Dedekind and Weber’s 1880 Theory of Algebraic Functions of one Variable.

Translated by Noel Robinson
B.A. (Oxon), MSc(OU), MASt(Cantab)

July 2012

Translator’s introduction.

This is an amateur translation by a student for students with little German to be able to get an overview of a master work. Out of respect for the original, this is a quasi-literal translation in which I have tried to stick a closely as possible to the layout (although I have taken the liberty of constructing a TOC). Needless to say this can sometimes seem a little “clunky” to a modern ear but the object was always the mathematics and not literature. (Personally I find the 19th Century German style and precision captivating, but watch out for the way of writing determinants as sums without indices!). So, for example, instead of using “vector space” to translate “Schaar” where this might have been technically accurate but seems a little anachronistic, I have used the more general term “family”. Also I have stuck with “integral rational function” throughout instead of just polynomial as this is what they wrote and it brings out the role in the function field more clearly.

Acknowledgements.

I found the digitized original document on-line at The Göttingen State and University Library. They have given their permission for its use in this translation and of course should be acknowledged in any copy of this document. They have some general terms and conditions for the use of material which I have reproduced before the start.

Although I have not found any full translation elsewhere (although one is now on its way I believe), I have read a translation of the introduction (curiously omitting one sentence) with which I have compared my efforts. It has proved most helpful in getting the sense right and I have probably borrowed or duplicated the occasional expression. ¹

¹ Bernhard Riemann 1826 - 1866 by Detlef Laugwitz, Translated by Abe Shenitzer, pages 154-156, Birkhäuser Boston, 2008
Contents

Part I.
§1. Algebraic function fields.
§2. Norm, trace, and discriminant.
§3. The system of integral functions of \( z \) in the field \( \Omega \).
§4. The module of functions.
§5. Congruences.
§6. The norm of one module relative to another.
§7. The ideals in \( o \).
§8. Multiplication and division of ideals.
§10. The complementary bases of a field \( \Omega \).
§11. The ramification ideal.
§12. The fractional functions of \( z \) in the field \( \Omega \).
§13. The rational transformations of the functions in the field \( \Omega \).

Part II.
§14. The points of the Riemann surface.
§15. The order numbers.
§16. Conjugate points and conjugate values.
§17. Representation of the functions in the field \( \Omega \) by polygon quotients.
§18. Equivalent polygons and polygon classes.
§20. Reduction in the dimension of the family by divisibility conditions.
§21. The dimensions of the polygon classes.
§22. The normal bases of \( o \).
§23. The differential quotient.
§24. The genus of the field \( \Omega \).
§25. The differentials in \( \Omega \).
§26. The differentials of the first kind.
§27. Polygon classes of the first and second kind.
§28. The Riemann-Roch theorem for proper classes.
§29. The Riemann-Roch theorem for improper classes of the first kind.
§30. Improper classes of the second kind.
§31. Differentials of the second and third kind.
§32. Residues.
§33. Relations between the differentials of first and second kinds.
Theorie der algebraischen Functionen einer Veränderlichen.
by Weber, H.; Dedekind, R.
in: Journal für die reine und angewandte Mathematik, (page(s) 181 - 290)
Berlin; 1882

The Goettingen library (see below) is owner of the original work (Volume 92 (1882)) on which this translation has been based. Please acknowledge this in any further distribution of this document. Their general Terms and Conditions are reproduced below.

Terms and Conditions
The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library. Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library’s online system to access or download a digitized document you accept there Terms and Conditions. Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library. For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact:
Niedersaechsische Staats- und Universitaetsbibliothek
Digitalisierungszentrum
37070 Goettingen
Germany
Email: gdz@sub.uni-goettingen.de
Introduction.

The aim of the investigations set out below is to develop the theory of algebraic functions of one variable, which is one of Riemann’s major achievements, from a simple and at the same time rigorous and fully general point of view. Previous studies of this subject are usually limited by certain restrictions made on the singularities of relevant functions and the so-called exceptional cases are either mentioned in passing as a boundary case or put to one side. Similarly, certain principles about continuity and expandability are assumed whose justification is based on various kinds of geometric intuition. It is possible to obtain a solid foundation for the basic ideas as well as for a general and full treatment of the theory if you start from a generalization of the theory of rational functions of one variable, in particular of the theorem that each integral rational function in one variable can be decomposed into linear factors. This generalization is simple and well known for the first case in which the number designated \( p \) by Riemann (the genus by Clebsch) is zero. For the general case, which is related to that mentioned above in the same way as the case of the most general algebraic numbers is related to that of the rational numbers, the right path was indicated by the practical methods used with great effect in number theory which are linked to Kummer’s creation of ideal numbers and which can be satisfactorily transferred to the theory of functions. ¹

If, in analogy with the theory of numbers, one understands a field of algebraic functions to be based on a system of such functions with the property that the application of the four basic operations to functions in the system always leads to functions in the same system, then the concept completely coincides with that of the Riemannian class of algebraic functions. Any of the functions in such a field can be taken as an independent variable so that any of the remaining functions can be considered as dependent on it. To each of these “representations” there corresponds a system of functions in the field, called integral functions, whose quotients make up the whole field. Within these integral functions we can further identify groups of functions characterised as integral rational functions having a common divisor. Although such a factor does not exist in the general case, when the relevant theorems on rational functions are applied not to the factor itself, but to the system of functions divisible by this factor, then there can be a complete

¹The ideal numbers of Kummer are first introduced by the paper: *On the theory of complex numbers* (Crelle’s Journal, vol 35); one finds a further development and a general presentation of the theory of algebraic numbers in the second and third edition of Dirichlet’s lectures about number theory, and in the paper by Dedekind: *Sur la théorie des nombres entiers algébrique* (Paris 1877. Reprinted from the Bulletin des sciences math. et astron. of Darboux and Höuel. But the knowledge of these writings is not assumed anywhere in our work.

From oral communications we have now learnt that Kronecker had several years ago made investigations related to the work of Weierstrass based on an approach similar to ours.
transfer to algebraic functions in general. In this way we arrive at the concept of an ideal, a name which comes from Kummer’s number theory, where the missing factors are introduced into the account as “ideal factors”.

Although the present study does not deal at all with "ideal" functions and all operations are executed only on systems of functions that actually exist, it seemed useful to retain the name "ideal", as it is already common in the theory of numbers.

After a proper explanation of multiplication, the rules for calculating with these ideals are just the same as for rational functions. In particular there follows the theorem that every ideal can be decomposed in one way into factors which themselves cannot be further decomposed and hence are called prime ideals. These prime ideals correspond to the linear factors in the theory of integral rational functions. Because of this, one can obtain a completely precise and general definition of “a point of the Riemann Surface”, i.e. a quite specific system of numerical values which the functions in the field may take in a consistent manner.

From this, a formal definition of the derivative then leads to the genus number and to a very general and elegant presentation of the differentials of the first kind. This leads to the proof of the Riemann-Roch theorem about the number of arbitrary constants in a function specified by its poles, and to the theory of differentials of the second and third kind. Up to this point, the continuity and expandability of the investigated functions has not been considered at all. For example, there would not be any gap remaining if one chose to restrict the usual domain of numbers to the system of algebraic numbers. Thus a well defined and fairly extensive part of the theory of algebraic functions is dealt with solely by means within its own sphere.

Of course, all these results can be obtained with much less effort and more modest means as special cases of the comprehensive and general theory of Riemann, but it is acknowledged that a rigorous justification of this theory presents certain difficulties and, until one is successful in completely overcoming these difficulties, the path we follow, or at least a related one, may probably be the only one for the theory of algebraic functions that leads to the goal with satisfactory rigour and generality. Thus even ideal theory itself would be remarkably simplified if the concept of Riemann surface and in particular that of a point on one were assumed, together with the same approach to the continuity of algebraic functions. Conversely, in our work the theory of ideals is algebraically justified by a long detour and from this a completely practical and rigorous definition of the “points of the Riemann Surface” is obtained, which can also serve to form the basis for the study of continuity and related issues. These questions, including the application to Abelian integrals and their periodic moduli, remain for the time being excluded from our study. We hope to return to them on another occasion.

Königsberg, 22 October 1880
Part I.

§1. Algebraic function fields.

A variable \( \theta \) is called an algebraic function of an independent variable \( z \) if an irreducible algebraic equation

\[
F(\theta, z) = 0
\]

is satisfied. \( F \) here means an expression of the form

\[
F(\theta, z) = a_0 \theta^n + a_1 \theta^{n-1} + \ldots + a_{n-1} \theta + a_n,
\]

where the coefficients \( a_0, a_1, \ldots a_n \) are integral rational functions of \( z \) without common divisor. The assumed irreducibility of equation (1.) implies that \( \theta \) does not satisfy an equation of lower degree in \( \theta \) and, as is clear from the algorithm of the greatest common divisor, it follows that if

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

is a second equation which \( \theta \) satisfies, then \( G(\theta, z) \) must be divisible by \( F(\theta, z) \) algebraically. Let us now also prove that \( G(\theta, z) \) in terms of \( z \) can not be of lower degree than \( F(\theta, z) \) and then only of the same degree if in \( G(\theta, z) \) we can isolate an independent factor of \( z \). Let us assume that the coefficients \( b_0, b_1, \ldots b_m \) were free from common factors and we denote by

\[
H(\theta, z) = c_0 \theta^{m-n} + c_1 \theta^{m-n-1} + \ldots + c_{m-n} 
\]

the quotient of \( G \) by \( F \) free of a denominator, then we have

\[
kG(\theta, z) = F(\theta, z).H(\theta, z),
\]

where \( k \) is an integral rational function of \( z \), and the following comparison of coefficients

\[
kb_0 = a_0 c_0, \\
k b_1 = a_0 c_1 + a_1 c_0, \\
k b_2 = a_0 c_2 + a_1 c_1 + a_2 c_0, \\
\ldots \ldots \ldots \ldots \ldots
\]

in which the \( c_0, c_1, \ldots c_{m-n} \) can also be assumed to be without a common divisor.

It follows first that \( k \) must be constant and can be set = 1, for if some linear factor of \( k \) divides \( a_0, a_1, \ldots a_{r-1}, c_0, c_1, \ldots c_{s-1} \) but not, \( a_r \) or \( c_s \) then from

\[
k b_{r+s} = \ldots a_{r-1} c_{s+1} + a_r c_s + a_{r+1} c_{s-1} + \ldots
\]
the contradiction follows that \(a, c\) has to be divisible by the same linear factor. From this it also follows that the degree of \(G(\theta, z)\) with respect to \(z\) is the sum of the degrees of \(F\) and \(H\) in terms of \(z\); since if \(a, c\) are the first among the coefficients \(a\) and \(c\) whose degree is the maximum value achieved, it follows from

\[
b_{r+s} = \ldots a_{r-1}c_{s+1} + a, c + a_{r+1}c_{s-1} + \ldots
\]

that the degree of \(b_{r+s}\) is equal to the sum of the degrees of \(a\) and \(c\).

Dividing the equation \((1.)\) by \(a_0\) it can also be set in the form

\[
(2.) \quad f(\theta, z) = \theta_n + b_1\theta_{n-1} + \ldots + b_{n-1}\theta + b_n = 0
\]

where the coefficients \(b_1, b_2, \ldots b_n\) can also be fractional rational functions of \(z\).

The system of all rational functions of \(\theta\) and \(z\), \(\Phi(\theta, z)\), has the property that it is closed under the elementary arithmetic operations of addition, subtraction, multiplication and division, and this system is hence known as a field of algebraic functions \(\Omega\) of degree \(n\). If for the moment \(\phi(\theta)\) is an integral rational function of \(\theta\) whose coefficients depend rationally on \(z\), we can by algebraic division specify precisely two such functions \(q(\theta)\) and \(r(\theta)\), the degree of the second of which does not exceed \(n - 1\), so that

\[
\phi(\theta) = q(\theta)f(\theta) + r(\theta)
\]

or because of \((2.)\)

\[
\phi(\theta) = r(\theta).
\]

If \(\phi(\theta)\) is not divisible by \(f(\theta)\) then these two functions have no common factor (because of the assumed irreducibility of \(f(\theta)\)), and therefore we can determine by the method of the greatest common divisor two functions \(f_1(\theta)\) and \(\phi_1(\theta)\) such that

\[
f(\theta)f_1(\theta) + \phi(\theta)\phi_1(\theta) = 1,
\]

in other words because of \((2.)\)

\[
\phi_1(\theta) = \frac{1}{\phi(\theta)}
\]

From these two observations taken together with the assumption of the irreducibility of \(f(\theta)\) we have the following

Proposition. Each function \(\zeta\) in the field \(\Omega\) can be written in a unique way in the following form:

\[
\zeta = x_0 + x_1\theta + \ldots + x_{n-1}\theta^{n-1}
\]

where the coefficients \(x_0, x_1, \ldots x_{n-1}\) are rational functions of \(z\). Conversely, every function of this form obviously belongs to the field \(\Omega\).
Choose arbitrarily \( n \) of the functions in the field \( \Omega \):

\[
\eta_1 = x_0^{(1)} + x_1^{(1)} \theta + \ldots + x_{n-1}^{(1)} \theta^{n-1}, \\
\eta_2 = x_0^{(2)} + x_1^{(2)} \theta + \ldots + x_{n-1}^{(2)} \theta^{n-1}, \\
\ldots \ldots \ldots \ldots \\
\eta_n = x_0^{(n)} + x_1^{(n)} \theta + \ldots + x_{n-1}^{(n)} \theta^{n-1}
\]

such however that the determinant

\[
\sum \pm x_0^{(1)} x_1^{(2)} \ldots x_{n-1}^{(n)}
\]

is not identically zero, it follows that every function in the field \( \Omega \) may also be expressed in the form

\[
\zeta = y_1 \eta_1 + y_2 \eta_2 + \ldots + y_n \eta_n
\]

whose coefficients \( y_1, y_2, \ldots y_n \) are rational functions of \( z \). Such a system of functions \( \eta_1, \eta_2, \ldots \eta_n \) is called a \textit{basis of the field} \( \Omega \).

For a system of functions \( \eta_1, \eta_2, \ldots \eta_n \) to form a similar basis of the field \( \Omega \), it is necessary and sufficient that no equation (identity) of the form

\[
y_1 \eta_1 + y_2 \eta_2 + \ldots + y_n \eta_n = 0
\]

exists between them in which the coefficients \( y_1, y_2, \ldots y_n \) do not all vanish. For example, the functions \( 1, \theta, \theta^2, \ldots \theta^{n-1} \) form a basis of \( \Omega \).

\section{§2. Norm, trace, and discriminant.}

Choose an arbitrary basis \( \eta_1, \eta_2, \ldots \eta_n \) for expressing the functions in \( \Omega \), if \( \zeta \) is any function in \( \Omega \) we can set:

\[
\begin{align*}
\zeta \eta_1 &= y_{1,1} \eta_1 + y_{1,2} \eta_2 + \ldots + y_{1,n} \eta_n, \\
\zeta \eta_2 &= y_{2,1} \eta_1 + y_{2,2} \eta_2 + \ldots + y_{2,n} \eta_n, \\
\ldots \ldots \ldots \ldots \\
\zeta \eta_n &= y_{n,1} \eta_1 + y_{n,2} \eta_2 + \ldots + y_{n,n} \eta_n
\end{align*}
\]

where the coefficients \( y_{i,j} \) are rational functions of \( z \). From this we get the equation

\[
\begin{vmatrix}
    y_{1,1} - \zeta & y_{1,2} & \cdots & y_{1,n} \\
    y_{2,1} & y_{2,2} - \zeta & \cdots & y_{2,n} \\
    \vdots & \vdots & \ddots & \vdots \\
    y_{n,1} & y_{n,2} & \cdots & y_{n,n} - \zeta
\end{vmatrix} = 0
\]

which, ordered in powers of \( \zeta \), has the form

\[
\phi(\zeta) = \zeta^n + b_1 \zeta^{n-1} + \ldots + b_{n-1} \zeta + b_n = 0
\]
and is completely independent of the choice of the selected basis $\eta_1, \eta_2, \ldots, \eta_n$, which follows without difficulty from the multiplication theory of determinants. Of the coefficients $b_1, b_2, \ldots, b_n$ for the function $\phi$, which are all rational functions of $z$ and are completely determined by the function $\zeta$, two of importance should be famously distinguished by special names. The function

\[(4) \quad (-1)^n b_n = \begin{vmatrix} y_{1,1} & y_{1,2} & \cdots & y_{1,n} \\ y_{2,1} & y_{2,2} & \cdots & y_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ y_{n,1} & y_{n,2} & \cdots & y_{n,n} \end{vmatrix} \]

is called the norm of the function $\zeta$ and is denoted by $N(\zeta)$. For this function we have the following theorems.

1. The only function whose norm is identically zero is the function "zero"; because if you make the assumption that $N(\zeta) = 0$ in the system (1.), it follows that since such a system of rational functions of $z$ do not all vanish, $y_1, y_2, \ldots y_n$ can be determined so that

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

then, since $\eta_1, \eta_2, \ldots, \eta_n$ form a basis for $\Omega$, $\zeta = 0$.

2. The norm of a rational function of $z$ is the $n^{th}$ power of this function. Since $\zeta$ is rational, the equations (1.) are reduced to the identities $\zeta \eta_h = \zeta \eta_h$, whence $N(\zeta) = \zeta^n$ follows.

3. If $\zeta'$ is any second function in the field $\Omega$ and the system of equations corresponding to System (1.) for this function is

$$\zeta' \eta_h = \sum_i y'_{h,i} \eta_i,$$

it follows that:

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

and hence by the multiplication theorem of the determinants

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

4. From 2. and 3. it follows that:

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

In other words:

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

5. Finally, from the definition of the function $\phi$, (2.) and (3.) we have the important theorem: If $t$ is an arbitrary constant (or a rational function of $z$), then

$$\phi(t) = N(t - \zeta)$$
Next, the function

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

is called the *trace* of $\zeta$ and denoted by $S(\zeta)$. These next theorems result directly from the definition:

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

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

If $x$ is a rational function of $z$ and $\zeta$ and $\zeta'$ are two functions in $\Omega$:

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

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

It has emerged from this consideration that every function $\zeta$ in $\Omega$ satisfies an equation of the $n$th degree, $\phi(\zeta) = 0$, whose coefficients depend rationally upon $z$. If this equation is irreducible, then the functions $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$ form a basis of $\Omega$. In the other case were

$$(10.) \quad \phi_1(\zeta) = \zeta^e + b_0\zeta^{e-1} + \ldots + b_{e-1}\zeta + b_e = 0$$

to be the equation of lowest degree whose coefficients in $z$ are rational which the function $\zeta$ satisfies, then $\phi_1(\zeta) = 0$ would be irreducible with $e < n$. Since nevertheless $\phi(\zeta)$ vanishes, then $\phi(\zeta)$ must be algebraically divisible by $\phi_1(\zeta)$, and as in §1 it follows that any rational function $\eta$ of $z$ and $\zeta$ is represented in the form

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

with coefficients $x_0, x_1, x_{e-1}$ that depend rationally on $z$. If now

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

is the equation of lowest degree which $\theta$ satisfies whose coefficients depend rationally on $z$ and $\zeta$, then there exists between the $e.f$ functions

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

a non-linear equation with coefficients depending rationally on $z$, whereas every function in $\Omega$ is representable linearly by means of these functions with coefficients rationally dependent on $z$. It is clear from this that these form a basis for $\Omega$, and that therefore

$$e.f = n,$$

1The equation $\phi_1(\zeta) = 0$ gives rise to an algebraic function field $\Omega_1$ of degree $e$, at the same time all these functions are included in the field $\Omega$ and can therefore be described as part of the field $\Omega$. 

}\text{\textsuperscript{1}}
So \( e \) divides \( n \).

Applying the basis (11.) to establish the Norm of \( \zeta \), it can be seen easily by means of equation (10.) that

\[
N(\zeta) = ((-1)^{n-b'_e}) = (-1)^n b'_e
\]

Further, since for an arbitrary constant \( t \) the function \( \zeta - t \) satisfies an equation of the same degree as \( \zeta \), we have the theorem:

10. The function \( \phi(t) \) (3.) is either irreducible or an integral power of an irreducible function.

If \( \eta_1, \eta_2, \ldots \eta_n \) is an arbitrary system of \( n \) functions in \( \Omega \), regardless of whether they form a basis or not, then we introduce for this system a rational function of \( z \) which we call the \textit{discriminant}, designated \( \Delta(\eta_1, \eta_2, \ldots \eta_n) \) and defined as follows

\[
(12.) \quad \Delta(\eta_1, \eta_2, \ldots \eta_n) = \begin{vmatrix}
S(\eta_1 \eta_1) & S(\eta_1 \eta_2) & \ldots & S(\eta_1 \eta_n) \\
S(\eta_2 \eta_1) & S(\eta_2 \eta_2) & \ldots & S(\eta_2 \eta_n) \\
\vdots & \vdots & \ddots & \vdots \\
S(\eta_n \eta_1) & S(\eta_n \eta_2) & \ldots & S(\eta_n \eta_n)
\end{vmatrix}
\]

The discriminant is not identical to zero if and only if the functions \( \eta_1, \eta_2, \ldots \eta_n \) form a basis for \( \Omega \).

As the first step in proving this statement we suppose that \( \Delta(\eta_1, \eta_2, \ldots \eta_n) = 0 \). In this case, a set of rational functions \( y_1, y_2, \ldots y_n \) of \( z \) can be determined that do not all vanish identically, such that

\[
y_1 S(\eta_1 \eta_k) + y_2 S(\eta_2 \eta_k) + \ldots + y_n S(\eta_n \eta_k) = S(\eta_k (y_1 \eta_1 + y_2 \eta_2 + \ldots + y_n \eta_n)) = 0 \quad (k = 1, 2, \ldots n)
\]

Then choose a quite arbitrary system of rational functions \( x_1, x_2, \ldots x_n \) of \( z \), and set:

\[
y_1 \eta_1 + y_2 \eta_2 + \ldots + y_n \eta_n = \eta,
\]
\[
x_1 \eta_1 + x_2 \eta_2 + \ldots + x_n \eta_n = \xi,
\]

so that:

\[
S(\xi \eta) = 0.
\]

But since the functions \( \eta_1, \eta_2, \ldots \eta_n \) form a basis for \( \Omega \), \( \xi \) can be an arbitrary function in \( \Omega \), so for example, since \( \eta \) does not vanish, could be \( \frac{1}{\eta} \). But then the last equation is certainly not satisfied and hence in this case the discriminant of \( \eta_1, \eta_2, \ldots \eta_n \) can \textit{not} vanish identically.

Keeping fixed this assumption that \( \eta_1, \eta_2, \ldots \eta_n \) is a basis of \( \Omega \), set:

\[
\eta'_k = x_{1,k} \eta_1 + x_{2,k} \eta_2 + \ldots + x_{n,k} \eta_n, \quad (k = 1, 2, \ldots n)
\]
thus whether the functions \( \eta'_1, \eta'_2, \ldots, \eta'_n \) form a basis of \( \Omega \) or not, depends on whether the determinant of the rational functions \( x_{h,k} \) of \( z \)

\[
X = \sum \pm x_{1,1}x_{2,2} \ldots x_{n,n}
\]
is different from zero or not. But if

\[
S(\eta'_h \eta'_k) = \sum_{i,i' \neq 1} x_{i,h}x_{i'k}S(\eta_i \eta_{i'})
\]

then from the multiplication theorem of determinants there follows the fundamental theorem of discriminants

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

what the correctness of the second part of the above statement also shows is that the discriminant of a system of functions always vanishes identically if they do not form a basis of \( \Omega \).

§3.

The system of integral functions of \( z \) in the field \( \Omega \).

Definition. A function \( \omega \) in the field \( \Omega \) will be called an integral function of \( z \) if in the equation of lowest degree as in §2 which it satisfies:

\[
(1.) \quad \phi(\omega) = \omega^e + b_1 \omega^{e-1} + \ldots + b_{e-1} \omega + b_e = 0,
\]

the coefficients \( b_1, b_2, \ldots, b_e \) are integral rational functions of \( z \); otherwise it is called a fractional function. The set of all integral functions of \( z \) in \( \Omega \) will be written as \( \mathfrak{o} \). Since according to §2 \( N(t - \omega) \) is an integral power of \( \phi(t) \), it follows that for an integral function \( \omega \) all the coefficients of \( N(t - \omega) \) are also integral rational functions of \( z \), that is in particular:

1. The norm and trace of an integral function are integral rational functions of \( z \).

From the definition of an integral function we have 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. Each function \( \eta \) in \( \Omega \) can, by multiplication by a non-zero integral rational function of \( z \), be transformed into a function of the system \( \mathfrak{o} \). Then \( \eta \) according to §2 satisfies an equation of the lowest degree of the form

\[
b_0 \eta^e + b_1 \eta^{e-1} + \ldots + b_{e-1} \eta + b_e = 0
\]

whose coefficients are integral rational functions of \( z \), and by means of the substitution \( b_0 \eta = \omega \) this changes to an equation of the form (1.) above for \( \omega \).
4. A function $\omega$ from the field $\Omega$ which satisfies any equation of the form

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

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

$$\phi(\omega) = \omega^e + b_1\omega^{e-1} + \ldots + b_e\omega + b_e = 0$$

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

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

which it is easy to show has the consequence that each of the coefficients of $\phi(\omega)$ and $\chi(\omega)$ are integral rational functions of $z$ (Gauss, Disq. Ar. art. 42). Hence we have the law of integral functions:

5. The sum, difference and product of two integral functions is again an integral function.

If $\omega'$ and $\omega''$ represent two integral functions in $\Omega$ which satisfy the respective equations

$$\omega'^{n'} + b'_1\omega'^{n'-1} + \ldots + b'_{n'-1}\omega' + b'_{n'} = 0,$$

$$\omega''^{n''} + b''_1\omega''^{n''-1} + \ldots + b''_{n''-1}\omega'' + b''_{n''} = 0,$$

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

$$\omega'^{n'}\omega''^{n''}$$

and by $\omega$ one of the three functions $\omega' \pm \omega'', \omega'\omega''$, we can set;

$$\omega\omega_1 = x_{1,1}\omega_1 + \ldots + x_{1,m}\omega_m,$$

$$\ldots \ldots \ldots \ldots \ldots \ldots$$

$$\omega\omega_m = x_{m,1}\omega_1 + \ldots + x_{m,m}\omega_m,$$

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

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

as an equation for $\omega$, whose coefficients are integral rational functions of $z$.

As a result, one has the corollary that each integral rational function of functions in $\sigma$ is itself a function in the system $\sigma$. 

---

Dedekind and Weber, Theory of the algebraic functions of one variable.
6. An integral function \( \omega \) is called \textit{divisible} by an other integral function \( \omega' \), if a third integral function \( \omega'' \) exists which satisfies the condition

\[
\omega = \omega' \omega''
\]

From this definition there follows immediately:

If \( \omega \) is divisible by \( \omega' \) and \( \omega' \) by \( \omega'' \), then \( \omega \) is also divisible by \( \omega'' \).

