$$

where the $x^{(1)}$ are rational functions of z_1 .

Every such function η satisfies an algebraic equation of degree n_1 whose coefficients depend rationally on z_1 , for

$$\begin{aligned} \eta\eta_1^{(1)} &= x_{1,1}^{(1)}\eta_1^{(1)} + x_{1,2}^{(1)}\eta_2^{(1)} + \dots + x_{1,n_1}^{(1)}\eta_{n_1}^{(1)}, \\ \eta\eta_2^{(1)} &= x_{2,1}^{(1)}\eta_1^{(1)} + x_{2,2}^{(1)}\eta_2^{(1)} + \dots + x_{2,n_1}^{(1)}\eta_{n_1}^{(1)}, \\ &\dots\dots\dots \\ \eta\eta_{n_1}^{(1)} &= x_{n_1,1}^{(1)}\eta_1^{(1)} + x_{n_1,2}^{(1)}\eta_2^{(1)} + \dots + x_{n_1,n_1}^{(1)}\eta_{n_1}^{(1)}, \end{aligned}$$

and consequently

$$\begin{vmatrix} x_{1,1}^{(1)} - \eta, & x_{1,2}^{(1)}, & \dots & x_{1,n_1}^{(1)} \\ x_{2,1}^{(1)}, & x_{2,2}^{(1)} - \eta, & \dots & x_{2,n_1}^{(1)} \\ \dots & \dots & \dots & \dots \\ x_{n_1,1}^{(1)}, & x_{n_1,2}^{(1)}, & \dots & x_{n_1,n_1}^{(1)} - \eta \end{vmatrix} = 0.$$

15

It can now be shown that one can select a function $\eta = \theta_1$ such that θ_1 does not at the same time satisfy an equation of lower degree whose coefficients depend rationally on z_1 .

To prove this assertion we rely on the following theorem, whose proof results easily by inference from $m - 1$ to m . If

$$F(x_1, x_2, \dots, x_m)$$

is an integral rational function of $x_1, x_2, \dots, x_m$ whose coefficients are functions in Ω that do not all vanish, then one can put for $x_1, x_2, \dots, x_m$ such constant

¹⁵ *Editorial note:* The entry $x_{n_1,2}^{(1)}$ is printed with a period where every other entry carries a comma; probably a comma that printed incompletely.

quantities, or quantities depending rationally on z_1 , that F passes over into a non-vanishing function in Ω . If therefore $F(x_1, x_2, \dots x_m)$ is equal to zero for *all* such $x_1, x_2, \dots x_m$, it follows also, for arbitrary $dx_1, dx_2, \dots dx_m$, constant or depending rationally on z_1 , that

$$dF = F'(x_1) dx_1 + F'(x_2) dx_2 + \dots + F'(x_m) dx_m = 0.$$

Now if

$$\theta_1 = x_1 \eta_1^{(1)} + x_2 \eta_2^{(1)} + \dots + x_{n_1} \eta_{n_1}^{(1)}$$

and

$$\begin{cases} 1 = x_{1,0} \eta_1^{(1)} + x_{2,0} \eta_2^{(1)} + \dots + x_{n_1,0} \eta_{n_1}^{(1)}, \\ \theta_1 = x_{1,1} \eta_1^{(1)} + x_{2,1} \eta_2^{(1)} + \dots + x_{n_1,1} \eta_{n_1}^{(1)}, \\ \dots\dots\dots \\ \theta_1^m = x_{1,m} \eta_1^{(1)} + x_{2,m} \eta_2^{(1)} + \dots + x_{n_1,m} \eta_{n_1}^{(1)}, \end{cases} \quad (5.)$$

then the $x_{k,h}$ are integral rational and homogeneous functions of degree h of $x_1, x_2, \dots x_{n_1}$ and depend, besides, rationally on z_1 .

If therefore

$$\varphi(\theta_1) = a_m \theta_1^m + a_{m-1} \theta_1^{m-1} + \dots + a_1 \theta_1 + a_0 = 0$$

is the equation of lowest degree which θ_1 satisfies, with coefficients depending rationally on z_1 , then the functions $a_0, a_1, \dots a_m$ satisfy the condition

$$a_0 x_{\iota,0} + a_1 x_{\iota,1} + \dots + a_m x_{\iota,m} = 0, \quad (\iota=1, 2, \dots n_1)$$

and at the same time $m \leq n_1$. Now since not all the determinants of m rows formed from the coefficients $x_{h,k}$ can vanish, because otherwise θ_1 would satisfy an equation of lower than the m^{th} degree, it follows from the latter equations that the $a_0, a_1, \dots a_m$ may be assumed to be integral homogeneous functions of $x_1, x_2, \dots x_{n_1}$.

Now if the equation $\varphi(\theta_1) = 0$ is to hold for all $x_1, x_2, \dots x_{n_1}$ depending rationally on z_1 , then by the above theorem also

$$d\varphi = \varphi'(\theta_1) d\theta_1 + da_m \theta_1^m + \dots + da_1 \theta_1 + da_0 = 0$$

must hold, and if $m < n_1$, the $dx_1, dx_2, \dots dx_{n_1}$ can be determined, without all of them vanishing, such that

$$da_m : da_{m-1} : \dots : da_1 : da_0 = a_m : a_{m-1} : \dots : a_1 : a_0$$

and consequently

$$\varphi'(\theta_1) d\theta_1 = 0$$

But since $\varphi'(\theta_1)$ is of degree $m-1$, $d\theta_1 = 0$ must hold, hence $dx_1 = 0, dx_2 = 0, \dots dx_{n_1} = 0$. Therefore only $m = n_1$ is possible.

If therefore θ_1 is so determined that the equation of lowest degree

$$F_1(\theta_1, z_1) = 0$$

actually reaches the degree n_1 , then all functions in Ω can be represented, and indeed in only one way, in the form

$$\eta = x_0^{(1)} + x_1^{(1)}\theta_1 + \cdots + x_{n_1-1}^{(1)}\theta_1^{n_1-1},$$

where the coefficients $x_0^{(1)}, x_1^{(1)}, \dots, x_{n_1-1}^{(1)}$ depend rationally on z_1 ; for under this assumption one can represent $\eta_1^{(1)}, \eta_2^{(1)}, \dots, \eta_{n_1}^{(1)}$ in the stated way by means of the equations (5.).

Thus z_1, θ_1 can be represented rationally by z, θ , and conversely z, θ rationally by z_1, θ_1 .

The variable z , which we have so far designated as the independent one, can therefore be any (non-constant) function of the field Ω whatever.

But while the totality of all functions of the field Ω remains entirely unchanged, the notions *basis, norm, trace, discriminant, integral function, module, ideal* are essentially dependent on the choice of the *independent* variable z .

Only in the special case when two variables z, z_1 depend linearly on one another is a basis of Ω with respect to z at the same time one with respect to z_1 ; likewise norms, traces and discriminants are in this case identical for z and z_1 .

If α, β are any two functions in Ω , then there exist between them equations whose left-hand side is an integral rational function of α and β .

Among these there is one (by § 1)

$$F(\alpha, \beta) = 0,$$

which is of the lowest possible degree both with respect to α and with respect to β , and this shall be called the *irreducible equation existing between α and β* . It is, apart from a constant factor, completely determined.

Part II.

§ 14. The points of the Riemann surface.

The considerations so far on the functions of the field Ω were of a purely formal nature. All the results were rational consequences, i.e. consequences derived according to the rules of literal calculation by means of the four species, of the irreducible equation existing between two functions in Ω . The numerical values of these functions nowhere came into consideration. One could even, without applying other principles, carry the formal treatment considerably further by regarding two functions of the field Ω not as connected by an equation but as independent variables, whereupon everything comes down to the algebraic divisibility of rational functions of two variables. We have also carried out this

way, which however is very cumbersome in exposition and mode of expression, and as regards rigour

accomplishes nothing more than the course used in the foregoing. But now that the formal part of the investigation has been carried so far, the question forces itself upon us *to what extent it is possible to assign to the functions in Ω such determinate numerical values that all the rational relations (identities) existing between these functions pass over into correct numerical equations*. In this investigation it proves expedient to regard the infinitely great too as *one* determinate number ∞ (constant), with which one calculates according to determinate rules^{*)}. The calculations carried out by means of the rational operations in the number domain thus extended always lead to a completely determinate numerical result, unless in the course of the calculation one of the signs $\infty \pm \infty$, $0 \cdot \infty$, $\frac{0}{0}$, $\frac{\infty}{\infty}$ occurs, signs to which no determinate value belongs. The occurrence of such an indeterminacy in an equation is not to be regarded as a contradiction, since in this case the equation no longer contains any determinate assertion at all, and so there can be no question of its truth or falsity either. Among the functions of the field Ω there are, besides infinitely many variables, also all the constants, i.e. numbers. Accordingly the requirement posed above leads to the following notion.

1. *Definition.* If all the individuals $\alpha, \beta, \gamma, \dots$ of the field Ω are replaced by determinate numerical values $\alpha_0, \beta_0, \gamma_0, \dots$ in such a way that

$$\begin{aligned} \text{(I.) } \alpha_0 &= \alpha, \quad \text{if } \alpha \text{ is constant, and in general} \\ \text{(II.) } (\alpha + \beta)_0 &= \alpha_0 + \beta_0, & \text{(IV.) } (\alpha\beta)_0 &= \alpha_0\beta_0, \\ \text{(III.) } (\alpha - \beta)_0 &= \alpha_0 - \beta_0, & \text{(V.) } \left(\frac{\alpha}{\beta}\right)_0 &= \frac{\alpha_0}{\beta_0} \end{aligned}$$

then to such a concurrence of determinate values a *point* $\mathfrak{P}$ shall be assigned (which, to make it perceptible, one may imagine as situated somewhere in space^{**)}), and we say that *at* $\mathfrak{P}$ $\alpha = \alpha_0$, or that α has the value α_0 *at* $\mathfrak{P}$. Two points are called different always and only

^{*)} To regard the infinite as a determinate value is in many ways customary and useful in the theory of functions. With *Riemann* this is expressed, e.g. in his regarding his surfaces representing the algebraic functions as closed.

^{**)} A geometric illustration of the “point” is, moreover, by no means necessary, and does not even contribute much to an easier comprehension. It suffices to regard the word “point” as a short and convenient expression for the co-existence of values described.

when there exists a function α in Ω which has different values at the two points.

From this definition of the point, its existence as well as the extent of the notion is now to be deduced. But first it must be emphasized that by this definition the “point” is an *invariant* notion belonging to the field Ω , which in no way depends on the choice of the independent variable by which one represents the functions of the field.

2. *Theorem.* If a point $\mathfrak{P}$ is given, and z is a variable in Ω that is finite at $\mathfrak{P}$ (such a one exists for every point; for if $z_0 = \infty$, then $(\frac{1}{z})_0 = 0$, hence finite), then every integral function ω of z too has a finite value ω_0 at $\mathfrak{P}$ — for between ω and z there exists a relation of the form

$$1 = a\frac{1}{\omega} + b\frac{1}{\omega^2} + \cdots + k\frac{1}{\omega^m},$$

where $a, b, \dots, k$, as *integral rational* functions of z , have finite values at $\mathfrak{P}$ by (II.), (III.), (IV.). Consequently $(\frac{1}{\omega})_0$ cannot be equal to 0, hence ω_0 cannot be equal to ∞ .

3. *Theorem.* If z is any variable finite at $\mathfrak{P}$, then the totality $\mathfrak{p}$ of all those integral functions π of z which vanish at $\mathfrak{P}$ is a prime ideal in z ; we say that the point $\mathfrak{P}$ *generates* this prime ideal $\mathfrak{p}$. If ω is an integral function of z which has the value ω_0 at $\mathfrak{P}$, then $\omega \equiv \omega_0 \pmod{\mathfrak{p}}$.

Proof. If $\pi'_0 = 0$, $\pi''_0 = 0$, then also $(\pi' + \pi'')_0 = \pi'_0 + \pi''_0 = 0$, and if ω is an arbitrary integral function of z , hence ω_0 finite, then from $\pi_0 = 0$ also $(\omega\pi)_0 = \omega_0\pi_0 = 0$ follows; hence $\mathfrak{p}$ is an *ideal* in z (§ 7, I., II.). The ideal $\mathfrak{p}$ is different from $\mathfrak{o}$, since it does not contain the function “1”.

If ω has the value ω_0 at $\mathfrak{P}$, then $(\omega - \omega_0)_0 = 0$, consequently $\omega \equiv \omega_0 \pmod{\mathfrak{p}}$, hence every integral function of z is congruent to a constant with respect to the modulus $\mathfrak{p}$. Therefore (§ 9, 7.) $\mathfrak{p}$ is a *prime ideal*.

4. *Theorem.* The same prime ideal $\mathfrak{p}$ cannot be generated by two different points.

For first, the value of every integral function ω at a point $\mathfrak{P}$ generating the ideal $\mathfrak{p}$ is completely determined by the congruence $\omega \equiv \omega_0 \pmod{\mathfrak{p}}$. But if η is an arbitrary function in Ω , then

by § 12, 1. two integral functions α, β , not both divisible by $\mathfrak{p}$, can be determined such that

$$\eta = \frac{\alpha}{\beta}$$

Now since the finite values α_0, β_0 do not both vanish, it follows from (V.)

$$\eta_0 = \frac{\alpha_0}{\beta_0},$$

which is therefore likewise completely determined by $\mathfrak{p}$.

It further follows from this that two points at which a variable z has finite values are different from one another if and only if there exists an *integral* function of z which has different values at the two.

5. *Theorem.* If z is any variable in Ω and $\mathfrak{p}$ a prime ideal in z , there is *one* (and by 4. also *only one*) point $\mathfrak{P}$ which generates this prime ideal, and which shall be called the *zero point* of the ideal $\mathfrak{p}$.

Proof. Let η be an arbitrary function in Ω , and ϱ one whose upper ideal is divisible by $\mathfrak{p}$ but not by $\mathfrak{p}^2$. Then by § 12, 6. an integer m , a finite constant c different from zero, and a function η_1 whose lower ideal is not divisible by $\mathfrak{p}$ can always be determined, and in only one way, such that

$$\eta = c\varrho^m + \eta_1\varrho^{m+1}.$$

We set

$$\eta_0 = 0, \quad c, \quad \infty,$$

according as m is positive, zero or negative. To this determination of the values of the functions of the field Ω there corresponds a point $\mathfrak{P}$, since the conditions (I.) to (V.), as one sees at once, are fulfilled^{*)}.

*) If $\eta' = c' \varrho^{m'} + \eta_1' \varrho^{m'+1}$, then e.g.

$$\frac{\eta}{\eta'} = \varrho^{m-m'} \left(\frac{c}{c'} + \varrho \eta_1'' \right),$$

where

$$\eta_1'' = \frac{c' \eta_1 - c \eta_1'}{c'(c' + \varrho \eta_1')}$$

is a function of the same nature as η_1 (the proof is still simpler in the remaining cases).

Every function whose upper ideal is divisible by $\mathfrak{p}$, hence in particular every function in $\mathfrak{p}$, receives by this stipulation the value zero at $\mathfrak{P}$, i.e. the point $\mathfrak{P}$ so determined generates the prime ideal $\mathfrak{p}$.

Every function whose lower ideal is divisible by $\mathfrak{p}$, and only such a one, has the value ∞ at $\mathfrak{P}$, and from this it emerges that an *integral* function of z is infinite at no point at which z has a finite value; and since a fractional function of z certainly contains a prime ideal in its lower ideal, and hence must be infinite at at least one point at which z is finite, conversely every function which is infinite at no point at which z has a finite value is an integral function of z .

6. From 3., 4., 5. there now results the following. In order to obtain all existing points $\mathfrak{P}$, and each only a single time, take an arbitrary variable z of the field Ω ; form all the prime ideals $\mathfrak{p}$ in z and construct the zero point for each of them; then all those points $\mathfrak{P}$ have been found at which z remains finite; if $\mathfrak{P}'$ is a point different from these, then at it $z' = \frac{1}{z}$ has the finite value zero; conversely every point $\mathfrak{P}'$ at which z' has the value zero is different from the points $\mathfrak{P}$. The prime ideal $\mathfrak{p}'$ in z' generated by such a point $\mathfrak{P}'$ (which consists of all integral functions of z' vanishing at $\mathfrak{P}'$) goes into z' , and conversely the zero point of every prime ideal $\mathfrak{p}'$ in z' going into z' is a point $\mathfrak{P}'$ at which $z' = 0$, hence $z = \infty$. With these supplementary points, finite in number and corresponding to the different $\mathfrak{p}'$, and those derived before from the prime ideals $\mathfrak{p}$ in z , the totality of all points $\mathfrak{P}$ is exhausted, whose aggregate forms the *Riemann surface* T .

§ 15. The order numbers.

1. *Definition.* If $\mathfrak{P}$ is a determinate point, we consider all the functions π in Ω vanishing at $\mathfrak{P}$, and assign to each of them a determinate *order number* according to the following point of view.

Such a function ϱ has the order number 1, or is called *infinitely small of the first order*, or 0^1 at $\mathfrak{P}$, if *all* the quotients $\frac{\pi}{\varrho}$ remain finite at $\mathfrak{P}$. If ϱ' is a function of the same kind as ϱ , then $\frac{\varrho'}{\varrho}$ is at $\mathfrak{P}$

neither 0 nor ∞ , and conversely, if $\frac{\varrho'}{\varrho}$ is neither 0 nor ∞ at $\mathfrak{P}$, then ϱ' is likewise infinitely small of the first order. If further for some function π there is a positive integral exponent r such that $\frac{\pi}{\varrho^r}$ becomes neither 0 nor ∞ at $\mathfrak{P}$, then the same holds of $\frac{\pi}{\varrho'^r}$, and π receives the order number r , or is called infinitely small of the order r at the point $\mathfrak{P}$. We shall also say that π is 0^r at $\mathfrak{P}$, or π is 0 at $\mathfrak{P}^r$.

To decide the question of the existence of such functions ϱ and such order numbers r , take an arbitrary variable z finite at $\mathfrak{P}$, denote by $\mathfrak{p}$ the prime ideal in z generated by $\mathfrak{P}$, and represent every function π (with the exception of the orderless constant 0) according to § 12 as the quotient of two relatively prime ideals in z . The upper ideal of each of these functions is then divisible by $\mathfrak{p}$, and among them there are also such whose upper ideal is not divisible by $\mathfrak{p}^2$; these have the order number 1; for the remaining functions π the order number is the exponent of the highest power of $\mathfrak{p}$ going into the upper ideal, as follows directly from the theorems of § 12.