If \( \omega' \) and \( \omega'' \) are divisible by \( \omega \), then \( \omega' \pm \omega'' \) is also divisible by \( \omega \), and in general if \( \omega_1, \omega_2, \omega_3, \ldots \) are divisible by \( \omega \) and \( \omega'_1, \omega'_2, \omega'_3, \ldots \) are arbitrary functions in \( \sigma \), then \( \omega'_1 \omega_1 + \omega'_2 \omega_2 + \omega'_3 \omega_3 + \ldots \) is also divisible by \( \omega \).

7. If the functions \( \eta_1, \eta_2, \ldots, \eta_n \) form a basis for \( \Omega \), then one can (from 3.) determine \( n \) non-zero integral rational functions of \( z, a_1, a_2, \ldots, a_n \), such that

\[
\omega_1 = a_1 \eta_1, \quad \omega_2 = a_2 \eta_2, \quad \ldots \quad \omega_n = a_n \eta_n
\]

are integral functions, and these also form a basis of \( \Omega \), since

\[
\Delta(\omega_1, \omega_2, \ldots, \omega_n) = a_1^2 a_2^2 \cdots a_n^2 \Delta(\eta_1, \eta_2, \ldots, \eta_n)
\]

is non-zero. This gives a basis \( \omega_1, \omega_2, \ldots, \omega_n \) of \( \Omega \) which consist of pure integral functions, and, since the \( S(\omega, \omega) \) are integral rational functions of \( z \), the discriminant of such a basis is itself a non-zero integral rational function of \( z \). Each function of the form

\[
(2.) \quad \omega = x_1 \omega_1 + x_2 \omega_2 + \ldots + x_n \omega_n,
\]

in which the \( x_1, x_2, \ldots, x_n \) are integral rational functions of \( z \), then belongs to the system \( \sigma \); but it is certainly not necessarily the case that conversely each function in \( \sigma \) can be expressed in this form.

Let us suppose then, that there are still other functions in \( \sigma \) than those of the form (2.), then choose a linear function \( z - c \) and some integral rational functions \( x_1, x_2, \ldots, x_n \) which are not all divisible by \( z - c \), so that

\[
\frac{x_1 \omega_1 + x_2 \omega_2 + \ldots + x_n \omega_n}{z - c}
\]

is an integral function. Let the functions \( x_1, x_2, \ldots, x_n \) have the constant remainders \( c_1, c_2, \ldots, c_n \) when divided by \( z - c \), which are not all zero, and it is then evident that

\[
\omega = \frac{c_1 \omega_1 + c_2 \omega_2 + \ldots + c_n \omega_n}{z - c}
\]

is also an integral function. If \( c_1 \) is non-zero then the \( n \) integral functions

\[
\omega \quad \text{and} \quad \omega_1, \omega_2, \ldots, \omega_n
\]

also form a basis for \( \Omega \) and at the same time, following \( \S2 \) (13.),

\[
\Delta(\omega, \omega_1, \ldots, \omega_n) = \frac{c_1^2}{(z - c)^2} \Delta(\omega_1, \omega_2, \ldots, \omega_n)
\]
is thus of a lower degree than $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$. Since now these two discriminants are integral rational functions of $z$, then by repeated application of this procedure one eventually arrives at integral functions, $\omega'_1, \omega'_2, \ldots, \omega'_n$, forming a basis of $\Omega$, whose discriminant has a degree that cannot be further reduced, and which thus has the property \textit{that any function $\omega$ in $\sigma$ is of the form}

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

\textit{with integral rational functions of $z$ as coefficients. Such a system will be called a basis of $\sigma$.}

If $\omega_1, \omega_2, \ldots, \omega_n$ is a basis for $\sigma$ and

$$\omega'_i = x_{i,1}\omega_1 + x_{i,2}\omega_2 + \ldots + x_{i,n}\omega_n, \quad (i=1,2,\ldots,n)$$

then the system $\omega'_1, \omega'_2, \ldots, \omega'_n$, will form a basis of $\sigma$ if and only if the determinant of the integral rational functions $x_{i,i'}$,

$$X = \sum \pm x_{1,i}x_{2,i} \ldots x_{n,i}$$

is a non-zero \textit{constant}. For suppose this determinant had any linear factor $z - c$, then constants $c_1, c_2, \ldots, c_n$, which do not all vanish, can be determined such that the $n$ integral rational functions of $z$

$$c_1x_{1,i} + c_2x_{2,i} + \ldots + c_nx_{n,i}$$

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

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

is an integral function and therefore $\omega'_1, \omega'_2, \ldots, \omega'_n$ is not a basis for $\sigma$.

Since now on the other hand

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

it follows that the discriminant of a basis of $\sigma$, apart from a constant factor, is independent of the choice of basis. In other words, one obtains a completely determined integral rational function of $z$ when the discriminant of an arbitrary basis of $\sigma$ has the coefficient of the highest power of $z$ made $= 1$ by division. \textit{This function will be called the discriminant of the field $\Omega$ or of the system $\sigma$ and be designated by $\Delta(\Omega)$ or $\Delta(\nu)$}.

§4.

The module of functions.

We consider in the following a system of functions which we call a \textit{module of functions} or also simply \textit{module} and define as follows. A system of functions (in
Ω) is called a module, if the same functions result from addition, subtraction and multiplication by integral rational functions of z.

With \( \alpha_1, \alpha_2, \ldots, \alpha_m \) any \( m \) given functions and with \( x_1, x_2, \ldots, x_m \), arbitrary integral rational functions of \( z \), then the set of all functions of the form

\[
\alpha = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_m\alpha_m
\]

forms a module. Such a one is called a finite module and will be designated by

\[
\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_m].
\]

The system of functions \( \alpha_1, \alpha_2, \ldots, \alpha_m \) is called the basis of this module.

A system of functions \( \alpha_1, \alpha_2, \ldots, \alpha_m \) is called rationally irreducible or the functions \( \alpha_1, \alpha_2, \ldots, \alpha_m \) are called rationally independent, if an equation of the form

\[
x_1\alpha_1 + x_2\alpha_2 + \ldots + x_m\alpha_m = 0
\]

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

First of all we prove the theorem:

1. Each finite module has a rationally irreducible basis.

The proof of this is a direct consequence of the following lemma:

If \( y_{1,1}, y_{2,1}, \ldots, y_{m,1} \) are integral rational functions without common divisor, then other integral rational functions \( y_{1,2}, y_{2,2}, \ldots, y_{m,m} \) can be determined so that

\[
\sum_{i=1}^{m} \pm y_{i,1} y_{i,2} \cdots y_{i,m} = 1
\]

Now if the functions \( \alpha_1, \alpha_2, \ldots, \alpha_m \) satisfy an equation

\[
\sum_{i=1}^{m} y_{i,1} \alpha_i = 0
\]

\( ^1 \)The theorem is correct and is known for \( m = 2 \). Let us assume, then, it was proved for \( m - 1 \), so, if \( \delta \) is greatest common divisor of \( y_{1,1}, y_{2,1}, \ldots, y_{m-1,1} \), we can satisfy the equation

\[
\begin{bmatrix}
  y_{1,1} & y_{2,1} & \cdots & y_{m-1,1} \\
  y_{1,3} & y_{2,3} & \cdots & y_{m-1,3} \\
  \cdots & \cdots & \cdots & \cdots \\
  y_{1,m} & x_{2,m} & \cdots & x_{m-1,m}
\end{bmatrix} = \delta
\]

and if we then determine integral rational functions \( x \) and \( y \) so that

\[
xy_{m,1} - y\delta = (-1)^{m-1}
\]

it follows that:

\[
\begin{bmatrix}
  y_{1,1} & y_{2,1} & \cdots & y_{m-1,1} & y_{m,1} \\
  x_{1,1} & x_{2,1} & \cdots & x_{m-1,1} & y \\
  y_{1,3} & y_{2,3} & \cdots & y_{m-1,3} & 0 \\
  \cdots & \cdots & \cdots & \cdots & \cdots \\
  y_{1,m} & y_{2,m} & \cdots & y_{m-1,m} & 0
\end{bmatrix} = 1.
\]
in which the integral rational functions $y_1, \ldots, y_m$ can be assumed to be without a common divisor, then one sets

$$\sum_{i=1}^{m} y_{i,2} \alpha_i = \beta_2,$$

$$\cdots \cdots \cdots \cdots$$

$$\sum_{i=1}^{m} y_{i,m} \alpha_i = \beta_m;$$

and the module $[\alpha_1, \alpha_2, \ldots, \alpha_m]$ is completely identical to the module $[\beta_2, \beta_3, \ldots, \beta_m]$, the basis of which contains one function less. If the functions $\beta_i$ are now not rationally independent, then one can further reduce them in the same way and eventually arrive at an irreducible basis, provided that the functions $\alpha$, do not all vanish (a case which we would completely exclude from the module concept). As a result, simply a basis will always be understood to be an irreducible basis.

2. Although further to the above one can find many different irreducible bases for one and the same module, it is still the case that the number of functions that are contained in one such is always the same, since if it contained more functions it could not be rationally irreducible. If $\alpha_1, \alpha_2, \ldots, \alpha_m; \beta_1, \beta_2, \ldots, \beta_m$ are two irreducible bases for the same module $a$, then, since both the $\alpha_k$ and the $\beta_k$ are contained in $a$:

$$\alpha_k = \sum_{i=1}^{m} p_i^{(k)} \beta_i; \quad \beta_k = \sum_{i=1}^{m} q_i^{(k)} \alpha_i,$$

where the coefficients $p, q$ are integral rational functions of $z$. But hence it follows that:

$$\sum_{i=1}^{m} q_i^{(k)} p_i^{(h)} = 0 \text{ or } 1,$$

depending on whether $h$ is different from $k$ or not, and from that:

$$\sum \pm p_1^{(1)} p_2^{(2)} \cdots p_m^{(m)} \sum \pm q_1^{(1)} q_2^{(2)} \cdots q_m^{(m)} = 1,$$

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

3. Definition. A module $a$ is said to be divisible by a module $b$ or $b$ a divisor (Thelier) of $a$, or $a$ a multiple of $b$ (also $b$ goes in $a$), when each function in $a$ is also included in $b$. $b$ is said to be a real divisor of $a$ when $a$ is divisible by $b$, but is not identical with $b$.  

4. Definition. The set $m$ of all those functions which are in both of the two modules $a$ and $b$, if it does not consist of the single function "zero", forms a module (from the general definition), which is called the least common multiple of $a$ and $b$.

\[ \text{The concept of divisibility of modules adopted here is in contrast to that of numbers insofar as the divisor contains more functions than the multiple.} \]
since each module which is both a multiple of $a$ and of $b$ is also a multiple of $m$. The least common multiple of any number of modules $a, b, c \ldots$, is accordingly the set of all of the functions which are at the same time included in $a, b, c \ldots$. You can form this in the same way by choosing any two of the modules $a, b, c \ldots$, and replacing them by their least common multiple.

5. **Definition.** If $\alpha$ is any function in $a$ and $\beta$ any function in $b$, then the set of all functions of the form $\alpha + \beta$ is a module, $\mathfrak{d}$, which is called greatest common divisor of the two modules $a$ and $b$. When $a$ and $b$ are finite modules then it is too. That is to say if

$$a = [\alpha_1, \alpha_2, \ldots, \alpha_r] \quad b = [\beta_1, \beta_2, \ldots, \beta_s]$$

then

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

From the definition of divisibility, $\mathfrak{d}$ is a divisor both of $a$ and of $b$. Conversely, if $\mathfrak{d}'$ is a divisor of $a$ and of $b$, then the functions $\alpha$ as well as the functions $\beta$ and therefore 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 any number of modules is arrived at in the same way.

6. **Definition.** If $a$ is a module, $\alpha$ any function in $a$ and $\mu$ an arbitrary function in $\Omega$, then the product $\mu a$ or $a \mu$ is understood to be the set of all functions $\mu \alpha$, which again is a module, if

$$a = [\alpha_1, \alpha_2, \ldots, \alpha_r]$$

is a finite module, then

$$\mu a = [\mu \alpha_1, \mu \alpha_2, \ldots, \mu \alpha_r]$$

is also a finite module, and from $\mu a = \mu b$ it would follow that $a = b$, if $\mu$ is different from zero.

7. **Definition.** If $a$ and $b$ are two modules and $\alpha$ and $\beta$ are any functions in $a$ and $b$ respectively, by the **product**

$$ab = ba = c$$

is understood the set of all products of a function $\alpha$ and a function $\beta$ and all sums of such products, that is the same as all functions which can be written as

$$\gamma = \sum \alpha \beta.$$
factors in multiplication applies. If the individual elements of such a product, \( m \) of them, are equal to one another and \( = a \), then it can be written as \( a^m \), and
\[
 a^{m+m'} = a^m a^{m'}
\]

In general a product \( ab \) is not divisible by \( a \). In contrast this theorem, whose proof follows directly from the definition, applies:

\section*{§5. Congruences.}

Two functions \( \alpha \) and \( \beta \) are called congruent with respect to the module \( a \)
\[
\alpha \equiv \beta \quad \text{(mod.} \quad a)\)

when the difference of the two functions, \( \alpha - \beta \), is contained in the module \( a \).

The following theorems are a direct result of the definition:

1. If \( \alpha \equiv \beta \) and \( \beta \equiv \gamma \) \( \text{(mod.} \quad a) \) then \( \alpha \equiv \gamma \) \( \text{(mod.} \quad a) \).

2. If \( \mathfrak{b} \) is any divisor of \( a \) then it follows from \( \alpha \equiv \beta \) \( \text{(mod.} \quad a) \) that \( \alpha \equiv \beta \) \( \text{(mod.} \quad \mathfrak{b}) \) also.

3. If \( \alpha \equiv \beta \) \( \text{(mod.} \quad a) \) and \( \mu \) is any function in \( \Omega \), it follows that \( \mu \alpha \equiv \mu \beta \) \( \text{(mod.} \quad \mu a) \), and, vice versa, the latter congruence follows from the former when \( \mu \) is different from zero.

4. If \( \alpha \equiv \beta \) and \( \alpha_1 \equiv \beta_1 \) \( \text{(mod.} \quad a) \), then \( \alpha \pm \alpha_1 \equiv \beta \pm \beta_1 \) \( \text{(mod.} \quad a) \).

If \( \lambda_1, \lambda_2, \ldots, \lambda_m \) are any given functions in \( \Omega \) and \( c_1, c_2, \ldots, c_m \) are arbitrary constants, then the set of all functions of the form
\[
c_1 \lambda_1 + c_2 \lambda_2 + \ldots + c_m \lambda_m
\]
is called a family and is denoted by \( (\lambda_1, \lambda_2, \ldots, \lambda_m) \). The system of functions \( \lambda_1, \lambda_2, \ldots, \lambda_m \) is called the basis of the family. The functions \( \lambda_1, \lambda_2, \ldots, \lambda_m \) are called linearly independent or their system linearly irreducible, if in an equation (identity) of the form
\[
c_1 \lambda_1 + c_2 \lambda_2 + \ldots + c_m \lambda_m = 0
\]

it can only be that the constant coefficients \( c_1, c_2, \ldots, c_m \) all vanish.
There is then the theorem that each family has a linear irreducible basis. Because if $c_1 \lambda_1 + c_2 \lambda_2 + \ldots + c_m \lambda_m = 0$ and $c_1$ is different from zero, then the family $(\lambda_1, \lambda_2, \ldots, \lambda_m)$ is identical to the family $(\lambda_2, \lambda_3, \ldots, \lambda_m)$, the basis for which has fewer functions. If this is not yet linearly irreducible then one can continue in the same way. Thus the result will be a basis which is plainly seen to be an irreducible basis. The number of functions which are 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 then the family is also called an $m$-fold. Any $m$ functions in such a family form an irreducible basis if and only if they are linearly independent.

The functions $\lambda_1, \lambda_2, \ldots, \lambda_m$ are called linearly independent with respect to the module $a$, if a congruence of the form

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

only holds if the constant coefficients $c_1, c_2, \ldots, c_m$ vanish. Two sums of the form $\sum c_i \lambda_i$ with different values of the constant coefficients $c_i$, are thus always incongruent with respect to the module $a$.

Now let $a$ and $b$ be two modules, and suppose, for now, that there exist only a finite number of functions $\lambda_1, \lambda_2, \ldots, \lambda_m$ in $b$ which are linearly independent with respect to the module $a$. Then each function $\beta$ in $b$ satisfies one and only one congruence of the form

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

with constant coefficients $c_1, c_2, \ldots, c_m$. The family $(\lambda_1, \lambda_2, \ldots, \lambda_m)$ will be called a complete residue system of the module $b$ with respect to the module $a$ and $\lambda_1, \lambda_2, \ldots, \lambda_m$ a basis for it, and this can be written as:

$$\beta \equiv (\lambda_1, \lambda_2, \ldots, \lambda_m) \pmod{a}.$$ 

If any system of $m$ functions $\lambda'_1, \lambda'_2, \ldots, \lambda'_m$ is chosen from $b$, then $m$ congruences are satisfied

$$\lambda'_b \equiv \sum \pm k_{b,i} \lambda_i \pmod{a}$$

with constants $k_{b,i}$, and this system forms a basis of a complete residue system for $b$ with respect to $a$ if and only if the determinant

$$\sum \pm k_{1,1} k_{2,2} \ldots k_{m,m}$$

is non-zero.
§6. The norm of one module relative to another.

If \((\lambda_1, \lambda_2, \ldots, \lambda_m)\) is any complete residue system of a module \(b\) relative to another \(a\), then it follows, because \(zb\) is divisible by \(b\), that there is a specific system of \(m^2\) constants \(c_{h,k}\), such that these congruences will be satisfied:

\[
\begin{align*}
z\lambda_1 & \equiv c_{1,1}\lambda_1 + c_{2,1}\lambda_2 + \ldots + c_{m,1}\lambda_m \\
z\lambda_2 & \equiv c_{1,2}\lambda_1 + c_{2,2}\lambda_2 + \ldots + c_{m,2}\lambda_m \\
\vdots & \vdots \\
z\lambda_m & \equiv c_{1,m}\lambda_1 + c_{2,m}\lambda_2 + \ldots + c_{m,m}\lambda_m \\
\end{align*}
\] (mod. \(a\))

and by solving this system it can be seen that each function \(\lambda_i\), and consequently each function \(\beta\) of the module \(b\), becomes changed, through multiplication by the integral rational function of the \(m^{th}\) degree in \(z\)

\[
(b, a) = (-1)^m \begin{vmatrix} c_{1,1} - z, & c_{2,1}, & \ldots & c_{m,1} \\
c_{1,2}, & c_{2,2} - z, & \ldots & c_{m,2} \\
\vdots & \vdots & \ddots & \vdots \\
c_{1,m}, & c_{2,m}, & \ldots & c_{m,m} - z \\
\end{vmatrix}
\]

into a function in the module \(a\). It is a clear consequence of the multiplication theorem of determinants that this function \((b, a)\) is independent of the choice of the basis \(\lambda_1, \lambda_2, \ldots, \lambda_m\) and therefore only depends on the two modules \(a\) and \(b\). It will be called the norm of \(a\) relative to \(b\).

If each function in \(b\) is at the same time a member of \(a\), so that \(b\) is divisible by \(a\), then \(m = 0\) and we set \((b, a) = 1\). If however \(b\) is not assumed to be as above and it contains a finite number of functions that are linearly independent of \(a\), then we set \((b, a) = 0\).

1. If \(m\) is the least common multiple and \(d\) the greatest common divisor of \(a\) and \(b\), then each congruence between functions in the module \(b\) relative to the module \(a\) is completely equivalent to the congruence of the same functions relative to the module \(m\); on the other hand each function in \(b\) is a function in \(d\) and conversely each function in \(d\) is congruent to a function in \(b\) relative to the module \(a\). From these comments we immediately have the important theorem:

\[
(b, a) = (b, m) = (d, a).
\]

Which also remains valid if \((b, a) = 0\).

2. If the module \(a\) is divisible by the module \(b\) and this by the third module \(c\), then

\[
(c, a) = (c, b)(b, a),
\]

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

\[
c \equiv (\rho_1, \rho_2, \ldots, \rho_s) \quad \text{(mod.} \ b),
\]

\[
b \equiv (\lambda_1, \lambda_2, \ldots, \lambda_s) \quad \text{(mod.} \ a),
\]

then

\[
(c, a) = \left(\sum_{r} \rho_r \lambda_r \right) \quad \text{(mod.} \ b)
\]

and

\[
(c, b) = \left(\sum_{r} \rho_r \lambda_r \right) \quad \text{(mod.} \ a).
\]
then the functions $\rho_1, \rho_2, \ldots, \rho_r, \lambda_1, \lambda_2, \ldots, \lambda_s$ taken together are linearly independent relative to the module $a$; because if

$$\sum_i c_i \rho_i + \sum_i c'_i \lambda_i \equiv 0 \pmod{a},$$

then it follows that because $a$ is divisible by $b$ and the functions $\lambda_i$ are contained in $b$,

$$\sum_i c_i \rho_i \equiv 0 \pmod{b}, \text{ therefore } c_i = 0,$$

$$\sum_i c'_i \lambda_i \equiv 0 \pmod{a}, \text{ therefore } c'_i = 0.$$

Furthermore, because each function $\gamma$ in $c$ satisfies a congruence of the form:

$$\gamma \equiv \sum c_i \rho_i + \sum c'_i \lambda_i \pmod{a},$$

then the $(r+s)$-fold family $(\rho_1, \rho_2, \ldots, \rho_r, \lambda_1, \lambda_2, \ldots, \lambda_s)$ is a complete residue system for $c$ relative to $a$, or

$$c \equiv (\rho_1, \rho_2, \ldots, \rho_r, \lambda_1, \lambda_2, \ldots, \lambda_s) \pmod{a}.$$

Therefore

$$z \rho_i = e_{1,i} \rho_i + \ldots + e_{r,i} \rho_r + \beta_i$$

$$z \rho_r = e_{1,r} \rho_1 + \ldots + e_{r,r} \rho_r + \beta_r,$$

wherein the $e_{i,j}$ are constants and the $\beta_i$ are functions in $b$, thus:

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

furthermore:

$$\begin{align*}
\beta_1 & \equiv h_{1,1} \lambda_1 + \ldots + h_{s,1} \lambda_s \\
\vdots & \ddots \vdots \\
\beta_r & \equiv h_{1,r} \lambda_1 + \ldots + h_{s,r} \lambda_s \\
z \lambda_1 & \equiv c_{1,1} \lambda_1 + \ldots + c_{s,1} \lambda_s \\
\vdots & \ddots \vdots \\
z \lambda_s & \equiv c_{1,s} \lambda_1 + \ldots + c_{s,s} \lambda_s
\end{align*} \pmod{a}$$

with constant coefficients $h_{i,j}$ and $c_{i,j}$, hence

$$(b, a) = (-1)^s \begin{vmatrix}
c_{1,1} - z, & \ldots & c_{s,1} \\
\vdots & \ddots & \vdots \\
c_{1,s}, & \ldots & e_{s,s} - z
\end{vmatrix},$$
and it follows that

\[
\begin{align*}
z \rho_1 &\equiv e_{1,1} \rho_1 + \ldots + e_{r,1} \rho_r + h_{1,1} \lambda_1 + \ldots + h_{s,1} \lambda_s \\
z \rho_r &\equiv e_{1,r} \rho_1 + \ldots + e_{r,r} \rho_r + h_{1,r} \lambda_1 + \ldots + h_{s,r} \lambda_s \\
z \lambda_1 &\equiv c_{1,1} \lambda_1 + \ldots + c_{s,1} \lambda_s \\
z \lambda_s &\equiv c_{1,s} \lambda_1 + \ldots + c_{s,s} \lambda_s
\end{align*}
\]

(mod. \(a\))

and from this

\[
\left| \begin{array}{cccc}
e_{1,1} - z_1 & \ldots & e_{r,1} - z_1 & h_{1,1} - z_1 \\
\vdots & \ddots & \vdots & \vdots \\
e_{1,r} - z & \ldots & e_{r,r} - z & h_{1,r} - z_1 \\
0 & \ldots & 0 & c_{1,1} - z_1 \\
\vdots & \ddots & \vdots & \vdots \\
0 & \ldots & 0 & c_{1,s} - z_1 \\
\end{array} \right| = (c, a)(b, a)
\]

3. When it is known that the basis-functions \(\beta_1, \beta_2, \ldots, \beta_s\), of a finite module \(b = [\beta_1, \beta_2, \ldots, \beta_s]\) are changed into functions in a module \(a\) through multiplication by non-zero integral rational functions of \(z\), then the norm of \(a\) relative to \(b\), \((b, a)\), is different from zero. At the same time, the least common multiple of \(a\) and \(b\) is a finite module \(m\), which can be supposed to have an irreducible basis of the form:

\[
\mu_1 = a_{1,1} \beta_1, \\
\mu_2 = a_{1,2} \beta_1 + a_{2,2} \beta_2, \\
\vdots \\
\mu_s = a_{1,s} \beta_1 + a_{2,s} \beta_2 + \ldots + a_{s,s} \beta_s,
\]

where the coefficients \(a_{i,j}\) are integral rational functions of \(z\) and in such a way that

\[(b, a) = a_{1,1} a_{2,2} \ldots a_{s,s}.
\]

To prove these important theorems we suppose \(a_1\) to be the greatest common divisor of \(a\) and \([\beta_1]\), \(a_2\) that of \(a_1\) and \([\beta_2]\) and so on, so that \(a_r\) is the set of all functions of the form

\[
\alpha_r = \alpha + y_1 \beta_1 + \ldots + y_r \beta_r
\]

where \(\alpha\) is a function in \(a\) and \(y_1, \ldots, y_r\) are integral rational functions of \(z\). Then \(a_r\) is the greatest common divisor of \(a\) and \(b\). Since now each module \(a_r\) is divisible by the next \(a_{r+1}\) then it also follows from 1. and 2. that

\[(b, a) = (a_s, a) = (a_s, a_{s-1})(a_{s-1}, a_{s-2}) \ldots (a_1, a),
\]

so to the determination of \((a_r, a_{r-1})\). We have

\[
\alpha_r = \alpha_r + y_r \beta_r \equiv y_r \beta_r \pmod{a_{r-1}},
\]
and from the given assumption there is a non-zero integral rational function $x_r$ of $z$ for which

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

therefore also

$$x_r \beta_r \equiv 0 \pmod{a_{r-1}}.$$

If now amongst all of the functions $x_r$ satisfying the latter congruence, $a_{r,r}$ is the one of lowest possible degree $m_r$ that at the same time has the coefficient of the highest power of $z$ equal to 1, then all other functions $x_r$ satisfying this congruence are divisible by $a_{r,r}$; because for any integral rational $q$

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

and if $x_r$ is not divisible by $a_{r,r}$ then such a $q$ can be chosen so that $x_r - qa_{r,r}$ becomes of lower degree than the $a_{r,r}$ given above. Then set

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

and thus determine $q$ so that the degree of $b_{r,r}$ becomes smaller than $m_r$, then it follows that:

$$\alpha_r \equiv b_{r,r} \beta_r \pmod{a_{r-1}}$$

and hence

$$a_r \equiv (\beta_r, z\beta_r, \ldots z^{m_r-1}\beta_r) \pmod{a_{r-1}}.$$

Therefore, if for the moment one sets:

$$a_{r,r} = c_0 + c_1z + \ldots + c_{m_r-1}z^{m_r-1} + z^{m_r},$$

$$\lambda_k = z^{k-1}\beta_r,$$

then it follows that:

$$z\lambda_{m_r} \equiv -c_0\lambda_1 - c_1\lambda_2 - \ldots - c_{m_r-1}\lambda_{m_r} \pmod{a_{r-1}}$$

hence

$$\pmatrix{-z, & 1, & 0, & \ldots & 0 \\ 0, & -z, & 1, & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0, & 0, & 0, & \ldots & 1 \\ -c_0, & -c_1, & -c_2, & \ldots & -c_{m_r-1} - z} = a_{r,r}.$$

This gives us, as in section 2, that the system of functions

$$\beta_1, \ z\beta_1, \ \ldots \ z^{m_1-1}\beta_1,$$

$$\beta_2, \ z\beta_2, \ \ldots \ z^{m_2-1}\beta_2,$$

$$\ldots \ \ldots \ \ldots \ \ldots$$

$$\beta_s, \ z\beta_s, \ \ldots \ z^{m_s-1}\beta_s,$$
forms a basis of a complete residue system of \( b \) relative to \( a \), and that
\[
(b, a) = a_{1,1}a_{2,2} \ldots a_{s,s}
\]
is of degree
\[
m = m_1 + m_2 + \ldots + m_s.
\]
Since \( a_{r,r} \beta_r \equiv 0 \pmod{a_{r-1}} \), then let a function \( \mu_r \) in \( a \) and integral rational functions \( a_{k,r} \) be determined so that
\[
\mu_r = a_{1,r} \beta_1 + a_{2,r} \beta_2 + \ldots + a_{r,r} \beta_r
\]
in this way the specified functions
\[
\begin{align*}
\mu_1 &= a_{1,1} \beta_1, \\
\mu_2 &= a_{1,2} \beta_1 + a_{2,2} \beta_2, \\
\vdots & \quad \vdots \\
\mu_s &= a_{1,s} \beta_1 + a_{2,s} \beta_2 + a_{s,s} \beta_s,
\end{align*}
\]
are rationally independent since none of the functions \( a_{1,1}, \ldots, a_{s,s} \) vanish, and at the same time they are all in both \( a \) and \( b \) and thus are also included in the least common multiple, \( m \), of these two modules. It remains to be proved that these form a basis of \( m \).