2. If a function η has the finite value η_0 at $\mathfrak{P}$, we say that η has this value r times at $\mathfrak{P}$, or at r points coinciding with $\mathfrak{P}$, or at $\mathfrak{P}^r$, if the function $\eta - \eta_0$ is infinitely small of the order r at $\mathfrak{P}$. But if $\eta_0 = \infty$, we say that η has the value ∞ r times at $\mathfrak{P}$, or at r points coinciding with $\mathfrak{P}$, or that η is ∞^r at $\mathfrak{P}$ or ∞ at $\mathfrak{P}^r$, if $\frac{1}{\eta}$ vanishes at $\mathfrak{P}^r$.

3. If a function η becomes ∞^r at $\mathfrak{P}$, we also attribute to it the order number $-r$; but if η becomes neither 0 nor ∞ at $\mathfrak{P}$, let it have the order number 0. Accordingly, at an arbitrary point $\mathfrak{P}$, a completely determinate *order number* belongs to every function of the field Ω , with the exception of the two constants 0 and ∞ .

4. If ϱ is a function which possesses the order number 1 at an arbitrary point $\mathfrak{P}$, and η a function with the (positive, negative or vanishing) order number m , then by the concluding theorem of § 12, for every arbitrary positive r , a series of constants $c_0, c_1, \dots, c_{r-1}$, of which the first does *not* vanish, and a function σ finite at $\mathfrak{P}$ can be determined such that

$$\eta = c_0 \varrho^m + c_1 \varrho^{m+1} + \dots + c_{r-1} \varrho^{m+r-1} + \sigma \varrho^{m+r}$$

5. From this it follows immediately that the order number of a product of two or more functions is equal to the sum of the order numbers of the individual factors.

The order number of a quotient of two functions is equal to the difference of the order numbers of the numerator and denominator.

If $\eta_1, \eta_2, \dots, \eta_s$ is a series of functions and m the algebraically smallest among

their order numbers, then

$$\begin{aligned}\eta_1 &= e_1\varrho^m + \sigma_1\varrho^{m+1}, \\ \eta_2 &= e_2\varrho^m + \sigma_2\varrho^{m+1}, \\ &\dots\dots\dots \\ \eta_s &= e_s\varrho^m + \sigma_s\varrho^{m+1},\end{aligned}$$

where the constants $e_1, e_2, \dots, e_s$ in any case do not all vanish. If therefore $c_1, c_2, \dots, c_s$ are constants, the order number of

$$\eta = c_1\eta_1 + c_2\eta_2 + \dots + c_s\eta_s,$$

if $c_1e_1 + c_2e_2 + \dots + c_se_s$ is different from zero, is likewise m , otherwise greater than m .

6. Complexes of points, which may also contain the same point several times, we call *polygons* and denote them by $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \dots$

Further let $\mathfrak{AB}$ denote the polygon composed of the points of $\mathfrak{A}$ and of $\mathfrak{B}$, in such a way that, if a point $\mathfrak{P}$ occurs r times in $\mathfrak{A}$ and s times in $\mathfrak{B}$, it occurs $(r+s)$ times in $\mathfrak{AB}$. From this follows the meaning of $\mathfrak{P}^r$ and of $\mathfrak{A} = \mathfrak{P}^r\mathfrak{P}_1^{r_1}\mathfrak{P}_2^{r_2}\dots$, and the laws of divisibility of polygons, in complete agreement with those of the divisibility of the integers and of ideals. The role of the prime factors is here taken over by the points; but in order to obtain the unit as well, one must admit the polygon $\mathfrak{O}$ containing no point at all (the zero-gon).

The number of points of a polygon is called its *order*. A polygon of the order n is also called briefly an *n-gon*.

The *greatest common divisor* of two polygons $\mathfrak{A}, \mathfrak{B}$ is that polygon which contains every point $\mathfrak{P}$ as often as it occurs *at least* in $\mathfrak{A}$ and $\mathfrak{B}$. If this is $\mathfrak{O}$, $\mathfrak{A}, \mathfrak{B}$ are called *relatively prime*.

The *least common multiple* of $\mathfrak{A}$ and $\mathfrak{B}$ is that polygon which contains every point as often as it occurs *at most* in $\mathfrak{A}$ and $\mathfrak{B}$.

If $\mathfrak{A}, \mathfrak{B}$ are relatively prime, then $\mathfrak{AB}$ is their least common multiple.

If $\mathfrak{A} = \mathfrak{P}^r\mathfrak{P}_1^{r_1}\mathfrak{P}_2^{r_2}\dots$ is an arbitrary polygon, there are always functions z in Ω which are infinite at none of the points $\mathfrak{A}$. For if z is infinite at some points of $\mathfrak{A}$, one can choose a constant c such that $z - c$ has the value 0 at none of the points of $\mathfrak{A}$, and then $\frac{1}{z-c}$ is finite at all points of the polygon $\mathfrak{A}$. If one takes such a variable z as the foundation, then the totality of all those integral functions of z which vanish at the points of the polygon $\mathfrak{A}$ (each counted according to its multiplicity) is an ideal $\mathfrak{a} = \mathfrak{p}^r\mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\dots$, and one can say that the polygon $\mathfrak{A}$ *generates* the ideal $\mathfrak{a}$, or that $\mathfrak{A}$ is the *zero polygon* of the ideal $\mathfrak{a}$. The notion of ideal accordingly coincides completely with the notion of a system of integral functions all of which vanish at the same fixed points. The ideal $\mathfrak{o}$ is generated by the zero-gon $\mathfrak{O}$.

The product of two or more ideals is generated by the product of the zero polygons of the factors, and the greatest common divisor and least common multiple of two ideals by the greatest common divisor and the least common multiple of the corresponding zero polygons.

7. *Theorem.* If z is any variable in Ω and n the degree of the field Ω with respect to z , then z takes every determinate value c at exactly n points. — For if $\mathfrak{o}$ denotes the system of all integral functions of z and c a finite constant, then

$$\mathfrak{o}(z - c) = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots, \quad e_1 + e_2 + \dots = n \quad (\S 9, 7.),$$

if $\mathfrak{p}_1, \mathfrak{p}_2, \dots$ denote mutually different prime ideals in z . If one denotes by $\mathfrak{P}_1, \mathfrak{P}_2, \dots$ the zero points of $\mathfrak{p}_1, \mathfrak{p}_2, \dots$, then by 2. z has the value c at e_1 points $\mathfrak{P}_1$ (or at $\mathfrak{P}_1^{e_1}$), at e_2 points $\mathfrak{P}_2$ (or at $\mathfrak{P}_2^{e_2}$), and so on, hence at the n points of the polygon $\mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \dots$. Conversely: if $\mathfrak{P}$ is a point at which z has the value c , and $\mathfrak{p}$ the prime ideal in z generated by $\mathfrak{P}$, then $z \equiv c \pmod{\mathfrak{p}}$, and consequently $\mathfrak{p}$ is one of the ideals $\mathfrak{p}_1, \mathfrak{p}_2, \dots$, and hence $\mathfrak{P}$ one of the points $\mathfrak{P}_1 \mathfrak{P}_2 \dots$. But the same result also holds for $c = \infty$; for because n is also the degree of Ω with respect to $\frac{1}{z}$, the latter variable takes the value 0, and consequently z the value ∞ , at exactly n points. From § 11 it follows that only for a finite number

of values of the constant c can one of the exponents $e_1, e_2, \dots$ be greater than 1.

The number n , i.e. the number of points at which the function z has any one constant value, shall be called the *order* of the function z . The constants, and *only* these, have the order zero. For all other functions in Ω the order is a positive integer. The order of a variable z is at the same time the degree of the field Ω with respect to z .

§ 16. Conjugate points and conjugate values.

1. *Definition.* If c is a determinate numerical value, there corresponds to it, as shown in § 15, a polygon $\mathfrak{A}$ of n (equal or different) points $\mathfrak{P}', \mathfrak{P}'', \dots \mathfrak{P}^{(n)}$, at which the variable z of the n^{th} order has just this value; these n points shall be called *conjugate with respect to z* ; by one of them (and by the variable z) the rest are determined. If one lets c take all values in succession, the polygon $\mathfrak{A} = \mathfrak{P}' \mathfrak{P}'' \dots \mathfrak{P}^{(n)}$ moves, and indeed in such a way that all its points always change. One thus obtains all points that exist at all, and only those (finite in number) several times at which $z - z_0$ or $\frac{1}{z}$ vanishes in higher than the first order. Therefore the product of all these polygons is

$$\Pi \mathfrak{A} = T \mathfrak{Z}_z,$$

where T is the simple totality of all points, the *Riemann surface*, and $\mathfrak{Z}_z$ a determinate finite polygon, which is called the *ramification* or *winding polygon of T in z* . Every point Ω contained in $\mathfrak{Z}_z$ is called a *ramification* or *winding point of T in z* , and indeed of the order s if it occurs exactly s times in $\mathfrak{Z}_z$. We have $s = e - 1$ if $z - z_0$ or $\frac{1}{z}$ is infinitely small of the e^{th} order at Ω . The order of the polygon $\mathfrak{Z}_z$ is called the *ramification* or *winding number* w_z of the surface T with respect to z . Those points of the ramification polygon at which z has a finite value together generate the *ramification ideal* in z (§ 11).

If one wishes to pass from this definition of the “absolute” *Riemann* surface, which is an invariant notion belonging to the field Ω , to the familiar conception of *Riemann*, one has to think of the surface

as spread out over a z -plane, which it then covers n -fold everywhere with the exception of the branch points.

2. *Theorem.* If

$$z' = \frac{c + dz}{a + bz},$$

where a, b, c, d denote constants whose determinant $ad - bc$ is different from zero, then

$$3_z = 3_{z'}; \quad w_z = w_{z'}.$$

For if at a point $\mathfrak{P}$ $z - z_0$ or $\frac{1}{z}$ is infinitely small of the e^{th} order, then at the same point

$$z' - z'_0 = \frac{(ad - bc)(z - z_0)}{(a + bz)(a + bz_0)},$$

or, if z_0 is infinite:

$$z' - z'_0 = \frac{-(ad - bc)}{b(a + bz)},$$

or, if $z'_0 = \infty$, hence $a + bz_0 = 0$:

$$\frac{1}{z'} = \frac{a + bz}{c + dz}$$

is also infinitely small of the e^{th} order.

If in particular $z' = \frac{1}{z}$, then the ramification number $w_z = w_{z'}$ is equal to the degree of the discriminant $\Delta_z(\Omega)$ increased by the number of vanishing roots of $\Delta_{z'}(\Omega) = 0$ (§ 11).

3. *Definition.* The values $\eta', \eta'', \dots \eta^{(n)}$ which an arbitrary function η in Ω takes at n points $\mathfrak{P}', \mathfrak{P}'', \dots \mathfrak{P}^{(n)}$ conjugate with respect to z are called *conjugate values of η with respect to z* .

4. *Theorem.* If $N_z(\eta)$ is the norm of an arbitrary function η with respect to z , then the value which this rational function of z possesses for $z = z_0$ is equal to the product $\eta' \eta'' \dots \eta^{(n)}$ of the conjugate values of η belonging to $z = z_0$, the case in which this product becomes indeterminate, i.e. in which one of these conjugate values is 0 and another ∞ , being disregarded. In the proof of this theorem we may assume that z_0 is finite; for if $z_0 = \infty$, we take as foundation, instead of z , the variable $z' = \frac{1}{z}$, whereby the norm remains unchanged. Further we may assume that the values $\eta', \eta'', \dots \eta^{(n)}$ are all finite; for if one of them is infinite, then by hyp. none of them is equal to 0, and we consider instead of η the function $\frac{1}{\eta}$.

Now under these assumptions let

$$\mathfrak{o}(z - z_0) = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \mathfrak{p}_3^{e_3} \dots$$

and let $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3, \dots$ be the zero points of the mutually different prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \dots$. We construct a system of integral functions λ, μ of z by the following rule: Let

λ_1	divisible	by	$\mathfrak{p}_1$,	not	by	$\mathfrak{p}_1^2$;
λ_2	"	"	$\mathfrak{p}_2$,	"	"	$\mathfrak{p}_2^2$;
λ_3	"	"	$\mathfrak{p}_3$,	"	"	$\mathfrak{p}_3^2$;
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
μ_1	divisible	by	$\mathfrak{p}_2^{e_2}, \mathfrak{p}_3^{e_3}, \dots$,	not	by	$\mathfrak{p}_1, \mathfrak{p}_2^{e_2+1}, \mathfrak{p}_3^{e_3+1}, \dots$;
μ_2	"	"	$\mathfrak{p}_1^{e_1}, \mathfrak{p}_3^{e_3}, \dots$,	"	"	$\mathfrak{p}_2, \mathfrak{p}_1^{e_1+1}, \mathfrak{p}_3^{e_3+1}, \dots$;
μ_3	"	"	$\mathfrak{p}_1^{e_1}, \mathfrak{p}_2^{e_2}, \dots$,	"	"	$\mathfrak{p}_3, \mathfrak{p}_1^{e_1+1}, \mathfrak{p}_2^{e_2+1}, \dots$ *).
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

The n functions

$$\begin{array}{ccccccc} \mu_1, & \mu_1 \lambda_1, & \mu_1 \lambda_1^2, & \dots & \mu_1 \lambda_1^{e_1-1}, \\ \mu_2, & \mu_2 \lambda_2, & \mu_2 \lambda_2^2, & \dots & \mu_2 \lambda_2^{e_2-1}, \\ \mu_3, & \mu_3 \lambda_3, & \mu_3 \lambda_3^2, & \dots & \mu_3 \lambda_3^{e_3-1}, \\ \dots & \dots & \dots & \dots & \dots \end{array}$$

which we denote by $\eta_1, \eta_2, \dots, \eta_n$, then form a basis of Ω ; this assertion is contained in the more general one now to be proved.

If

$$(z - z_0)\zeta = x_1\eta_1 + x_2\eta_2 + \dots + x_n\eta_n$$

with integral rational coefficients $x_1, x_2, \dots, x_n$, and ζ has finite values $\zeta', \zeta'', \zeta''', \dots$ at the points $\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3, \dots$, then all the coefficients $x_1, x_2, \dots, x_n$ must be divisible by $z - z_0$. Indeed, e.g. at the point $\mathfrak{P}_1$ the left-hand side is infinitely small of at least the order e_1 . Hence by § 15, 5. also

$$x_1\eta_1 + x_2\eta_2 + \dots + x_{e_1}\eta_{e_1} = \mu_1(x_1 + x_2\lambda_1 + \dots + x_{e_1}\lambda_1^{e_1-1})$$

must be infinitely small of this order. But this is possible only if $x_1, x_2, \dots, x_{e_1}$ vanish at $\mathfrak{P}_1$, hence are divisible by $z - z_0$, q. e. d.

*) The possibility of determining such functions follows from § 9, 3., note, or also from § 11, 2., according to which one can set, e.g.,

$$\lambda = \varrho - b, \quad \mu\lambda^e = \psi(\varrho).$$

Accordingly we can set:

$$\begin{aligned} \eta\mu_1\lambda_1^r &= \mu_1(x_1^{(0)} + x_1^{(1)}\lambda_1 + \dots + x_1^{(e_1-1)}\lambda_1^{e_1-1}) \\ &\quad + \mu_2(x_2^{(0)} + x_2^{(1)}\lambda_2 + \dots + x_2^{(e_2-1)}\lambda_2^{e_2-1}) \\ &\quad + \mu_3(x_3^{(0)} + x_3^{(1)}\lambda_3 + \dots + x_3^{(e_3-1)}\lambda_3^{e_3-1}) + \dots, \end{aligned}$$

where the $x_1^{(0)}, x_1^{(1)}, \dots, x_2^{(0)}, \dots$ are rational functions of z which all remain finite for $z = z_0$. At the points $\mathfrak{P}_2, \mathfrak{P}_3, \dots$ the left-hand side is infinitely small of at

least the order $e_2, e_3, \dots$. The same holds at $\mathfrak{P}_2$ of $\mu_1, \mu_3, \dots$ but not of μ_2 , and at $\mathfrak{P}_3$ of $\mu_1, \mu_2, \dots$ but not of $\mu_3, \dots$; consequently for $z = z_0$

$$\begin{aligned} x_2^{(0)} = 0, \quad x_2^{(1)} = 0, \quad \dots \quad x_2^{(e_2-1)} = 0, \\ x_3^{(0)} = 0, \quad x_3^{(1)} = 0, \quad \dots \quad x_3^{(e_3-1)} = 0, \\ \dots \dots \dots \end{aligned}$$

At $\mathfrak{P}_1$ the left-hand side is infinitely small of at least the order r ; therefore, if $r < e_1$, for $z = z_0$

$$x_1^{(0)} = 0, \quad x_1^{(1)} = 0, \quad \dots \quad x_1^{(r-1)} = 0, \quad x_1^{(r)} = \eta'.$$

The same consideration can be applied to the functions $\eta\mu_2\lambda_2^r, \eta\mu_3\lambda_3^r, \dots$. If therefore one sets

$$\begin{aligned} \eta\eta_1 &= x_{1,1}\eta_1 + x_{1,2}\eta_2 + \dots + x_{1,n}\eta_n, \\ \eta\eta_2 &= x_{2,1}\eta_1 + x_{2,2}\eta_2 + \dots + x_{2,n}\eta_n, \\ &\dots \dots \dots \\ \eta\eta_n &= x_{n,1}\eta_1 + x_{n,2}\eta_2 + \dots + x_{n,n}\eta_n, \end{aligned}$$

then in the determinant

$$N(\eta) = \Sigma \pm x_{1,1}x_{2,2} \dots x_{n,n}$$

all the terms standing to the left of the diagonal will vanish for $z = z_0$, while of the diagonal terms e_1 become equal to η' , e_2 equal to η'' , e_3 equal to η''' , $\dots$. Hence for $z = z_0$

$$N(\eta) = \eta'^{e_1} \eta''^{e_2} \eta'''^{e_3} \dots$$

q. e. d.

5. Since by the definition of the trace (§ 2)

$$S(\eta) = x_{1,1} + x_{2,2} + \dots + x_{n,n}$$

the same considerations lead to the theorem:

For $z = z_0$

$$S(\eta) = e_1\eta' + e_2\eta'' + e_3\eta''' + \dots,$$

which however holds only under the assumption that the values $\eta', \eta'', \eta''', \dots$ are finite.