Let \( m_r \) be the least common multiple of \( a \) and \( \beta_1, \beta_2, \ldots, \beta_r \), \( m_s = m \), such that among the modules \( m_1, m_2, \ldots, m_s \), each is divisible by all of the following and thus also by \( m \), and
\[
\nu_r = z_1 \beta_1 + z_2 \beta_2 + \ldots + z_r \beta_r,
\]
is a function in \( m_r \) and hence also in \( a \).

Accordingly,
\[
z_r \beta_r \equiv 0 \pmod{a_{r-1}},
\]
so
\[
z_r = x_r a_{r,r},
\]
where \( x_r \) is an integral rational function. Therefore,
\[
\nu_r - x_r \mu_r \equiv 0 \pmod{m_{r-1}}, \quad \nu_1 - x_1 \mu_1 = 0,
\]
from which it follows that:
\[
\nu_r = x_1 \mu_1 + x_2 \mu_2 + \ldots + x_r \mu_r,
\]
so
\[
m_r = [\mu_1, \mu_2, \ldots, \mu_r], \\
m = [\mu_1, \mu_2, \ldots, \mu_s],
\]
Q.E.D.
Hence an irreducible basis of the module \( m \) contains exactly as many functions as an irreducible basis of \( b \). Instead of the basis \( \mu_1, \mu_2, \ldots, \mu_s \), choose another, \( \mu'_1, \mu'_2, \ldots, \mu'_s \), so that the \( \mu'_1, \mu'_2, \ldots, \mu'_s \) are of the form

\[
\mu'_k = a'_{1,k} \beta_1 + a'_{2,k} \beta_2 + \ldots + a'_{s,k} \beta_s
\]

with integral rational coefficients \( a'_{i,k} \), and from §4, 2. we have

\[
(b, a) = \text{const.} \sum \pm a'_{1,1} a'_{2,2} \ldots a'_{s,s}
\]

4. In particular, if we make the assumption that \( a \) was also a finite module whose irreducible basis has as many functions as \( b \), and moreover let \( a \) be divisible by \( b \), then when

\[
a = [\alpha_1, \alpha_2, \ldots, \alpha_s]
\]

let integral rational functions \( b_{i,k} \) of \( z \) be so determined that

\[
\alpha_k = b_{1,k} \beta_1 + b_{2,k} \beta_2 + \ldots + b_{s,k} \beta_s,
\]

and the requirement in 3. that the function \( \beta \) can be changed into a function in the module \( a \) by multiplication by an integral rational function of \( z \) is fulfilled, thus one sees how to solve this system of equations. At the same time, \( a \) is itself the least common multiple of \( a \) and \( b \), and hence

\[
(b, a) = \text{const.} \sum \pm b_{1,1} b_{2,2} \ldots b_{n,n}.
\]

5. If \( m \) is the least common multiple of the two modules \( a \) and \( b \) and \( \nu \) is any function in \( \Omega \), then it follows without difficulty from the definition that \( \nu m \) is the least common multiple of \( \nu a \) and \( \nu b \). If \( (b, a) = 0 \) then \( (\nu b, \nu a) = 0 \) as well. If however \( (b, a) \) and \( \nu \) are non-zero, then

\[
(\nu b, \nu a) = (b, a),
\]

if in 3. one replaces the basis functions \( \mu_i \) and \( \beta_i \) of \( m \) and \( b \) by \( \nu \mu_i \) and \( \nu \beta_i \).

§7.

The ideals in \( \sigma \).

A system \( a \) of integral functions of \( z \) in the field \( \Omega \) is called an ideal if it satisfies both of following conditions:

I. The sum and difference of any two functions in \( a \) again yields a function in \( a \).

II. The product of any function in \( a \) with any function in \( \sigma \) (§3) is again a function in \( a \).

Every ideal is also a module and all the concepts and definitions already established can be applied to an ideal.
The module \( \mathfrak{o} \) (the system of all integral functions of \( z \)) is itself an ideal, and each ideal is divisible by \( \mathfrak{o} \). Likewise, if \( \mu \) is any function different from zero in \( \mathfrak{o} \), then the module \( \mathfrak{o}\mu \) (the system of all integral functions divisible by \( \mu \)) is an ideal. Such an ideal is called a principal ideal. If \( \omega_1, \omega_2, \ldots, \omega_n \) is a basis of \( \mathfrak{o} \), then
\[
\mathfrak{o}\mu = [\omega_1\mu, \omega_2\mu, \ldots, \omega_n\mu]
\]
and \( \mathfrak{o}\mu \) is the least common multiple of \( \mathfrak{o} \) and \( \mathfrak{o}\mu \). Therefore from §6, 4. and the definition (4.) in §2:
\[
(1) \quad (\mathfrak{o}, \mathfrak{o}\mu) = \text{const.} N(\mu)
\]
and consequently is non-zero.

If \( \alpha \) is any ideal and \( \alpha \) is any function in \( \alpha \), then (because of II.) the principal ideal \( \mathfrak{o}\alpha \) is divisible by \( \alpha \), and consequently from §6, 2.:
\[
(2) \quad (\mathfrak{o}, \mathfrak{o}\alpha) = (\mathfrak{o}, \alpha)(\alpha, \mathfrak{o}\alpha)
\]
and thus \( \langle \alpha, \mathfrak{o}\alpha \rangle \) is also non-zero. Since again \( \alpha \) is the least common multiple of \( \alpha \) and \( \mathfrak{o} \), then according to §6, 3. \( \alpha \) has an irreducible basis which consists of \( n \) integral functions \( \alpha_1, \alpha_2, \ldots, \alpha_n \), accordingly they also form a basis for the field \( \Omega \).

The norm of \( \alpha \) relative to \( \mathfrak{o} \), i.e. the integral rational function \( (\mathfrak{o}, \alpha) \) of \( z \) is called the norm of the ideal \( \alpha \) and is written as \( N(\alpha) \). The degree of this integral rational function is called the degree of the ideal \( \alpha \).

If
\[
\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_n], \quad \mathfrak{o} = [\omega_1, \omega_2, \ldots, \omega_n]
\]
and
\[
\begin{align*}
\alpha_1 &= a_{1,1}\omega_1 + a_{2,1}\omega_2 + \ldots + a_{n,1}\omega_n, \\
\alpha_1 &= a_{1,2}\omega_1 + a_{2,2}\omega_2 + \ldots + a_{n,2}\omega_n, \\
&\ldots \\
\alpha_n &= a_{1,n}\omega_1 + a_{2,n}\omega_2 + \ldots + a_{n,n}\omega_n
\end{align*}
\]
with integral rational coefficients \( a_{i,j} \), then §6, 4. gives:
\[
(3) \quad N(\alpha) = \text{const.} \sum a_{1,1}a_{2,2}\ldots a_{n,n}
\]
Since each function in \( \mathfrak{o} \), and hence also the function “1”, becomes changed into a function in the ideal \( \alpha \) through multiplication by \( N(\alpha) \), then \( N(\alpha) \) is always a function in \( \alpha \).

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

If \( \alpha \) is a function in \( \alpha \), then it follows from (1.), (2.) and (3.) that:
\[
(4) \quad N(\alpha) = \text{const.} N(\alpha)(\alpha, \mathfrak{o}\alpha),
\]
i.e. the norm of each function contained in \( \alpha \) is divisible by the norm of \( \alpha \).
The following theorem applies to the congruences relative to an ideal module and fundamentally distinguishes the ideal from the general module.

If \( \mu, \mu_1, \nu, \nu_1 \) are functions in \( \sigma \) which satisfy the congruences

\[
\mu \equiv \mu_1, \quad \nu \equiv \nu_1 \pmod{a},
\]

then we also have

\[
\mu \nu \equiv \mu_1 \nu_1 \pmod{a}.
\]

§8. Multiplication and division of ideals.

The fundamental properties I. and II. of an ideal and the definitions in §4 in particular provide the following:

1. The least common multiple, the greatest common divisor and the product of two (and therefore also of any number) of ideals are themselves ideals. Similarly, if \( \nu \) is a function in \( \sigma \) and \( a \) is an ideal, then the product \( a \nu \) is an ideal.

2. The product of several ideals is divisible by each of its factors, and for any ideal \( a \)

\[
a \sigma = a;
\]

since from I. and II., each function in \( a \sigma \) is also a function in \( a \) and conversely, because \( \sigma \) also contains the function “1” each function in \( a \) is also a function in \( a \sigma \).

3. A principal ideal \( a \mu \) is divisible by a principal ideal \( a \nu \) if and only if the integral function \( \mu \) is divisible by the integral function \( \nu \).

In addition, we now include the following definitions:

4. Definition. A function \( \alpha \) in \( \sigma \) will be called divisible by \( a \), if the principal ideal \( a \sigma \) is divisible by \( a \), or, what amounts to the same thing, if \( \alpha \) is a function in \( a \).

5. Definition. Two ideals \( a \) and \( b \) are called relatively prime when their greatest common divisor is \( \sigma \). The necessary and sufficient condition for this is that functions \( \alpha \) in \( a \) an \( \beta \) in \( b \) exist such that

\[
\alpha + \beta = 1,
\]

or, to put it another way, that a suitable function can be found such that either in \( a \) the congruence \( \alpha \equiv 1 \pmod{b} \) or in \( b \) the congruence \( \beta \equiv 1 \pmod{a} \) is satisfied.

6. Definition. An ideal \( p \) different from \( \sigma \) is called a prime ideal if no other ideal except \( p \) and \( \sigma \) divides \( p \).

On the basis of these definitions, the following theorems on the divisibility of ideals now result.
7. If \( a \) and \( b \) are two ideals with the least common multiple \( m \) and the greatest common divisor \( d \), then as a consequence of §6, 1. and 2.

\[
\begin{align*}
N(m) &= N(b)(b, m) = N(b)(b, a), \\
N(a) &= N(d)(d, a) = N(d)(b, a),
\end{align*}
\]

hence \((b, a)\) is not zero, and

\[
N(a)N(b) = N(m)N(d)
\]

8. If the ideal \( a \) is divisible by the ideal \( b \), then, from §6, 2.,

\[
N(a) = (b, a)N(b),
\]

and thus \( N(a) \) is divisible by \( N(b) \).

In the special case when \((b, a) = 1\), it then also follows that \( b \) is divisible by \( a \), and that:

9. If \( a \) is divisible by \( b \) and at the same time \( N(a) = N(b) \), then \( a = b \), i.e. both ideal are identical.

10. If \( a \) is divisible by \( a_1 \) and \( b \) by \( b_1 \), then \( ab \) is divisible by \( a, b_1 \) (§4, 7.).

11. If an ideal \( a \) is divisible by a principal ideal \( o\mu \), then all the functions in \( a \) are of the form \( \beta\mu \) and the set of functions \( \beta \) is again an ideal, \( b \), so that one can put

\[
a = \mu b.
\]

12. If \( \mu \) is an arbitrary non-zero function in \( o \) and the ideal \( a\mu \) is divisible by the ideal \( b\mu \), then \( a \) is divisible by \( b \), and from \( a\mu = b\mu \) it follows that \( a = b \).

13. The least common multiple of two ideals \( a \) and \( o\nu \), one of which is a principal ideal, has, further to 11., the form \( r\nu \) where \( r \) is an ideal. On the other hand, \( a\nu \) is a common multiple of \( a \) and \( o\nu \) and thus is divisible by \( r\nu \), then from 12. \( r \) is a divisor of \( a \).

14. If \( a \) is an ideal and \( \nu \) is a function in \( o \), then according to §6, 2. and 5.:

\[
(o, a\nu) = (o, o\nu)(o\nu, a\nu) = (o, o\nu)(o, a),
\]

so

\[
N(a\nu) = \text{const}.N(a)N(\nu).
\]

If \( r\nu \) is the least common multiple and \( \delta \) the greatest common divisor of the two ideals \( a \) and \( o\nu \), then it follows from 7. that

\[
N(a) = N(r)N(\delta).
\]

15. Each of the various ideals \( a \) of \( o \) is divisible by a prime ideal \( p \).
Suppose \(a\) is not a prime ideal, then it has at least one proper divisor different from \(o\) and let \(p\) be one such whose norm is of the lowest possible degree. This can not have a proper divisor \(p'\) different from \(o\) for then \(p'\) would also be a divisor of \(a\) and at the same time (from 8.) \(N(p')\) would be of lower degree than \(N(p)\). This is contrary to the assumptions about \(p\) and hence \(p\) is a prime ideal.

16. If \(a\) is relatively prime to \(b\), then \(ab\) is the least common multiple of \(a\) and \(b\) and consequently any ideal divisible both by \(a\) and by \(b\) is also divisible by \(ab\).

Because, by assumption, there are two functions \(\alpha_i\) and \(\beta_i\) in \(a\) and \(b\) such that (from 5.):

\[
\alpha_i + \beta_i = 1.
\]

If on the other hand, \(\alpha = \beta\) is a function in the least common multiple \(m\) of \(a\) and \(b\), then

\[
\alpha = \beta = \alpha_i \beta + \alpha \beta_i,
\]

is also a function in \(ab\). Therefore \(m\) is divisible by \(ab\). Conversely (according to 2.) \(ab\) is divisible by \(m\), so \(m\) is identical with \(ab\) and in this case it follows from 7. that

\[
N(ab) = N(a)N(b)
\]

17. If \(a\) is an arbitrary ideal and \(p\) is a prime ideal, then either \(a\) is divisible by \(p\) or \(a\) is relatively prime to \(p\); for \(p\) has no other divisor than \(o\) and \(p\) so the greatest common divisor of \(a\) and \(p\) can be none other than either \(o\) or \(p\).

18. If \(a\) is relatively prime to \(b\) and to \(c\), then \(a\) is relatively prime to \(bc\).

By assumption (5.), there are functions in \(b\) and \(c\) satisfying the two congruences

\[
\beta \equiv 1, \quad \gamma \equiv 1 \pmod{a}
\]

therefore, pursuant to §7

\[
\beta \gamma \equiv 1 \pmod{a}.
\]

Since \(\beta \gamma\) is in \(bc\), the assertion is thus proved.

It further follows from this that, in the case when the product \(ab\) is divisible by a prime ideal, at least one of the factors \(a\) and \(b\) must be itself divisible by \(p\) and, applying this to a primary ideal, when the product two integral functions, \(\mu \nu\) is in \(p\), at least one of the two factors \(\mu\) or \(\nu\) must itself be in \(p\).

19. If \(a\) is relatively prime to \(c\) and \(ab\) is divisible by \(c\), then \(b\) is divisible by \(c\). By assumption, there is a function \(\alpha\) in \(a\) which satisfies the congruence

\[
\alpha \equiv 1 \pmod{c}.
\]

If now \(\beta\) is an arbitrary function in \(b\), then we have the following

\[
\beta \equiv \alpha \beta \equiv 0 \pmod{c}
\]

hence \(\beta\) is in \(c\) and thus \(b\) is divisible by \(c\).
§9.
Laws of the divisibility of ideals.

Although all these theorems, most of which are immediate consequences of the definition of an ideal, are not sufficient for a complete proof, there is predominantly an analogy between the laws of divisibility of ideals and those for integral rational functions. We illustrate this with the proof of the following theorem:

1. If $\alpha$ is an ideal and $k$ is an arbitrary integral rational function of $z$, then a function $\alpha$ in $\alpha$ can be chosen such that $(\alpha, \alpha \alpha)$ has no common factor with $k$.  

Suppose

$$\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_n],$$

$$\sigma = [\omega_1, \omega_2, \ldots, \omega_n],$$

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

$$\alpha \omega_1 = x_{1,1} \alpha_1 + x_{1,2} \alpha_2 + \ldots + x_{1,n} \alpha_n,$$

$$\alpha \omega_2 = x_{2,1} \alpha_1 + x_{2,2} \alpha_2 + \ldots + x_{2,n} \alpha_n,$$

$$\ldots$$

$$\alpha \omega_n = x_{n,1} \alpha_1 + x_{n,2} \alpha_2 + \ldots + x_{n,n} \alpha_n,$$

then ($\S$6, 4.)

$$(\alpha, \alpha \alpha) = \text{const.} \sum \pm x_{1,1} x_{2,2} \ldots x_{n,n}.$$ 

Now if $\sum \pm x_{1,1} x_{2,2} \ldots x_{n,n}$ is divisible by a linear factor $z - c$ of $k$, i.e. vanishes for $z = c$, then you have a system of constants $c_1, c_2, \ldots, c_n$, not all zero, so determined that the integral rational function

$$c_1 x_{k,1} + c_2 x_{k,2} + \ldots + c_n x_{k,n}$$

vanish for $z = c$, thus is divisible by $z - c$, and then we set

$$\omega = c_1 \omega_1 + c_2 \omega_2 + \ldots + c_n \omega_n.$$
where the coefficients \(a_1, a_2, \ldots, a_n\) are independent of \(t\) and are rational functions of \(z\). It can not be that at the same time \(a_1\) is divisible by \(z - c\) and \(a_2\) is divisible by \((z - c)^2, \ldots, a_n\) by \(z - c)^n\), because otherwise, contrary to the assumption, \(\frac{\omega}{z - c}\) would be an integral function (§2, 5. and §3, 4.). Therefore all the elements of \(N(\omega')\) cannot be divisible by \((z - c)^n\) and thus if \((z - c)^n - r\) is the highest power of \((z - c)\) by which they are divisible, then, if \(r > 0,\)

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

where the integral rational functions \(b_1, b_2, \ldots, b_n\) do not all vanish for \(z = c\). There are therefore only a finite number of constant values \(t\) for which \(f(t)\) is divisible by \((z - c)^n\) and at the same time is divisible by no other linear factor of \(k\). If, when this is done,

\[
t \alpha - \alpha' = \alpha'',
\]

which is also a function in \(a\), it follows that

\[
\alpha \omega' = (z - c) \alpha'',
\]

\[
N(\alpha'') = \frac{N(\alpha) N(\omega')}{(z - c)^n}
\]

and consequently, since, according to §7 (4.)

\[
(a, o \alpha) = \text{const.} \frac{N(\alpha)}{N(a)}
\]

we have:

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

Therefore the function \((a, o \alpha'')\) has at least one less factor \(z - c\) than \((a, o \alpha)\), while at the same time it has no more other linear factors of \(k\) than \((a, o \alpha)\) has. By repeated application of this procedure we derive the proof of the stated theorem.

2. Every ideal \(a\) can be represented as the greatest common divisor of two principal ideals \(o \mu\) and \(o \nu\), one of which except for being divisible by \(a\) is entirely arbitrary.

**Proof.** Choose any non-zero function \(\nu\) in \(a\) and a second function \(\mu\) such that the two functions \((a, o \nu)\) and \((a, o \mu)\) have no common divisor (as in 1). If now \(\alpha\) is an arbitrary function in \(a\), then according to §6 \((a, o \mu)\alpha\) is in \(o \mu\) and \((a, o \nu)\alpha\) is in \(o \nu\), so that there are two functions \(\omega\) and \(\omega'\) in \(o\) for which

\[
(a, o \mu)\alpha = \mu \omega, \quad (a, o \nu)\alpha = \nu \omega'.
\]

1This conclusion no longer applies in the analogous question for number theory.
If, as is possible after the assumption about \((a, \sigma \mu)\) and \((a, \sigma \nu)\), we choose two integral rational functions \(g\) and \(h\) of \(z\) satisfying the condition

\[ g(a, \sigma \mu) + h(a, \sigma \nu) = 1, \]

it follows that

\[ \alpha = g\mu \omega + h\nu \omega', \]

i.e. \(a\) is divisible by the greatest common divisor of \(\sigma \mu\) and \(\sigma \nu\). Since conversely the latter is divisible by \(a\) (because \(\sigma \mu\) and \(\sigma \nu\) are divisible by \(a\)), then it is equal to \(a\). Q.E.D.

3. Every ideal \(a\) can be transformed by multiplication by an ideal \(m\) into a principal ideal \(\sigma \mu = am\).

**Proof.** Choose, (as in 1.), a function \(\mu\) in \(a\) such that \((a, \sigma \mu)\) has no divisor in common with \(N(a)\); then a second function \(\nu\) so that \((a, \sigma \nu)\) has no common divisor with \((a, \sigma \mu)\). Then (from 2.) \(a\) is the greatest common divisor of \(\sigma \mu\) and \(\sigma \nu\). The least common multiple of \(\sigma \mu\) and \(\sigma \nu\) is, (according to §8, 13), of the form \(m\nu\), where \(m\) is a divisor of \(\sigma \mu\). Then in accordance with §8, 14

\[ N(m) = \frac{N(\sigma \mu)}{N(a)} = (a, \sigma \mu) \]

has, by assumption, no common divisor with \(N(a)\). So again we determine two integral rational functions \(g\) and \(h\) of \(z\) so that

\[ gN(m) + hN(a) = 1, \]

then it follows from §8, 5, since \(N(m)\) is in \(m\) and \(N(a)\) is in \(a\), that \(m\) and \(a\) are relatively prime ideals, and hence, according to §8, 16,

\[ N(ma) = N(m)N(a) = N(\sigma \mu). \]

Since \(\sigma \mu\) is divisible by \(m\) and by \(a\) it is also divisible by \(ma\) (§8, 16), so according to §8, 9

\[ ma = \sigma \mu, \]

Q.E.D. \(^1\)

4. If an ideal \(c\) is divisible by an ideal \(a\), then there is one and only one ideal \(b\) which satisfies the condition

\[ ab = c \]

which is called the *quotient of \(c\) by \(a\).*

If \(ab\) is divisible by \(ab'\), then \(b\) is divisible by \(b'\), and from \(ab = ab'\) it would follow that \(b = b'\).

\(^1\)You can choose the ideal \(m\) so that it is at the same time relatively prime to an arbitrary ideal \(b\). This is achieved when the function \(\mu\) is taken so that \((a, \sigma \mu) = N(m)\) has no divisor in common with \(N(a)N(b)\) (§8, 8.).
Proof. Let \( c \) be divisible by \( a \) and (in accordance with 3.) \( am = a\mu \). \( cm \) is then also divisible by \( am = a\mu \) and hence \( cm = b\mu \) (§8, 10. and 11.); thus, by multiplying the last equation by \( a \),

\[
c\mu = ab\mu
\]

and from §8, 12.

\[
c = ab,
\]

which proves the first part of the theorem. 1

Furthermore, if \( ab \) is divisible by \( ab' \), then (§8, 10.) \( \mu b \) is divisible by \( \mu b' \), hence \( b \) by \( b' \). – If \( ab = ab' \), it follows that \( \mu b = \mu b' \) and hence \( b = b' \) (§8, 12.).

5. Every ideal different from \( \sigma \) is either a prime ideal or it can be represented in only one way as a product of prime ideals alone.

Proof. If the ideal \( a \) is different from \( \sigma \), then it is (§8, 15.) divisible by a prime ideal \( p \), and consequently (from 4.) \( a_1 = p, a_1 \) wherein \( a_1 \) is a proper divisor of \( a \) (because (from 4.) \( a_1 = a \) would imply \( p = \sigma \)). Thus the degree of \( N(a_1) \) is lower than that of \( N(a) \). If \( a_1 \) is different from \( \sigma \), then one concludes also that \( a_1 \) must be \( = p_2 a_2 \), whence the degree of \( N(a_2) \) is again lower than that of \( N(a_1) \). The process is continued in this way and then finally you get after a finite number of decompositions to an ideal of the form \( a_{r-1} = p_r a_r \), where \( N(a_r) = 1 \), hence \( a_r = \sigma \). Therefore, we have

\[
a = p_1 p_2 \ldots p_r.
\]

If it were possible to have a second form of product decomposition, say

\[
p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s,
\]

then (§8, 18.) among the prime ideals \( p_1, p_2, \ldots p_r \) there must be at least one, say \( p_1 \), that is divisible by \( q_1 \) and thus be \( = q_1 \), so from 4.

\[
p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s.
\]

From this we also have \( p_s = q_s \) and so on.