Theorem 4. yields, for an arbitrary constant t (or one depending rationally on z), for $z = z_0$

$$N(t - \eta) = (t - \eta')^{e_1} (t - \eta'')^{e_2} (t - \eta''')^{e_3} \dots,$$

and from this, by comparison of the coefficients of equal powers of t , an expression for each of these coefficients by the conjugate values (symmetric functions).

6. If $\eta_1, \eta_2, \dots, \eta_n$ is a basis of Ω , then by application of 5. there results at once the value of the discriminant of this system for $z = z_0$

$$\Delta_z(\eta_1, \eta_2, \dots, \eta_n) = (\Sigma \pm \eta'_1 \eta''_2 \dots \eta_n^{(n)})^2,$$

if $\eta'_i, \eta''_i, \dots, \eta_i^{(n)}$ denote all the conjugate values of η_i belonging to $z = z_0$, equal or different, but assumed to be finite.

§ 17. Representation of the functions of the field Ω by quotients of polygons.

A function η of the field Ω has an order number different from zero at only a finite number of points; the sum of all the order numbers is equal to 0, hence the sum of the positive equal to the sum of the negative order numbers, and indeed equal to the order of the function η (§ 15). If the order numbers of a function η are known for every point $\mathfrak{P}$, then the function η is thereby determined up to a constant factor; for if η' has everywhere the same order number as η , then $\frac{\eta}{\eta'}$ has (by § 15, 5.) everywhere the order number zero and is therefore (by § 15, 7.) a constant.

If therefore we form a polygon $\mathfrak{A}$, into which we take every point at which η has a positive order number as often as this order number indicates, and a second polygon $\mathfrak{B}$, into which we take in a corresponding way the points at which η has a negative order number, then the polygons $\mathfrak{A}, \mathfrak{B}$ are of equal order, and indeed of the order of the function η . By these polygons $\mathfrak{A}, \mathfrak{B}$ the function η is therefore determined up to a constant factor. We set in symbolic notation

$$\eta = \frac{\mathfrak{A}}{\mathfrak{B}},$$

and call $\mathfrak{A}$ the *upper polygon*, $\mathfrak{B}$ the *lower polygon* of the function η^*).

By this stipulation the two polygons $\mathfrak{A}, \mathfrak{B}$ are relatively prime; but it is expedient to extend the notation so that common factors are also admitted in $\mathfrak{A}, \mathfrak{B}$, which is done by the stipulation that

$$\frac{\mathfrak{M}\mathfrak{A}}{\mathfrak{M}\mathfrak{B}} = \frac{\mathfrak{A}}{\mathfrak{B}}$$

shall hold, if $\mathfrak{M}$ denotes an arbitrary polygon. If according to this generalized notation we set

$$\eta = \frac{\mathfrak{A}}{\mathfrak{B}},$$

then a point $\mathfrak{P}$ at which η possesses the order number m can be taken m_1 times into $\mathfrak{A}$ and m_2 times into $\mathfrak{B}$, if $m_1 - m_2 = m$. Even now the order of $\mathfrak{A}$ is equal to that of $\mathfrak{B}$, but no longer equal to the order of the function η .

From this definition there follows immediately (by § 15, 5.) the theorem: If

$$\eta = \frac{\mathfrak{A}}{\mathfrak{B}}, \quad \eta' = \frac{\mathfrak{A}'}{\mathfrak{B}'},$$

then

$$\eta\eta' = \frac{\mathfrak{A}\mathfrak{A}'}{\mathfrak{B}\mathfrak{B}'}, \quad \frac{\eta}{\eta'} = \frac{\mathfrak{A}\mathfrak{B}'}{\mathfrak{B}\mathfrak{A}'}.$$

By § 14, 5. a function η' is an integral function of η if and only if every point going into the lower polygon of η' is also contained in that of η .

§ 18. Equivalent polygons and polygon classes.

1. *Definition.* Two polygons $\mathfrak{A}, \mathfrak{A}'$ with the same number of points are called *equivalent*, if there exists a function η in Ω which (by § 17) has the notation:

*) All functions of the simple family (η) accordingly have the same notation $\frac{\mathfrak{A}}{\mathfrak{B}}$, and it would therefore be more correct to set $(\eta) = \frac{\mathfrak{A}}{\mathfrak{B}}$; however, this notation leads to unnecessary prolixity.

$$\eta = \frac{\mathfrak{A}}{\mathfrak{A}'}.$$

2. *Theorem.* If $\mathfrak{A}$ is equivalent to $\mathfrak{A}'$ and to $\mathfrak{A}''$, then $\mathfrak{A}'$ is also equivalent to $\mathfrak{A}''$; for from

$$\eta' = \frac{\mathfrak{A}'}{\mathfrak{A}}; \quad \eta'' = \frac{\mathfrak{A}''}{\mathfrak{A}}$$

it follows:

$$\frac{\eta'}{\eta''} = \frac{\mathfrak{A}'}{\mathfrak{A}''}.$$

3. *Definition and theorem.* All the polygons $\mathfrak{A}', \mathfrak{A}'', \dots$ equivalent to a given polygon $\mathfrak{A}$ form a *polygon class* A . By 2. every polygon whatever then occurs in one and *only* one class; for if $\mathfrak{A}, \mathfrak{B}$ are two equivalent polygons which lead to the classes A, B , then by 2. every polygon of the class B is at the same time contained in A and conversely, and therefore the two classes are identical.

All the polygons of a class have the same order, which shall be called the *order of the class*.

4. But there may exist polygons which are equivalent to no other, and each of which therefore forms a class by itself. Such polygons may be called *isolated*.

5. If $\mathfrak{M}$ is an arbitrary polygon, and $\mathfrak{A}$ equivalent to $\mathfrak{A}'$, then $\mathfrak{M}\mathfrak{A}$ is also equivalent to $\mathfrak{M}\mathfrak{A}'$; but conversely too, from the equivalence of $\mathfrak{M}\mathfrak{A}$ with $\mathfrak{M}\mathfrak{A}'$ follows the equivalence of $\mathfrak{A}$ with $\mathfrak{A}'$.

6. If $\mathfrak{A}$ is equivalent to $\mathfrak{A}'$, and $\mathfrak{B}$ to $\mathfrak{B}'$, then $\mathfrak{A}\mathfrak{B}$ is also equivalent to $\mathfrak{A}'\mathfrak{B}'$. The class C to which the product $\mathfrak{A}\mathfrak{B}$ belongs therefore comprises all the products of any two polygons of the classes A, B of $\mathfrak{A}$ and $\mathfrak{B}$ (but besides, in certain circumstances, infinitely many other polygons as well), and shall be designated as the *product* of the two classes A, B :

$$C = AB = BA.$$

The definition of the product of several classes and the validity of the fundamental theorem of multiplication follow from this of themselves.

7. If A, B, D are three classes which satisfy the condition

$$DA = DB$$

then $A = B$ follows; for if $\mathfrak{A}, \mathfrak{B}, \mathfrak{D}$ are three polygons of the classes A, B, D , it follows from the assumption that $\mathfrak{D}\mathfrak{B}$ is equivalent to $\mathfrak{D}\mathfrak{A}$, and consequently $\mathfrak{B}$ to $\mathfrak{A}$.

8. If a polygon $\mathfrak{A}$ of the class A goes into a polygon $\mathfrak{C}$ of the class C , then the same holds of every polygon $\mathfrak{A}'$ of the class A ; for from $\mathfrak{C} = \mathfrak{A}\mathfrak{B}$ it follows by 5. that $\mathfrak{C}' = \mathfrak{A}'\mathfrak{B}$ is contained in C , and we may therefore say, although conversely not every polygon of the class C need be divisible by a polygon of the class A , *that the class C is divisible by the class A* . If $\mathfrak{B}'$ is any polygon of the class B of $\mathfrak{B}$, then $\mathfrak{C}'' = \mathfrak{A}'\mathfrak{B}'$ too is contained in C , and consequently

$$C = AB.$$

If therefore C is divisible by A , there is one and (by 7.) *only* one class B which satisfies the condition

$$C = AB$$

§ 19. The polygon families.

1. If $\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s$ are determinate and indeed equivalent polygons, and $\mathfrak{A}$ an arbitrary polygon of the same class A , then there exist s functions in Ω

$$\eta_1 = \frac{\mathfrak{A}_1}{\mathfrak{A}}, \quad \eta_2 = \frac{\mathfrak{A}_2}{\mathfrak{A}}, \quad \dots \quad \eta_s = \frac{\mathfrak{A}_s}{\mathfrak{A}}.$$

If one sets, as in § 15, 5., for an arbitrary point $\mathfrak{P}$

$$\begin{aligned} \eta_1 &= e_1 \varrho^m + \sigma_1 \varrho^{m+1}, \\ \eta_2 &= e_2 \varrho^m + \sigma_2 \varrho^{m+1}, \\ &\dots\dots\dots \\ \eta_s &= e_s \varrho^m + \sigma_s \varrho^{m+1}, \end{aligned}$$

where ϱ is 0^1 at $\mathfrak{P}$, $e_1, e_2, \dots, e_s$ denote constants which do not all vanish, and $\sigma_1, \sigma_2, \dots, \sigma_s$ functions finite at $\mathfrak{P}$, it follows that every function η of the family $(\eta_1, \eta_2, \dots, \eta_s)$, i.e. every function of the form

$$\eta = c_1 \eta_1 + c_2 \eta_2 + \dots + c_s \eta_s$$

has at $\mathfrak{P}$ an order number which is not smaller than m , and from this, by § 17, that the function η can be put in the form

$$\eta = \frac{\mathfrak{A}'}{\mathfrak{A}}$$

where $\mathfrak{A}'$ is likewise contained in the class A .

If for $\mathfrak{A}$ one chooses any other polygon $\mathfrak{B}$ of the class A , and sets

$$\begin{aligned} \zeta &= \frac{\mathfrak{A}}{\mathfrak{B}}, \\ \eta_1 \zeta &= \eta'_1 = \frac{\mathfrak{A}_1}{\mathfrak{B}}, \quad \eta_2 \zeta = \eta'_2 = \frac{\mathfrak{A}_2}{\mathfrak{B}}, \quad \dots \quad \eta_s \zeta = \eta'_s = \frac{\mathfrak{A}_s}{\mathfrak{B}}, \end{aligned}$$

then also

$$\eta \zeta = \eta' = c_1 \eta'_1 + c_2 \eta'_2 + \dots + c_s \eta'_s,$$

and consequently

$$\eta' = \frac{\mathfrak{A}'}{\mathfrak{B}}.$$

Every polygon generated by the denominator $\mathfrak{A}$ and a system of constants $c_1, c_2, \dots, c_s$ is therefore also generated by every other denominator $\mathfrak{B}$ belonging to the same class, and the totality of all the polygons $\mathfrak{A}'$ corresponding to the different values of the constants $c_1, c_2, \dots, c_s$ depends only on the polygons $\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s$. This totality shall therefore be called a *polygon family* with the basis $\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s$ and denoted by

$$(\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s)$$

2. If the polygons $\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s$ have a greatest common divisor $\mathfrak{M}$, then by 1. it is also a divisor of every polygon $\mathfrak{A}'$ of the family $(\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s)$, and can be called the *divisor of the family*; but a polygon $\mathfrak{A}' = \mathfrak{M}\mathfrak{B}$ can be determined in this family such that $\mathfrak{B}$ becomes relatively prime to an arbitrarily given polygon. For if, keeping the notation of 1., a point $\mathfrak{P}$ is contained exactly μ times in $\mathfrak{M}$ and ν times in $\mathfrak{A}$, then, if

$$\eta = e\varrho^m + \sigma\varrho^{m+1}$$

is set, m is never smaller than $\mu - \nu$, and $m = \mu - \nu$ if one chooses the constants $c_1, c_2, \dots, c_s$ such that

$$e = c_1e_1 + c_2e_2 + \dots + c_se_s$$

is different from zero. The point $\mathfrak{P}$ is therefore contained at least μ times in $\mathfrak{A}'$, and under the latter assumption also not more often than μ times. Now since one can always choose the constants $c_1, c_2, \dots, c_s$ such that an arbitrary number of expressions of the form

$$\Sigma c_i e_i, \quad \Sigma c_i e'_i, \quad \dots,$$

in none of which all the constants $e_i, e'_i, \dots$ vanish, have values different from zero, the correctness of the stated assertion follows.

3. If the functions $\eta_1, \eta_2, \dots, \eta_s$ in 1. are linearly dependent or independent, the same holds of the functions $\eta'_1, \eta'_2, \dots, \eta'_s$. Correspondingly we shall also call the polygons $\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s$ *linearly dependent* or *independent*, and their system *linearly reducible* or *irreducible*.

Since by § 5, 4. every family of functions possesses an irreducible basis, it follows that every polygon family also has an *irreducible basis*. If s is the number of polygons of such a basis, the family is called an *s-fold one*, or s the *dimension of the family*. Any s polygons of such a family form an irreducible basis of it or not, according as they are linearly independent or dependent. (Cf. § 5, 4.).

4. If the polygons $\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s$ are linearly dependent or independent, then, if $\mathfrak{M}$ denotes an arbitrary polygon, $\mathfrak{M}\mathfrak{A}_1, \mathfrak{M}\mathfrak{A}_2, \dots, \mathfrak{M}\mathfrak{A}_s$ too are linearly dependent or independent, and conversely.

§ 20. Lowering of the dimension of the family by conditions of divisibility.

1. Let

$$S = (\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s)$$

be an s -fold family with the divisor $\mathfrak{M}$. We ask for the manifold of those polygons $\mathfrak{A}'$ of the family S which contain an arbitrarily given point at least once more often than the divisor $\mathfrak{M}$ of the family.

If the point $\mathfrak{P}$ is contained μ times in $\mathfrak{M}$ and ν times in an arbitrary polygon $\mathfrak{A}$ equivalent to $\mathfrak{A}_1, \mathfrak{A}_2, \dots$, then, if as in § 19 we set

$$\begin{aligned} \frac{\mathfrak{A}_1}{\mathfrak{A}} &= \eta_1 = e_1 \varrho^m + \sigma_1 \varrho^{m+1}, \\ \frac{\mathfrak{A}_2}{\mathfrak{A}} &= \eta_2 = e_2 \varrho^m + \sigma_2 \varrho^{m+1}, \\ &\dots\dots\dots \\ \frac{\mathfrak{A}_s}{\mathfrak{A}} &= \eta_s = e_s \varrho^m + \sigma_s \varrho^{m+1} \end{aligned}$$

$m = \mu - \nu$, and of the constants $e_1, e_2, \dots, e_s$ at least one, say e_s , is different from zero. The polygons $\mathfrak{A}'$ sought are then characterized by the equation

$$\frac{\mathfrak{A}'}{\mathfrak{A}} = \eta' = c_1 \eta_1 + c_2 \eta_2 + \dots + c_s \eta_s,$$

where the constants $c_1, c_2, \dots, c_s$ are bound to the condition

$$c_1 e_1 + c_2 e_2 + \dots + c_s e_s = 0.$$

Accordingly we can set

$$\frac{\mathfrak{A}'}{\mathfrak{A}} = e_s \eta' = c_1 (e_s \eta_1 - e_1 \eta_s) + \dots + c_{s-1} (e_s \eta_{s-1} - e_{s-1} \eta_s).$$

But from this it follows, if we set

$$\begin{aligned} \eta'_1 &= e_s \eta_1 - e_1 \eta_s, \\ \eta'_2 &= e_s \eta_2 - e_2 \eta_s, \\ &\dots\dots\dots \\ \eta'_{s-1} &= e_s \eta_{s-1} - e_{s-1} \eta_s \end{aligned}$$

that the functions η' form an $(s-1)$ -fold family $(\eta'_1, \eta'_2, \dots, \eta'_{s-1})$; for the functions $\eta'_1, \eta'_2, \dots, \eta'_{s-1}$ are linearly independent if, as assumed, the functions $\eta_1, \eta_2, \dots, \eta_s$ are. Hence the polygons $\mathfrak{A}'$ too form an $(s-1)$ -fold family

$$S' = (\mathfrak{A}'_1, \mathfrak{A}'_2, \dots, \mathfrak{A}'_{s-1}),$$

if

$$\frac{\mathfrak{A}'_l}{\mathfrak{A}} = e_s \eta_l - e_l \eta_s$$

is set. The divisor of this family is divisible by $\mathfrak{M}\mathfrak{P}$, though not necessarily identical with it.

2. From this it follows at once that the polygons of a family S which are divisible by an arbitrary r -gon $\mathfrak{R}$ form an *at least* $(s - r)$ -fold family. For let us assume that this has already been proved for an r -gon $\mathfrak{R}$; then the correctness of the assertion for an $(r + 1)$ -gon $\mathfrak{P}\mathfrak{R}$ follows immediately from 1, since by the addition of the point $\mathfrak{P}$ the dimension is not changed further if $\mathfrak{P}$ is contained in the divisor of the family already reduced by $\mathfrak{R}$, and is otherwise lowered by 1.

From this it follows as a special case that in an s -fold family there is always *at least one* polygon which is divisible by a given $(s - 1)$ -gon.

3. If $r \leq s$, one can choose the r -gon $\mathfrak{R}$ such that the polygons of the family S divisible by $\mathfrak{R}$ form an exactly $(s - r)$ -fold family. To this end choose a point $\mathfrak{P}$ which is not contained in the divisor of S ; the polygons in S divisible by $\mathfrak{P}$ form by 1. an $(s - 1)$ -fold family S' ; choose a second point $\mathfrak{P}'$ which is not contained in the divisor of S' ; the polygons in S' which are divisible by $\mathfrak{P}'$, i.e. the polygons in S which are divisible by $\mathfrak{P}\mathfrak{P}'$, form an $(s - 2)$ -fold

family, and so on; at the same time it is clear from this mode of formation that $\mathfrak{R}$ may be assumed relatively prime to an arbitrarily given polygon. If $r = s$, then accordingly no polygon divisible by $\mathfrak{R}$ will exist in S .

§ 21. The dimensions of the polygon classes.

1. *The polygons of a class form a family of finite dimension, which shall be called the dimension of the class.*

Proof. If in a class A , whose order may be m , one selects any s polygons $\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s$, then all the polygons of the family $(\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s)$ belong at the same time to the class A . The number of linearly independent polygons contained in A can therefore certainly not be greater than $m + 1$, because otherwise (by § 20, 2.) one could find in the class a polygon divisible by an arbitrary $(m + 1)$ -gon, which is absurd. If therefore s is the maximum number of linearly independent polygons $\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s$ of the class A , every polygon of this class must be contained in the family $(\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s)$, and s is the *dimension of the class*. The system of polygons $\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_s$ shall be called a *basis of the class*.