Assembling into powers the prime ideals that are equal to each other in the decomposition so obtained, one can write

\[
a = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}.
\]

Any divisor \( a_1 \) of \( a \) can then not be divisible by any prime ideal different from \( p_1, p_2, \ldots p_r \), and not more often than \( a \) is. One thus obtains all divisors of \( a \), the number of which is finite and is \( = (e_1 + 1)(e_2 + 1) \ldots (e_r + 1) \), where in

\[
p_1^{h_1} p_2^{h_2} \ldots p_r^{h_r}
\]

1This definition of the quotient of two ideals is in full agreement with that given in §4, 8.
the exponent $h_i$ runs through the series of numbers 0, 1, 2, ..., $e_i$ ($p^0$ being understood as the ideal $\mathfrak{o}$). If $a$ and $b$ are ideals
\[ a = p_1^{e_1}p_2^{e_2} \cdots p_r^{e_r}; \quad b = p_1^{f_1}p_2^{f_2} \cdots p_r^{f_r}, \]
(where the exponents $e$ and $f$ of some factor may be zero), we thus obtain the greatest common divisor and the lowest common multiple of $a$ and $b$ in the form
\[ p_1^{g_1}p_2^{g_2} \cdots p_r^{g_r}, \]
where for the former one takes $g_1, g_2, \ldots, g_r$ to be the smaller and for the latter the larger of the numbers $e_1, f_1; e_2, f_2; \ldots, e_r, f_r$.

6. If $a$ and $b$ are any two ideals, then in general
\[ N(ab) = N(a)N(b). \]

**Proof.** If, as in 5., we have $a = p_1a_1$, then because $a_1$ is a proper divisor of $a$, there is a function $\eta$ in $a_1$ which is not divisible by $a$. The least common multiple and the greatest common divisor of $a$ and $\mathfrak{o}\eta$ are respectively $p_1\eta$ and $a_1$, which follows immediately (see 5.) from the decomposition of $a$ and $\mathfrak{o}\eta$ into their prime factors. It follows from this according to §8, 14. that
\[ N(a) = N(p_1)N(a_1). \]
By repeating the same conclusion for $a_1$ and so on, it will be seen that when $a = p_1p_2 \ldots p_r$ then:
\[ N(a) = N(p_1)N(p_2) \ldots N(p_r) \]
and thus
\[ N(ab) = N(a)N(b). \]

7. Every prime ideal is an ideal of the first degree (§7) and vice versa, every ideal of the first-degree is a prime ideal.

**Proof.** If $p$ is a prime ideal, then $N(p)$ is divisible by $p$ and therefore at least one linear factor of $N(p)$, say $z - c$, is divisible by $p$ (§8, 18.). If $\omega$ is any function in $\mathfrak{o}$ which satisfies the equation:
\[ \omega^n + a_1\omega^{n-1} + \ldots + a_{n-1}\omega + a_n = 0, \]
then, by reducing the constant terms $a_1^{(0)}, a_2^{(0)}, \ldots, a_n^{(0)}$ in the integral rational functions $a_1, a_2, \ldots, a_n$ by $(z - c)$ and by decomposing the integral function
\[ \omega^n + a_1^{(0)}\omega^{n-1} + \ldots + a_{n-1}^{(0)}\omega + a_n^{(0)}, \]

\[ 1 \text{Through this theorem the theory of algebraic functions differs significantly from the analogous theory of algebraic numbers.} \]
into its linear factors \((\omega - b_1)(\omega - b_2) \ldots (\omega - b_n)\) one obtains:

\[(\omega - b_1)(\omega - b_2) \ldots (\omega - b_n) = (z-c)\omega' \equiv 0 \pmod{p}.

So at least one of the factors \(\omega - b_1, \omega - b_2, \ldots\) must be divisible by \(p\), that is we have

\[\omega \equiv b \pmod{p},\]

where \(b\) is a constant. Since every function in \(\mathfrak{O}\) is congruent to a constant \(\pmod{p}\), then according to §6 \((\mathfrak{O},p) = N(p) = z-c\) is a linear function of \(z\), so the first part of the assertion is proved.

Conversely: if \(q\) is an ideal of the first degree and

\[N(q) = z-c,\]

then \(q\) is certainly divisible by a prime ideal \(p\), and since \(N(q)\) is divisible by \(N(p)\) we have \(N(p) = N(q) = z-c\), so (§8, 9.)

\[p = q.\]

This gives the result that the degree of an ideal is equal to the number of the prime factors into which it can be split. If therefore

\[\mathfrak{O}(z-c) = p_1^{e_1}p_2^{e_2}p_3^{e_3} \ldots\]

then

\[e_1 + e_2 + e_3 + \ldots = n.\]

A further result is that an integral rational function of \(z\) is divisible by a prime ideal \(p\) if and only if it is divisible by the norm of \(p\).

§10.

The complementary bases of a field \(\Omega\).

1. **Definition.** If the functions \(\alpha_1, \alpha_2, \ldots, \alpha_n\) form a basis for \(\Omega\) and we use the abbreviations

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

\[\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sum \pm a_{1,1}a_{2,2} \ldots a_{n,n} = a \quad (§2),\]

then since \(a\) is different from zero, a specific system of functions \(\alpha'_1, \alpha'_2, \ldots, \alpha'_n\) can be determined from the linear equations

\[(1.) \quad \alpha_r = \sum_{i=1}^{n} a_{r,i} \alpha'_i,\]

and since

\[\Delta(\alpha'_1, \alpha'_2, \ldots, \alpha'_n) = \frac{1}{a}\]
is different from zero, the functions $\alpha'_1, \alpha'_2, \ldots, \alpha'_n$ also form a basis for $\Omega$. This is called the **complementary basis** to $\alpha_1, \alpha_2, \ldots, \alpha_n$.

2. If the indices $r$ and $s$ belong to the number series $1, 2, \ldots, n$, then we designate by $(r, s)$ the number 1 or 0 according to whether $r$ and $s$ are equal or different, so we have

\[ S(\alpha_r, \alpha'_s) = (r, s), \]

then it follows from the solution of the equations (1.) that

\[ \alpha'_s = \sum_i a'_r, \alpha_i; \]
\[ a'_{r,s} = a'_{s,r}; \quad \sum_i a_{r,i} a'_{s,i} = (r, s), \]

and hence:

\[ \alpha_r, \alpha'_s = \sum_i a'_{i,s} \alpha_i; \quad S(\alpha_r, \alpha'_s) = \sum_i a'_{i,r} \alpha_i = (r, s) \]

Conversely, if a system of functions $\beta$, satisfies the conditions $S(\alpha_r, \beta_s) = (r, s)$, then $\beta_s = \alpha'_s$; since if we write $\beta_s = \sum_i b_{r,s} \alpha'_i$ it follows from (2.) that

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

From this it follows immediately that the relationship of the $\alpha_i$ to the $\alpha'_i$ is a mutual one, that is, the basis $\alpha_1, \alpha_2, \ldots, \alpha_n$ is complimentary to $\alpha'_1, \alpha'_2, \ldots$, $\alpha'_n$.

3. If $\eta$ is an arbitrary function in $\Omega$, then we can always put

\[ \eta = \sum_i x_i \alpha_i = \sum_i x'_i \alpha'_i, \]

and by applying (2.) we have:

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

so:

\[ \eta = \sum_i \alpha_i S(\eta \alpha'_i) = \sum_i \alpha'_i S(\eta \alpha_i). \]

4. If $\eta$ is an arbitrary non-zero function in $\Omega$, then

\[ \frac{\alpha'_1}{\eta}, \frac{\alpha'_2}{\eta}, \ldots, \frac{\alpha'_n}{\eta} \]

is a complementary basis to $\eta \alpha_1, \eta \alpha_2, \ldots, \eta \alpha_n$. This follows from 2. since

\[ S(\eta \alpha_r, \frac{\alpha'_s}{\eta}) = S(\alpha_r, \alpha'_s) = (r, s). \]

5. When two bases $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $\beta_1, \beta_2, \ldots, \beta_n$ of $\Omega$ are related by the $n$ equations

\[ \beta_s = \sum_i x_{i,s} \alpha_i, \]
with rational coefficients \( x_{i,s} \), then their complementary bases are related by the \( n \) equations

\[
\alpha'_r = \sum_i x_{r,i} \beta'_i
\]

(transpose substitution). This is an immediate consequence of 3. since

\[
x_{r,s} = S(\alpha'_r \beta'_s)
\]

6. If we have

\[
\sum_i \alpha_i \alpha'_i = 1,
\]

then:

\[
\sum_{i,i'} a_{i,i'} \alpha'_i \alpha'_i = \sum_{i,i'} a_{i,i'} \alpha_i \alpha_i = 1
\]

That is if we initially set

\[
\sum \alpha_i \alpha_i = \sigma,
\]

it follows from 3., (applied to the functions \( \eta \alpha_r \)), that

\[
\eta \alpha_r = \sum_i \alpha_i S(\eta \alpha_i \alpha'_i),
\]

Consequently, from the definition of the trace in §2, (5.)

\[
S(\eta) = \sum_i S(\eta \alpha_i \alpha'_i) = S(\sum \eta \alpha_i \alpha'_i),
\]

so:

\[
S(\eta \sigma) = S(\eta),
\]

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

\[
\sigma = \sum_i \alpha_i S(\sigma \alpha'_i) = \sum_i \alpha_i S(\alpha'_i) = 1.
\]

We go a little more closely into the construction of complementary bases in two special cases:

7. Let \( \omega_1, \omega_2, \ldots \omega_n \) be a basis of \( \sigma \) and \( \epsilon_1, \epsilon_2, \ldots \epsilon_n \) the complementary basis (of \( \Omega \)). Let

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

which are integral rational functions, and

\[
D = \text{const.} \sum \pm \epsilon_{1,1} \epsilon_{2,2} \ldots \epsilon_{n,n},
\]

the discriminant of \( \Omega \); it then follows from 2.

\[
\epsilon_r = \frac{1}{D} \sum_i \frac{\partial D}{\partial e_{i,r}} \omega_i,
\]
which shows that the functions $D_{\epsilon r}$ belong to the rational functions. But from 6. it also follows that

$$D = \sum_{i,i'} \frac{\partial D}{\partial e_{i,i'}} \omega_i \omega_{i'}',$$

and from this

$$\epsilon_r \epsilon_s = \frac{1}{D^2} \sum_{i,i'} \frac{\partial D}{\partial e_{r,i}} \frac{\partial D}{\partial e_{s,i'}} \omega_i \omega_{i'},$$

and hence according to a known theorem of determinants:

$$\epsilon_r \epsilon_s = \frac{1}{D} \frac{\partial D}{\partial e_{r,s}} + \frac{1}{D^2} \sum_{i,i'} \left( \frac{\partial D}{\partial e_{r,i}} \frac{\partial D}{\partial e_{s,i'}} - \frac{\partial D}{\partial e_{r,i'}} \frac{\partial D}{\partial e_{s,i}} \right) \omega_i \omega_{i'}',$$

from which the important result follows that the functions $D_{\epsilon r} \epsilon_s$ belong to the integral functions.

8. Let $\theta$ be a function in $\Omega$ such that $1, \theta, \theta^2, \ldots \theta^{n-1}$ form a basis for $\Omega$ and therefore

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

with rational coefficients $a$ is irreducible. The complimentary basis to $1, \theta, \theta^2, \ldots \theta^{n-1}$ is to be sought. If, when $t$ represents an undetermined constant, we put

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

then:

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

and the functions $\eta_0, \eta_1, \ldots \eta_{n-1}$ also form a basis for $\Omega$ as the determinant of the equations (5.) is $(-1)^{\frac{n(n-1)}{2}}$ and thus different from zero. Therefore each function $\zeta$ in $\Omega$ can represented in the form

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

The sequence of rational functions $y_0, y_1, \ldots y_{n-1}$ is now continued by the functions $y_n, y_{n+1}, \ldots$ obtained by the recursion

$$(6.) \quad a_n y_r + a_{n-1} y_{r+1} + \ldots + a_2 y_{r+n-2} + a_1 y_{r+n-1} + y_{r+n} = 0$$
Now, by (5.)

\[
\begin{align*}
\theta \eta_0 &= -a_n \eta_{n-1}, \\
\theta \eta_1 &= \eta_0 - a_n \eta_{n-1}, \\
\theta \eta_2 &= \eta_1 - a_n \eta_{n-1}, \\
&\quad \vdots \\
\theta \eta_{n-1} &= \eta_{n-2} - a_1 \eta_{n-1},
\end{align*}
\]

so

\[
\zeta \theta = y_1 \eta_0 + y_2 \eta_1 + \ldots + y_{n-1} \eta_{n-2} + y_n \eta_{n-1},
\]

and similarly in general for any positive integer \( r \):

\[
\zeta \theta^r = y_r \eta_0 + y_{r+1} \eta_1 + \ldots + y_{r+n-2} \eta_{n-2} + y_{r+n-1} \eta_{n-1},
\]

or, when the \( \eta_0, \eta_1, \ldots, \eta_{n-1} \) are expressed in terms of \( 1, \theta, \theta^2, \ldots, \theta^{n-1} \):

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

in which

\[
\begin{align*}
x_0^{(r)} &= y_r a_{n-1} + y_{r+1} a_{n-2} + \ldots + y_{r+n-2} a_1 + y_{r+n-1}, \\
x_1^{(r)} &= y_r a_{n-2} + y_{r+1} a_{n-3} + \ldots + y_{r+n-2}, \\
&\quad \vdots \\
x_{n-2}^{(r)} &= y_r a_1 + y_{r+1}, \\
x_{n-1}^{(r)} &= y_r.
\end{align*}
\]

Therefore we have (according to the definition of \( S, \) §2 (5.))

\[
S(\zeta) = \sum_{r=0}^{n-1} x_r^{(r)} = y_r a_{n-1} + 2y_r a_{n-2} + \ldots + (n-1)y_{n-2} a_1 + ny_{n-1},
\]

thus, on setting \( \zeta = \eta_r \):

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

where we have set \( a_0 = 1 \).

If, therefore, we use the abbreviation

\[
S(\theta^r) = s_r,
\]

it follows, as long as \( r \leq n \), using (5.)

\[
(n-r)a_r = a_r s_0 + a_{r-1}s_1 + \ldots + a_1 s_{r-1} + s_r
\]

and from (4) in general

\[
0 = a_n s_r + a_{n-1}s_{r+1} + \ldots + a_1 s_{r+n-1} + s_{r+n}.
\]
But it also follows from these formulae that:

\[
\begin{align*}
    f'(\theta) &= n\theta^{n-1} + (n-1)a_1\theta^{n-2} + \cdots + 2a_{n-2}\theta + a_{n-1} \\
    \theta^r f'(\theta) &= s_r\eta_0 + s_{r+1}\eta_1 + \cdots + s_{r+n-2}\eta_{n-2} + s_{r+n-1}\eta_{n-1}.
\end{align*}
\]

Now bearing in mind the value of the determinant of the system of equations (5.) and the definition the norm and the discriminant in §2 (4.) and (12.), we have this important formula

\[
N f'(\theta) = (-1)^{\frac{1}{2}n(n-1)} \Delta(1, \theta, \theta^2, \ldots \theta^{n-1}).
\]

The equations (10.) are obtained by considering the definition 1. of the complementary basis of \(1, \theta, \theta^2, \ldots \theta^{n-1}\), that is:

\[
\frac{\eta_0}{f'(\theta)} \frac{\eta_1}{f'(\theta)} \cdots \frac{\eta_{n-1}}{f'(\theta)}.
\]

9. Let \(a = [\alpha_1, \alpha_2, \ldots \alpha_n]\) represent a module whose basis is at the same time a basis of \(\Omega\), then we obtain from the basis \(\alpha'_1, \alpha'_2, \ldots \alpha'_n\) of \(\Omega\) complementary to \(\alpha_1, \alpha_2, \ldots \alpha_n\), another module, \(a' = [\alpha'_1, \alpha'_2, \ldots \alpha'_n]\) which is called the complementary module to \(a\). Similarly, as is immediately clear from 5. in conjunction with §4, 2., this is independent of the choice of the basis of \(a\).

10. We consider the special case of \(e = [\epsilon_1, \epsilon_2, \ldots \epsilon_n]\), the complimentary module to \(\sigma = [\omega_1, \omega_2, \ldots \omega_n]\). If we set

\[
\omega_i \epsilon_s = \sum_i e^{(i)}_{r,i} \omega_i,
\]

then from 3.

\[
e^{(i)}_{r,s} = e^{(i)}_{s,r} = S(\omega_i, \omega_j, \epsilon_i)
\]

is a rational function of \(z\), and it follows that:

\[
\omega_i \epsilon_s = \sum_i e^{(i)}_{r,s} \epsilon_i.
\]

From this it follows that the module \(\sigma e\) (§4, 7.) is divisible by \(e\); On the other hand, since \(\sigma\) contains the function 1, \(e\) is divisible by \(\sigma e\), so

\[
\sigma e = e,
\]

that is, the module \(e\), although it does not contain only integral functions, has the characteristic property II. §7 of ideals. The same is also true in its turn of the
module \( e^2 \). Since, from 7., the two modules \( D e \) and \( D e^2 \) contain only integral functions, then they are the same ideal, and from 7. we now have

\[
N(D e) = D^{n-1}.
\]

11. Let \( \theta \) be a function in \( \mathfrak{o} \) such that \( 1, \theta, \theta^2, \ldots, \theta^{n-1} \) are a basis for \( \Omega \), thus in the irreducible equation

\[
f(\theta) = \theta^n + a_1\theta^{n-1} + \ldots + a_{n-1}\theta + a_n = 0
\]

the coefficients are integral rational functions of \( z \), then we can determine for \( r = 0, 1, 2, \ldots, n-1 \) the integral rational functions \( k_r^{(i)} \) where

\[
\theta^r = \sum_{i=1}^{n} k_r^{(i)} \omega_i.
\]

Applying theorems 5. and 8. to this, we have:

\[
f'(\theta)e_s = k_s^{(0)} \eta_0 + k_s^{(1)} \eta_1 + \ldots + k_s^{(n-1)} \eta_{n-1},
\]

and from this it follows that the module

\[
f'(\theta)e = f
\]

contains only integral functions. From 10. we conclude that this is an ideal.

§11. The ramification ideal.

1. Lemma. Suppose any two of the ideals \( a, b, c, \ldots \) are relatively prime, then there always exists a function which is congruent to a given function in \( \mathfrak{o} \) relative to each of them.

Proof. We set

\[
m = abc \ldots = aa_1 = bb_1 = cc_1 = \ldots;
\]

the greatest common divisor of \( a_1 = bc \ldots, b_1 = ac \ldots, c_1 = ab \ldots \) is then equal to \( \mathfrak{o} \), at same time there can be no prime ideal amongst the \( a_1, b_1, c_1, \ldots \). Consequently, one can (§4, 5.) choose \( \alpha_1 \) from \( a_1, \beta_1 \) from \( b_1, \gamma_1 \) from \( c_1, \ldots \), such that

\[
\alpha_1 + \beta_1 + \gamma_1 + \ldots = 1
\]

then:

\[
\begin{align*}
\alpha_1 & \equiv 1, \quad \beta_1 \equiv 0, \quad \gamma_1 \equiv 0, \ldots \pmod{a}, \\
\alpha_1 & \equiv 0, \quad \beta_1 \equiv 1, \quad \gamma_1 \equiv 0, \ldots \pmod{b}, \\
\alpha_1 & \equiv 0, \quad \beta_1 \equiv 0, \quad \gamma_1 \equiv 1, \ldots \pmod{c}, \\
& \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots
\end{align*}
\]
Therefore, there are given functions $\lambda, \mu, \nu, \ldots$ in $\mathfrak{o}$, such that

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

satisfies the conditions

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

2. Let $p, p_1, p_2, \ldots$ be the prime ideals, all different from one another, that divide an arbitrary linear function $z - c$ and

$$\phi(z - c) = p^i p_1^i p_2^i \ldots, \quad e + e_1 + e_2 + \ldots = n \quad (§9, 7).$$

Choose functions $\lambda, \lambda_1, \lambda_2 \ldots$ divisible respectively by $p, p_1, p_2, \ldots$ but not by $p^2, p_1^2, p_2^2, \ldots$, and let $b, b_1, b_2, \ldots$ represent arbitrary constants distinct from one another. Let a function $\zeta$ thus be determined in accordance with 1. which satisfies the congruences

$$\zeta \equiv b + \lambda \pmod{p^2}, \quad \zeta \equiv b_1 + \lambda_1 \pmod{p_1^2}, \quad \zeta \equiv b_2 + \lambda_2 \pmod{p_2^2}, \ldots,$$

then

$$\zeta \equiv b \pmod{p}, \quad \zeta \equiv b_1 \pmod{p_1}, \quad \zeta \equiv b_2 \pmod{p_2}, \ldots,$$

so that, if $a$ stands for some constant, then $\zeta - a$ is divisible by at most one of the prime ideals $p, p_1, p_2, \ldots$ and is not divisible by one of their squares. If $\phi(t) = \prod(t - a)$ is an integral function of the variable $t$ with constant coefficients, then $\phi(\zeta) = \prod(\zeta - a)$ is divisible by $p^m$ if and only if $\phi(t)$ is algebraically divisible by $(t - b)^m$, and if $p^m$ is the highest power of $p$ arising in $\phi(\zeta)$, then $p^{m-1}$ is the highest power of $p$ arising in $\phi'(\zeta)$. Therefore $\phi(\zeta)$ will be divisible by $z - c$ and hence $\phi(t)$ must be divisible by the $n^{th}$ degree function

$$\psi(t) = (t - b)^c(t - b_1)^{c_1}(t - b_2)^{c_2} \ldots$$

Consequently, the congruence

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

is only satisfied by such integral rational $x$ that are divisible by $z - c$. Thus, in terms of integral rational functions $k_1^{(0)}, k_1^{(1)} \ldots$ of $z$ and a basis $\omega_1, \omega_2, \ldots \omega_n$ of $\mathfrak{o}$, we can write:

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

so the determinant

$$k = \sum \pm k_1^{(0)} k_2^{(1)} \ldots k_n^{(n-1)}$$
It therefore follows that

\[ N(t - \zeta) = f(t, z) \]

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

\[ f(t, c) = \psi(t) \]

from which, for a later application, we conclude:

\[ S(\zeta) \equiv eb + e_1 b_1 + e_2 b_2 + \ldots \quad (\text{mod. } z - c), \]

and by applying the same reasoning to the functions \( \zeta^2, \zeta^3, \ldots \), if none of the constants \( b \) vanish, we can of course write:

\[ S(\zeta^2) = eb^2 + e_1 b_1^2 + e_2 b_2^2 + \ldots \quad (\text{mod. } z - c), \]
\[ S(\zeta^3) = eb^3 + e_1 b_1^3 + e_2 b_2^3 + \ldots \quad (\text{mod. } z - c), \]
\[ \ldots \]

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

\[ f'(\zeta, c) \equiv f'(\zeta, z) \quad (\text{mod. } p^e), \]

then \( p^{e-1} \) is the highest power of \( p \) in \( f'(\zeta, z) \). From this we get

\[ \sigma f'(\zeta, z) = mp^{e-1}p_1^{e_1-1} \ldots, \]

where \( m \) and consequently also \( N(p) \) are relatively prime to \( z - c \).

If now \( D \) is the discriminant of \( \Omega \) then, in accordance with §10, (11.) and §2, (13.), we have (apart from constant factors)

\[ Nf'(\zeta, z) = \Delta(1, \zeta, \zeta^2, \ldots \zeta^{n-1}) = Dk^2 = (z - c)^{n-s}N(m), \]

where \( s \) is the number of different prime ideals \( p, p_1, p_2, \ldots \) dividing \( z - c \), then, since \( k \) and \( N(m) \) are not divisible by \( z - c \), \( (z - c)^{n-s} \) is the highest power of \( z - c \) occurring in \( D \). Consequently:

\[ (1.) \quad D = \prod (z - c)^{n-s}, \]

where the product symbol \( \prod \) refers to all those linear expressions \( z - c \) with fewer than \( n \) distinct prime factors, so that they are divisible by the second or a higher power of a prime ideal.

There are thus only a finite number of linear functions \( z - c \) which are divisible by the square of a prime ideal.

We now set

\[ (2.) \quad \Delta = \prod p^{e-1}, \]
where the product symbol $\prod$ refers to all those prime ideals $p$ which divide their norm to a higher power than the first namely, the $e^b$, and this ideal $\mathfrak{z}$ is called the ramification ideal. It follows immediately from (1.) and (2.) that

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

Further, since $n - s \geq e - 1$, we have $e(n - s) - 2(e - 1) \geq 0$, then $D$ is divisible by $p^{2(e - 1)}$, thus also by $\mathfrak{z}^2$, and with $\mathfrak{d}$ also denoting an ideal, we can set:

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

3. If a function $\rho$ in $\mathfrak{o}$ is divisible by each prime ideal dividing $z - c$, then $S(\rho)$ is divisible by $z - c$.

Proof. Let $\zeta$ be the same function as in section 2., so that we can write:

$$ xp = x_0 + x_1\zeta + x_2\zeta^2 + \ldots + x_{n-1}\zeta^{n-1}, $$

where the coefficients $x, x_0, x_1, \ldots x_{n-1}$, are all rational functions of $z$ without a common divisor and the first of which is not divisible by $z - c$ (cf 2.). It follows from our assumption about the function $\rho$ that if the constants $b$ have the same meaning as in 2., we have

$$ x_0 + x_1b + x_2b^2 + \ldots + x_{n-1}b^{n-1} \equiv 0 \pmod{z - c}, $$

$$ x_0 + x_1b_1 + x_2b_1^2 + \ldots + x_{n-1}b_1^{n-1} \equiv 0 \pmod{z - c}, $$

$$ x_0 + x_1b_2 + x_2b_2^2 + \ldots + x_{n-1}b_2^{n-1} \equiv 0 \pmod{z - c}, $$

$$ \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots $$

and hence, by multiplying the congruences by $e, e_1, e_2, \ldots$ and adding:

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

So, as $x$ is not divisible by $z - c$, we have

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

Q.E.D.

4. Now let

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

be the product of each distinct linear factor of $D$ and

$$ r = pp_1p_2 \ldots $$

be the product of each distinct prime ideal dividing $r$. If as above $\mathfrak{z}$ is the ramification ideal, then we have

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

\[ N(\tau) = \frac{\tau^n}{D}. \]

Each function \( \rho \) in \( \tau \) has, according to 3., the property that \( S(\rho) \) is divisible by \( r \).

If now, as in §10

\[ \epsilon = [\epsilon_1, \epsilon_2, \ldots, \epsilon_n] \]

is the complementary module to \( \sigma \) and \( \rho \) is an arbitrary function in \( \tau \), we can write

\[ \rho = x_1\epsilon_1 + x_2\epsilon_2 + \ldots + x_n\epsilon_n \]

where, according to §10, 3.

\[ x_i = S(\rho\omega_i) \]

then, since \( \rho\omega_i \) is a function in \( \tau \), \( x_i \) is an integral rational function of \( z \) that is divisible by \( r \). From this it follows that the ideal \( \tau \) is divisible by the module \( r\epsilon \).