The isolated polygons form classes of dimension 1.

2. If there are in a class C s , and not more, linearly independent polygons divisible by a given polygon $\mathfrak{A}$ of the class A

$$\mathfrak{C}_1 = \mathfrak{A}\mathfrak{B}_1, \quad \mathfrak{C}_2 = \mathfrak{A}\mathfrak{B}_2, \quad \dots \quad \mathfrak{C}_s = \mathfrak{A}\mathfrak{B}_s,$$

then C is divisible by A , and there exist in C also just as many linearly independent polygons

$$\mathfrak{C}'_1 = \mathfrak{A}'\mathfrak{B}_1, \quad \mathfrak{C}'_2 = \mathfrak{A}'\mathfrak{B}_2, \quad \dots \quad \mathfrak{C}'_s = \mathfrak{A}'\mathfrak{B}_s,$$

which are divisible by an arbitrary polygon $\mathfrak{A}'$ equivalent to $\mathfrak{A}$. (§ 18, 8.; § 19, 4.). This number s therefore depends only on the two classes A , C and can

fittingly be denoted by (A, C) . The value of the symbol (A, C) is to be set equal to 0 if C is not divisible by A . The dimension of a class A is accordingly denoted by (O, A) , where O denotes the class consisting of the zero-gon $\mathfrak{O}$. If (by § 18, 8.)

$$C = AB,$$

it follows:

$$(A, C) = (A, AB) = (O, B); \quad (1.)$$

for the polygons $\mathfrak{B}_1, \mathfrak{B}_2, \dots \mathfrak{B}_s$, which are all contained in B , are linearly independent, hence (O, B) is certainly not smaller than s . If conversely $\mathfrak{B}$ is an arbitrary polygon of the class B , then $\mathfrak{A}\mathfrak{B}$ is contained in C , hence also in the family $(\mathfrak{A}\mathfrak{B}_1, \mathfrak{A}\mathfrak{B}_2, \dots \mathfrak{A}\mathfrak{B}_s)$, and consequently $\mathfrak{B}$ is contained in the family $(\mathfrak{B}_1, \mathfrak{B}_2, \dots \mathfrak{B}_s)$, i.e. $(O, B) = s$.

If a is the order of the class A , then by § 20, 2. $(A, C) \geq (O, C) - a$, and from this follows by means of (1.) the general theorem

$$(O, B) \geq (O, AB) - a. \quad (2.)$$

3. If all¹⁶ the basis polygons of a class A have the greatest common divisor $\mathfrak{M}$, then this is also a divisor of all the polygons of the class A . If $\mathfrak{M}$ is equal to the zero-gon $\mathfrak{O}$, the class is called a *proper* one, in the opposite case an *improper* one with the divisor $\mathfrak{M}$.

If in all the polygons of an improper class A one suppresses the divisor $\mathfrak{M}$, one obtains a proper class A' of lower order but of the same dimension. This relation of A to A' shall be expressed by the sign

$$A = \mathfrak{M}A'.$$

4. The¹⁷ divisor $\mathfrak{M}$ of an improper class A is always an isolated polygon. For if

$$A = \mathfrak{M}A',$$

then by § 19, 2. one can choose in the proper class A' a polygon $\mathfrak{A}'$ such that it is relatively prime to $\mathfrak{M}$. If therefore $\mathfrak{M}'$ is equivalent to $\mathfrak{M}$, then $\mathfrak{M}'\mathfrak{A}'$ is equivalent to $\mathfrak{M}\mathfrak{A}'$, hence contained in A , and consequently divisible by $\mathfrak{M}$. Hence $\mathfrak{M}'$ too is divisible by $\mathfrak{M}$, and since $\mathfrak{M}$ and $\mathfrak{M}'$ are of the same order,

$$\mathfrak{M} = \mathfrak{M}'.$$

Accordingly the single polygon $\mathfrak{M}$ forms a class M , and the notation $\mathfrak{M}A'$ is equivalent to MA' (§ 18, 6.).

¹⁶ *Editorial note:* Printed “sämmmtlichen” with three m; read “sämmtlichen”. An apparent misprint.

¹⁷ *Editorial note:* Printed “Dêr” with a circumflex-like mark over the e; read “Der”. Probably a stray or damaged piece of type.

§ 22. The normal bases of $\mathfrak{o}$.

1. In what follows we consider the system $\mathfrak{o}$ of the integral functions ω of an arbitrary variable z in Ω , and at the same time the system $\mathfrak{o}'$ of the integral functions ω' of $z' = \frac{1}{z}$. From the definition of the integral functions

it becomes clear at once that the two systems $\mathfrak{o}, \mathfrak{o}'$ have *only* the constants in common with each other, but that on the other hand *every* function ω can be converted into a function ω' by multiplication by a determinate positive power of z' . If $\omega z'^r$ is contained in $\mathfrak{o}'$, the same also holds of $\omega z'^{r+1}, \omega z'^{r+2}, \dots$. In the series of functions

$$\omega, \quad \frac{\omega}{z} = z'\omega, \quad \frac{\omega}{z^2} = z'^2\omega, \quad \dots$$

therefore, from a determinate term $\omega z'^r$ on, all the following functions will be contained in $\mathfrak{o}'$, while all the preceding ones are not contained in it. The smallest number r for which $z'^r\omega$ is contained in $\mathfrak{o}'$ shall be called the *exponent* of the function ω with respect to z . The constants, and only these, have the exponent zero. If ω is different from zero, and r its exponent, then $r+1$ is the exponent of $(z-c)\omega$; for if $\omega = z^r\omega'$, then

$$\begin{aligned} \frac{(z-c)\omega}{z^{r+1}} &= (1-cz')\omega' \quad \text{is contained in } \mathfrak{o}', \\ \frac{(z-c)\omega}{z^r} &= z\omega' - c\omega' \quad \text{is not contained in } \mathfrak{o}', \end{aligned}$$

since $c\omega'$, it is true, but not $z\omega' = \frac{\omega}{z^{r-1}}$, is contained in $\mathfrak{o}'$. From this it follows in general:

If x is an integral rational function of z of degree s , and r the exponent of ω , then $(r+s)$ is the exponent of $x\omega$.

2. We now select a system of functions $\lambda_1, \lambda_2, \dots, \lambda_n$ in $\mathfrak{o}$ according to the following rule:

Let λ_1 be a constant different from zero, e.g. 1; let λ_2 be, among those functions in $\mathfrak{o}$ which are not congruent to a constant with respect to the modulus $\mathfrak{o}z$, one of the lowest possible exponent r_2 , and so on; in general let λ_s be, among those functions in $\mathfrak{o}$ which are not congruent to a function of the family $(\lambda_1, \lambda_2, \dots, \lambda_{s-1}) \pmod{\mathfrak{o}z}$, one of the lowest possible exponent r_s . Since $(\mathfrak{o}, \mathfrak{o}z) = N(z) = z^n$ is of the n^{th} degree, there are in $\mathfrak{o}$ n , and not more, functions linearly independent with respect to the modulus $\mathfrak{o}z$ (§ 6), and therefore the series of functions $\lambda_1, \lambda_2, \lambda_3, \dots$ can contain neither more nor fewer than n terms. Then (§ 5)

$$\mathfrak{o} \equiv (\lambda_1, \lambda_2, \dots, \lambda_n) \pmod{\mathfrak{o}z}.$$

The exponents $r_1, r_2, \dots, r_n$ of the functions $\lambda_1, \lambda_2, \dots, \lambda_n$ satisfy the requirement

$$r_1 = 0, \quad 1 \leq r_2 \leq r_3 \leq \dots \leq r_n.$$

Every function in $\mathfrak{o}$ whose exponent is $< r_s$ is congruent with respect to the modulus $\mathfrak{o}z$ to a function from the $(s-1)$ -fold family

$$(\lambda_1, \lambda_2, \dots, \lambda_{s-1}).$$

These functions $\lambda_1, \lambda_2, \dots, \lambda_n$ form a basis of $\mathfrak{o}$, as results from the following consideration.

If this were not the case, one could (§ 3, 7.) determine a linear function $z - c$ and a system of constants $a_1, a_2, \dots, a_n$, not all vanishing, such that

$$a_1\lambda_1 + a_2\lambda_2 + \dots + a_n\lambda_n = (z - c)\omega$$

If among the constants a the last non-vanishing one is a_s , then also

$$a_1\lambda_1 + a_2\lambda_2 + \dots + a_s\lambda_s = (z - c)\omega,$$

and the exponent of ω is certainly smaller than r_s (because $\frac{(z-c)\omega}{z^{r_s}}$ is contained in $\mathfrak{o}'$). Hence ω , and consequently, since a_s is different from 0, also λ_s , is congruent to a function of the family $(\lambda_1, \lambda_2, \dots, \lambda_{s-1}) \pmod{\mathfrak{o}z}$, which is contrary to the assumption.

The functions $\lambda_1, \lambda_2, \dots, \lambda_n$ therefore form a basis of $\mathfrak{o}$, and this shall be called a *normal basis*. The characteristic properties of the normal basis are:

I. The functions $\lambda_1, \lambda_2, \dots, \lambda_n$ are linearly independent with respect to the modulus $\mathfrak{o}z$.

II. Every function in $\mathfrak{o}$ whose exponent is smaller than the exponent r_s of λ_s is contained in the form

$$c_1\lambda_1 + c_2\lambda_2 + \dots + c_{s-1}\lambda_{s-1} + z\omega_s,$$

where $c_1, c_2, \dots, c_{s-1}$ are constants and ω_s a function in $\mathfrak{o}$.

3. The functions contained in $\mathfrak{o}'$

$$\lambda'_1 = \frac{\lambda_1}{z^{r_1}}, \quad \lambda'_2 = \frac{\lambda_2}{z^{r_2}}, \quad \dots \quad \lambda'_n = \frac{\lambda_n}{z^{r_n}}$$

form a *normal basis* of $\mathfrak{o}'$.

For if ω is a function in $\mathfrak{o}$ not divisible by z , of exponent r , then the exponent of $\omega' = \frac{\omega}{z^r}$ with respect to z' is likewise r ; for $\frac{\omega'}{z'^r} = \omega$ is contained in $\mathfrak{o}$, but $\frac{\omega'}{z'^{r-1}} = \frac{\omega}{z}$ is not. Since the functions $\lambda_1, \lambda_2, \dots, \lambda_n$ are all not divisible by z ,

the exponents of $\lambda'_1, \lambda'_2, \dots, \lambda'_n$ with respect to z' are accordingly $r_1, r_2, \dots, r_n$ respectively. This premised, we prove that the system of functions $\lambda'_1, \lambda'_2, \dots, \lambda'_n$ possesses the properties I., II., if $\mathfrak{o}, z$ are there replaced by $\mathfrak{o}', z'$.

If the condition I. were not fulfilled, the constants $a_1, a_2, \dots, a_s$, of which the last does not vanish, could be determined such that

$$a_1\lambda'_1 + a_2\lambda'_2 + \dots + a_s\lambda'_s = z'\omega',$$

hence also (by multiplication by z'^{r_s})

$$a_1z'^{r_s-r_1}\lambda_1 + a_2z'^{r_s-r_2}\lambda_2 + \dots + a_s\lambda_s = \omega,$$

where

$$\omega = z'^{r_s-1}\omega',$$

would thus be a function in $\mathfrak{o}$ whose exponent is smaller than r_s . But this, since a_s is different from zero, is impossible because of the assumption about the λ , and consequently the condition I. is fulfilled; from this it follows:

$$\mathfrak{o}' \equiv (\lambda'_1, \lambda'_2, \dots, \lambda'_n) \pmod{\mathfrak{o}'z'}.$$

If the condition II. were not fulfilled, and λ' were a function in $\mathfrak{o}'$ whose exponent is $r < r_s$, which is not contained in the form

$$a_1\lambda'_1 + a_2\lambda'_2 + \dots + a_{s-1}\lambda'_{s-1} + z'\omega',$$

then one could choose $e \geq s$ such that

$$\lambda' = a_1\lambda'_1 + a_2\lambda'_2 + \dots + a_e\lambda'_e + z'\omega'$$

with constant coefficients, of which the last, a_e , does not vanish. Accordingly also $r_e \geq r_s > r$.

Hence $\lambda = z^{r_e-1}\lambda'$ is a function in $\mathfrak{o}$, and there results, by multiplication by z^{r_e} ,

$$z\lambda = a_1z^{r_e-r_1}\lambda_1 + a_2z^{r_e-r_2}\lambda_2 + \dots + a_e\lambda_e + z^{r_e-1}\omega'.$$

Therefore $\omega = z^{r_e-1}\omega'$ is a function in $\mathfrak{o}$ whose exponent is (by 1.) $\leq r_e - 1$, and which satisfies the congruence

$$\omega \equiv a'_1\lambda_1 + a'_2\lambda_2 + \dots + a'_e\lambda_e \pmod{\mathfrak{o}z},$$

where $a'_e = -a_e$ is different from zero. But then, because of the property II. of the functions λ , the exponent of $\omega \geq r_e$ would have to hold, from which the contradiction becomes clear.

It is thereby proved that the system of functions $\lambda'_1, \lambda'_2, \dots, \lambda'_n$ forms a normal basis of $\mathfrak{o}'$.

4. We now form the discriminant of Ω with respect to the variables z and z' with the help of the two normal bases λ, λ' ; we have:

$$\begin{aligned} \Delta_z(\Omega) &= \text{const.} \Delta(\lambda_1, \lambda_2, \dots, \lambda_n), \\ \Delta_{z'}(\Omega) &= \text{const.} \Delta(\lambda'_1, \lambda'_2, \dots, \lambda'_n). \end{aligned}$$

But if for λ'_i one puts the expressions $z'^{r_i}\lambda_i$, it follows from the theorem § 2, (13.)

$$\Delta_{z'}(\Omega) = \text{const.} z'^{2(r_1+r_2+\dots+r_n)} \Delta_z(\Omega).$$

If $\Delta_z(\Omega)$ is of degree δ , then $\Delta_{z'}(\Omega)$ possesses the root $z' = 0$ $(2(r_1 + r_2 + \dots + r_n) - \delta)$ times, and from this there results by § 16, 2. the *ramification number*

$$w_z = 2(r_1 + r_2 + \dots + r_n),$$

which is accordingly always an *even number*.

§ 23. The differential quotients.

1. Since every function of the field Ω different from zero has the value zero at only a finite number of points, it follows that a function in Ω of which infinitely many zero points can be shown to exist is necessarily identically zero, or that two functions in Ω which have the same value at infinitely many points must be identical.

2. If α, β are any two variables of the field Ω , there exists in Ω a function, to be denoted by $\left(\frac{d\alpha}{d\beta}\right)$, which at infinitely many points $\mathfrak{P}$ satisfies the condition:

$$\left(\frac{d\alpha}{d\beta}\right)_0 = \left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0,$$

and which is called the *differential quotient* of α with respect to β . For if $F(\alpha, \beta) = 0$ is the irreducible equation existing between α, β , then, if we first exclude those points (finite in number) at which α_0 or $\beta_0 = \infty$ or $F'(\alpha_0) = 0$ or $F'(\beta_0) = 0$,

$$0 = F(\alpha, \beta) = F(\alpha_0, \beta_0) + (\alpha - \alpha_0)F'(\alpha_0) + (\beta - \beta_0)F'(\beta_0) + \frac{1}{2}\{(\alpha - \alpha_0)^2 F''(\alpha_0, \alpha_0) + 2(\alpha - \alpha_0)(\beta - \beta_0)F''(\alpha_0, \beta_0) + (\beta - \beta_0)^2 F''(\beta_0, \beta_0)\} + \dots$$

Of the two quotients $\left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0, \left(\frac{\beta - \beta_0}{\alpha - \alpha_0}\right)_0$ one is certainly finite; if it is the former, we derive from the last equation the following:

$$0 = \frac{\alpha - \alpha_0}{\beta - \beta_0} F'(\alpha_0) + F'(\beta_0) + (\beta - \beta_0) \frac{1}{2} \left\{ \left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)^2 F''(\alpha_0, \alpha_0) + 2 \left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right) F''(\alpha_0, \beta_0) + F''(\beta_0, \beta_0) \right\} + \dots,$$

from which it follows for the point $\mathfrak{P}$:

$$\left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0 = -\frac{F'(\beta_0)}{F'(\alpha_0)} = -\left(\frac{F'(\beta)}{F'(\alpha)}\right)_0.$$

If $\left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0$ were infinite, we would infer in the same way with respect to $\frac{\beta - \beta_0}{\alpha - \alpha_0}$.
Thus

$$\left(\frac{d\alpha}{d\beta}\right) = -\frac{F'(\beta)}{F'(\alpha)} \quad (1.)$$

has the required property. This still remains true when one of the two functions α, β is constant; for if e.g. α is constant, then $F(\alpha, \beta) = \alpha - \alpha_0$ is independent of β , hence $F'(\alpha) = 1, F'(\beta) = 0$.

3. From the foregoing it follows that, if β is not constant, then apart from a *finite* number of points $\left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0$ is a finite value. If therefore γ is a third

variable in Ω , then at infinitely many points

$$\left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0 = \left(\frac{\alpha - \alpha_0}{\gamma - \gamma_0}\right)_0 \left(\frac{\gamma - \gamma_0}{\beta - \beta_0}\right)_0,$$

hence also

$$\left(\frac{d\alpha}{d\beta}\right)_0 = \left(\frac{d\alpha}{d\gamma}\right)_0 \left(\frac{d\gamma}{d\beta}\right)_0.$$

But by this and by 1. the identity is satisfied:

$$\left(\frac{d\alpha}{d\beta}\right) = \left(\frac{d\alpha}{d\gamma}\right) \left(\frac{d\gamma}{d\beta}\right)^*. \quad (2.)$$

4. In consequence of this last theorem we can assign to each of the functions $\alpha, \beta, \gamma, \dots$ of the field Ω a function $d\alpha, d\beta, d\gamma, \dots$ (differential) in

*) One can also define the differential quotient by the equation

$$\left(\frac{d\alpha}{d\beta}\right) = -\frac{F'(\beta)}{F'(\alpha)}$$

and arrive by algebraic division at the proof of the theorem

$$\left(\frac{d\alpha}{d\beta}\right) = \left(\frac{d\alpha}{d\gamma}\right) \left(\frac{d\gamma}{d\beta}\right)$$

such a way that in general

$$\frac{d\alpha}{d\beta} = \left(\frac{d\alpha}{d\beta}\right)$$

holds. The differentials of the constants, and *only* these, are to be set equal to zero; the rest are completely determined as soon as one of them has been assumed arbitrarily. If there exists between the variables $\alpha, \beta, \gamma, \dots$ a rational equation

$$F(\alpha, \beta, \gamma, \dots) = 0,$$

then it follows from it that

$$F'(\alpha) d\alpha + F'(\beta) d\beta + F'(\gamma) d\gamma + \dots = 0; \quad (3.)$$

for in the same way as in 2. one infers that this equation is satisfied for infinitely many points.