Thus also the ideal \( D\tau \) is divisible by the ideal \( rD\epsilon \). At the same time we have

\[ N(D\tau) = r^nD^{n-1}, \quad N(rD\epsilon) = r^nD^{n-1} \quad (\text{§10, 10}); \]

therefore, pursuant to §8, 9.

\[ D\tau = rD\epsilon \]

or

\[ (6.) \quad \tau = r\epsilon. \]

It follows from the above remark about \( \rho \) that, if \( \epsilon \) represents any function in \( \epsilon \), then \( S(\epsilon) \) is a rational function of \( z \). From the formula (6.), it follows by multiplying by \( \zeta \) that, in accordance with (5.)

\[ \tau\zeta = r\epsilon\zeta = \sigma r \]

and hence

\[ (7.) \quad \epsilon\zeta = \sigma. \]

Multiplying the last equation by \( D \), results from (4.) in

\[ \epsilon D\zeta = \zeta^2\sigma; \]

therefore

\[ (8.) \quad D\epsilon = \zeta\sigma \]

and by multiplying this equation by \( \epsilon \) results from (7.) in

\[ (9.) \quad D\epsilon^2 = \sigma. \]

4.(sic) If \( \theta \) is an integral function of \( z \) in \( \Omega \) and \( N(t - \theta) = f(t) \), then \( f'(\theta) \) is divisible by the ramification ideal \( \zeta \).
Proof. If \(f(t)\) is reducible, then \(f'(θ) = 0\) and thus certainly divisible by \(ζ\).
Otherwise, according to §10, 11.

\[ cf'(θ) = \frac{f}{ζ} \]

is an ideal, hence by multiplication by \(ζ\) according to (7.)

(10.) \(ζf'(θ) = fζ.\)

At the same time, it follows that if in §10, 11. we put

\[
θ^r = \sum k_i^{(r)} \omega_i,
\]

\[
k = \sum \pm k_1^{(0)} k_2^{(1)} \ldots k_n^{(n-1)},
\]

then

\[
NF'(θ) = NF(ζ) = DN(f) = const. k^2 D \quad (§10, (11.) and §2, (13.)),
\]

thus:

(11.) \(N(f) = const. k^2\)
a complete square.

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

1. Any function \(η\) in \(Ω\) can be represented, in accordance with §3, 3., in infinitely many ways as a quotient of two integral functions of \(z\), (the denominator may even be an integral rational function of \(z\)). Thus we can write

\[ η = \frac{ν}{µ} \]

with \(µ\) and \(ν\) integral functions of \(z\) (functions in \(ο\)). If now \(m\) is the greatest common divisor of two principal ideals \(οµ\) and \(ον\), then, if \(a\) and \(b\) are relatively prime ideals and

(1.) \(οµ = am, \quad ον = bm,\)

it follows that (§4, 6.)

(2.) \(aν = bµ \quad \text{or} \quad aη = b.\)

So if \(α\) is an arbitrary function in \(a\), then \(αη\) is included in \(b\), thus in any case is an integral function of \(z\). If conversely \(α\) is an integral function of \(z\) which has the property that \(αη = β\) is an integral function, it follows that

\[ αν = βµ, \]
So according to (1.)
\[ \alpha b = \beta b; \]
then since \( a \) and \( b \) are relatively prime, \( \alpha \) must be divisible by \( a \) and by \( \beta \), from which it follows that:

\( a \) is the set of all those integral functions \( \alpha \) which have the property that \( \alpha \eta \)

is an integral function, and the set all of such functions \( \alpha \eta \) is the ideal \( b \), in other words:

\( b \) is the least common multiple of \( \sigma \eta \) and \( \omega \), just as \( a \) is the least common

multiple of \( \frac{\sigma}{\eta} \) and \( \omega \). Accordingly, if \( a' \) and \( b' \) are two ideals satisfying the condition

\[ a' \eta = b' \]
then \( a' \) is divisible by \( a \). If then
\[ a' = na, \]
it follows that:
\[ b' = nab = nb. \]
Conversely, it is also the case for an arbitrary ideal \( n \) that
\[ nab = nb. \]

2. If now \( a \) and \( b \) are two ideals satisfying the condition
\[ a \eta = b, \]
regardless of whether or not they are relatively prime, the quotient \( \frac{b}{a} \) is, according
to §4, 8., the set of all of those functions \( \gamma \) which have property that \( a \gamma \) is divisible
by \( b \). Included in these functions are certainly all of the functions of the form \( \omega \eta \),
where \( \omega \) represents an arbitrary function in \( \sigma \). But conversely, if \( \gamma \) is any function
of this form, then because \( a \gamma \) is divisible by \( b \), it is also divisible by \( \sigma \), hence it is
an ideal (since it has the properties I. and II. from §7), so if \( c \) is also an ideal:
\[ a \gamma = cb \]
and by multiplication with \( \eta \)
\[ b \gamma = cb \eta. \]
If now as above \( \eta = \frac{\nu}{\mu} \), and \( \gamma = \frac{\rho}{\sigma} \) where \( \rho \) and \( \sigma \) are integral functions, it then
follows that
\[ b \rho \mu = cb \nu \sigma \]
so:
\[ c \rho \mu = c \nu \sigma, \quad c \gamma = c \eta. \]
Both together yield the theorem

\[
(3.) \quad \sigma \eta = \frac{b}{a}.
\]

If in this representation \(b\) and \(a\) are relatively prime, which from 1. can always be assumed, then \(b\) will be called the over-ideal and \(a\) the under-ideal of the function \(\eta\).

3. Again, if in general

\[
a \eta = b, \quad \text{so} \quad \sigma \eta = \frac{b}{a},
\]

and \(\alpha\) is any function in \(a\), \(\beta\) is an associated function in \(b\), then

\[
\eta = \frac{\beta}{\alpha} \quad \text{and} \quad a\beta = b\alpha.
\]

It follows by constructing the norms

\[
N(\eta) = \text{const} \frac{N(a)}{N(b)}.
\]

4. If \(\eta\) and \(\eta'\) are two functions in \(\Omega\) and as described in 1.

\[
a \eta = b; \quad a' \eta' = b',
\]

no matter whether \(a\) and \(b\); \(a'\) and \(b'\) are relatively prime or not, it follows that

\[
aa'\eta\eta' = bb'.
\]

Then from

\[
\sigma \eta = \frac{b}{a}, \quad \sigma \eta' = \frac{b'}{a'},
\]

we have the equations

\[
\sigma \eta\eta' = \frac{bb'}{aa'}, \quad \frac{1}{\eta} = \frac{a}{b}, \quad \sigma \eta' = \frac{ba'}{ab'}
\]

5. If \(a \eta = b\) and \(a \eta' = b'\), then also

\[
a(\eta \pm \eta') = b''
\]

will be an ideal because, if \(\alpha \eta\) and \(\alpha \eta'\) are integral functions then \(\alpha(\eta \pm \eta')\) is always one as well. Then we have

\[
\sigma \eta = \frac{b}{a}, \quad \sigma \eta' = \frac{b'}{a},
\]

and it follows that

\[
\sigma (\eta \pm \eta') = \frac{b''}{a}.
\]
If both the ideals \( b \) and \( b' \) have a common divisor then this is also a divisor of \( b'' \).

6. If now \( \rho \) is a function in \( \Omega \) whose over-ideal is divisible by any given prime ideal \( p \) but not by \( p^2 \), (such functions always exist, they can even be integral functions of \( z \)) then

\[
\sigma \rho = \frac{mp}{n},
\]

where \( m \) and \( n \) are ideals that are not divisible by \( p \). Further, let \( \eta \) be any function in \( \Omega \) whose under-ideal is not divisible by \( p \), then

\[
\sigma \eta = \frac{b}{a}
\]

and \( a \) is not divisible by \( p \). Choose any function \( \alpha \) in \( a \) that is not divisible by \( p \) and a corresponding function \( \beta \) in \( b \) such that

\[
\eta = \frac{\beta}{\alpha}
\]

Let

\[
\alpha \equiv \alpha_0, \quad \beta \equiv \beta_0 \pmod{p}, \quad c_0 = \frac{\beta_0}{\alpha_0},
\]

where \( \alpha_0, \beta_0 \) and \( c_0 \) are constants and the first is different from zero. From 5. we have

\[
\sigma (\eta - c_0) = \sigma \frac{\beta - c_0 \alpha}{\alpha} = \frac{b_1}{a},
\]

and it follows from

\[
a (\beta - c_0 \alpha) = b_1 \alpha, \quad \beta - c_0 \alpha \equiv 0 \pmod{p}
\]

that \( \alpha \) is not divisible by \( p \) and that \( b_1 \), must be divisible by \( p \). Then if we set

\[
\eta - c_0 = \rho \eta_1,
\]

the under-ideal of \( \eta_1 \) is in turn not divisible by \( p \). In this way a definite sequence of constants \( c_0, c_1, \ldots, c_{r-1}, \ldots \) can be determined such that;

\[
\eta = c_0 + \rho \eta_1,
\eta_1 = c_1 + \rho \eta_2,
\eta_{r-1} = c_{r-1} + \rho \eta_r,
\]

where the \( \eta_1, \eta_2, \ldots, \eta_r, \ldots \) represent functions whose under-ideals can have no other prime factors than the under-ideal of \( \eta \) and the over-ideal of \( \rho \) except for \( p \). Accordingly, for each positive integer \( r \) we have

\[
\eta = c_0 + c_1 \rho + \ldots + c_{r-1} \rho^{r-1} + \eta_r \rho^r.
\]

If the under-ideal of \( \zeta \) is divisible by \( p^r \) and not divisible by \( p^{r+1} \), then we can apply the same approach to the function \( \eta = \zeta \rho^r \) and obtain

\[
\zeta = c_0 \rho^{-r} + c_1 \rho^{-r+1} + \ldots + c_{r-1} \rho^{-r+r} + \eta_r \rho^{-r+r}.
\]
§13.

The rational transformations of the functions in the field $\Omega$.

If $z_1$ is an arbitrary, non-constant function in the field $\Omega$ (a variable in $\Omega$), then, as shown in §2, there exists an irreducible algebraic equation between $z_1$ and $z$ which is free from denominators and is of degree $e$ with respect to $z_1$ and of degree $e_1$, with respect to $z$. As just shown, $e$ is a divisor of $n$, $n = ef$. Let this equation be

\[ G(z_1^e, z) = 0. \]

With the help of this equation, let any rational function $\zeta$ of $z$ and $z_1$ be expressed in the two forms (§1)

\[
\begin{align*}
\zeta &= x_0 + x_1 z_1 + \ldots + x_{e-1} z_1^{e-1}, \\
\zeta &= x_0^{(1)} + x_1^{(1)} z + \ldots + x_{e_1-1}^{(1)} z_1^{e_1-1}
\end{align*}
\]

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

If now $\theta$ is a function such that $1, \theta, \theta^2, \ldots, \theta^{n-1}$ form a basis $^1$ of $\Omega$ (with respect to $z$), then, in accordance with §2, the $n$ functions

\[
\begin{align*}
1, z_1, z_1^2, \ldots, z_1^{e-1}, \\
\theta, \theta z_1, \theta z_1^2, \ldots, \theta z_1^{e-1}, \\
\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \\
\theta^{f-1}, \theta^{f-1} z_1, \theta^{f-1} z_1^2, \ldots, \theta^{f-1} z_1^{e-1}
\end{align*}
\]

likewise provide such a basis, and from this it follows, by (2.), that between the $e_1 f = n_1$ functions

\[
\begin{align*}
1, z, z^2, \ldots, z^{e_1-1}, \\
\theta, \theta z, \theta z^2, \ldots, \theta z^{e_1-1}, \\
\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \\
\theta^{f-1}, \theta^{f-1} z, \theta^{f-1} z^2, \ldots, \theta^{f-1} z^{e_1-1}
\end{align*}
\]

which we may represent with the abbreviations,

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

there exists an equation of the form

\[ x_1^{(1)} \eta_1^{(1)} + x_2^{(1)} \eta_2^{(1)} + \ldots + x_{n_1}^{(1)} \eta_{n_1}^{(1)} = 0 \]

\(^1\)Instead of the basis $1, \theta, \theta^2, \ldots, \theta^{n-1}$, one could also use any other basis of $\Omega$ to support this approach, but it is sufficient for our purpose to choose this one.
only if the rational functions \( x_1^{(1)}, x_2^{(1)}, \ldots, x_{n_1}^{(1)} \) of \( z_1 \) all vanish. From this it follows by (2.) that each function \( \eta \) in \( \Omega \) is in fact representable in a unique way in the form:
\[
\eta = x_1^{(1)} \eta_1^{(1)} + x_2^{(1)} \eta_2^{(1)} + \ldots + x_{n_1}^{(1)} \eta_{n_1}^{(1)},
\]
where the \( x^{(1)} \) are rational functions of \( z_1 \).

Each such function \( \eta \) satisfies an algebraic equation of degree \( n_1 \), whose coefficients depend rationally on \( z_1 \), because we have
\[
\begin{align*}
\eta \eta_1^{(1)} &= x_1^{(1)} \eta_1^{(1)} + x_2^{(1)} \eta_2^{(1)} + \ldots + x_{n_1}^{(1)} \eta_{n_1}^{(1)}, \\
\eta \eta_2^{(1)} &= x_2^{(1)} \eta_1^{(1)} + x_2^{(1)} \eta_2^{(1)} + \ldots + x_{2,n_1}^{(1)} \eta_{n_1}^{(1)}, \\
\quad \ldots \quad \ldots \ldots \ldots \ldots \ldots \ldots \quad \ldots \quad \ldots \ldots \\
\eta \eta_{n_1}^{(1)} &= x_{n_1-1,1}^{(1)} \eta_1^{(1)} + x_{n_1-1,2}^{(1)} \eta_2^{(1)} + \ldots + x_{n_1-1,n_1}^{(1)} \eta_{n_1}^{(1)},
\end{align*}
\]
and consequently
\[
\begin{vmatrix}
x_1^{(1)} - \eta, & x_2^{(1)}, & \ldots & x_{n_1}^{(1)} \\
x_2^{(1)}, & x_2^{(1)} - \eta, & \ldots & x_{2,n_1}^{(1)} \\
\quad \ldots \quad \ldots \ldots \ldots \quad \ldots \quad \ldots \ldots \\
x_{n_1-1,1}^{(1)}, & x_{n_1-1,2}^{(1)}, & \ldots & x_{n_1-1,n_1}^{(1)} - \eta
\end{vmatrix} = 0.
\]

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

We stop short ourselves of the proof of this claim at the following theorem, whose proof is easy obtained by the passage from \( m - 1 \) to \( m \).

If
\[
F(x_1, x_2, \ldots, x_m)
\]
is an integral rational function of \( x_1, x_2, \ldots, x_m \), whose coefficient functions are in \( \Omega \) and are not all zero, then we can set for the variables \( x_1, x_2, \ldots, x_m \) parameters that are constant or depend rationally on \( z_1 \) such that \( F \) turns into a non-vanishing function in \( \Omega \). If thus \( F(x_1, x_2, \ldots, x_m) \) is equal to zero for all such \( x_1, x_2, \ldots, x_m \), it follows also for \( dx_1, dx_2, \ldots, dx_m \) arbitrary constants or rationally dependent on \( z_1 \) that
\[
dF = F'(x_1)dx_1 + F'(x_2)dx_2 + \ldots + F'(x_m)dx_m = 0.
\]
If now
\[
\theta_1 = x_1^{(1)} \eta_1^{(1)} + x_2^{(1)} \eta_2^{(1)} + \ldots + x_{n_1}^{(1)} \eta_{n_1}^{(1)}
\]
and
\[
\begin{align*}
1 &= x_{1,0}^{(1)} \eta_1^{(1)} + x_{2,0}^{(1)} \eta_2^{(1)} + \ldots + x_{n_1,0}^{(1)} \eta_{n_1}^{(1)}, \\
\theta_1 &= x_{1,1}^{(1)} \eta_1^{(1)} + x_{2,1}^{(1)} \eta_2^{(1)} + \ldots + x_{n_1,1}^{(1)} \eta_{n_1}^{(1)}, \\
\quad \ldots \quad \ldots \ldots \ldots \quad \ldots \quad \ldots \ldots \\
\theta_m^{(1)} &= x_{1,m}^{(1)} \eta_1^{(1)} + x_{2,m}^{(1)} \eta_2^{(1)} + \ldots + x_{n_1,m}^{(1)} \eta_{n_1}^{(1)},
\end{align*}
\]
then the $x_{k,h}$ are rational and homogeneous functions of degree $h$ of $x_1, x_2, \ldots x_{n_1}$ and also rationally dependent on $z_1$.

If then
\[
\phi(\theta_1) = a_m \theta_1^m + a_{m-1} \theta_1^{m-1} + \ldots + a_1 \theta_1 + a_0 = 0
\]
is the lowest degree equation which $\theta_1$ satisfies whose coefficients depend rationally on $z_1$, then the functions $a_0, a_1, \ldots a_m$ satisfy the condition
\[
a_0 x_{1,0} + a_1 x_{1,1} + \ldots + a_m x_{1,m} = 0 \quad (i=1,2,\ldots n_1)
\]
and also $m \leq n_1$. Then not all of the coefficients $x_{k,h}$ which form an $m$-rowed determinant can vanish, because otherwise $\theta_1$ would satisfy an equation of less than the $m^{th}$ degree, it follows from the latter equations that we can assume that the $a_0, a_1, \ldots a_m$ are homogeneous integral functions of $x_1, x_2, \ldots x_{n_1}$.

Now if the equation $\phi(\theta_1) = 0$ exists for all $x_1, x_2, \ldots x_{n_1}$ rationally dependent on $z_1$, then according to the above proposition it must also be the case that
\[
d\phi = \phi'(\theta_1) d\theta_1 + da_m \theta_1^m + \ldots + da_1 \theta_1 + da_0 = 0,
\]
and if $m < n_1$, then the $dx_1, dx_2, \ldots dx_{n_1}$ can be determined so that they do not all vanish because
\[
da_m : da_{m-1} : \ldots : da_1 : da_0 = a_m : a_{m-1} : \ldots : a_1 : a_0
\]
and hence
\[
\phi'(\theta_1) d\theta_1 = 0.
\]
Since however, $\phi'(\theta_1)$ is of degree $m - 1$, then we must have $d\theta_1 = 0$, so that $dx_1 = 0, dx_2 = 0, \ldots dx_{n_1} = 0$. Therefore, it can only be that $m = n_1$.

If therefore $\theta_1$ is so determined that the equation of lowest degree
\[
F_1(\theta_1, z_1) = 0
\]
of degree $n_1$ is actually achieved, then all the functions in $\Omega$ can be represented (and indeed in only one way) in the form
\[
\eta = x_0^{(1)} + x_1^{(1)} \theta_1 + \ldots + x_{n_1-1}^{(1)} \theta_1^{n_1-1},
\]
where the coefficients $x_0^{(1)}, x_1^{(1)}, \ldots, x_{n_1-1}^{(1)}$ are rationally dependent on $z_1$; for with this assumption one can represent $\eta_1^{(1)}, \eta_2^{(1)}, \ldots, \eta_{n_1}^{(1)}$ in the specified manner by means of the equation (5).

Thus both $z_1$ and $\theta_1$ can be represented rationally in terms $z$ and $\theta$ and, vice versa, $z$ and $\theta$ can be represented rationally in terms of $z_1$ and $\theta_1$.

The variable $z$, which we have previously referred to as independent, can therefore be any (non-constant) function in the field $\Omega$. But while the totality of
all the functions in the field \( \Omega \) remain completely unchanged, the concepts: basis, norm, trace, discriminant, integral function, module and ideal depend fundamentally on the choice of the independent variable \( z \).

In the particular case when two variables \( z \) and \( z_1 \) are linearly dependent on each other, a basis for \( \Omega \) with respect to \( z \) is at the same time one such with respect to \( z_1 \); then in this case norms, traces, and discriminants are identical for \( z \) and \( z_1 \).

If \( \alpha \) and \( \beta \) are any two functions in \( \Omega \), then there exists equations between the two whose left-hand side is an integral rational function of \( \alpha \) and \( \beta \).

Among these is one (according to §1)

\[ F(\alpha, \beta) = 0, \]

which is of the lowest possible degree both in terms of \( \alpha \) and in terms of \( \beta \), and this will be called the the irreducible equation existing between \( \alpha \) and \( \beta \). This is completely determined, apart from a constant factor.

\textbf{Part II.}

§14. The points of the Riemann surface.

The previous observations about the functions in the field \( \Omega \) were of a purely formal nature. All results were rational, that is, in accordance with the rules of arithmetic with conclusions deduced by means of the four basic operations from the irreducible equation that exists between two functions in \( \Omega \). The numerical values of these functions were not considered anywhere. Even without employing other principles, the formal treatment can still be pursued much further, as one considers two functions in the field \( \Omega \) not as connected by an equation, but as independent variables, in which case everything comes down to the algebraic divisibility of rational functions of two variables. We have carried out this project too, but it is very cumbersome in presentation and mode of expression and with respect to rigour provides nothing more than the development used previously. But once the formal part of the study has been carried out thus far, the suggested question is to what extent can the functions in \( \Omega \) take such specific numerical values that rational relations (identities) that exist between all of these functions translate into valid numerical equations? It turns out to be appropriate in this investigation to consider also the infinitely great as a specific number \( \infty \) (constant), with which calculations can be made according to certain rules. The calculations carried out by means of rational operations in the domain of numbers thus extended always lead to a specific numerical result, unless in the course of the calculation one of the symbols

\footnote{Considering the infinite as a specific value is often customary and useful in the theory of functions. This is advocated by Riemann for example in viewing the algebraic function as being represented by a closed surface.}
∞ ± ∞, 0.∞, 0\,\infty, \infty 0, \infty 0 occurs, which take no particular value. The occurrence of such uncertainty in an equation is not to be interpreted as a contradiction since in this case the equation does not make any definite assertion at all and so can say nothing about the truth or falsity of the same. Among the functions in the field Ω can also be found, in addition to infinitely many variables, all the constants, i.e. numbers. In this way the query raised above leads to the following idea.

1. **Definition.** If all the individual elements α, β, γ, . . . of the field Ω are replaced by certain numerical values, α₀, β₀, γ₀ . . ., such that

   (I.) \( α₀ = α \), in the case where α is a constant, and in general

   (II.) \((α + β)₀ = α₀ + β₀\), (IV.) \((αβ)₀ = α₀β₀\),

(III.) \((α − β)₀ = α₀ − β₀\), (V.) \(\left(\frac{α}{β}\right)₀ = \frac{α₀}{β₀}\)

then a definite set of values will thus be assigned to a point \( P \) (which one may consider for visualization as somehow located in space \( ^1 \)), and we say \( α = α₀ \) at \( P \) or \( α \) has the value \( α₀ \) at \( P \). Two points are called distinct if and only if there is a function \( α \) in \( Ω \) which has different values at the two points.

From this definition of points the existence of the same as well as the scope of the concept will now be deduced. Firstly however, it is to be emphasized that according to this definition, a “point” belonging to a field \( Ω \) is an invariant concept that in no way depends on the choice of the independent variable by which the functions in the field are represented.

2. **Theorem.** Given a point \( P \) and a variable \( z \) from \( Ω \) that is finite at \( P \), (such a one exists for every point, for if \( z₀ = \infty \), then \( \left(\frac{1}{z}\right)₀ = 0 \) is finite), then has every integral function \( ω \) of \( z \) also has a finite value \( ω₀ \) at \( P \) — because there is a relation between \( ω \) and \( z \) of the form

\[ 1 = a \frac{1}{ω} + b \frac{1}{ω²} + \ldots + k \frac{1}{ωⁿ}, \]

where \( a, b, \ldots k \) as integral rational functions of \( z \) from (II.), (III.) and(IV.), have finite values at \( P \). Consequently \( \left(\frac{1}{ω}\right)₀ \) cannot be equal to 0, so \( ω₀ \) is not equal to \( \infty \).

3. **Theorem.** If \( z \) is any variable finite at \( P \), then the set \( p \) consisting of all those integral functions \( π \) of \( z \) which vanish at \( P \) is a prime ideal in \( z \); we say, the point \( P \) generates this prime ideal \( p \). If \( ω \) is an integral function of \( z \) which has the value \( ω₀ \) at \( P \), then \( ω \equiv ω₀ \) (mod. \( p \)).

\(^1\)A geometric visualization of “points” is, incidentally, by no means necessary and contributes very little to an illumination of the conception. It is sufficient to consider the word “point” as a short and convenient expression for the described coexistent values.
Proof. If \( \pi'_0 = 0 \) and \( \pi''_0 = 0 \), then also \( (\pi'_0 + \pi''_0)_0 = \pi'_0 + \pi''_0 = 0 \), and if \( \omega \) is an arbitrary integral function of \( z \), i.e. \( \omega_0 \), is finite, then it follows from \( \pi_0 = 0 \) that \( (\omega \pi)_0 = \omega_0 \pi_0 = 0 \) as well; so \( p \) is an ideal in \( z \) (§7, I., II.). The ideal \( p \) is different from \( o \), since it does not contain the function “1”.

If \( \omega \) has the value \( \omega_0 \) at \( \mathcal{P} \), then \( (\omega - \omega_0)_0 = 0 \), therefore, \( \omega \equiv \omega_0 \) (mod. \( p \)), so any integral function of \( z \) is congruent to a constant modulo \( p \). Therefore, (§9, 7.) \( p \) is a prime ideal.

4. Theorem. The same prime ideal \( p \) cannot be generated by two different points.

Because first of all the value of each integral function \( \omega \) at one of the points \( \mathcal{P} \) that generate the ideal \( p \) is completely defined by the congruence \( \omega \equiv \omega_0 \) (mod. \( p \)). But if \( \eta \) is an arbitrary function in \( \Omega \), then from §12, 1. it can be defined by two integral functions \( \alpha \) and \( \beta \), which are not both divisible by \( p \), such that

\[
\eta = \frac{\alpha}{\beta}.
\]

Since the finite values \( \alpha_0 \) and \( \beta_0 \), do not both vanish, then it follows from (V.) that

\[
\eta_0 = \frac{\alpha_0}{\beta_0}
\]

is thus likewise completely determined by \( p \).

It now results from this that two points at which a variable \( z \) has finite values differ from each other if and only if there exists an integral function of \( z \) which has different values in both.

5. Theorem. If \( z \) is any variable in \( \Omega \) and \( p \) is a prime ideal in \( z \), then there is one (and, from 4., only one) point \( \mathcal{P} \) which generates the prime ideal, and which will be called the null point of the ideal \( p \).

Proof. Let \( \eta \) be an arbitrary function in \( \Omega \) and \( \rho \) one such that the over-ideal is divisible by \( p \) but not by \( p^2 \). There can then be determined, according to §12, 6., in one and only one way an integer \( m \), a non-zero finite constant \( c \) and a function \( \eta_1 \) whose under-ideal is not divisible by \( p \), such that

\[
\eta = cp^m + \eta_1 \rho^{m+1}.
\]

We set

\[
\eta_0 = 0, \quad c, \quad \infty,
\]

depending on whether \( m \) is positive, zero or negative.
Dedekind and Weber, Theory of the algebraic functions of one variable.

Determination of the value of functions in the field \( \Omega \) corresponds to a point \( \mathfrak{P} \), since it can be clearly seen at once that the conditions (I.) to (V.) are satisfied.  

Every function whose over-ideal is divisible by \( p \), so in particular every function in \( p \), takes the value zero at \( \mathfrak{P} \) in this set up, i.e. the point \( \mathfrak{P} \) thus determined generates the prime ideal \( p \).

All the functions whose under-ideal is divisible by \( p \), and only these, have the value \( \infty \) at \( \mathfrak{P} \) and from this it is apparent that an integral function of \( z \) is not infinite at any point at which \( z \) has a finite value, and that a fractional function of \( z \), whose under-ideal is certainly divisible by a prime ideal, must thus be infinite at at least one point at which \( z \) is finite, then, conversely, every function which is not infinite at any point at which \( z \) has a finite value, is an integral function of \( z \).

6. From 3., 4. and 5. we now have the following result. To obtain every point \( \mathfrak{P} \), and each one only once, one takes an arbitrary variable \( z \) in the field \( \Omega \); one forms all prime ideals \( p \) in \( z \) and constructs the null point for each of them, then all those points \( \mathfrak{P} \) are found at which \( z \) remains finite; if \( \mathfrak{P}' \) is a different point from these, then \( z' = \frac{1}{z} \) has the finite value zero at it, conversely, every point \( \mathfrak{P}' \) at which \( z' \) has the value zero is different from the points \( \mathfrak{P} \). The prime ideal \( p' \) in \( z' \) generated by such a point \( \mathfrak{P}' \) (which consists of all integral functions of \( z' \) vanishing at \( \mathfrak{P}' \)) contains \( z' \), and conversely the null point of each of the prime ideals \( p' \) in \( z' \) that occur is a point \( \mathfrak{P}' \) at which \( z' = 0 \) so \( z = \infty \). The totality of all points \( \mathfrak{P} \) consists of the finite number of these additional points corresponding to the distinct \( p' \) and those derived previously from the prime ideals \( p \) in \( z \), the collection constitutes the Riemann surface \( T \).

§15.

The order numbers.

1. Definition. If \( \mathfrak{P} \) is a certain point, we consider all the functions \( \pi \) in \( \Omega \) that vanish at \( \mathfrak{P} \) and assign to each of them a certain order number from the following point of view.

Such a function \( \rho \) has order number 1, or is called infinitely small of the first order or 0' at \( \mathfrak{P} \), if all the quotients \( \frac{\pi}{\rho} \) remain finite at \( \mathfrak{P} \). If \( \rho' \) is a similar function to \( \rho \), then \( \frac{\rho'}{\rho} \) is neither 0 nor \( \infty \) at \( \mathfrak{P} \), and conversely, if \( \frac{\rho'}{\rho} \) is neither 0 nor \( \infty \) at \( \mathfrak{P} \), then \( \rho' \) is also infinitely small of the first order. Moreover, if for any function \( \pi \)

\[ \eta' = c' \rho^{m'} + \eta_1' \rho^{m'+1} \]

then, for example

\[ \frac{\eta}{\eta'} = \rho^{m-m'} \left( \frac{c}{c'} + \rho \eta_1'' \right) \]

in which

\[ \eta_1'' = \frac{c' \eta_1 - c \eta'}{c'(c' + \rho \eta_1')} \]

is a function of the same nature as \( \eta_1 \), (the proof in the remaining cases is even easier).
there is a positive integer exponent $r$ such that $\frac{\pi}{\rho^r}$ is neither 0 nor $\infty$ at $\mathfrak{P}$, then the same is true of $\frac{\pi}{\rho^{r'}}$, and $\pi$ is given the order number $r$ or is called infinitely small of order $r$ at the point $\mathfrak{P}$. We will also say that $\pi$ is $0$ at $\mathfrak{P}$ or $\pi$ is $0$ at $\mathfrak{P}^r$.

For the question of the existence of such a function $\rho$ and to determine such order numbers $r$, we take an arbitrary variable $z$ that is finite at $\mathfrak{P}$ and we denote by $p$ the prime ideal in $z$ generated by $\mathfrak{P}$. In line with §12, we set every function $\pi$ (with the exception of the orderless constant 0) as represented by the quotient of two relatively prime ideals in $z$. The over-ideal of each of these functions is then divisible by $p$, and there are amongst them some whose over-ideal is not divisible by $p^2$; these have the order number 1; for the remaining functions $\pi$ the order number is the exponent of the highest power of $p$ that divides the over-ideal, which follows from the theorem in §12 without further details.

2. If a function $\eta$ has the finite value $\eta_0$ at $\mathfrak{P}$, then we say $\eta$ has this value $r$ times at $\mathfrak{P}$ or in $r$ points that coincide with $\mathfrak{P}$, or in $\mathfrak{P}^r$, when the function $\eta - \eta_0$ is infinitely small of order $r$ at $\mathfrak{P}$. But if $\eta_0 = \infty$ then we say $\eta$ has the value $\infty$ at $\mathfrak{P}$ or at $r$ points coincident with $\mathfrak{P}$, or $\eta$ was $\infty$ at $\mathfrak{P}$ or $\infty$ at $\mathfrak{P}^r$, if $\frac{1}{\eta}$ vanishes at $\mathfrak{P}^r$.

3. Should a function $\eta$ be $\infty$ at $\mathfrak{P}$, then we also set its order number to $-r$, but when $\eta$ is neither 0 nor $\infty$ at $\mathfrak{P}$, then it has the order number 0. Accordingly, each function in the field $\Omega$ gives rise to a certain determined order number at an arbitrary point $\mathfrak{P}$, with the exception of the two constants 0 and $\infty$.

4. If $\rho$ is a function which at an arbitrary point $\mathfrak{P}$ has the order number 1 and $\eta$ is a function with the (positive, negative or zero) order $m$, then, in accordance with conclusion of §12, for any arbitrary positive $r$ a sequence of constants $c_0, c_1, \ldots, c_{r-1}$, the first of which does not vanish, and a function $\sigma$ finite at $\mathfrak{P}$ can be determined such that

$$
\eta = c_0\rho^m + c_1\rho^{m+1} + \ldots + c_{r-1}\rho^{m+r-1} + \sigma\rho^{m+r}
$$

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 between the order numbers of the numerator and denominator.

If $\eta_1, \eta_2, \ldots, \eta_s$ is a sequence of functions and $m$ is the algebraically smallest of their order numbers, then we have

$$
\eta_1 = e_1\rho^m + \sigma_1\rho^{m+1},
\eta_2 = e_2\rho^m + \sigma_2\rho^{m+1},
\ldots, \ldots, \ldots, \ldots, \ldots,
\eta_s = e_s\rho^m + \sigma_s\rho^{m+1},
$$
where at least some of the constants \(e_1, e_2, \ldots e_s\) do not vanish. If additionally \(c_1, c_2, \ldots c_s\) are constants, then the order number of

\[
\eta = c_1 \eta_1 + c_2 \eta_2 + \ldots + c_s \eta_s,
\]

is \(m\) as well if \(c_1 e_1 + c_2 e_2 + \ldots + c_s e_s\) is different from zero, otherwise it is greater than \(m\).

6. A complex of points, which can contain the same point several times, is called a polygon and denoted by \(A, B, C, \ldots\)

Further, \(AB\) represents the polygon composed of the points of \(A\) and of \(B\) in such a way that when a point \(P\) occurs \(r\)-times in \(A\) and \(s\)-times in \(B\), it occurs \((r+s)\)-times in \(AB\). From this follows the meaning of \(\mathfrak{P}\) and of \(\mathfrak{A} = \mathfrak{P}^i \mathfrak{P}_1^j \mathfrak{P}_2^j \ldots\), and the laws of divisibility of polygons are in perfect accordance with those of the divisibility of integers and ideals. The role of prime factors is take over by the points; but in order to maintain unity, one must even include the polygon \(O\) containing no points (the null-gon).

The number of points of a polygon is called its order. A polygon of order \(n\) is called for short an \(n\)-gon.

The greatest common divisor of two polygons \(\mathfrak{A}\) and \(\mathfrak{B}\) is that polygon which contains every point \(P\) the least number of times it occurs in \(\mathfrak{A}\) or \(\mathfrak{B}\). If this is \(O\) then \(\mathfrak{A}\) and \(\mathfrak{B}\) are called relatively prime.

The least common multiple of \(\mathfrak{A}\) and \(\mathfrak{B}\) is that polygon which contains every point the most number of times that it occurs in \(\mathfrak{A}\) or \(\mathfrak{B}\). If \(\mathfrak{A}\) and \(\mathfrak{B}\) are relatively prime, their least common multiple is \(\mathfrak{AB}\).

If \(\mathfrak{A} = \mathfrak{P}^i \mathfrak{P}_1^j \mathfrak{P}_2^j \ldots\) is any polygon, then there are always functions \(z\) in \(\Omega\) which are infinite at no point of \(\mathfrak{A}\). Because if \(z\) is infinite at some points of \(\mathfrak{A}\), then a constant \(c\) can be chosen such that \(z - c\) has the value \(0\) at none of the points of \(\mathfrak{A}\), thus \(1 \over z - c\) is finite at all points of the polygon \(\mathfrak{A}\). If things are based on such a variable \(z\), then the set 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 \(\alpha = p^i p_1^j p_2^j \ldots\) and one can say that the polygon \(\mathfrak{A}\) generates the ideal \(\alpha\), or \(\mathfrak{A}\) is the null polygon of the ideal \(\alpha\). Hence the concept of an ideal coincides completely with the concept a system of integral functions which all vanish at the same fixed points. The ideal \(o\) is generated by the null-gon \(O\).

The product of two or more ideals is generated by the product of the null polygons of the factors, the greatest common divisor and least common multiple of two ideals by the greatest common divisor and least common multiple of the corresponding null polygons.

7. Theorem. If \(z\) is any variable in \(\Omega\) and \(n\) is the degree of the field \(\Omega\) with respect to \(z\), then \(z\) takes each particular value \(c\) at exactly \(n\) points. — For, if \(o\) is the system of integral functions of \(z\) and \(c\) represents a finite constant, then we
have
\[ o(z - c) = p_1^{e_1} p_2^{e_2} \ldots, \quad e_1 + e_2 + \ldots = n \quad (\S 9, 7.), \]
where \( p_1, p_2, \ldots \) are prime ideals in \( z \) that differ from each other. If one writes \( \mathfrak{P}_1, \mathfrak{P}_2, \ldots \) for the null points of \( p_1, p_2, \ldots \) then according to 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 \( \mathfrak{P}_2^{e_2} \)) etc., i.e. at the \( n \) points of the polygon \( \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \ldots \). Conversely: if \( \mathfrak{P} \) is a point where \( z \) has the value \( c \) and \( p \) is the prime ideal in \( z \) generated by \( \mathfrak{P} \), then \( z \equiv c \pmod{p} \) and hence \( p \) is one of the ideals \( p_1, p_2, \ldots \), and therefore \( \mathfrak{P} \) is one of the points \( \mathfrak{P}_1, \mathfrak{P}_2, \ldots \). The same result is also true for \( c = \infty \); for \( n \) is also the degree of \( \Omega \) with respect to \( z \), so the latter variable takes the value 0 and hence \( z \) the value \( \infty \) at exactly \( n \) points. It follows from \( \S 11 \), that for only a finite number of values of the constants \( c \) can one of the exponents \( e_1, e_2, \ldots \) be greater than 1.

The number \( n \), i.e., the number of points at which the function \( z \) has each constant value, will be called the order of the function \( z \). The constants, and only these, are of order zero. For all other functions in \( \Omega \) the order is a positive integer. The order of a variable \( z \) is also the degree of the field \( \Omega \) with respect to \( z \).

\( \S 16. \)
Conjugate points and conjugate values.

1. Definition. If \( c \) is a certain numerical value then, as shown in \( \S 15 \), there is a corresponding polygon \( \mathfrak{A} \) of \( n \) (identical or distinct) points \( \mathfrak{P}_1, \mathfrak{P}_2, \ldots \mathfrak{P}^{(n)} \), at which the \( n \)th order variable \( z \) has precisely this value; these \( n \) points shall be called conjugate with respect to \( z \); the others are determined by any one of them (and by the variable \( z \)). Let \( c \) gradually assumed all values so that the polygon \( \mathfrak{A} = \mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}^{(n)} \) moves in such a way in fact that all its points alter as a result. In this way one obtains in general all the existing points repeating only those (of which there are a finite number), at which \( z - z_0 \), or \( \frac{1}{z} \) vanishes to higher order than the first. Therefore the product of all these polygons
\[
\prod \mathfrak{A} = T \mathfrak{Z},
\]
where \( T \) is the collection of all the simple points, is the Riemann surface, \( \mathfrak{Z} \), is a finite polygon, which is called the ramification (branching) or winding-polygon of \( T \) in \( z \). Each point \( \Omega \) contained in \( \mathfrak{Z} \), is called a ramification- or winding-point of \( T \) in \( z \), in fact of order \( s \) if it occurs exactly \( s \)-times in \( \mathfrak{Z} \). We have \( s = e - 1 \) if \( z - z_0 \) or \( \frac{1}{z} \) is infinitely small of the \( e \)th order at \( \Omega \). The order of the polygon \( \mathfrak{Z} \) is called the ramification- or winding-number \( w \) 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 \( z \)(\( \S 11 \)).

In order to move from this definition of the “absolute” Riemann surface, which is an invariant concept associated with the field \( \Omega \), to the well known idea of
Riemann, you have to think of the surface itself as spread out in a $z$-plane, which it then covers $n$-times everywhere except at the branch points.

2. **Theorem** If

$$z' = \frac{c + dz}{a + bz},$$

where $a, b, c$ and $d$ are constants whose determinant $ad - bc$ is non-zero, then we have

$$\mathfrak{g} = \mathfrak{g}'; \quad w_z = w_{z'}.$$

For if at a point $\mathfrak{P}$ either $z - z_0$ 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 in the case where $z_0$ is infinite:

$$z' - z'_0 = \frac{-(ad - bc)}{b(a + bz_0)},$$

or if $z'_0 = \infty$, thus $a + bz_0 = 0$:

$$\frac{1}{z'} = \frac{(a + bz)}{(c + dz)},$$

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 $\Delta_z(\Omega)$ multiplied by the number of vanishing roots of $\Delta_{z'}(\Omega) = 0$ (§11).

3. **Definition.** The values $\eta', \eta'', \ldots \eta^{(n)}$ which any function $\eta$ in $\Omega$ takes at $n$ points $\mathfrak{P}', \mathfrak{P}'', \ldots \mathfrak{P}^{(n)}$ that are conjugate with respect to $z$, are called *conjugate values of $\eta$ with respect to $z$*.

4. **Theorem.** If $N_1(\eta)$ is the norm of an arbitrary function $\eta$ with respect to $z$, then the value which this rational function of $z$ has for $z = z_0$ equals the product $\eta' \eta'' \ldots \eta^{(n)}$ of the conjugate values of $\eta$ associated with $z = z_0$. It remains to be seen how to deal with the case when this product is undefined, that is one of these conjugate values is 0 and another is $\infty$. In proving this theorem we can assume that $z_0$ is finite, for if $z_0 = \infty$, we set $z = \frac{1}{z}$ as the underlying variable instead of $z$, which does not change the norm. Furthermore, we can assume that the values $\eta', \eta'', \ldots \eta^{(n)}$ are all finite, because if one of them is infinite, then by arrangement none of them is equal to 0 and we consider the function $\frac{1}{\eta}$ instead of $\eta$.

Under these conditions we now have

$$o(z - z_0) = p_{1z} \beta_1^2 p_{2z} \beta_2^3 \ldots.$$
wherein:

must also be infinitely small of this order. This is only possible when vanish at $P$

by which we can for example set $P$ and $P$ with integral rational coefficients

rule: Let $\lambda$ construct a system of integral functions $\mu$ of $z$ according to the following rule: Let

where

by $\eta$ of the order $e$

If we have

the point $P$. Therefore, according to $\$15, 5.

of $\Omega$; which claim is contained in the generalisation now to be proved.

If we have

with integral rational coefficients $x_1, x_2, \ldots x_n$, and $\zeta$ has the finite values $\zeta', \zeta'', \zeta''', \ldots$

at the points $P_1, P_2, P_3, \ldots$, then all the coefficients $x_1, x_2, \ldots x_n$ must be divisible by $z - z_0$. In fact if, for example, the left-hand side is infinitely small at least of the order $e_1$ at the point $P_1$. Therefore, according to $\$15, 5.

must also be infinitely small of this order. This is only possible when $x_1, x_2, \ldots x_{e_1}$ vanish at $P_1$, so are divisible by $z - z_0$. Q.E.D.

After that we can set:

\[ \eta \mu_1 \lambda_1 = \mu_1 (x_1^{(0)} + x_1^{(0)} \lambda_1 + x_1^{(0)} \lambda_1^{e_1 - 1}) + \mu_2 (x_2^{(0)} + x_2^{(0)} \lambda_2 + x_2^{(0)} \lambda_2^{e_2 - 1}) + \mu_3 (x_3^{(0)} + x_3^{(0)} \lambda_3 + x_3^{(0)} \lambda_3^{e_3 - 1}) + \ldots, \]

wherein: $x_1^{(0)}, x_1^{(1)}, \ldots x_2^{(0)}, \ldots$ are rational functions of $z$ and they all remain finite for $z = z_0$. The left-hand side is infinitely small at least of order $e_2, e_3, \ldots$ at

\[ \lambda = \rho - b, \quad \mu \lambda = \psi(\rho). \]
the points \( P_2, P_3, \ldots \). The same is true of \( \mu_1, \mu_3, \ldots \) for \( P_2 \), but not of \( \mu_2 \), of \( \mu_1, \mu_2, \ldots \) for \( P_3 \) but not of \( \mu_3, \ldots \), hence for \( z = z_0 \) we have

\[
\begin{align*}
x_2^{(0)} &= 0, & x_3^{(1)} &= 0, & \ldots & x_3^{(e_3-1)} &= 0, \\
x_3^{(0)} &= 0, & x_3^{(1)} &= 0, & \ldots & x_3^{(e_3-1)} &= 0, \\
\cdots & & \cdots & & \cdots & & \cdots
\end{align*}
\]

At \( P_1 \), the left-hand side is infinitely small at least of order \( r \); therefore, when \( r < e_1 \), for \( z = z_0 \) we have

\[
x_1^{(0)} = 0, \quad x_1^{(1)} = 0, \quad \ldots \quad x_1^{(r-1)} = 0, \quad x_1^{(r)} = \eta'.
\]

Let the same consideration apply to the functions of \( \eta \mu_2 \), \( \eta \mu_3 \), \( \ldots \). Thus set

\[
\begin{align*}
\eta \eta_1 &= x_{1,1} \eta_1 + x_{1,2} \eta_2 + \ldots + x_{1,n} \eta_n, \\
\eta \eta_2 &= x_{2,1} \eta_1 + x_{2,2} \eta_2 + \ldots + x_{2,n} \eta_n, \\
\cdots & & \cdots & & \cdots \\
\eta \eta_n &= x_{n,1} \eta_1 + x_{n,2} \eta_2 + \ldots + x_{n,n} \eta_n,
\end{align*}
\]

so that in the determinant

\[
N(\eta) = \sum \pm x_{1,1} x_{2,2} \ldots x_{n,n}
\]

all the elements standing to the left of the diagonal vanish for \( z = z_0 \), while for the diagonal elements \( e_1 \) is equal to \( \eta' \), \( e_2 \) is equal to \( \eta'' \), \( e_3 \) is equal to \( \eta''' \ldots \). So for \( z = z_0 \) we have

\[
N(\eta) = \eta^n \eta'^2 \eta''' \cdots
\]

Q.E.D.

5. Since from the definition of the trace (§2) we have

\[
S(\eta) = x_{1,1} + x_{2,2} + \ldots + x_{n,n}
\]

then the same considerations lead to the theorem:

For \( z = z_0 \)

\[
s(\eta) = e_1 \eta' + e_2 \eta'' + e_3 \eta''' + \ldots,
\]

which only holds on condition that the values \( \eta', \eta'', \eta''' \ldots \), are finite.

For any \( t \) that is constant (or rationally dependent on \( z \)), Theorem 4. yields for \( z = z_0 \)

\[
N(t - \eta) = (t - \eta')^{e_1} (t - \eta'')^{e_2} (t - \eta''')^{e_3} \cdots,
\]

and from this, by comparing the coefficients of equal powers of \( t \) for each of these coefficients, we have an expression for the conjugate values (symmetric functions).

6. If \( \eta_1, \eta_2, \ldots, \eta_n \) is a basis for \( \Omega \), then by the application of 5. we have immediately the value of the discriminant of this system for \( z = z_0 \)

\[
\Delta_z(\eta_1, \eta_2, \ldots, \eta_n) = (\sum \pm \eta_1 \eta_2^{(n)} \ldots \eta_n^{(n)})^2,
\]

where \( \eta_1, \eta_2, \ldots, \eta_n^{(n)} \) all equal or different but assumed to be finite, represent conjugate values of \( \eta_i \) associated with \( z = z_0 \).
§17.

Representation of the functions in the field $\Omega$ by polygon quotients.

A Function $\eta$ from the field $\Omega$ has a non-zero order number at only a finite number of points; the sum of all the order numbers is equal to 0 thus the sum of the positive is equal to the sum of the negative order numbers and indeed equal to the order of the function $\eta$ (§15). If the order numbers of a function $\eta$ are known for each point $\mathfrak{B}$, then the function $\eta$ is thereby determined up to a constant factor; because if $\eta'$ has the same order number everywhere as $\eta$, then $\frac{\eta}{\eta'}$ has (according to §15, 5) the order number zero everywhere, and is thus (according to §15, 7) a constant.

Therefore, if we construct a polygon $\mathfrak{A}$ in which we include each point where $\eta$ has a positive order number as many times as this order number indicates, and a second polygon $\mathfrak{B}$ in which we include in a corresponding manner the points where $\eta$ has a negative order number, then the polygons $\mathfrak{A}$ and $\mathfrak{B}$ are of the same order, namely the order of the function $\eta$. Thus the function $\eta$ is determined by these polygons $\mathfrak{A}$ and $\mathfrak{B}$ up to a constant factor. We put it in symbolic form

$$ \eta = \frac{\mathfrak{A}}{\mathfrak{B}}, $$

and call $\mathfrak{A}$ the over-gon, $\mathfrak{B}$ the under-gon of the function $\eta$.  

As a result of this arrangement, the two polygons $\mathfrak{A}$ and $\mathfrak{B}$ are relatively prime; however, it is convenient to extend the form here to allow common factors in $\mathfrak{A}$ and $\mathfrak{B}$, which is achieved by the rule that

$$ \frac{\mathfrak{MA}}{\mathfrak{MB}} = \frac{\mathfrak{A}}{\mathfrak{B}} $$

where the $\mathfrak{M}$ represents any polygon. With this generalised definition, write

$$ \eta = \frac{\mathfrak{A}}{\mathfrak{B}}, $$

thus a point $\mathfrak{P}$ in which $\eta$ has the order number $m$, can be included $m_1$-times in $\mathfrak{A}$ and $m_2$-times in $\mathfrak{B}$, where $m_1 - m_2 = m$. The order of $\mathfrak{A}$ is now also equal to that of $\mathfrak{B}$ but no longer equal to the order of the function $\eta$.

Directly from this definition we have (following §15, 5.) the theorem: If

$$ \eta = \frac{\mathfrak{A}}{\mathfrak{B}}, \quad \eta' = \frac{\mathfrak{A}'}{\mathfrak{B}'} $$


then

$$ \eta \eta' = \frac{\mathfrak{A} \mathfrak{A}'}{\mathfrak{B} \mathfrak{B}'}, \quad \frac{\eta}{\eta'} = \frac{\mathfrak{A} \mathfrak{B}'}{\mathfrak{B} \mathfrak{A}'} $$

According to §14, 5. a function $\eta'$ is an integral function of $\eta$ if and only if each point occurring in the under-gon of $\eta'$ is also contained in that of $\eta$.

---

1All functions in the simple family $(\eta)$ have from this the same form $\frac{\mathfrak{A}}{\mathfrak{B}}$ and it would, therefore, be more correct to put $(\eta) = \frac{\mathfrak{A}}{\mathfrak{B}}$; however, this form is unnecessarily long-winded.
§18. Equivalent polygons and polygon classes.

1. Definition. Two polygons $\mathfrak{A}$ and $\mathfrak{A}'$, with the same number of points are called equivalent if a function $\eta$ exists in $\Omega$ which (according to §17) is of the form:

$$\eta = \frac{\mathfrak{A}}{\mathfrak{A}'}.$$

2. Theorem. If $\mathfrak{A}$ is equivalent to $\mathfrak{A}'$ and to $\mathfrak{A}''$, then $\mathfrak{A}'$ is also equivalent to $\mathfrak{A}''$; because from

$$\eta' = \frac{\mathfrak{A}'}{\mathfrak{A}}; \quad \eta'' = \frac{\mathfrak{A}''}{\mathfrak{A}}$$

it follows that:

$$\eta' \eta'' = \frac{\mathfrak{A}'}{\mathfrak{A}''}.$$

3. Definition and theorem. All polygons $\mathfrak{A}', \mathfrak{A}'', \ldots$ equivalent to a given polygon $\mathfrak{A}$ form a polygon class $\mathfrak{A}$. From 2. any polygon occurs in one and in only one class; for if $\mathfrak{A}$ and $\mathfrak{B}$ are two equivalent polygons which end up in the classes $\mathfrak{A}$ and $\mathfrak{B}$, then from 2. each polygon of class $\mathfrak{B}$ is also contained in $\mathfrak{A}$ and vice versa, and therefore both classes are identical.

All polygons of the same class have the same order, which will be called the order of the class.

4. But polygons may exist that are equivalent with no other and therefore form a class of their own. We want to call such polygons isolated.

5. If $\mathfrak{M}$ is an arbitrary polygon and $\mathfrak{A}$ is equivalent to $\mathfrak{A}'$, then $\mathfrak{MA}$ is also equivalent to $\mathfrak{MA}'$; but conversely the equivalence of $\mathfrak{A}$ to $\mathfrak{A}'$ also follows from the equivalence of $\mathfrak{MA}$ to $\mathfrak{MA}'$.