Immediate consequences of the last theorem are the familiar rules for the differentiation of sums, differences, products and quotients:

$$d(\alpha \pm \beta) = d\alpha \pm d\beta, \quad (4.)$$

$$d(\alpha\beta) = \alpha d\beta + \beta d\alpha, \quad (5.)$$

$$d\left(\frac{\alpha}{\beta}\right) = \frac{\beta d\alpha - \alpha d\beta}{\beta^2}. \quad (6.)$$

5. If ω is an *integral* function of z , then in general $\frac{d\omega}{dz}$ will not be an integral function of z . But it is evident from the expression (§ 3, 7.)

$$\omega = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n$$

since the differential quotients of the integral rational functions $x_1, x_2, \dots, x_n$ are again integral rational functions, that the lower ideals of all the functions $\frac{d\omega}{dz}$ must go into a determinate ideal, namely into the least common multiple of the lower ideals of $\frac{d\omega_1}{dz}, \frac{d\omega_2}{dz}, \dots, \frac{d\omega_n}{dz}$. It is to be investigated which ideal this is. To this end let $z - c$ be an arbitrary linear function of z and

$$\mathfrak{o}(z - c) = \mathfrak{p}^e \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots,$$

where the prime ideals $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \dots$ are different from one another. Now let ζ be the same function as in § 11, 2., i.e. an integral function of z which at the points $\mathfrak{P}, \mathfrak{P}_1, \mathfrak{P}_2, \dots$ generated by the prime ideals $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \dots$ has values all different, and each of them only simply;

then ω can be represented in the form

$$\omega = y_0 + y_1\zeta + \cdots + y_{n-1}\zeta^{n-1},$$

where the rational functions $y_0, y_1, \dots, y_{n-1}$ of z may indeed be fractional, but certainly do not contain the factor $z - c$ in the denominator. From this it follows that the lower ideal of $\frac{d\omega}{dz}$ can be divisible by no higher powers of the ideals $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \dots$ than the lower ideal of $\frac{d\zeta}{dz}$. But if

$$f(\zeta, z) = 0$$

is the irreducible equation existing between ζ and z , then by § 11, 2.

$$\mathfrak{o}f'(\zeta) = \mathfrak{m}\mathfrak{p}^{e-1} \mathfrak{p}_1^{e_1-1} \mathfrak{p}_2^{e_2-1} \dots$$

and $\mathfrak{m}$ is relatively prime to $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \dots$. But since

$$\frac{d\zeta}{dz} = -\frac{f'(z)}{f'(\zeta)}$$

the lower ideal of $\frac{d\zeta}{dz}$, and consequently also that of $\frac{d\omega}{dz}$, can contain none of the factors $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \dots$ more often than $(e-1), (e_1-1), (e_2-1), \dots$ times. Now since $z - c$ can be any linear function whatever, it follows that $\frac{d\omega}{dz}$ can have no other lower ideal than one which goes into the ramification ideal $\mathfrak{z} = \Pi \mathfrak{p}^{e-1}$ (§ 11). Hence, if $\mathfrak{a}$ denotes an ideal:

$$\mathfrak{z} \frac{d\omega}{dz} = \mathfrak{a},$$

hence by § 11, (7.)

$$\mathfrak{o} \frac{d\omega}{dz} = \mathfrak{e}\mathfrak{a},$$

from which it emerges that the functions $\frac{d\omega}{dz}$ all belong to the module $\mathfrak{e}$ complementary to $\mathfrak{o}$.

6. If the irreducible equation $F(\omega, z) = 0$ between ω and z is of the n^{th} degree with respect to ω , hence $1, \omega, \omega^2, \dots, \omega^{n-1}$ a basis of Ω , then by § 11, (10.)

$$\mathfrak{o}F'(\omega) = \mathfrak{z}\mathfrak{k},$$

and therefore, because of

$$\frac{d\omega}{dz} = -\frac{F'(z)}{F'(\omega)}$$

$\mathfrak{o}F'(z)$ must be divisible by the ideal $\mathfrak{k}$,

$$\mathfrak{o}F'(z) = \mathfrak{k}\mathfrak{a},$$

$\mathfrak{k}$ can therefore be called the *ideal of the double points* with respect to ω, z .

7. If $\mathfrak{P}$ is a point at which $z - c$ is infinitely small of the first order (hence not a branch point in z), then by 5. the functions $\frac{d\omega}{dz}$ are all finite at $\mathfrak{P}$. If therefore η is any function in Ω which is finite at $\mathfrak{P}$, one can represent it as the quotient of two integral functions $\frac{\alpha}{\beta}$, of which β does not vanish at $\mathfrak{P}$, and therefore by (6.) $\frac{d\eta}{dz}$ too is finite at $\mathfrak{P}$.

8. Now let α, β be any two variables in Ω ; the behaviour of $\frac{d\alpha}{d\beta}$ at any point $\mathfrak{P}$ is to be investigated.

Choose a variable z in Ω which is infinitely small of the first order at $\mathfrak{P}$. If α has a finite value α_0 at $\mathfrak{P}$, then by § 15, 1., 2. one can determine a positive integer r and a function α' finite and different from zero at $\mathfrak{P}$ such that

$$\alpha = \alpha_0 + z^r \alpha'$$

This still holds when α is infinite at $\mathfrak{P}$; only then r is a negative integer, and α_0 is to be replaced by an arbitrary finite constant, e.g. 0. Likewise one can set

$$\beta = \beta_0 + z^s \beta'$$

r and s are then the order numbers of $\alpha - \alpha_0, \beta - \beta_0$ at the point $\mathfrak{P}$, which can be positive as well as negative, but not 0. From (2.) there then results:

$$\frac{d\alpha}{d\beta} = z^{r-s} \frac{r\alpha' + z \frac{d\alpha'}{dz}}{s\beta' + z \frac{d\beta'}{dz}}$$

or

$$\frac{\beta - \beta_0}{\alpha - \alpha_0} \frac{d\alpha}{d\beta} = \frac{r + z \frac{d\alpha'}{\alpha' dz}}{s + z \frac{d\beta'}{\beta' dz}}.$$

If one now again denotes by the index 0 the value of a function at the point $\mathfrak{P}$, then, since

$$\left(\frac{d\alpha'}{\alpha' dz} \right)_0, \quad \left(\frac{d\beta'}{\beta' dz} \right)_0$$

are finite by 7.,

$$\left(\frac{\beta - \beta_0}{\alpha - \alpha_0} \frac{d\alpha}{d\beta} \right)_0 = \frac{r}{s}, \quad (7.)$$

hence finite and different from zero. From this it follows that *the order number of the differential quotient $\frac{d\alpha}{d\beta}$ is equal to the difference of the order numbers of $\alpha - \alpha_0$ and $\beta - \beta_0$* . If $r \geq s$, then $\left(\frac{\alpha - \alpha_0}{\beta - \beta_0} \right)_0$, and consequently $\left(\frac{d\alpha}{d\beta} \right)_0$, is zero or infinite. If on the other hand $r = s$, both values are finite and different from 0, and we therefore have in all cases

$$\left(\frac{\alpha - \alpha_0}{\beta - \beta_0} \right)_0 = \left(\frac{d\alpha}{d\beta} \right)_0. \quad (8.)$$

Here α_0, β_0 are the values of α, β at $\mathfrak{P}$ if these values are finite, otherwise arbitrary constants, e.g. 0.

9. If a, b are the order numbers of $\alpha - \alpha_0, \beta - \beta_0$ at $\mathfrak{P}$, then, if a, b are positive, the point $\mathfrak{P}$ occurs $(a - 1)$ times resp. $(b - 1)$ times in the ramification polygons $\mathfrak{Z}_\alpha, \mathfrak{Z}_\beta$ in α, β . But if a is negative, $\mathfrak{Z}_\alpha$ contains the point $\mathfrak{P}$ $(-a - 1)$ times, and correspondingly when b is negative (§ 16, 1.). If therefore one denotes by $\mathfrak{A}, \mathfrak{B}$ the lower polygons of α, β , one obtains, because the order number of $\frac{d\alpha}{d\beta}$ is (as just proved) always equal to $a - b$, the following expression for this function as a quotient of polygons

$$\frac{d\alpha}{d\beta} = \frac{\mathfrak{Z}_\alpha \mathfrak{B}^2}{\mathfrak{Z}_\beta \mathfrak{A}^2}. \quad (9.)$$

§ 24. The genus of the field Ω .

1. If one denotes by w_α, w_β the ramification numbers and by n_α, n_β the orders of the variables α, β , then from the formula (9.) of the preceding §, since the numerator and denominator of $\frac{d\alpha}{d\beta}$ must contain equally many points, there follows the important relation

$$w_\alpha - 2n_\alpha = w_\beta - 2n_\beta;$$

if therefore one sets

$$p = \frac{1}{2}w - n + 1 \quad (1.)$$

which by § 22, 4. is an integer, then this is independent of the choice of the variable and is a number characteristic of the field Ω ,

which is called the *genus* of the field Ω . That this number is never negative follows if for $\frac{1}{2}w$ one substitutes the value $r_1 + r_2 + \dots + r_n$ from § 22. One then obtains

$$p = (r_2 - 1) + (r_3 - 1) + \dots + (r_n - 1), \quad (2.)$$

which, since $r_2, r_3, \dots, r_n \geq 1$, cannot become negative.

2. Let α, β be two functions in Ω of the orders m, n , of such a nature that all functions in Ω can be represented rationally by α, β . Then

$$\begin{aligned} F(\alpha, \beta) &= a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n \\ &= b_0\beta^m + b_1\beta^{m-1} + \cdots + b_{m-1}\beta + b_m = 0 \end{aligned}$$

is the irreducible equation existing between α, β , where $a_0, a_1, \dots, a_n$ are integral rational functions of β , and likewise $b_0, b_1, \dots, b_m$ integral rational functions of α .

Let further

$$\alpha = \frac{\mathfrak{A}_1}{\mathfrak{A}}, \quad \beta = \frac{\mathfrak{B}_1}{\mathfrak{B}}$$

and $\mathfrak{A}_1$ relatively prime to $\mathfrak{A}$, and $\mathfrak{B}_1$ to $\mathfrak{B}$, so that $\mathfrak{A}, \mathfrak{A}_1$ are of the order m , and $\mathfrak{B}, \mathfrak{B}_1$ of the order n . Now

$$\begin{aligned} F'(\alpha) &= na_0\alpha^{n-1} + (n-1)a_1\alpha^{n-2} + \cdots + a_{n-1}, \\ \alpha F'(\alpha) &= -a_1\alpha^{n-1} - 2a_2\alpha^{n-2} - \cdots - na_n, \end{aligned}$$

from which it emerges that

$$F'(\alpha) = \frac{\mathfrak{K}}{\mathfrak{A}^{n-2}\mathfrak{B}^m}$$

and likewise

$$F'(\beta) = \frac{\mathfrak{L}}{\mathfrak{A}^n\mathfrak{B}^{m-2}}$$

must hold. It is now to be shown that the polygon $\mathfrak{K}$ is divisible by $\mathfrak{B}_\beta$, and $\mathfrak{L}$ by $\mathfrak{B}_\alpha$.

For $\mathfrak{K}$ this is easily seen under the assumption that at all points of $\mathfrak{B}_\beta$ the function β has a finite value and a_0 a value different from zero; for

$$\alpha' = a_0\alpha$$

is an integral function of β , and if one sets

$$f(\alpha') = a^{n-1}F(\alpha, \beta)$$

¹⁸ then

$$f'(\alpha') = a_0^{n-2}F'(\alpha).$$

Now since by § 11, 5. $\mathfrak{o}_\beta f'(\alpha')$ is divisible by the ramification ideal in β generated by $\mathfrak{B}_\beta$, the correctness of the assertion follows from this. The analogous holds for $F'(\beta)$.

If one now makes arbitrary linear substitutions for α, β :

$$\begin{aligned} \alpha &= \frac{c + d\alpha'}{a + b\alpha'}, & \beta &= \frac{c' + d'\beta'}{a' + b'\beta'}, \\ (a + b\alpha')(d - b\alpha) &= ad - bc, \\ (a' + b'\beta')(d' - b'\beta) &= a'd' - b'c', \end{aligned}$$

¹⁸ Editorial note: Printed a^{n-1} without the subscript; a_0^{n-1} is meant, as $\alpha' = a_0\alpha$ and the next line has a_0^{n-2} . Possibly a dropped subscript.

then by § 16, 2.

$$\mathfrak{Z}_\alpha = \mathfrak{Z}_{\alpha'}; \quad \mathfrak{Z}_\beta = \mathfrak{Z}_{\beta'},$$

and the irreducible equation existing between α', β' reads:

$$F_1(\alpha', \beta') = (a + b\alpha')^n (a' + b'\beta')^m F(\alpha, \beta) = 0.$$

But under all circumstances the constants $a, b, c, d; a', b', c', d'$ can be chosen such that the assumptions stated above are fulfilled both for α' and for β' .

For if one puts the coefficients a'_0, b'_0 of α'^n, β'^m in $F_1(\alpha', \beta')$ into the form

$$\begin{aligned} a'_0 &= (a' + b'\beta')^m (a_0 d^n + a_1 d^{n-1} b + \dots + a_n b^n) = \left(\frac{a' d' - b' c'}{d' - b' \beta} \right)^m (a_0 d^n + a_1 d^{n-1} b + \dots + a_n b^n), \\ b'_0 &= (a + b\alpha')^n (b_0 d'^m + b_1 d'^{m-1} b' + \dots + b_m b'^m) = \left(\frac{ad - bc}{d - b\alpha} \right)^n (b_0 d'^m + b_1 d'^{m-1} b' + \dots + b_m b'^m), \end{aligned}$$

one easily recognizes that only for a finite number of values of the ratios $d : b, d' : b'$ can the functions $a'_0, d' - b'\beta$ vanish at a point of $\mathfrak{Z}_\beta$, and $b'_0, d - b\alpha$ at a point of $\mathfrak{Z}_\alpha$.

Now if we set

$$\alpha' = \frac{\mathfrak{A}'_1}{\mathfrak{A}'}, \quad \beta' = \frac{\mathfrak{B}'_1}{\mathfrak{B}'},$$

it follows (§ 19, 1.)

$$d - b\alpha = \frac{\mathfrak{A}_2}{\mathfrak{A}}, \quad a + b\alpha' = \frac{\mathfrak{A}'_2}{\mathfrak{A}'},$$

hence:

$$\mathfrak{A}_2 \mathfrak{A}'_2 = \mathfrak{A} \mathfrak{A}'.$$

But if, as assumed, b is different from zero, then $\mathfrak{A}_2$ is relatively prime to $\mathfrak{A}$, because at a point of $\mathfrak{A}$ the order number of $d - b\alpha$ is the same as that of α (§ 15, 5.), and consequently

$$\mathfrak{A}_2 = \mathfrak{A}', \quad \mathfrak{A}'_2 = \mathfrak{A},$$

hence:

$$a + b\alpha' = \frac{\mathfrak{A}}{\mathfrak{A}'},$$

and likewise:

$$a' + b'\beta' = \frac{\mathfrak{B}}{\mathfrak{B}'},$$

But now, since $F(\alpha, \beta) = 0$:

$$F'_1(\alpha') = (ad - bc)(a + b\alpha')^{n-2} (a' + b'\beta')^m F'(\alpha),$$

and if therefore, as assumed:

$$F'_1(\alpha') = \frac{\mathfrak{A} \mathfrak{Z}_\beta}{\mathfrak{A}'^{n-2} \mathfrak{B}'^m},$$

it follows

$$F'(\alpha) = \frac{\mathfrak{A}\mathfrak{Z}_\beta}{\mathfrak{A}^{n-2}\mathfrak{B}^m}$$

and in the same way

$$F'(\beta) = \frac{\mathfrak{A}\mathfrak{Z}_\alpha}{\mathfrak{A}^n\mathfrak{B}^{m-2}}.$$

That the polygon $\mathfrak{A}$ occurring in the numerator of these two expressions must be the same in both follows from

$$\frac{d\alpha}{d\beta} = -\frac{F'(\beta)}{F'(\alpha)} = \frac{\mathfrak{B}^2\mathfrak{Z}_\alpha}{\mathfrak{A}^2\mathfrak{Z}_\beta}.$$

Now the order of the polygon $\mathfrak{A}^{n-2}\mathfrak{B}^m$ is

$$m(n-2) + mn = 2m(n-1),$$

hence the order of $\mathfrak{A}$

$$2r = 2m(n-1) - w_\beta$$

is always an even number, and from this there results

$$p = \frac{1}{2}w_\beta - n + 1 = (n-1)(m-1) - r. \quad (3.)$$

The polygon $\mathfrak{A}$ is called the *polygon of the double points* in (α, β) .

§ 25. The differentials in Ω .

If z, z_1 are any two variables in Ω of the orders n, n_1 and the ramification numbers w, w_1 , and further $\mathfrak{Z}, \mathfrak{Z}_1$ the ramification polygons and $\mathfrak{A}, \mathfrak{A}_1$ the lower polygons of z, z_1 , then (§ 23)

$$\frac{dz}{dz_1} = \frac{\mathfrak{Z}\mathfrak{A}_1^2}{\mathfrak{Z}_1\mathfrak{A}^2}. \quad (1.)$$

Every function ω in Ω can be put in the form

$$\omega = \frac{\mathfrak{A}^2\mathfrak{A}}{\mathfrak{Z}\mathfrak{B}}, \quad (2.)$$

where $\mathfrak{A}, \mathfrak{B}$ denote polygons whose orders a, b satisfy the condition

$$2n + a = w + b$$

or (§ 24)

$$a = b + 2p - 2. \quad (3.)$$

If one now explains a function ω_1 by the equation

$$\omega dz = \omega_1 dz_1,$$

then by (1.) ω_1 receives the notation

$$\omega_1 = \frac{\mathfrak{U}_1^2 \mathfrak{A}}{\mathfrak{Z}_1 \mathfrak{B}}.$$

In what follows we call such expressions as

$$\omega dz = \omega_1 dz_1$$

differentials in Ω , and denote them symbolically by a sign such as $d\varpi$. Such a differential is hereby explained *invariantly*, i.e. independently of the choice of the variable z , and is completely determined by the two polygons $\mathfrak{A}$, $\mathfrak{B}$.

We can, without danger of misunderstanding, use the symbolic notation

$$d\varpi = \frac{\mathfrak{A}}{\mathfrak{B}},$$

hence for example also

$$dz = \frac{\mathfrak{Z}}{\mathfrak{U}^2}$$

This notation of a differential by a quotient of polygons differs from the similar notation of the functions in Ω (§ 17) in that in the latter the numerator and denominator are of equal order, while with the differentials the order of the numerator exceeds that of the denominator by $2p - 2$. As in the notation of § 17, common divisors which $\mathfrak{A}$ and $\mathfrak{B}$ may contain can be suppressed here too. If $\mathfrak{A}$ and $\mathfrak{B}$ are relatively prime, $\mathfrak{A}$ is called the upper polygon and $\mathfrak{B}$ the lower polygon of the differential $d\varpi$.

Under the general notion of the differential in Ω set up here there fall, as special cases, also the differentials of the functions of the field Ω explained in § 23, 4. These we call *proper differentials*,

while the others, which cannot be represented as differentials of functions existing in Ω , are called *improper or Abelian differentials*.

Functions of the form (2.), which by our present stipulation can be denoted by $\frac{d\varpi}{dz}$, we call *differential quotients with respect to z* , and likewise distinguish between *proper* and *improper* differential quotients, according as $d\varpi$ is a proper or an improper differential*).

There now arises the task of establishing the extent of the notion of differentials, i.e. of finding all the polygons $\mathfrak{A}$, $\mathfrak{B}$ which can be the upper and lower polygon of a differential. We premise on this the following general remarks:

The necessary and sufficient condition for $\frac{\mathfrak{A}}{\mathfrak{B}}$ to be a differential is that for an arbitrary variable z

$$\frac{\mathfrak{U}^2 \mathfrak{A}}{\mathfrak{Z} \mathfrak{B}}$$

be a function in Ω , hence that $\mathfrak{U}^2 \mathfrak{A}$ be equivalent to $\mathfrak{Z} \mathfrak{B}$. But this relation persists if $\mathfrak{A}$, $\mathfrak{B}$ themselves are replaced by equivalent polygons $\mathfrak{A}'$, $\mathfrak{B}'$. If we keep $\mathfrak{B}$ fixed, and $\frac{\mathfrak{A}}{\mathfrak{B}}$ is a differential, then accordingly

$$\frac{\mathfrak{A}'}{\mathfrak{B}}, \quad \frac{\mathfrak{A}''}{\mathfrak{B}}, \quad \dots$$

will represent differentials if and only if the polygons $\mathfrak{A}, \mathfrak{A}', \mathfrak{A}'', \dots$ all belong to the same class A . If the polygons $\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3, \dots$ form a basis of A , hence

$$A = (\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3, \dots),$$

then the corresponding differential quotients with respect to an arbitrary variable z , $\frac{d\varpi_1}{dz}, \frac{d\varpi_2}{dz}, \frac{d\varpi_3}{dz}, \dots$, form the basis of a family of functions of finite dimension, and correspondingly we shall also call $d\varpi_1, d\varpi_2, d\varpi_3, \dots$ the basis of a *family of differentials*

$$(d\varpi_1, d\varpi_2, d\varpi_3, \dots)$$

*) The quotient $\frac{d\varpi}{d\varpi'}$ of any two proper or improper differentials always has the meaning of a determinate function in Ω . In what follows, however, we restrict ourselves to the consideration of such quotients in which at least the denominator is a proper differential.

of the same dimension. This says that every differential $d\varpi$ whose lower polygon is $\mathfrak{B}$ or a divisor of $\mathfrak{B}$ can be represented in the form

$$d\varpi = c_1 d\varpi_1 + c_2 d\varpi_2 + c_3 d\varpi_3 + \dots$$

with constant coefficients $c_1, c_2, c_3, \dots$

§ 26. The differentials of the first kind.

We consider first the simplest among the differentials in Ω , namely those whose lower polygon is the zero-gon $\mathfrak{O}$. Such differentials (whose existence, admittedly, has still to be proved) are called *differentials of the first kind*. The upper polygon $\mathfrak{W}$ of such a differential dw , whose order is $2p - 2$, is designated as the *fundamental polygon* of dw and is called a *complete polygon of the first kind*, while every divisor of such a one is called simply a *polygon of the first kind*. If $\mathfrak{W} = \mathfrak{A}\mathfrak{B}$, then $\mathfrak{A}, \mathfrak{B}$ are called *supplementary polygons* of each other. A polygon which is not a divisor of a complete polygon of the first kind, hence in particular every polygon of more than $2p - 2$ points, is called a *polygon of the second kind*.

1. By what was remarked above, all the complete polygons of the first kind form a polygon class W , whose dimension is to be determined; if this dimension turns out > 0 , then the existence of the polygons of the first kind is thereby proved at the same time. But this dimension is the same as the dimension of the family of differentials of the first kind, or also, for an arbitrary variable z , of the family of *differential quotients of the first kind*, if we designate as differential quotients of the first kind with respect to z the functions

$$u = \frac{dw}{dz}$$

Such a function u has by § 25, (2.) the expression

$$u = \frac{\mathfrak{A}^2 \mathfrak{W}}{3},$$

and one easily recognizes from the consideration of the order numbers at the various points that such a differential quotient of the first kind is completely defined by the following two properties:

I. At every point $\mathfrak{P}$ at which z has a finite value z_0 ,

$$(u(z - z_0))_0 = 0.$$

II. At a point $\mathfrak{P}$ at which z is infinite,

$$(zu)_0 = 0.$$

If, as in § 11, 4.,

$$r = (z - c)(z - c_1)(z - c_2) \dots$$

denotes the product of all the mutually different linear factors of the discriminant $\Delta_z(\Omega)$, and $\mathfrak{r}$ the product of all the mutually different prime ideals going into r , then the condition I. is completely equivalent to the condition that ru be a function in $\mathfrak{r}$, or that u must be a function of the module $\mathfrak{e}$ complementary to $\mathfrak{o}$ (§ 11, 4. (6.)). In order therefore to obtain the totality of the functions u , one has to look among the functions in $\mathfrak{e}$ for those which satisfy the condition II.

2. For this purpose we take as foundation a *normal basis* $\lambda_1, \lambda_2, \dots, \lambda_n$ of $\mathfrak{o}$ (§ 22) and denote the basis complementary to it by $\mu_1, \mu_2, \dots, \mu_n$, so that every function satisfying the condition I., hence also every differential quotient of the first kind, is contained in the form

$$u = y_1\mu_1 + y_2\mu_2 + \dots + y_n\mu_n, \quad (1.)$$

where $y_1, y_2, \dots, y_n$ are *integral* rational functions of z . But from the fundamental properties of the complementary basis there results (§ 10, 3.)

$$y_s = S(u\lambda_s); \quad \frac{y_s}{z^{r_s-1}} = S\left(uz \cdot \frac{\lambda_s}{z^{r_s}}\right).$$

Now since $\frac{\lambda_s}{z^{r_s}}$ is contained in $\mathfrak{o}'$, hence finite for $z = \infty$, and uz by II. vanishes at every such point, it follows (§ 16, 5.) that $\frac{y_s}{z^{r_s-1}}$ must vanish for $z = \infty$, i.e. that the integral rational function y_s cannot exceed the degree $r_s - 2$.

Therefore, if $r_s < 2$, y_s must vanish; hence under all circumstances (§ 22, 2.)

$$y_1 = 0; \quad S(u) = 0$$

(Abel's theorem for differentials of the first kind) and, if $r_s \geq 2$:

$$y_s = c_0 + c_1z + c_2z^2 + \dots + c_{r_s-2}z^{r_s-2}. \quad (2.)$$

It remains to be shown that these conditions are also sufficient, i.e. that every function of the form (1.), in which the y_s have the expression (2.), satisfies the requirement II., or, what is the same, that, if $r_s \geq 2$, $z^{r_s-1}\mu_s$ vanishes at all points at which z becomes infinite.

This results at once from the consideration of the system $\mathfrak{o}'$ of the integral functions of $z' = \frac{1}{z}$, for which by § 22, 3. the functions

$$\lambda'_1 = \frac{\lambda_1}{z^{r_1}}, \quad \lambda'_2 = \frac{\lambda_2}{z^{r_2}}, \quad \dots \quad \lambda'_n = \frac{\lambda_n}{z^{r_n}}$$

form a normal basis. The basis complementary to this is by § 10, 5.

$$\mu'_1 = z^{r_1} \mu_1, \quad \mu'_2 = z^{r_2} \mu_2, \quad \dots \quad \mu'_n = z^{r_n} \mu_n,$$

and since (because of the property I., applied to z', μ')

$$z' \mu'_s = 0 \quad \text{for} \quad z' = 0,$$

it follows

$$z^{r_s-1} \mu_s = 0 \quad \text{for} \quad z = \infty$$

q. e. d.

But since the functions $z^h \mu_s$ are linearly independent (because of the rational independence of the functions μ_s), there results from this, by § 24, (2.), the *fundamental theorem*:

The family of differentials of the first kind is of the dimension

$$(r_2 - 1) + (r_3 - 1) + \dots + (r_n - 1) = p,$$

and accordingly p is also the dimension of the class W of the complete polygons of the first kind.

As a basis of the family of differential quotients of the first kind with respect to z one can choose the p functions $z^h \mu_s$ ($h \leq r_s - 2$), and the fundamental polygons $\mathfrak{W}_1, \mathfrak{W}_2, \dots, \mathfrak{W}_p$ of the corresponding differentials dw form a basis of the class W .

3. For the sake of a later application, a special kind of differential quotients of the first kind u' shall be considered here, namely those in which the condition II. is replaced by the following condition, which includes it.

III. At every point $\mathfrak{P}$ at which z is infinite, let

$$(z^k u')_0 = 0,$$

where k is a given positive integer.

The functions u' can be represented by

$$u' = \frac{\mathfrak{U}^{k+1} \mathfrak{W}'}{3}$$

and likewise form a family; similarly the polygons $\mathfrak{W}'$ form a class W' , whose order is

$$w - n(k + 1) = 2p - 2 - n(k - 1).$$

The polygons $\mathfrak{W}'$, however, are *not* independent of the choice of the variable z .

The dimension of the class W' can be determined by the same method as that of the class W . For since the condition I. is fulfilled, the functions u' are likewise contained in the form (1.); but now

$$\frac{y_s}{z^{r_s-k}} = S \left(u' z^k \frac{\lambda_s}{z^{r_s}} \right)$$

must vanish for $z = \infty$, and therefore the degree of the integral rational function y_s cannot exceed the number $r_s - k - 1$. Thus y_s vanishes identically as soon as $r_s < k + 1$; otherwise

$$y_s = c_0 + c_1 z + \cdots + c_{r_s-k-1} z^{r_s-k-1}. \quad (3.)$$

If conversely y_s has this form, then the condition III. is satisfied by the function

$$u' = \sum_s y_s \mu_s$$

for, as proved in 2.,

$$z^k (z^{r_s-k-1} \mu_s) = z^{r_s-1} \mu_s$$

has the value 0 for $z = \infty$.

From this it follows that the dimension of the family of the functions u' , and consequently also of the class W' , is

$$= \sum_{\iota} (r_{\iota} - k)$$

where, however, only those terms of the sum are to be retained which have a positive value. If all $r_{\iota} - k \leq 0$, the functions sought do not exist at all.

§ 27. Polygon classes of the first and second kind.

If $\mathfrak{A}$ is a polygon of the first kind, then all the polygons equivalent to $\mathfrak{A}$ are likewise of the first kind. For if $\mathfrak{A}$ and $\mathfrak{B}$ are supplementary polygons and

$$\mathfrak{A}\mathfrak{B} = \mathfrak{W},$$

then, if A, B are the classes of $\mathfrak{A}$ and $\mathfrak{B}$:

$$AB = W,$$

and, if $\mathfrak{A}'$ is equivalent to $\mathfrak{A}$, $\mathfrak{A}'\mathfrak{B} = \mathfrak{W}'$ too is equivalent to $\mathfrak{W}$ (§ 18, 5.).

We therefore call such classes as contain polygons of the first kind *polygon classes of the first kind*, and the rest *polygon classes of the second kind*.

The class W of the complete polygons of the first kind is called the *principal class*, and two classes A, B which satisfy the condition

$$AB = W,$$

supplementary classes.

If

$$\eta = \frac{\mathfrak{A}'}{\mathfrak{A}}$$

is a function in Ω , and $\mathfrak{A}'$ relatively prime to $\mathfrak{A}$, hence the class A of $\mathfrak{A}$ a proper one, then we call η a function of the *first* or *second kind*, according as the class A is of the first or of the second kind.

If A is an arbitrary class of the first kind and q the number of mutually independent polygons $\mathfrak{W}$ which are divisible by some polygon $\mathfrak{A}$ of the class A , then by § 21, 2.

$$q = (A, W) = (O, B)$$

i.e. equal to the dimension of the supplementary class B of A . Likewise (B, W) is equal to the dimension of the class A . If A is a class of the second kind, then $(A, W) = 0$. Since p is the dimension of W , then by § 20, 2., 3. every class whose order is $\leq p - 1$ is of the first kind, and there are in particular classes A of the order $p - k$ such that $(A, W) = (O, B) = k$. From the same theorems it follows that there are classes of the order p which are of the second kind.

§ 28. The Riemann-Roch theorem for proper classes.

The *Riemann-Roch* theorem, which in its usual mode of expression teaches the number of arbitrary constants contained in a function that becomes infinite at a certain number of given points, contains, in our mode of presentation, a relation between the dimension and the order of a class, resp. between a class and its supplementary class. Restricting ourselves first to *proper* classes, we premise the following remarks to the derivation of this fundamental relation.

1. In a proper class A one can by § 19, 2. always select two polygons $\mathfrak{A}, \mathfrak{A}'$ relatively prime to each other (one of them may be assumed arbitrarily in the class). If therefore one sets

$$z = \frac{\mathfrak{A}'}{\mathfrak{A}}$$

and, if $\mathfrak{A}''$ denotes an arbitrary third polygon of the class A :

$$\omega = \frac{\mathfrak{A}''}{\mathfrak{A}}, \quad \frac{\omega}{z} = \frac{\mathfrak{A}''}{\mathfrak{A}'},$$

then by § 17 ω is an *integral* function of z , and $\frac{\omega}{z}$ an integral function of $\frac{1}{z}$. Therefore (§ 22) the exponent of $\omega \leq 1$.

If conversely ω is an integral function of z whose exponent is ≤ 1 , then it has the form

$$\omega = \frac{\mathfrak{A}''}{\mathfrak{A}},$$

where $\mathfrak{A}''$ is a polygon of the class A . For if

$$\omega = \frac{\mathfrak{A}_1''}{\mathfrak{A}_1}, \quad \frac{\omega}{z} = \frac{\mathfrak{A}_1'' \mathfrak{A}}{\mathfrak{A}_1 \mathfrak{A}'}$$

and $\mathfrak{A}_1''$ is assumed relatively prime to $\mathfrak{A}_1$, then first, since ω is to be an integral function of z , $\mathfrak{A}_1$ can contain no point which is not also contained in $\mathfrak{A}$. But neither can $\mathfrak{A}_1$ contain any point more often than $\mathfrak{A}$, because otherwise $\frac{\omega}{z}$ would be infinite at such a point (which cannot occur in $\mathfrak{A}'$), and hence would not be an integral function of $\frac{1}{z}$. Therefore $\mathfrak{A}$ is divisible by $\mathfrak{A}_1$, and ω can be put into the form $\frac{\mathfrak{A}_1''}{\mathfrak{A}_1}$.

2. In order therefore to obtain the totality of the polygons of the class A , we have only to look for those integral functions of z whose exponent is ≤ 1 .

If n is the order of the class A , hence also the order of the variable z , and $\lambda_1, \lambda_2, \dots, \lambda_n$ form a normal basis of $\mathfrak{o}$ with the exponents $r_1, r_2, \dots, r_n$, among them r_s the last which is ≤ 1 , then every function ω whose exponent is ≤ 1 can by § 22, 2. be represented in the form

$$\omega = c_1 \lambda_1 + c_2 \lambda_2 + \dots + c_s \lambda_s + z \omega_1.$$

But since the exponent of $z \omega_1$ cannot be greater than 1, ω_1 must be a constant, and therefore

$$\omega = c_1 \lambda_1 + c_2 \lambda_2 + \dots + c_s \lambda_s + c_{s+1} z.$$

Conversely every function of this form satisfies the requirement posed. Hence $s+1$ is the dimension of the class A , which accordingly, in agreement with § 21, 1., is always $\leq n+1$. But the upper limit $n+1$ can be reached only in the case $p=0$, and is also actually reached, because in this case $r_2, r_3, \dots, r_n = 1$. From this it follows

that a *single point* $\mathfrak{P}$ can belong to a proper class *only* if $p=0$.

3. If one of the exponents $r_{s+1}, r_{s+2}, \dots, r_n$ is greater than 2, then certainly also $r_n > 2$, and by § 26, 2., if $\mathfrak{Z}$ denotes the ramification polygon in z ,

$$\mu_n = \frac{\mathfrak{A}^2 \mathfrak{W}}{\mathfrak{Z}}, \quad \mu_n z = \frac{\mathfrak{A}^2 \mathfrak{W}_1}{\mathfrak{Z}} = \frac{\mathfrak{A} \mathfrak{A}' \mathfrak{W}}{\mathfrak{Z}}$$

are differential quotients of the first kind with respect to z , hence

$$\mathfrak{A} \mathfrak{W}_1 = \mathfrak{A}' \mathfrak{W}$$

or, since $\mathfrak{A}, \mathfrak{A}'$ are relatively prime,

$$\mathfrak{W} = \mathfrak{A} \mathfrak{B}, \quad \mathfrak{W}_1 = \mathfrak{A}' \mathfrak{B},$$

i.e. the class A is of the *first* kind (z a variable of the first kind). If therefore we first make the assumption that A is a class of the *second* kind, it follows

$$r_{s+1} = 2, \quad r_{s+2} = 2, \quad \dots \quad r_n = 2$$

and

$$p = (r_2 - 1) + \dots + (r_s - 1) + (r_{s+1} - 1) + \dots + (r_n - 1) = n - s.$$

The dimension $s+1$ of the class A is therefore

$$(O, A) = n - p + 1.$$

4. Let us make secondly the assumption that A is of the *first* kind and, as in § 27,

$$q = (A, W),$$

then there exist q linearly independent complete polygons of the first kind divisible by $\mathfrak{A}$, and the differential quotients of the first kind with respect to z corresponding to them, of which there are likewise q , and not more, linearly independent ones, have the expression

$$v = \frac{\mathfrak{A}^3 \mathfrak{B}}{3},$$

where $\mathfrak{B}$ denotes a polygon of $2p - 2 - n$ points; the class B of $\mathfrak{B}$ is the supplementary class of A , and therefore its dimension is equal to q (§ 27).