6. If $\mathfrak{A}$ is equivalent to $\mathfrak{A}'$ and $\mathfrak{B}$ to $\mathfrak{B}'$, then $\mathfrak{AB}$ is also equivalent to $\mathfrak{A'B'}$. The class $C$ to which the product $\mathfrak{AB}$ belongs thus contains all the products of any two polygons from the classes $\mathfrak{A}$ and $\mathfrak{B}$, (but under some circumstances infinitely many other polygons besides), and will be referred to as the product of the two classes $\mathfrak{A}$ and $\mathfrak{B}$:

$$C = AB = BA.$$
8. If a polygon $\mathcal{A}$ of the class $A$ divides a polygon $\mathcal{C}$ of the class $C$, then the same is true of each polygon $\mathcal{A}'$ of the Class $A$, because from $\mathcal{C} = \mathcal{A}\mathcal{B}$ it follows from 5. that $\mathcal{C}' = \mathcal{A}'\mathcal{B}$ is contained in $C$, and we can thus say that the class $C$ is divisible by the class $A$, although conversely not every polygon of the class $C$ needs to be divisible by a polygon of the class $A$. If $\mathcal{B}'$ is any polygon of the class $B$ of $\mathcal{B}$, then also $\mathcal{A}' = \mathcal{A}'\mathcal{B}'$ is contained in $C$ and it follows that

$$C = AB.$$ 

Thus if $C$ is divisible by $A$, then there is one, and (according to 7.), only one class $B$ satisfying the condition

$$C = AB.$$ 

§19.

Families of polygons.

1. If $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_s$ are particular equivalent polygons and $\mathcal{A}$ is any polygon in the same class $A$, then there exist $s$ functions in $\Omega$

$$\eta_1 = \frac{\mathcal{A}_1}{\mathcal{A}}, \quad \eta_2 = \frac{\mathcal{A}_2}{\mathcal{A}}, \ldots, \eta_s = \frac{\mathcal{A}_s}{\mathcal{A}}.$$ 

If, as in §15, 5. for any point $\mathfrak{P}$ we set

$$\eta_1 = e_1 \rho^m + \sigma_1 \rho^{m+1},$$
$$\eta_2 = e_2 \rho^m + \sigma_2 \rho^{m+1},$$
$$\ldots$$
$$\eta_s = e_s \rho^m + \sigma_s \rho^{m+1},$$

in which $\rho$ at $\mathfrak{P}$ is 0	extsuperscript{i} and $e_1, e_2, \ldots, e_s$ are constants which do not all vanish, and $\sigma_1, \sigma_2, \ldots, \sigma_s$ denote functions finite at $\mathfrak{P}$, then it follows that each function $\eta$ of the family $(\eta_1, \eta_2, \ldots, \eta_s)$, that is every function of the form

$$\eta = c_1 \eta_1 + c_2 \eta_2 + \ldots + c_s \eta_s,$$

has an order number at $\mathfrak{P}$ which is not less than $m$, and thus from §17 that the function $\eta$ can be put in the form

$$\eta = \frac{\mathcal{A}'}{\mathcal{A}},$$

where $\mathcal{A}'$ is also included in the class $A$.

If we choose for $\mathcal{A}$ any other polygon $\mathcal{B}$ from Class $A$, and put

$$\zeta = \frac{\mathcal{A}}{\mathcal{B}},$$
$$\eta_1 \zeta = \eta'_1 = \frac{\mathcal{A}_1}{\mathcal{B}}, \quad \eta_2 \zeta = \eta'_2 = \frac{\mathcal{A}_2}{\mathcal{B}}, \ldots, \eta_s \zeta = \eta'_s = \frac{\mathcal{A}_s}{\mathcal{B}},$$
then also
\[ \eta' = c_1 \eta_1' + c_2 \eta_2' + \ldots + c_s \eta_s' \]
and hence
\[ \eta' = \frac{A'}{B}. \]

Any polygon generated by the denominator \( A \) and a system of constants \( c_1, c_2, \ldots, c_s \) is therefore also generated by any other denominator \( B \) belonging to the same class, and the set of all polygons \( \mathfrak{A}' \) and the corresponding different values of the constants \( c_1, c_2, \ldots, c_s \), depends only on the polygons \( \mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s \). This set will therefore be known as a family of polygons with a basis \( \mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s \) and be designated by \( (\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s) \).

2. If the polygons \( \mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s \) have a greatest common divisor \( \mathfrak{M} \), then from 1. the same is also a divisor of each polygon \( \mathfrak{A}' \) of the family \( (\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s) \), and can be called the divisor of the family; but a polygon in this family in the form \( \sum c_i \eta_i = \sum c_i \eta_i' \) can be defined such that \( B \) will be relatively prime to an arbitrarily given polygon. To be precise, by retaining the terminology from 1. if a point \( P \) is included exactly \( \mu \)-times in \( M \) and \( \nu \)-times in \( A \), then, when we set
\[ e = c_1 e_1 + c_2 e_2 + \ldots + c_s e_s \]
is different from zero. The point \( \Psi \) is therefore included at least \( \mu \)-times in \( M \), and under the latter condition also not more than \( \mu \)-times. But because the constants \( c_1, c_2, \ldots, c_s \) can always be chosen such that any number of copies of the form
\[ \sum c_i e_i, \sum c_i e_i', \ldots, \]
in none of which all the constants \( e_i, e_i' \) vanish, have non-zero values, thus the correctness of the stated claim follows.

3. If the functions \( \eta_1, \eta_2, \ldots, \eta_s \) in 1. are linearly dependent or independent, then the same is true of the functions \( \eta_1', \eta_2', \ldots, \eta_s' \). We will correspondingly also call the polygons \( \mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s \) linearly dependent or independent and their system linearly reducible or irreducible.

Since according to §5, 4. each family of functions determines an irreducible basis, it follows that each family of polygons has an irreducible basis. If \( s \) is the number of polygons in such a basis, then the family is called an \( s \)-fold and \( s \) is the dimension of the family. Any \( s \) polygons of such a family form an irreducible basis or not depending on whether they are linearly independent or dependent. (See §5, 4.)
§20.
Reduction in the dimension of the family by divisibility conditions.

1. If

\[ S = (A_1, A_2, \ldots, A_s) \]

is an \( s \)-fold family with divisor \( M \). The question is which of the various polygons \( A' \) of the family \( S \) contain an arbitrarily given point at least once more often than the divisor \( M \) of the family.

If the point \( P \) is included \( \mu \)-times in \( M \) and \( \nu \)-times in an arbitrary polygon \( A \) equivalent to \( A_1, A_2, \ldots \), then, if we set in §19

\[
\begin{align*}
\frac{A_1}{A} &= \eta_1 = e_1 \rho^m + \sigma_1 \rho^{m+1}, \\
\frac{A_2}{A} &= \eta_2 = e_2 \rho^m + \sigma_2 \rho^{m+1}, \\
\vdots & \vdots \vdots \vdots \\
\frac{A_s}{A} &= \eta_s = e_s \rho^m + \sigma_s \rho^{m+1},
\end{align*}
\]

we have \( m = \mu - \nu \) and at least one of the constants \( e_1, e_2, \ldots, e_s \), say \( e_s \), different from zero. The required polygon \( A' \) is then given by the characteristic equation

\[
\frac{A'}{A} = \eta' = c_1 \eta_1 + c_2 \eta_2 + \ldots + c_s \eta_s,
\]

where the constants \( c_1, c_2, \ldots, c_s \) are subject to the condition

\[
c_1 e_1 + c_2 e_2 + \ldots + c_s e_s = 0.
\]

From this we can put

\[
\frac{A'}{A} = e_s \eta' = c_1 (e_s \eta_1 - e_1 \eta_s) + \ldots + c_{s-1} (e_s \eta_{s-1} - e_{s-1} \eta_s).
\]

But from this it will be seen that, when we set

\[
\begin{align*}
\eta'_1 &= e_s \eta_1 - e_1 \eta_s, \\
\eta'_2 &= e_s \eta_2 - e_1 \eta_s, \\
\vdots & \vdots \vdots \vdots \\
\eta'_{s-1} &= e_s \eta_{s-1} - e_1 \eta_s,
\end{align*}
\]

the functions \( \eta' \) form an \((s - 1)\)-fold family \((\eta'_1, \eta'_2, \ldots, \eta'_{s-1})\); because the functions \( \eta'_1, \eta'_2, \ldots, \eta'_{s-1} \) are linearly independent when, as assumed, the functions \( \eta_1, \eta_2, \ldots, \eta_s \) are. The polygons \( A' \) thus also form an \((s - 1)\)-fold family

\[
S' = (A'_1, A'_2, \ldots, A'_{s-1}),
\]
when we set

\[
\frac{A'}{A} = e, \eta - e, \eta .
\]

The divisor of this family is divisible by \( MP \), although not necessarily identical with it.

2. From this it follows immediately that the polygons of a family \( S \) which are divisible by any \( r \)-gon \( R \) form at least an \((s - r)\)-fold family. Because if we assume that this had been proved for an \( r \)-gon \( R \), then the validity of the assertion follows immediately from 1. for an \((r + 1)\)-gon \( PR \) in that by the appearance of the point \( P \), when \( P \) is included in the divisor of the family already reduced by \( R \), the dimension is not changed, or is decreased by 1.

From this it follows as a special case, that there is at least one polygon in an \( s \)-fold family which is divisible by a given \((s - 1)\)-gon.

3. If \( r \leq s \), You can choose the \( r \)-gon \( R \) such that the polygons of the family \( S \) that are divisible by \( R \) form an exactly \((s - r)\)-fold family. To this end choose a point \( P \) which is not contained in a divisor of \( S \); from 1. the polygons of \( S \) that are divisible by \( P \) form an \((s - 1)\)-fold family \( S' \); choose a second point \( P' \) which is not contained in a divisor of \( S' \), the polygons in \( S' \) that are not divisible by \( P' \), that is the polygons in \( S \) that are not divisible by \( PPP' \), form an \((s - 2)\)-fold family and so on; it is also evident from this method of construction that we can assume that \( R \) is relatively prime to an arbitrarily given polygon. If \( r = s \) there will be no polygon in \( S \) divisible by \( R \).

§21.

The dimensions of the polygon classes.

1. The polygons of a class form a family of finite dimension, which will be called the dimension of the class.

Proof. Choose from a class \( A \) whose order is \( m \) say, any \( s \) polygons \( A_1, A_2, \ldots, A_s \) so that all the polygons of the family \( (A_1, A_2, \ldots, A_s) \) belong at the same time in the class \( A \). The number of linearly independent polygons which are contained in \( A \) can certainly not therefore be greater than \( m + 1 \), because otherwise (from §20, 2.) one can find a polygon in the class that is divisible by an arbitrary \((m + 1)\)-gon, which is absurd. Therefore, if \( s \) is the maximum number of linearly independent polygons \( A_1, A_2, \ldots, A_1 \) of the class \( A \), then each polygon in this class must be contained in the family \( (A_1, A_2, \ldots, A_s) \) and \( s \) is the dimension of the class. The system of polygons \( A_1, A_2, \ldots, A_s \) will be called a basis of the class.

The isolated polygons form classes of dimension 1.

2. Given \( s \) and no more linearly independent polygons in a class \( C \) which are divisible by a given polygon in class \( A \),

\[
C_1 = AB_1, \quad C_2 = AB_2, \ldots, C_s = AB_s,
\]
then $C$ is divisible by $A$ and there also exist in $C$ the same number of linearly independent polygons

$$C'_1 = \mathfrak{A}' \mathfrak{B}_1, \quad C'_2 = \mathfrak{A}' \mathfrak{B}_2, \ldots \quad C'_s = \mathfrak{A}' \mathfrak{B}_s,$$

which are divisible by an arbitrary polygon $\mathfrak{A}'$ that is equivalent to $\mathfrak{A}$. (§18, 8.; §19, 4.). This number $s$ depends therefore only on the two classes $A$ and $C$ and can reasonably be denoted by $(A, C)$. The value of symbol $(A, C)$ is set equal to 0 when $C$ is not divisible by $A$. The dimension of a class $A$ is hereinafter denoted by $(O, A)$, where $O$ represents the class corresponding to the null-gon $O$.

If, (according to §18, 8.), $C = AB$, it follows that:

$$(1.) \quad (A, C) = (A, AB) = (O, B);$$

because the polygons $\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_s$, all of which are contained in $B$, are linearly independent so $(O, B)$ is certainly not smaller than $s$. If, conversely, $\mathfrak{B}$ is any polygon of the class $B$, then $\mathfrak{A} \mathfrak{B}$ is contained in $C$ and thus also contained in the family $(\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_s)$ 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 hence by means of (1.) we have the general result

$$(2.) \quad (O, B) \geq (O, AB > -a)$$

3. If all of 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 null-gon $O$, then the class is called proper, otherwise improper with divisor $\mathfrak{M}$.

If one reduces all polygons in an improper class $A$ by the divisor $\mathfrak{M}$, one obtains a proper class $A'$ of lower order but of the same dimension. This relationship between $A$ and $A'$ will be written as

$$A = \mathfrak{M} A';$$

4. The divisor $\mathfrak{M}$ of an improper class $A$ is always an isolated polygon. If to be precise

$$A = \mathfrak{M} A';$$

then, according to §19, 2., one can choose a polygon $\mathfrak{A}'$ in the proper class $A'$ that is relatively prime to $\mathfrak{M}$. Thus $\mathfrak{M}'$ is equivalent to $\mathfrak{M}$, hence $\mathfrak{M}' \mathfrak{A}'$ is equivalent to $\mathfrak{M} A'$ and thus included in $A$ so consequently is divisible by $\mathfrak{M}$. $\mathfrak{M}'$ is therefore also divisible by $\mathfrak{M}$ and since $\mathfrak{M}$ and $\mathfrak{M}'$ are of the same order,

$$\mathfrak{M} = \mathfrak{M}'.$$

Accordingly the unique polygon $\mathfrak{M}$ forms a class $M$ and the designation $\mathfrak{M} A'$ is synonymous with $MA'$ (§18, 6.).
§22.

The normal bases of $\sigma$.

1. We will consider in the following the system $\sigma$ of the integral functions $\omega$ of an arbitrary variable $z$ in $\Omega$, and at the same time the system $\sigma'$ of integral functions $\omega'$ of $z' = \frac{1}{z}$. From the definition of integral functions it is immediately clear that the two systems $\sigma$ and $\sigma'$ have only the constants in common, however on the other hand, every function $\omega$ can be transformed into a function $\omega'$ by multiplication by a certain positive power of $z'$. If $\omega z^r$ is included in $\sigma'$, then the same is true of $\omega z^{r+1}, \omega z^{r+2}, \ldots$. In the sequence of functions

$$\omega, \frac{\omega}{z} = z'\omega, \frac{\omega}{z^2} = z'^2\omega, \ldots$$

after a particular term $\omega z^r$ all of the following functions would thus be contained in $\sigma'$, while all the preceding would not be included. The smallest number $r$ for which $z^r \omega$ is contained in $\sigma'$ will be called the exponent of the function $\omega$ with respect to $z$. The constants, and only these, have the exponent of zero. If $\omega$ is different from zero and $r$ is its exponent, then $r + 1$ is the exponent of $(z - c)\omega$; for if $\omega = z^r \omega'$, then

$$\frac{(z - c)\omega}{z^{r+1}} = (1 - cz')\omega' \quad \text{is contained in } \sigma',$$

$$\frac{(z - c)\omega}{z^r} = zw' - cw' \quad \text{is not contained in } \sigma',$$

then in fact $cw'$ is not, but $zw' = \frac{\omega}{z^{r-1}}$ is contained in $\sigma'$. It follows that in general:

*If $x$ is an integral rational function of $z$ of degree $s$ and $r$ is the exponent of $\omega$, then $(r + s)$, the exponent of $x\omega$."

2. We now choose a system of functions $\lambda_1, \lambda_2, \ldots \lambda_n$ in $\sigma$ in accordance with the following rule:

If $\lambda_1$ is a non-zero constant, such as 1; $\lambda_2$ is one of those functions in $\sigma$ which is not congruent to a constant in the module $\sigma z$ and of as low as possible exponent $r_2$, and so on; in general $\lambda_s$ is one of the functions in $\sigma$ which is not congruent to a function of the family $(\lambda_1, \lambda_2, \ldots \lambda_{s-1})$ (mod. $\sigma z$) and of as low an exponent as possible $r_s$. Then $(\sigma, \sigma z) = N(z) = z^n$ is of the $n^{th}$ degree, so there are $n$ and no more functions in $\sigma$ which are linearly independent of the module $\sigma z$ (§6), and therefore the sequence of functions $\lambda_1, \lambda_2, \lambda_3, \ldots$ can contain no more and no less than $n$ elements. Therefore we have (§5)

$$\sigma \equiv (\lambda_1, \lambda_2, \ldots \lambda_n) (\text{mod. } \sigma z)$$

The exponents $r_1, r_2, \ldots r_n$ of the functions $\lambda_1, \lambda_2, \ldots \lambda_n$ satisfy the condition

$$r_1 = 0, \quad 1 \leq r_2 \leq r_3 \ldots \leq r_n.$$
Each function in $\sigma$ of exponent of $< r$ is congruent with respect to the module $\sigma z$ to a function from the $(s - 1)$-fold family

$$(\lambda_1, \lambda_2, \ldots, \lambda_{s-1})$$

These functions $\lambda_1, \lambda_2, \ldots, \lambda_n$ form a basis of $\sigma$, as is apparent from the following consideration.

Were it not the case, one could determine (§3, 7.) a linear function $z - c$ and a system of constants $a_1, a_2, \ldots, a_n$, not all vanishing, such that

$$a_1\lambda_1 + a_2\lambda_2 + \ldots + a_n\lambda_n = (z - c)\omega.$$  

If $a_s$ is the last of the non-zero constants $a$, then we also have

$$a_1\lambda_1 + a_2\lambda_2 + \ldots + a_s\lambda_s = (z - c)\omega,$$

and the exponent of $\omega$ is of course less than $r_s$, (because $(z - c)\omega$ is contained in $\sigma$). Thus $\omega$ and consequently therefore $a_s$ are different from 0, also $\lambda_s$ is congruent to a function from the family $(\lambda_1, \lambda_2, \ldots, \lambda_{s-1}) \pmod{\sigma z}$, which is contrary to the assumption.

The functions $\lambda_1, \lambda_2, \ldots, \lambda_n$ therefore constitute a basis for $\sigma$ and this will be called a normal basis. The characteristic properties of the normal basis are:

I. The functions $\lambda_1, \lambda_2, \ldots, \lambda_n$ are linearly independent in the module $\sigma z$.

II. Every function in $\sigma$ whose exponent is less than the exponent $r_s$ of $\lambda_s$ is of the form

$$c_1\lambda_1 + c_2\lambda_2 + \ldots + c_{s-1}\lambda_{s-1} + z\omega_s$$

where $c_1, c_2, \ldots, c_{s-1}$ are constants and $\omega$ is a function in $\sigma$.

3. The functions

$$\lambda'_1 = \frac{\lambda_1}{z^{r_1}}, \quad \lambda'_2 = \frac{\lambda_2}{z^{r_2}}, \ldots, \lambda'_n = \frac{\lambda_n}{z^{r_n}},$$

contained in $\sigma'$ form a normal basis for $\sigma'$.

To be precise, if $\omega$ is a function in $\sigma$ of exponent $r$ that is not divisible by $z$, then the exponent of $\omega' = \frac{\omega}{z^{r'}}$ in terms of $z'$ is also $r$; because in fact $\frac{\omega'}{z^{r'}} = \omega$ is contained in $\sigma$ but not $\frac{\omega'}{z^{r'-1}} = \frac{\omega}{z}$. Since the functions $\lambda_1, \lambda_2, \ldots, \lambda_n$ are not all divisible by $z$, then consequently the exponents of $\lambda'_1, \lambda'_2, \ldots, \lambda'_n$ with respect to $z'$ are respectively $r_1, r_2, \ldots, r_n$. This said, we show that the system of functions $\lambda'_1, \lambda'_2, \ldots, \lambda'_n$ has the properties I. and II. when $\sigma$ and $z$ are replaced there by $\sigma'$ and $z'$.

If the condition I. were not satisfied, then let the constants $a_1, a_2, \ldots, a_n$, the last of which does not vanish, be determined so that

$$a_1\lambda'_1 + a_2\lambda'_2 + \ldots + a_n\lambda'_n = z'\omega'.$$
thus also (by multiplying by $z^{r_1^*}$)

$$a_1 z^{r_1^* - r_1} \lambda_1 + a_2 z^{r_2^* - r_2} \lambda_2 + \ldots + a_s \lambda_s = \omega,$$

in which

$$\omega = z^{r_1^* - 1} \omega',$$

thus we have a function in $\mathfrak{o}$ with an exponent less than $r$. However, this is impossible since $a_s$ is non-zero because of the assumption about $\lambda$, therefore the requirement I. is met; it follows from this that:

$$\mathfrak{o}' \equiv (\lambda_1', \lambda_2', \ldots, \lambda_n') \ (\text{mod. } \mathfrak{o}' z').$$

If the condition II. were not satisfied and $\lambda'$ were a function in $\mathfrak{o}'$ with exponent $r < r_1$, it is not of the form

$$a_1 \lambda_1' + a_2 \lambda_2' + \ldots + a_{s-1} \lambda_{s-1}' + z' \omega',$$

so you could choose $e \geq s$ such that

$$\lambda' = a_1 \lambda_1' + a_2 \lambda_2' + \ldots + a_e \lambda_e' + z' \omega'$$

with constant coefficients, the last of which $a_e$ does not vanish. In this way we also have $r_e \geq r > r.

Accordingly, $\lambda = z^{r_1^* - 1} \lambda'$ is a function in $\mathfrak{o}$ and multiplication by $z^{r_1^*}$ gives

$$z \lambda = a_1 z^{r_1^* - r_1} \lambda_1 + a_2 z^{r_2^* - r_2} \lambda_2 + \ldots + a_s \lambda_s + z^{r_1^* - 1} \omega'.$$

Therefore, $\omega = z^{r_1^* - 1} \omega'$ is a function in $\mathfrak{o}$ with exponent (according to 1.) $\leq r_1 - 1$ and that satisfies the congruence

$$\omega \equiv a_1' \lambda_1 + a_2' \lambda_2 + \ldots + a_s' \lambda_s \ (\text{mod. } \mathfrak{o} z),$$

wherein $a_e' = -a_e$ is non-zero. In this way, because of the property II. of the function $\lambda$, the exponent of $\omega$ must be $\geq r_1$, from which the contradiction is clear.

This establishes that the system of functions $\lambda_1', \lambda_2', \ldots, \lambda_n'$ forms a normal basis of $\mathfrak{o}'$.

4. We now form the discriminant of $\Omega$ with respect to the variables $z$ and $z'$ with the help of the two normal bases $\lambda$ and $\lambda'$; we have:

$$\Delta_z(\Omega) = \text{const.} \Delta(\lambda_1, \lambda_2, \ldots, \lambda_n),$$

$$\Delta_{z'}(\Omega) = \text{const.} \Delta(\lambda_1', \lambda_2', \ldots, \lambda_n').$$

But if we replace $\lambda_j'$ by the expression $z^{r_j^*} \lambda_j$, it then follows from the theorem §2, (13.) that

$$\Delta_{z'}(\Omega) = \text{const.} z^{2(r_1 + r_2 + \ldots + r_n)} \Delta_z(\Omega).$$

If $\Delta_z(\Omega)$ is of degree $\delta$, then $\Delta_{z'}(\Omega)$ has the root $z' = 0$ ($2(r_1 + r_2 + \ldots + r_n) - \delta$)-times, and from this it follows by §16, 2. that the branch number

$$w_z = 2(r_1 + r_2 + \ldots + r_n),$$

is thus always an even number.
§23. The differential quotient.

1. Since any non-zero function in the field \( \Omega \) has the value zero at only a finite number of points, it follows that a function in \( \Omega \) for which an infinite number of zeros can be established is necessarily identical to zero, or that two functions in \( \Omega \) which have the same value at an infinite number of points must be identical.

2. If \( \alpha \) and \( \beta \) are any two variables in the field \( \Omega \), then there exists in \( \Omega \) a function designated by \( \left( \frac{d\alpha}{d\beta} \right) \) which at an infinite number of points \( P \) satisfies the condition:

\[
\left( \frac{d\alpha}{d\beta} \right)_0 = \left( \frac{\alpha - \alpha_0}{\beta - \beta_0} \right)_0,
\]

which is called the differential quotient of \( \alpha \) by \( \beta \). To be precise, if \( F(\alpha, \beta) = 0 \) is an existing irreducible equation between \( \alpha \) and \( \beta \), then, when we initially exclude those points (of which only a finite number exist) in which either \( \alpha_0 \) or \( \beta_0 \) is \( 0 \) or \( F'(\alpha_0) \) or \( F'(\beta_0) \) is \( 0 \), we have

\[
0 = F(\alpha, \beta) = F(\alpha_0, \beta_0) + (\alpha - \alpha_0)F'(\alpha_0) + (\beta - \beta_0)F'(\beta_0)
+ \frac{1}{2} \{(\alpha - \alpha_0)^2F''(\alpha_0, \alpha_0) + 2(\alpha - \alpha_0)(\beta - \beta_0)F''(\alpha_0, \beta_0) + (\beta - \beta_0)^2F''(\beta_0, \beta_0)\} + \ldots
\]

Of the two quotients \( \left( \frac{\alpha - \alpha_0}{\beta - \beta_0} \right)_0 \) and \( \left( \frac{\beta - \beta_0}{\alpha - \alpha_0} \right)_0 \) one is certainly finite; if it is the former, then from the last equation we learned the following:

\[
0 = \frac{\alpha - \alpha_0}{\beta - \beta_0} F'(\alpha_0) + F'(\beta_0)
+ (\beta - \beta_0) \frac{1}{2} \left\{ \left( \frac{\alpha - \alpha_0}{\beta - \beta_0} \right)^2 F''(\alpha_0, \alpha_0) + 2 \left( \frac{\alpha - \alpha_0}{\beta - \beta_0} \right) F''(\alpha_0, \beta_0) + F''(\beta_0, \beta_0) + \ldots \right\} + \ldots,
\]

from which it follows for the point \( P \) that;

\[
\left( \frac{\alpha - \alpha_0}{\beta - \beta_0} \right)_0 = - \frac{F'(\beta_0)}{F'(\alpha_0)} = - \left( \frac{F'(\beta)}{F'(\alpha)} \right)_0
\]

if \( \left( \frac{\alpha - \alpha_0}{\beta - \beta_0} \right)_0 \) were to be infinite we would conclude likewise with reference to \( \frac{\beta - \beta_0}{\alpha - \alpha_0} \). Therefore

\[
(1.) \quad \left( \frac{d\alpha}{d\beta} \right)_0 = \frac{F'(\beta)}{F'(\alpha)}
\]

has the required property. This remains true even when one of the two functions \( \alpha \) or \( \beta \) is a constant; because if for example \( \alpha \) is a constant, then \( F(\alpha, \beta) = \alpha - \alpha_0 \) is independent of \( \beta \), so \( F'(\alpha) = 1 \), \( F'(\beta) = 0 \).
3. From the above it follows that if $\beta$ is not constant then except for a finite number of points $\left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0$ has a finite value. Therefore if $\gamma$ is a third variable in $\Omega$, then at infinitely many points

$$\left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0 = \left(\frac{\alpha - \alpha_0}{\gamma - \gamma_0}\right)_0 \left(\frac{\gamma - \gamma_0}{\beta - \beta_0}\right)_0,$$

including

$$\left(\frac{d\alpha}{d\beta}\right)_0 = \left(\frac{d\alpha}{d\gamma}\right)_0 \left(\frac{d\gamma}{d\beta}\right)_0.$$

But and from this and 1. the following identity is satisfied:

$$\left(2.\right) \left(\frac{d\alpha}{d\beta}\right) = \left(\frac{d\alpha}{d\gamma}\right) \left(\frac{d\gamma}{d\beta}\right).$$

4. As a result of these last theorems, we can assign to each of the functions $\alpha, \beta, \gamma, \ldots$ in the field $\Omega$ a function $d\alpha, d\beta, d\gamma, \ldots$ (the differential) in such a manner that in general we have

$$d\alpha = \frac{d\alpha}{d\beta} d\beta.$$

The differential of the constants, and only these, are set to zero; the remainder are completely determined once one of them is arbitrarily assumed. If between the variables $\alpha, \beta, \gamma, \ldots$ there exists a rational equation

$$F(\alpha, \beta, \gamma, \ldots)$$

then it follows from this that

$$\left(3.\right) F'(\alpha)d\alpha + F'(\beta)d\beta + F'(\gamma)d\gamma + \ldots = 0;$$

because in the same manner as in 2. one concludes that this equation is satisfied for infinite number of points.