But these functions v have the property that at the vertices of $\mathfrak{A}$, i.e. for $z = \infty$, not only zv but also

$$z^2 v = \frac{\mathfrak{A} \mathfrak{A}'^2 \mathfrak{B}}{3}$$

vanishes, and they are completely determined by this and by the requirement of being differential quotients

of the first kind. For if

$$v = \frac{\mathfrak{A}^2 \mathfrak{W}}{3}, \quad vz^2 = \frac{\mathfrak{A}'^2 \mathfrak{W}}{3},$$

then, if $z^2 v$ is to vanish at all points of $\mathfrak{A}$, $\mathfrak{W}$ must be divisible by $\mathfrak{A}$, since $\mathfrak{A}'$ is assumed relatively prime to $\mathfrak{A}$. Therefore by § 26, 3:

$$q = (r_{s+1} - 2) + (r_{s+2} - 2) + \cdots + (r_n - 2),$$

on the other hand

$$p = (r_{s+1} - 1) + (r_{s+2} - 1) + \cdots + (r_n - 1),$$

consequently:

$$p - q = n - s, \quad s = n - p + q.$$

In this is contained the *Riemann-Roch theorem*, to which, with regard to § 27, we can give the following expression for this case: *If A , B are supplementary classes of the first kind, of which at least one is a proper one, and a , b their orders, hence*

$$a + b = 2p - 2,$$

then

$$(O, A) - \frac{1}{2}a = (O, B) - \frac{1}{2}b.$$

5. If we do not exclude the case $(A, W) = 0$, we can combine the *Riemann-Roch* theorem for both cases thus:

If A is a proper class of the order n , then its dimension is

$$(O, A) = n - p + 1 + (A, W).$$

Since the dimension of a proper class (if it does not consist of the single zero-gon) must be at least $= 2$, it further follows, if $(A, W) = 0$,

$$n \geq p + 1,$$

and from this the theorem due to *Riemann*:

Every function whose order is $\leq p$ is a function of the first kind.

6. With the help of these theorems it can easily be proved *that the principal class W of the complete polygons of the first kind is always a proper one.*

For if $\mathfrak{M}$ is the divisor of W , then by § 19, 2. a polygon $\mathfrak{A}\mathfrak{M}$ can be found in W such that $\mathfrak{A}$ is relatively prime to $\mathfrak{M}$. The class A of $\mathfrak{A}$ is a proper one (§ 21, 3.), and at the same time $\mathfrak{A}\mathfrak{M}$ is the only polygon of the class W divisible by $\mathfrak{A}$ (because every polygon in W has the divisor $\mathfrak{M}$). Hence

$$(A, W) = 1.$$

Now p is the dimension of W , hence also that of A , and consequently by the *Riemann-Roch* theorem the order of A is equal to $2p - 2$, i.e. just as great as that of W . Consequently $\mathfrak{M} = \mathfrak{O}$.

§ 29. The Riemann-Roch theorem for improper classes of the first kind.

If A is a class of the first kind with the divisor $\mathfrak{M}$ and

$$A = \mathfrak{M}A',$$

then A' is a proper class of the first kind. Let B be the supplementary class of A , B' that of A' ; a , b the orders of the classes A , B ; m the order of $\mathfrak{M}$. The whole class B is obtained if in all the polygons of the class B' divisible by $\mathfrak{M}$ one suppresses the factor $\mathfrak{M}$; for if

$$\mathfrak{A}\mathfrak{B} = \mathfrak{A}'\mathfrak{M}\mathfrak{B} = \mathfrak{W},$$

then $\mathfrak{M}\mathfrak{B}$ belongs to the class B' , and conversely, if

$$\mathfrak{A}'\mathfrak{B}' = \mathfrak{A}'\mathfrak{M}\mathfrak{B} = \mathfrak{W}$$

then $\mathfrak{B}$ belongs to the class B .

But from this there results by § 21, 2.

$$(O, B) \geq (O, B') - m.$$

Now A' is a proper class of the same dimension as A and of the order $a - m$, hence (§ 28, 5.)

$$(O, A) = (O, A') = a - m - p + 1 + (A', W),$$

or

$$(O, A) = (O, B') - m + a - p + 1;$$

therefore

$$(O, A) \leq (O, B) + a - p + 1 = (O, B) + \frac{1}{2}(a - b),$$

hence

$$(O, A) - \frac{1}{2}a \leq (O, B) - \frac{1}{2}b.$$

But since the classes A, B can be interchanged with each other, it follows in the same way

$$(O, B) - \frac{1}{2}b \leq (O, A) - \frac{1}{2}a,$$

i.e.

$$(O, A) - \frac{1}{2}a = (O, B) - \frac{1}{2}b,$$

whereby the Riemann-Roch theorem is proved in general for polygon classes of the first kind, in the same form as in § 28, 4.*).

§ 30. Improper classes of the second kind.

The condition is now to be sought under which a polygon class A of the second kind of the order n can be an improper one at all, whereby the general validity of the *Riemann-Roch* theorem will result of itself.

1. Every class A can always be converted into a proper class AN by multiplication by another class N of the order ν . For if $\mathfrak{A}$ is an arbitrary polygon in A , choose a variable z which remains finite at all points of $\mathfrak{A}$ (§ 15, 6.). If then η is an arbitrary function of the ideal in z generated by $\mathfrak{A}$, the upper polygon of η is divisible by $\mathfrak{A}$, hence of the form $\mathfrak{A}\mathfrak{N}$, and the class of $\mathfrak{A}\mathfrak{N}$ is a proper one.

2. The dimension of the proper class AN of the second kind is by § 28, 3.

$$(O, AN) = n + \nu - p + 1,$$

and from this it follows by § 21, 2.

$$(O, A) \geq n - p + 1.$$

Now if the divisor $\mathfrak{M}$ of the class A is of the order m , and

$$A = \mathfrak{M}A',$$

then A' is a proper class of the same dimension as A , and consequently (§ 28, 5.)

$$(O, A) = (O, A') = n - m - p + 1 + (A', W),$$

hence

$$(A', W) \geq m,$$

i.e. A' must certainly be of the first kind if A is an improper class. If therefore B' is the supplementary class of A' , then also

$$(O, B') \geq m.$$

*) In the terminology of *Christoffel* (Ueber die canonische Form der *Riemannschen* Integrale erster Gattung, Annali di Matematica pura ed applicata, Serie II, Tomo IX)

$$(A, W) + a - p = (O, B) + a - p = (O, A) - 1$$

is the “excess” and

$$(A, W) - 1 = (O, B) - 1$$

the “defect” of the point system $\mathfrak{A}$.

But if $(O, B') > m$, then by § 20, 2. a polygon $\mathfrak{M}\mathfrak{B}$ divisible by $\mathfrak{M}$ could be found in B' , and we would have

$$\mathfrak{A}'\mathfrak{M}\mathfrak{B} = \mathfrak{A}\mathfrak{B} = \mathfrak{W},$$

hence A of the first kind, contrary to the assumption. Hence

$$(A', W) = m$$

and consequently

$$(O, A) = n - p + 1,$$

in which again the *Riemann-Roch* theorem for this case is contained, exactly in the form of § 28, 3.

3. If the class A contains only one single isolated polygon, then $(O, A) = n - p + 1 = 1$, consequently $n = p$, i.e. an isolated polygon of the second kind always has the order p . Conversely, by 2., every polygon of the second kind of the order p is an isolated one.

4. Keeping the notation of 2., $(O, B') = m$, and therefore, by the often applied theorem (§ 20, 2.), a polygon divisible by an arbitrary $(m - 1)$ -gon can be found in B' . If therefore, separating off an arbitrary point $\mathfrak{P}$ of $\mathfrak{M}$, one sets

$$\mathfrak{M} = \mathfrak{P}\mathfrak{M}',$$

then a polygon $\mathfrak{M}'\mathfrak{B}$ is contained in B' , and hence

$$\mathfrak{A}'\mathfrak{M}'\mathfrak{B} = \mathfrak{W}.$$

The polygon $\mathfrak{A}'\mathfrak{M}' = \mathfrak{A}''$ and its class A'' are therefore of the *first kind*, and A has, if P denotes the class of $\mathfrak{P}$, the form

$$A = PA''.$$

At the same time $(A'', W) = (O, B'') = 1$ must hold, i.e. the supplementary class B'' of A'' contains only one single isolated polygon $\mathfrak{B}''$, since otherwise a

polygon divisible by $\mathfrak{P}$ would exist in B'' , and hence A too would be of the first kind, contrary to the assumption.

5. If conversely A'' is a class of the first kind for which $(A'', W) = 1$, so that the supplementary class B'' of A'' consists of an isolated polygon $\mathfrak{B}''$; if further $\mathfrak{P}$ is a point not going into $\mathfrak{B}''$, and P its class, then $A = PA''$ is an improper class of the second kind of the order n , into whose divisor $\mathfrak{P}$ goes.

That A is of the second kind follows first from the assumption that $\mathfrak{P}$ does not go into $\mathfrak{B}''$. The dimension of A is therefore by 2.

$$(O, A) = n - p + 1,$$

where n denotes the order of A ; on the other hand the dimension of the class A'' is by §§ 28 and 29:

$$(O, A'') = n - p + (A'', W) = n - p + 1;$$

hence A and A'' are of the same dimension. But all the polygons of the class A'' pass over by multiplication by $\mathfrak{P}$ into polygons of the class A , and because of the equality of the dimensions the latter class too is thereby completely exhausted. Therefore all the polygons of the class A contain the factor $\mathfrak{P}$, which accordingly also goes into the divisor of A .

6. In the special case where the genus p of the field Ω has the value 0, polygons and classes of the first kind do not occur at all. Hence in this case no improper classes exist either. The dimension of every class is greater by 1 than its order. In particular, therefore, every point $\mathfrak{P}$ too belongs to a proper class of dimension 2, and therefore in this case there exist in Ω functions z which are of the first order. By such a one every other function of the field can be expressed *rationally*, for the irreducible equation existing between z and another variable of the field is of the first degree with respect to the latter (§ 15, 7.).

§ 31. The differentials of the second and third kind.

1. If now, in the notation introduced in § 25,

$$d\varpi = \frac{\mathfrak{A}}{\mathfrak{B}}$$

is an arbitrary differential in Ω , hence, if a, b are the orders of $\mathfrak{A}$ and $\mathfrak{B}$,

$$a = b + 2p - 2,$$

and if $\mathfrak{A}, \mathfrak{B}$ are assumed relatively prime, then, if $\mathfrak{U}, \mathfrak{Z}$ denote the lower polygon and ramification polygon for an arbitrary variable z , $\mathfrak{U}^2\mathfrak{A}$ must be equivalent to $\mathfrak{Z}\mathfrak{B}$ (§ 25). If therefore one denotes by U, Z, A, B the classes of the polygons $\mathfrak{U}, \mathfrak{Z}, \mathfrak{A}, \mathfrak{B}$, then

$$U^2A = ZB$$

must hold. But on the other hand, if W is the principal class of the first kind,

$$U^2W = Z,$$

from which the relation

$$A = BW$$

results. If conversely $\mathfrak{A}$ is an arbitrary polygon of the class BW , then from this follows the equivalence of $\mathfrak{U}^2\mathfrak{A}$ with $\mathfrak{Z}\mathfrak{B}$, hence the existence of a differential with the notation $\frac{\mathfrak{A}}{\mathfrak{B}}$. From this it follows that $\mathfrak{B}$ can be the lower polygon of a differential $d\varpi$ if and only if there exists in BW a polygon relatively prime to $\mathfrak{B}$, i.e. if the divisor of the class BW is relatively prime to $\mathfrak{B}$. The dimension of the class BW then gives at the same time the dimension of the family of differentials $d\varpi$ belonging to the lower polygon $\mathfrak{B}$ (§ 25). The theorems § 30, 4., 5. therefore yield, since $(W, W) = 1$, the following result.

a) If $\mathfrak{B}$ consists of a single point (if $b = 1$), then the class BW is an improper one with the divisor $\mathfrak{B}$; hence the order b of the lower polygon of a differential $d\varpi$ cannot be equal to one.

b) If $b \geq 2$, then BW is always a proper class of the second kind, and therefore its dimension is

$$b + p - 1.$$

Any polygon whatever of more than one point can therefore be the lower polygon of a differential, and among the differentials belonging to a lower polygon of the order b there exist $b + p - 1$ linearly independent ones.

2. We now look, under the assumption that $b \geq 2$, for a basis of the class A of such a kind that every element $\mathfrak{A}_r$ of this basis yields a differential $d\varpi_r$ of the simplest possible nature, namely one whose lower polygon is a power of a single point or the product of only two different points.

Suppose that such a basis has already been found for the class BW

$$\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3, \dots, \mathfrak{A}_{b+p-1}, \quad (1.)$$

then from it, if P denotes the class of an arbitrary point $\mathfrak{P}$, we form a basis of the same kind for the class BPW of the dimension $b + p$, namely

$$\mathfrak{P}\mathfrak{A}_1, \mathfrak{P}\mathfrak{A}_2, \dots, \mathfrak{P}\mathfrak{A}_{b+p-1}, \mathfrak{A}'. \quad (2.)$$

The first $b + p - 1$ of these polygons actually belong to the class BPW and are independent of one another, because the polygons (1.) are; at the same time the differentials formed from them

$$d\varpi_r = \frac{\mathfrak{P}\mathfrak{A}_r}{\mathfrak{P}\mathfrak{B}} = \frac{\mathfrak{A}_r}{\mathfrak{B}}$$

are identical with those formed from (1.). It therefore only remains to form $\mathfrak{A}'$, where two cases are to be distinguished.

a) If $\mathfrak{P}$ goes into $\mathfrak{B}$ and $\mathfrak{B} = \mathfrak{M}\mathfrak{P}^m$, $\mathfrak{M}$ not divisible by $\mathfrak{P}$, then $P^{m+1}W$ is a proper class (because $m + 1 \geq 2$, § 30, 4.), in which consequently there exists a polygon $\mathfrak{N}$ not divisible by $\mathfrak{P}$; if one now sets $\mathfrak{A}' = \mathfrak{M}\mathfrak{N}$, then $\mathfrak{A}'$ belongs to the class BPW and is not divisible by $\mathfrak{P}$, and consequently is also not contained in the family $(\mathfrak{P}\mathfrak{A}_1, \mathfrak{P}\mathfrak{A}_2, \dots, \mathfrak{P}\mathfrak{A}_{b+p-1})$, whose divisor is $\mathfrak{P}$; consequently the

polygons (2.) are independent of one another, and since their number is $b + p$, they form a basis of the class BPW . The differential formed from $\mathfrak{A}'$

$$d\varpi' = \frac{\mathfrak{A}'}{\mathfrak{P}\mathfrak{B}} = \frac{\mathfrak{N}}{\mathfrak{P}^{m+1}}$$

has the required form, since its lower polygon is a power of a single point.

b) If $\mathfrak{P}$ does not go into $\mathfrak{B}$, choose once for all a point $\mathfrak{P}_1$ going into $\mathfrak{B}$ and set $\mathfrak{B} = \mathfrak{M}\mathfrak{P}_1$ (no matter whether $\mathfrak{M}$ is divisible by $\mathfrak{P}_1$ or not). Then choose in the proper class PP_1W a polygon $\mathfrak{N}$ not divisible by $\mathfrak{P}$ and $\mathfrak{P}_1$; then $\mathfrak{A}' = \mathfrak{M}\mathfrak{N}$ again belongs to the class PBW , and since $\mathfrak{A}'$ is not divisible by $\mathfrak{P}$, it follows as above that the polygons (2.) form a basis of BPW . At the same time

$$d\varpi' = \frac{\mathfrak{A}'}{\mathfrak{P}\mathfrak{B}} = \frac{\mathfrak{N}}{\mathfrak{P}\mathfrak{P}_1},$$

hence of the required form.

It still remains to describe the beginning of this operation. If $b = 0$, hence $\mathfrak{B} = \mathfrak{O}$, then

$$BW = W = (\mathfrak{W}_1, \mathfrak{W}_2, \dots, \mathfrak{W}_p)$$

(the principal class of the first kind).

If $b = 2$, choose from the proper class BW a polygon $\mathfrak{N}$ which is relatively prime to $\mathfrak{B}$; then

$$BW = (\mathfrak{B}\mathfrak{W}_1, \mathfrak{B}\mathfrak{W}_2, \dots, \mathfrak{B}\mathfrak{W}_p, \mathfrak{N}).$$

If one starts from this basis in order to determine, in the way described above, a basis (1.) which corresponds to the arbitrarily given polygon

$$\mathfrak{B} = \mathfrak{P}_1^{m_1} \mathfrak{P}_2^{m_2} \mathfrak{P}_3^{m_3} \dots$$

and determines the two polygons $\mathfrak{A}'_r, \mathfrak{B}'_r$ from the condition

$$d\varpi_r = \frac{\mathfrak{A}'_r}{\mathfrak{B}} = \frac{\mathfrak{A}'_r}{\mathfrak{B}'_r},$$

so that they have no common divisor, then the polygons $\mathfrak{B}'_r$ which occur as lower polygons of the differentials $d\varpi_r$ are the following:

a) p times the denominator $\mathfrak{O}$ occurs, and the corresponding differentials $d\varpi_r$ are the *differentials of the first kind*.

b) Once each there occur the lower polygons $\mathfrak{P}_1^2, \mathfrak{P}_1^3, \dots, \mathfrak{P}_1^{m_1}$ (if $m_1 \geq 2$), $\mathfrak{P}_2^2, \mathfrak{P}_2^3, \dots, \mathfrak{P}_2^{m_2}$; $\mathfrak{P}_3^2, \mathfrak{P}_3^3, \dots, \mathfrak{P}_3^{m_3}, \dots$

The differentials $d\varpi_r$ belonging to the lower polygons $\mathfrak{P}^r$ are, when a more precise distinction is necessary, denoted by $dt_{(\mathfrak{P}^{r-1})}$ and are called *differentials of the second kind*.

c) Finally the products $\mathfrak{P}_1\mathfrak{P}_2, \mathfrak{P}_1\mathfrak{P}_3, \dots$ (with $\mathfrak{P}_1$ held fixed) occur once each. The corresponding differentials $d\varpi_r$ are denoted by $d\pi_{(\mathfrak{P}_1, \mathfrak{P}_r)}$ and are called *differentials of the third kind*.

Every differential $d\varpi$ whose lower polygon is $\mathfrak{B}$ can be represented in the form

$$d\varpi = \sum_r^r c_r d\varpi_r \quad (3.)$$

with constant coefficients c_r , which is called the *normal form* of the differential $d\varpi$. If each of the individual differentials $d\varpi_r$ has been chosen in a determinate way, then the normal form can also be produced *in only one single way*, which follows immediately from the linear independence of the differentials $d\varpi_r$.

§ 32. The residues.

1. If $d\varpi$ is an arbitrary differential in Ω and $\mathfrak{P}$ a point which occurs m times in its lower polygon $\mathfrak{B}$ ($m \geq 0$), choose a variable z such that it becomes ∞^1 at $\mathfrak{P}$. Then one can set (by § 15, 4.), and indeed in only one way,

$$\frac{d\varpi}{dz} = a_{m-2}z^{m-2} + a_{m-3}z^{m-3} + \cdots + a_1z + a_0 + a_{-1}z^{-1} + \eta z^{-2}, \quad (1.)$$

where the a are constants and η a function in Ω which is finite at $\mathfrak{P}$. The coefficient $-a_{-1}$ of $-z^{-1}$ in this expression is called the *residue of the differential $d\varpi$ with respect to the point $\mathfrak{P}$* . From this definition the following theorems result:

2. The residue with respect to a point $\mathfrak{P}$ can be different from zero only if $m > 0$, i.e. if the point $\mathfrak{P}$ actually occurs in the lower polygon of $d\varpi$, and is therefore always equal to 0 for the differentials of the first kind.

3. The residue of a sum of differentials is equal to the sum of the residues of the individual differentials.

4. The residue of a *proper* differential is always equal to 0. For if σ is a function in Ω , and, where the b denote constants and σ' a function finite at $\mathfrak{P}$,

$$\sigma = b_m z^m + b_{m-1} z^{m-1} + \cdots + b_1 z + \sigma',$$

then there results, by differentiation of this expression with respect to z , since $\frac{d\sigma'}{dz}$ is infinitely small of at least the second order at $\mathfrak{P}$ (§ 23, 10.)¹⁹, that in the expression for $\frac{d\sigma}{dz}$ a term with z^{-1} does not occur at all, whereby the assertion is proved.

5. The residue of a differential $d\varpi$ is independent of the choice of the variable z . For if z_1 is a second variable of the same nature as z , hence, where a is constant and ζ finite at $\mathfrak{P}$:

$$z = az_1 + \zeta, \quad (2.)$$

then there results, if for brevity

$$\alpha = \frac{a_{m-2}z^{m-1}}{m-1} + \frac{a_{m-3}z^{m-2}}{m-2} + \cdots + a_0z$$

¹⁹*Editorial note:* Printed "§ 23, 10.", but § 23 has only articles 1.9. and formulas (1.)(9.). The fact used is presumably § 23, 8.: the order of $\frac{d\alpha}{d\beta}$ is the difference of the orders of $\alpha - \alpha_0$ and $\beta - \beta_0$ (following formula (7.)). Here z is ∞^1 in $\mathfrak{P}$ and σ' is finite there, so $\frac{d\sigma'}{dz}$ has order at least $1 - (-1) = 2$.

is set:

$$\frac{d\varpi}{dz_1} = \frac{d\varpi}{dz} \frac{dz}{dz_1} = \frac{d\alpha}{dz_1} + a_{-1}z^{-1} \frac{dz}{dz_1} - \eta \frac{dz^{-1}}{dz_1}.$$

Now, if ζ' , ζ'' are functions finite at $\mathfrak{P}$, then, as follows easily by § 23 and § 15, 4.:

$$z^{-1} \frac{dz}{dz_1} = z_1^{-1} + z_1^{-2} \zeta', \quad \frac{dz^{-1}}{dz_1} = z_1^{-2} \zeta'',$$

and from this follows by 3., 4. the correctness of the stated assertion*).

6. *The sum of the residues of every differential $d\varpi$ with respect to all points $\mathfrak{P}$ is always equal to zero.*

*) In the definition of the residue one can also take as foundation a variable r which is infinitely *small* of the first order at $\mathfrak{P}$. If then

$$\frac{d\varpi}{dr} = a_m r^{-m} + \cdots + a_1 r^{-1} + \eta$$

and η is finite at $\mathfrak{P}$, then a_1 is the residue of $d\varpi$ with respect to $\mathfrak{P}$.

In proving this important theorem we can restrict ourselves to the consideration of the residues which belong to all the mutually different points going into the lower polygon $\mathfrak{B}$ of $d\varpi$; to these, however, we add as many mutually different arbitrary points with vanishing residues as are needed to obtain a polygon $\mathfrak{P}_1 \mathfrak{P}_2 \dots \mathfrak{P}_n$ consisting entirely of simple points and belonging to a proper class. Then we choose a variable z of the order n whose lower polygon is just this polygon, which therefore becomes ∞^1 at each of the points $\mathfrak{P}_1, \mathfrak{P}_2, \dots \mathfrak{P}_n$ and only at these. Among these are then found all the mutually different points going into $\mathfrak{B}$. Under this assumption there results for $\iota = 1, 2, \dots n$

$$\frac{d\varpi}{dz} = a_{m-2}^{(\iota)} z^{m-2} + a_{m-3}^{(\iota)} z^{m-3} + \cdots + a_0^{(\iota)} + a_{-1}^{(\iota)} z^{-1} + \eta^{(\iota)} z^{-2}, \quad (3.)$$

where $\eta^{(\iota)}$ denotes a function finite at $\mathfrak{P}_\iota$. If we also admit the value 0 for the constants $a^{(\iota)}$, the exponent m can be assumed independent of ι (m is then, if not all $a_{m-2}^{(\iota)}$ vanish, the exponent of the highest power of a single point which occurs in $\mathfrak{B}$). The theorem to be proved then consists in this, that $\sum a_{-1}^{(\iota)} = 0$. To prove it, we form the trace of the function $\frac{d\varpi}{dz}$ for the variable z (§ 2), and in doing so make use of an extension of the procedure of § 16, 4. We choose a system of functions $\varrho_1, \varrho_2, \dots \varrho_n$ in Ω as follows: Let

$\varrho_1 = 0^m$	at $\mathfrak{P}_2, \mathfrak{P}_3, \dots \mathfrak{P}_n,$	finite	and	different	from	zero	at	$\mathfrak{P}_1,$
$\varrho_2 = 0^m$	at $\mathfrak{P}_1, \mathfrak{P}_3, \dots \mathfrak{P}_n,$	"	"	"	"	"	"	$\mathfrak{P}_2,$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\varrho_n = 0^m$	at $\mathfrak{P}_1, \mathfrak{P}_2, \dots \mathfrak{P}_{n-1},$	"	"	"	"	"	"	$\mathfrak{P}_n.$

Now if $x_1, x_2, \dots x_n$ are rational functions of z , and

$$\eta = x_1 \varrho_1 + x_2 \varrho_2 + \cdots + x_n \varrho_n$$

is a function in Ω which is finite for $z = \infty$, i.e. at $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_n$, then $x_1, x_2, \dots, x_n$ must likewise be finite for $z = \infty$. For if the $x_1, x_2, \dots, x_n$ are *not* all finite for $z = \infty$, there exists a positive exponent r of such a nature that the products $x_1 z^{-r}, x_2 z^{-r}, \dots, x_n z^{-r}$ are all finite for $z = \infty$, and at least one of them, say $x_1 z^{-r}$, is different from zero; but then the equation

$$\eta z^{-r} = x_1 z^{-r} \varrho_1 + \dots + x_n z^{-r} \varrho_n$$

contains the contradiction that at the point $\mathfrak{P}_1$ the left-hand side and all the terms of the right-hand side except the first vanish.

From this it follows at the same time, if one sets $\eta = 0$, that the functions $\varrho_1, \varrho_2, \dots, \varrho_n$ form a basis of Ω . If therefore one sets, denoting by $x_{\iota, \iota'}$ rational functions of z ,

$$\frac{d\varpi}{dz} \varrho_\iota = x_{\iota, 1} \varrho_1 + x_{\iota, 2} \varrho_2 + \dots + x_{\iota, n} \varrho_n, \quad (\iota=1, 2, \dots, n) \quad (4.)$$

then (§ 2)

$$S\left(\frac{d\varpi}{dz}\right) = x_{1,1} + x_{2,2} + \dots + x_{n,n}. \quad (5.)$$

Now, as emerges from (3.), $z^{-m+2} \frac{d\varpi}{dz} \varrho_\iota$ is finite for $z = \infty$, and from this it follows, by the property of the functions ϱ just proved, that the

$$z^{-m+2} x_{\iota, \iota'}$$

too are finite for $z = \infty$. Now, e.g., at the point $\mathfrak{P}_2$ the functions $\varrho_1, \varrho_3, \dots, \varrho_n$ are infinitely small of the m^{th} order, while ϱ_2 is finite there and different from zero. Therefore at $\mathfrak{P}_2$ the functions

$$z \frac{d\varpi}{dz} \varrho_1, \quad z x_{1,1} \varrho_1, \quad z x_{1,3} \varrho_3, \quad \dots \quad z x_{1,n} \varrho_n$$

will all vanish, and consequently $z x_{1,2}$ too must vanish for $z = \infty$. The same follows for $z x_{1,3}, \dots, z x_{1,n}$, and in general for $z x_{\iota, \iota'}$ as soon as ι, ι' are different from each other. Therefore $z^2 x_{\iota, \iota'}$ will be finite for $z = \infty$.

If one now sets, letting x_ι denote a new rational function,

$$x_{\iota, \iota} = a_{m-2}^{(\iota)} z^{m-2} + a_{m-3}^{(\iota)} z^{m-3} + \dots + a_{-1}^{(\iota)} z^{-1} + x_\iota z^{-2}, \quad (6.)$$

then it follows from (3.)

$$x_{\iota, \iota} - \frac{d\varpi}{dz} = z^{-2} (x_\iota - \eta^{(\iota)}),$$

and from (4.)

$$(\eta^{(\iota)} - x_\iota) \varrho_\iota = z^2 x_{\iota, 1} \varrho_1 + \dots + z^2 x_{\iota, \iota-1} \varrho_{\iota-1} + z^2 x_{\iota, \iota+1} \varrho_{\iota+1} + \dots + z^2 x_{\iota, n} \varrho_n.$$

Now since at $\mathfrak{P}_\iota$ $\eta^{(\iota)}$ is finite and ϱ_ι different from zero, and further all the terms of the right-hand side are zero, it follows that x_ι too is finite at the point $\mathfrak{P}_\iota$,

and consequently, since it is rational, for $z = \infty$. From (5.) and (6.) there then results

$$S\left(\frac{d\varpi}{dz}\right) = \sum a_{m-2}^{(\iota)} z^{m-2} + \sum a_{m-3}^{(\iota)} z^{m-3} + \dots + \sum a_{-1}^{(\iota)} z^{-1} + \sum x_{\iota} z^{-2}. \quad (7.)$$

But now on the other hand, if again $\mathfrak{U}$ is the lower polygon and $\mathfrak{Z}$ the ramification polygon of z :

$$\frac{d\varpi}{dz} = \frac{\mathfrak{U}^2 \mathfrak{A}}{\mathfrak{Z} \mathfrak{B}},$$

and $\mathfrak{B}$ contains no point which is not also contained in $\mathfrak{U}$. From this it follows, as in § 26, that $\frac{d\varpi}{dz}$, regarded as a function of z , is a function of the module $\mathfrak{e}$ complementary to $\mathfrak{o}$, and consequently

$$S\left(\frac{d\varpi}{dz}\right)$$

is an *integral* rational function of z (§ 11, 4.). If one takes this into account, there follows from (7.) $\sum x_{\iota} = 0$, and further the theorem to be proved

$$\sum a_{-1}^{(\iota)} = 0.$$

We can also give this theorem the following expression: The residue of a differential of the second kind $dt_{(\mathfrak{P}^r)}$ with respect to the point $\mathfrak{P}$ is zero.

The residues of an integral of the third kind $d\pi_{(\mathfrak{P}_1, \mathfrak{P}_2)}$ with respect to $\mathfrak{P}_1, \mathfrak{P}_2$ are equal and opposite to each other, and certainly different from zero, since otherwise $d\pi$ would be a differential of the first kind.

From these remarks it further follows by means of 4. that a proper differential $d\sigma$, represented in the normal form, can contain no differential of the third kind. It deserves further to be mentioned that the residues of the *logarithmic* differential $\frac{d\sigma}{\sigma}$ are integers, namely the order numbers of the function σ (in consequence of § 23).

§ 33. Relations between differentials of the first and second kind.

1. Let σ be a function in Ω with the lower polygon

$$\mathfrak{B}' = \mathfrak{P}_1^{m_1-1} \mathfrak{P}_2^{m_2-1} \dots \quad (m_1, m_2, \dots \geq 2)$$

and the ramification polygon (§ 16)

$$\mathfrak{S} = \mathfrak{S}' \mathfrak{P}_1^{m_1-2} \mathfrak{P}_2^{m_2-2} \dots,$$

where $\mathfrak{S}'$ is not divisible by the points $\mathfrak{P}_1, \mathfrak{P}_2, \dots$, which are assumed different. Accordingly, in the symbolic notation of § 25, the proper differential is

$$d\sigma = \frac{\mathfrak{S}}{\mathfrak{B}'^2} = \frac{\mathfrak{S}'}{\mathfrak{P}_1^{m_1} \mathfrak{P}_2^{m_2} \dots},$$

from which it emerges first *that a proper differential can never be of the first kind.*

2. The proper differential $d\sigma$, which in its representation by the normal form can contain only differentials of the first and second kind, belongs to the family of those differentials whose lower polygon is

$$\mathfrak{B} = \mathfrak{P}_1^{m_1} \mathfrak{P}_2^{m_2} \dots = \mathfrak{B}' \mathfrak{P}_1 \mathfrak{P}_2 \dots$$

Conversely, therefore, one will also always find at least one proper differential $d\sigma$ in such a family, provided that $m_1, m_2, \dots \geq 2$ and that $\mathfrak{B}'$ belongs to a *proper polygon class*. For by 1. all that is required for this is that there exist in Ω a function σ with the lower polygon $\mathfrak{B}'$.

3. From this there now results the following important theorem. *All differentials of the second kind can be represented linearly, with constant coefficients, by p particular suitably chosen differentials of the second kind, by differentials of the first kind, and by proper differentials.*

To see this, choose an arbitrary polygon $\mathfrak{A}$ of the second kind of the order p . Now if $\mathfrak{P}$ is an arbitrary point and r a positive exponent, then the polygon $\mathfrak{A}\mathfrak{P}^r$ is likewise of the second kind, and consequently the divisor $\mathfrak{M}$ of the corresponding class cannot be divisible by $\mathfrak{P}$, because otherwise $\mathfrak{A}\mathfrak{P}^{r-1}$, and hence also $\mathfrak{A}$, would be a polygon of the first kind (§ 30, 4.). If therefore one sets

$$\mathfrak{A}\mathfrak{P}^r = \mathfrak{M}\mathfrak{B}',$$

then $\mathfrak{P}$ will not go into $\mathfrak{M}$, and consequently $\mathfrak{B}'$ contains the factor $\mathfrak{P}$ exactly r times more often than $\mathfrak{A}$. At the same time $\mathfrak{B}'$ belongs to a proper class. Now if

$$\mathfrak{B}' = \mathfrak{P}^{m+r} \mathfrak{P}'^{m'} \mathfrak{P}''^{m''} \dots,$$

then the powers of points $\mathfrak{P}^m, \mathfrak{P}'^{m'}, \mathfrak{P}''^{m''}, \dots$ all go into $\mathfrak{A}$. If therefore we set

$$\mathfrak{B} = \mathfrak{P}^{m+r+1} \mathfrak{P}'^{m'+1} \mathfrak{P}''^{m''+1} \dots = \mathfrak{B}' \mathfrak{P} \mathfrak{P}' \mathfrak{P}'' \dots,$$

then by 2. there certainly exists a proper differential $d\sigma$ in the family of differentials belonging to the lower polygon $\mathfrak{B}$. Its representation by the normal form certainly contains the differential

$$dt_{(\mathfrak{P}^{m+r})} \tag{1.}$$

and besides all or some of the differentials

$$\begin{cases} dt_{(\mathfrak{P})}, & dt_{(\mathfrak{P}^2)}, & \dots & dt_{(\mathfrak{P}^m)} \dots dt_{(\mathfrak{P}^{m+r-1})}, \\ dt_{(\mathfrak{P}')} & dt_{(\mathfrak{P}'^2)}, & \dots & dt_{(\mathfrak{P}'^{m'})}, \\ dt_{(\mathfrak{P}'')} & dt_{(\mathfrak{P}''^2)}, & \dots & dt_{(\mathfrak{P}''^{m''})} \\ \dots & \dots & \dots & \dots \end{cases} \tag{2.}$$

together with differentials of the first kind. Hence the differential (1.) can be expressed linearly, with constant coefficients, by (2.), by differentials of the first kind, and by $d\sigma$.

If therefore the p -gon of the second kind is

$$\mathfrak{A} = \mathfrak{P}_1^{m_1} \mathfrak{P}_2^{m_2} \dots$$

one recognizes, by repeated application of the procedure described here, that all differentials of the second kind can be represented, in the way our theorem states, by the p differentials

$$\begin{cases} dt_{(\mathfrak{P}_1)} \dots dt_{(\mathfrak{P}_1^{m_1})}, \\ dt_{(\mathfrak{P}_2)} \dots dt_{(\mathfrak{P}_2^{m_2})}, \\ \dots \end{cases} \quad (3.)$$

Braunschweig and Königsberg i. Pr., October 1880.