The known rules for the differentiation of sums, differences, products and quotients follow immediately from the last theorem:

$$\left(4.\right) d(\alpha \pm \beta) = d\alpha \pm d\beta,$$

$$\left(5.\right) d(\alpha \beta) = \alpha d\beta + \beta d\alpha,$$

$$\left(6.\right) d\left(\frac{\alpha}{\beta}\right) = \frac{\beta d\alpha - \alpha d\beta}{\beta^2}.$$

---

1One can also define the differential quotient by the equation

$$\left(\frac{d\alpha}{d\beta}\right) = -\frac{F'(\beta)}{F'(\alpha)}$$

and by algebraic division obtain a proof of the theorem

$$\left(\frac{d\alpha}{d\beta}\right) = \left(\frac{d\alpha}{d\gamma}\right) \left(\frac{d\gamma}{d\beta}\right).$$
5. If $\omega$ is an integral function of $z$, then in general $\frac{d\omega}{dz}$ will not be an integral function of $z$. However it is apparent from the expression (§3, 7.)

$$\omega = x_1\omega_1 + x_2\omega_2 + \ldots + x_n\omega_n,$$

that the differential quotients of the integral rational functions $x_1, x_2, \ldots x_n$ are again integral rational functions so that the under-ideals of all of the functions $\frac{d\omega}{dz}$ must divide a certain ideal, namely the least common multiple of the under-ideals $\frac{d\omega_1}{dz}, \frac{d\omega_2}{dz}, \ldots, \frac{d\omega_n}{dz}$. Which ideal this is shall be investigated. To this end, let $z - c$ be an arbitrary linear function of $z$ and

$$o(z - c) = p^e p_1^{e_1} p_2^{e_2} \ldots,$$

where the prime ideals $p, p_1, p_2, \ldots$ are different from each other. If $\zeta$ was the same function as in §11, 2., that is an integral function of $z$ which has distinct values at the points $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \ldots$ generated by the prime ideals $p, p_1, p_2, \ldots$, and each of them only once, then let $\omega$ itself be represented in the form

$$\omega = y_0 + y_1\zeta + \ldots + y_{n-1}\zeta^{n-1},$$

where the rational functions $y_0, y_1, \ldots y_{n-1}$ of $z$ could in fact be fractional but the factor $z - c$ certainly could not be included in the denominator. From this it follows that the under-ideal of $\frac{d\omega}{dz}$ can be divisible by no higher powers of the ideals $p, p_1, p_2, \ldots$, than the under-ideal of $\frac{d\zeta}{dz}$. If, however

$$f(\zeta, z) = 0$$

is an irreducible equation between $\zeta$ and $z$, then by §11, 2.

$$o f'(\zeta) = mp^{e-1} p_1^{e_1-1} p_2^{e_2-1} \ldots$$

and $m$ is relatively prime to $p, p_1, p_2, \ldots$. However, since

$$\frac{d\zeta}{dz} = -\frac{f'(z)}{f'(\zeta)},$$

then the under-ideal of $\frac{d\zeta}{dz}$, and therefore also of $\frac{d\omega}{dz}$, contains none of the factors $p, p_1, p_2, \ldots$ more often than $(e - 1), (e_1 - 1), (e_2 - 1), \ldots$ times. Since $z - c$ can be any linear function, it follows that $\frac{d\omega}{dz}$ can have no other under-ideal than such as arises in the ramification ideal $\mathfrak{z} = \prod p^{e-1}$ (§11). We have, therefore, when $a$ represents an ideal:

$$\mathfrak{z} \frac{d\omega}{dz} = a.$$
so according to §11, (7.)

\[ \frac{d\omega}{dz} = e \alpha, \]

which shows that all the functions \( \frac{d\omega}{dz} \) belong to the module \( e \) complimentary to \( \alpha \).

6. If the irreducible equation \( F(w, z) = 0 \) between \( \omega \) and \( z \) is of the \( n \)th degree in \( \omega \) so that \( 1, \omega, \omega^2, \ldots \omega^{n-1} \) is a basis of \( \Omega \), then by §11 (10.)

\[ \alpha F'(\omega) = 3 \mathfrak{f}, \]

and therefore since

\[ \frac{d\omega}{dz} = -\frac{F'(z)}{F'(\omega)} \]

\( \alpha F'(z) \) must be divisible by the ideal \( \mathfrak{f} \),

\[ \alpha F'(z) = \mathfrak{f} \alpha, \]

we can therefore call \( \mathfrak{f} \) the **double point ideal** with respect to \( \omega \) and \( z \).

7. If \( \mathcal{P} \) is a point at which \( z - c \) is infinitely small of the first order (i.e. not a branch point in \( z \)), then from 5. all the functions \( \frac{d\omega}{dz} \) are finite at \( \mathcal{P} \). So if \( \eta \) is any function in \( \Omega \) which is finite at \( \mathcal{P} \), then this can be represented as a quotient of two integral functions \( \frac{\alpha}{\beta} \), of which \( \beta \) does not vanish at \( \mathcal{P} \), and therefore according to (6.) \( \frac{d\eta}{dz} \) is also finite at \( \mathcal{P} \).

8. Now let \( \alpha \) and \( \beta \) be any two variables in \( \Omega \), the behaviour of \( \frac{d\alpha}{d\beta} \) at any point \( \mathcal{P} \) shall be investigated.

Choose a variable \( z \) in \( \Omega \) which is infinitely small of the first order at \( \mathcal{P} \). If \( \alpha \) has a finite value \( \alpha_0 \) at \( \mathcal{P} \), then in accordance with §15, 1. and 2. we can determine a positive integer \( r \) and a non-zero function \( \alpha' \) which is finite at \( \mathcal{P} \) such that

\[ \alpha = \alpha_0 + z^r \alpha'. \]

This applies even if \( \alpha \) is infinite at \( \mathcal{P} \), for then \( r \) is just a negative integer and \( \alpha_0 \) is replaced by any finite constant, such as 0. Similarly, one can put

\[ \beta = \beta_0 + z^s \beta'; \]

\( r \) and \( s \) are then the order numbers of \( \alpha - \alpha_0 \) and \( \beta - \beta_0 \) at the point \( \mathcal{P} \), which can be positive as well as negative but not 0. From (2.) it then follows that:

\[ \frac{d\alpha}{d\beta} = z^{r-s} \frac{r\alpha' + z^s \omega'}{s\beta' + z^s \omega'} \]
or

\[
\frac{\beta - \beta_0}{\alpha - \alpha_0} \frac{d\alpha}{d\beta} = \frac{r + z \frac{d\alpha'}{\alpha'd\zeta}}{s + z \frac{d\beta'}{\beta'd\zeta}}
\]

Denoting again by the subscript 0 the value of a function at the point \( \mathfrak{P} \), then in accordance with 7.,

\[
\left( \frac{d\alpha'}{\alpha'd\zeta} \right)_0, \left( \frac{d\beta'}{\beta'd\zeta} \right)_0
\]

are finite,

\[
(7.) \quad \left( \frac{\beta - \beta_0}{\alpha - \alpha_0} \frac{d\alpha}{d\beta} \right)_0 = \frac{r}{s}
\]

is thus 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 between the order numbers of \( \alpha - \alpha_0 \) and \( \beta - \beta_0 \). If \( r \neq s \), then \( \left( \frac{\alpha - \alpha_0}{\beta - \beta_0} \right)_0 \) and consequently \( \left( \frac{d\alpha}{d\beta} \right)_0 \) are zero or infinity. If however \( r = s \), then both values are finite and different from zero, and we have therefore in all cases

\[
(8.) \quad \left( \frac{\alpha - \alpha_0}{\beta - \beta_0} \right)_0 = \left( \frac{d\alpha}{d\beta} \right)_0,
\]

in which \( \alpha_0 \) and \( \beta_0 \) are the values of \( \alpha \) and \( \beta \) at the point \( \mathfrak{P} \) when these values are finite, otherwise arbitrary constants such as 0.

9. If \( a \) and \( b \) are the order numbers of \( \alpha - \alpha_0 \) and \( \beta - \beta_0 \) at \( \mathfrak{P} \), then if \( a \) and \( b \) are positive, the point \( \mathfrak{P} \) occurs \((a - 1)\)-times, respectively \((b - 1)\)-times in the ramification polygons \( \mathfrak{Z}_\alpha \) and \( \mathfrak{Z}_\beta \) for \( \alpha \) and \( \beta \). But if \( a \) is negative, then \( \mathfrak{Z}_\alpha \) contains the point \( \mathfrak{P} \) \((-a - 1)\)-times, and similarly if \( b \) is negative (§16, 1.). Thus denoting by \( A \) and \( B \) the under-gons of \( \alpha \) and \( \beta \), since the order number of \( \frac{d\alpha}{d\beta} \) (as just demonstrated) is always equal to \( a - b \), one obtains the following expression for this function as a polygon quotient

\[
(9.) \quad \frac{d\alpha}{d\beta} = \frac{\mathfrak{Z}_\alpha A^2}{\mathfrak{Z}_\beta B^2}.
\]

§24.

The genus of the field \( \Omega \).

1. If we denote by \( w_\alpha \) and \( w_\beta \) the ramification numbers and by \( n_\alpha \) and \( n_\beta \) the orders of the variables \( \alpha \) and \( \beta \), then it follows from the formula (9.) of the previous §, since the numerator and the denominator of \( \frac{d\alpha}{d\beta} \) must contain the same number of points, that we have the important relation

\[
w_\alpha - 2n_\alpha = w_\beta - 2n_\beta;
\]
so if we also set
\[(1)\quad p = \frac{1}{2}w - n + 1,\]
which according to §22, 4. is an integer, then this is independent of the choice of variables and is a characteristic number for the field \(\Omega\) which is called the \textit{genus} of the field \(\Omega\). That this number is never negative will be seen when the value \(r_1 + r_2 + \ldots + r_n\) from §22 is substituted for \(\frac{1}{2}w\). We then obtain
\[(2)\quad p = (r_2 - 1) + (r_3 - 1) + \ldots + (r_n - 1),\]
which, since \(r_2, r_3, \ldots, r_n \geq 1\), cannot be negative.

2. Let \(\alpha\) and \(\beta\) be two functions in \(\Omega\) with orders \(m\) and \(n\), such that all functions in \(\Omega\) are represented rationally by \(\alpha\) and \(\beta\). Then
\[
F(\alpha, \beta) = a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n
\]
\[
= b_0\beta^m + b_1\beta^{m-1} + \ldots + b_{m-1}\beta + b_m = 0
\]
is an irreducible equation that exists between \(\alpha\) and \(\beta\) where \(a_0, a_1, \ldots, a_n\) are integral rational functions of \(\beta\) and \(b_0, b_1, \ldots, b_m\) are similarly integral rational functions of \(\alpha\).

Further, we have
\[
\alpha = \frac{A_1}{A}, \quad \beta = \frac{B_1}{B}
\]
where \(A_1\) is relatively prime to \(A\) and \(B_1\) to \(B\) so that \(A\) and \(B_1\) are of order \(m\) while \(B\) and \(B_1\) are of order \(n\). Then we have
\[
F'(\alpha) = na_0\alpha^{n-1} + (n - 1)a_1\alpha^{n-2} + \ldots + a_{n-1},
\]
\[
\alpha F'(\alpha) = -a_1\alpha^{n-1} - 2a_2\alpha^{n-2} + \ldots - na_n,
\]
which shows that
\[
F''(\alpha) = \frac{\mathfrak{K}}{A^{n-2}B^m}
\]
and likewise we must have
\[
F'(\beta) = \frac{\mathfrak{L}}{A^nB^{m-2}}.
\]
We now establish that the polygon \(\mathfrak{K}\) is divisible by \(\mathfrak{G}_\beta\) and \(\mathfrak{L}\) by \(\mathfrak{G}_\alpha\).

For \(\mathfrak{K}\), this is easy to see with the assumption that at every point of \(\mathfrak{G}_\beta\) the function \(\beta\) has a finite value and \(a_0\) is non-zero; for if
\[
\alpha' = a_0\alpha
\]
is an integral function of \(\beta\), and if one puts
\[
f(\alpha') = a^{n-1}F(\alpha, \beta)
\]
then we have
\[
f'(\alpha') = a_0^{n-2}F'(\alpha).
\]
Since now according to §11, 5. \( \sigma \beta' f'(\alpha') \) is divisible by the ramification ideal generated by \( \mathcal{Z}_\beta \), the validity of the assertion thus follows. The same holds for \( F'(\beta) \) by analogy.

If we now make arbitrary linear substitutions for \( \alpha \) and \( \beta \):

\[
\alpha = \frac{c + d\alpha'}{a + b\alpha'}; \quad \beta = \frac{c' + d'\beta'}{a' + b'\beta'}
\]

\[
(a + b\alpha')(d - b\alpha) = ad - bc,
\]

\[
(a' + b'\beta')(d' - b'\beta) = a'd' - b'c',
\]

then by §16, 2.

\[
\mathcal{Z}_\alpha = \mathcal{Z}_\alpha'; \quad \mathcal{Z}_\beta = \mathcal{Z}_\beta',
\]

and an irreducible equation exists between \( \alpha' \) and \( \beta' \):

\[
F'(\alpha', \beta') = (a + b\alpha')^n(a' + b'\beta')^m F(\alpha, \beta) = 0.
\]

In all circumstances, the constants \( a, b, c, d; \ a', b', c', d' \) can be chosen so that the assumptions stated above are satisfied for both \( \alpha' \) and \( \beta' \).

Because if the coefficients \( a_0' \) and \( b_0' \) of \( \alpha' \) and \( \beta' \) in \( F(\alpha', \beta') \) are put in the form

\[
a_0' = (a' + b'\beta')^m(a_0d^n + a_1d^{n-1}b + \ldots + a_nb^n) = \left( \frac{a'd' - b'c'}{d' - b'\beta} \right)^m(a_0d^n + a_1d^{n-1}b + \ldots + a_nb^n),
\]

\[
b_0' = (a + b\alpha')^n(b_0d'^m + b_1d'^{m-1}b' + \ldots + b_md'^{m}) = \left( \frac{ad - bc}{d - b\alpha} \right)^n(b_0d'^m + b_1d'^{m-1}b' + \ldots + b_md'^{m}),
\]

then it will be easily recognized that for only a finite number of values of the ratios \( d : b \) and \( d' : b' \) can the functions \( a_0' \) and \( d' - b'\beta \) vanish at a point in \( \mathcal{Z}_\beta \), and \( b_0' \) and \( d - b\alpha \) vanish at a point of \( \mathcal{Z}_\alpha \).

If we now put

\[
\alpha' = \frac{\mathfrak{A}'}{\mathfrak{A}}, \quad \beta' = \frac{\mathfrak{B}'}{\mathfrak{B}},
\]

then it follows (§19, 1.) that

\[
d - b\alpha = \frac{\mathfrak{A}'}{\mathfrak{A}}, \quad a + b\alpha' = \frac{\mathfrak{B}'}{\mathfrak{B}},
\]

so:

\[
\mathfrak{A}'\mathfrak{A}' = \mathfrak{A}\mathfrak{B}.
\]

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 \( \alpha \) (§15, 5.) and consequently

\[
\mathfrak{A}_2 = \mathfrak{A}' \quad \mathfrak{A}_2' = \mathfrak{A}.
\]
thus:
\[ a + b\alpha' = \frac{\mathfrak{A}}{\mathfrak{A}'} \]

and similarly:
\[ a' + b'\beta' = \frac{\mathfrak{B}}{\mathfrak{B}'} \]

But now, since \( F(\alpha, \beta) = 0 \), we have:
\[ F'(\alpha') = (ad - bc)(a + b\alpha')^{n-2} (a' + b'\beta')^m F'(\alpha), \]

and since, as was assumed:
\[ F'(\alpha') = \frac{\mathfrak{R} \mathfrak{S}_\beta}{\mathfrak{A}^{n-2} \mathfrak{B}^m}, \]

it follows that
\[ F'(\alpha) = \frac{\mathfrak{R} \mathfrak{S}_\beta}{\mathfrak{A}^{n-2} \mathfrak{B}^m} \]

and in the same manner
\[ F'(\beta) = \frac{\mathfrak{R} \mathfrak{S}_\alpha}{\mathfrak{A}^n \mathfrak{B}^{m-2}}. \]

The fact that the polygon \( \mathfrak{R} \) appearing in the numerator of both these expressions must be the same in both expressions, gives us
\[ \frac{d\alpha}{d\beta} = -\frac{F'(\beta)}{F'(\alpha)} = \frac{\mathfrak{B}^2 \mathfrak{S}_\alpha}{\mathfrak{A}^2 \mathfrak{S}_\beta}. \]

Now the order of the polygons \( \mathfrak{A}^{n-2} \mathfrak{B}^m \) is
\[ m(n - 2) + mn = 2m(n - 1), \]

So the order of \( \mathfrak{R} \)
\[ 2r = 2m(n - 1) - w_\beta \]

is always an even number, and from this we have
\[ (3.) \quad p = \frac{1}{2} w_\beta - n + 1 = (n - 1)(m - 1) - r. \]

The polygon \( \mathfrak{R} \) is called the **polygon of the double point** in \((\alpha, \beta)\).

§25.  The differentials in \( \Omega \).

If \( z \) and \( z_1 \) are any two variables in \( \Omega \) of orders \( n \) and \( n_1 \) and ramification numbers \( w \) and \( w_1 \), if also \( \mathfrak{S} \) and \( \mathfrak{S}_1 \) are the ramification polygons and \( \mathfrak{U} \) and \( \mathfrak{U}_1 \) the under-gons of \( z \) and \( z_1 \), then (§23)
\[ (1.) \quad \frac{dz}{dz_1} = \frac{\mathfrak{S} \mathfrak{U}_1^2}{\mathfrak{S}_1 \mathfrak{U}^2}. \]
Each function $\omega$ in $\Omega$ can be put in the form
\[
(2.) \quad \omega = \frac{U^2 \mathfrak{A}}{B \mathfrak{B}}
\]
where $\mathfrak{A}$ and $\mathfrak{B}$ are polygons whose orders $a$ and $b$ satisfy the condition
\[
2n + a = w + b
\]
or (§24)
\[
(3.) \quad a = b + 2p - 2.
\]
If we define a function $\omega_1$ by the equation
\[
\omega dz = \omega_1 dz_1,
\]
then for $\omega_1$ we get from (1.) the expression
\[
\omega_1 = \frac{U^2 \mathfrak{A}}{B_1 \mathfrak{B}}.
\]
In future, we call such expressions as $\omega dz = \omega_1 dz_1$

differentials in $\Omega$ and denote them symbolically by $d\omega$. As a result such a differential is invariant, i.e. acknowledged to be independent of the choice of the variable $z$ and completely determined by the two polygons $\mathfrak{A}$ and $\mathfrak{B}$.

We can without danger of misunderstanding use the symbolic expression
\[
d\omega = \frac{\mathfrak{A}}{\mathfrak{B}}.
\]
as also, for example,
\[
dz = \frac{B}{U^2}.
\]
This expression for a differential as a quotient of polygons is different from the similar expression for the functions in $\Omega$ (§17), in that in the latter the numerator and denominator are of the same order, whereas amongst the differentials the order of the numerator exceeds that of the denominator by $2p - 2$. As with the expression in §17, any common divisor which $\mathfrak{A}$ and $\mathfrak{B}$ have can also be suppressed here. If $\mathfrak{A}$ and $\mathfrak{B}$ are relatively prime, then $\mathfrak{A}$ is called the upper-gon and $\mathfrak{B}$ the under-gon of the differential $d\omega$.

Within the defined general concept of the differentials in $\Omega$ there is as well the special case as explained in §23, 4. of the differentials of functions in the field $\Omega$. These we call the proper differentials whilst the others, which cannot be represented as differentials of functions that exist in $\Omega$, will be known as improper or Abelian differentials.
Functions of the form (2.), which can be designated by \( \frac{d\tilde{\omega}}{dz} \) in accordance with our framework that has now been set up, we call the differential quotient with respect to \( z \) and we also distinguish between proper and improper differential quotients, depending on whether \( d\tilde{\omega} \) is a proper or improper differential. \(^1\)

Now comes the task of determining the scope of the concept of differentials, that is to find all polygons \( \mathcal{A} \) and \( \mathcal{B} \) that can be the over- and under-gons of a differential. We preface this with the following general observations:

The necessary and sufficient condition for \( \frac{\mathcal{A}}{\mathcal{B}} \) to be a differential, is that for any variable \( z \)

\[
\frac{\mathcal{U}^2 \mathcal{A}}{\mathcal{B} \mathcal{B}' } \text{ is a function in } \Omega, \text{ so that } \mathcal{U}^2 \mathcal{A} \text{ is equivalent to } \mathcal{B} \mathcal{B}'. \text{ This ratio continues to exist however when } \mathcal{A} \text{ and } \mathcal{B} \text{ are replaced by equivalent polygons } \mathcal{A}' \text{ and } \mathcal{B}'. \text{ If we fix } \mathcal{B} \text{ and } \frac{\mathcal{A}}{\mathcal{B}} \text{ is a differential, then }
\]

\[
\frac{\mathcal{A'}}{\mathcal{B'}} \frac{\mathcal{A''}}{\mathcal{B''}} \cdots
\]

will represent differentials if and only if the polygons \( \mathcal{A}, \mathcal{A}', \mathcal{A}'', \ldots \) all belong to the same class \( A \). If the polygons \( \mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \ldots \) form a basis for \( A \), thus

\[
A = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \ldots),
\]

then the corresponding differential quotients with respect to an arbitrary variable \( z, \frac{d\tilde{\omega}_1}{dz}, \frac{d\tilde{\omega}_2}{dz}, \frac{d\tilde{\omega}_3}{dz}, \ldots \), form the basis for a family of functions of finite dimension, and we will accordingly also call \( d\tilde{\omega}_1, d\tilde{\omega}_2, d\tilde{\omega}_3, \ldots \) a basis for a family of differentials

\[
(d\tilde{\omega}_1, d\tilde{\omega}_2, d\tilde{\omega}_3, \ldots)
\]

of the same dimension. This implies that each differential \( d\tilde{\omega} \), whose under-gon is \( \mathcal{B} \) or a divisor of \( \mathcal{B} \), can be expressed in the form

\[
d\tilde{\omega} = c_1d\tilde{\omega}_1 + c_2d\tilde{\omega}_2 + c_3d\tilde{\omega}_3 + \ldots
\]

with constant coefficients \( c_1, c_2, c_3, \ldots \)

---

\(^1\)The quotient of any two proper or improper differentials \( \frac{d\tilde{\omega}}{dz} \) has always emphasized the importance of a particular function in \( \Omega \). We limit ourselves in the following, however, to the consideration of such quotients in which at least the denominator is a proper differential.
§26.
The differentials of the first kind.

We first consider the simplest of the differentials in $\Omega$, namely those whose under-gon is the null-gon $\mathcal{O}$. Such differentials (whose existence has yet to be proved of course) are called differentials of the first kind. The over-gon $\mathcal{W}$ of such a differential $d\omega$ whose order is $2p - 2$, will be referred to as the fundamental polygon of $d\omega$ and is called a complete polygon of the first kind, while each divisor of one such will be called simply a polygon of the first kind. If $\mathcal{W} = \mathfrak{A}\mathfrak{B}$ then $\mathfrak{A}$ and $\mathfrak{B}$ are called complementary polygons of each other. A polygon that is not a divisor of a complete polygon of the first kind, thus in particular each polygon of more than $2p - 2$ points, is called a polygon of the second kind.

1. From the above remarks, all the complete polygons of the first kind form a polygon class $W$ whose dimension is to be determined; if this dimension is $> 0$ then at the same time the existence of the polygons of the first kind will have been demonstrated. But this dimension is the same as the dimension of the family of differentials of the first kind, or also, for any variable $z$, the family of differential quotients of the first kind, when we define as differential quotients of the first kind with respect to $z$ the functions

$$u = \frac{d\omega}{dz}.$$ 

Such a function $u$ has from §25, (2.) the expression

$$u = \frac{U^2 \mathcal{W}}{Z},$$

and it can easily be seen from the observation of order numbers at the different points that such a differential coefficient of the first kind is completely defined by the following two properties:

I. For each point $\Psi$ at which $z$ has a finite value $z_0$, we have

$$(u(z - z_0))_0 = 0.$$ 

II. For a point $\Psi$ at which $z$ is infinite, we have

$$(zu)_0 = 0$$

If we set as in §11, 4.

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

to represent the product of all the distinct linear factors of the discriminant $\Delta_z(\Omega)$, and $r$ the product of all the distinct prime ideals dividing $r$, then the condition I. is tantamount to the requirement that $ru$ be a function in $r$, or that $u$ must be a function in the module $e$ complementary to $o$ (§11, 4. (6.)). In order to obtain the
totality of functions \( u \), one has to find those amongst the functions in \( e \) that satisfy the condition II.

2. For this purpose we use a normal basis, \( \lambda_1, \lambda_2, \ldots, \lambda_n \), underlying \( o \) (§22) and designate the complementary basis of this by \( \mu_1, \mu_2, \ldots, \mu_n \), so that each function satisfies the condition I., thus also each differential quotient of the first kind is of the form

\[
(1.) \quad u = y_1\mu_1 + y_2\mu_2 + \ldots + y_n\mu_n
\]

where \( y_1, y_2, \ldots, y_n \) are integral rational functions of \( z \). But from the fundamental properties of the complementary basis (§10, 3.) we have

\[
y_s = S(u\lambda_s); \quad \frac{y_s}{z^{r_s-1}} = S\left(uz, \frac{\lambda_s}{z^{r_s}}\right).
\]

Now \( \frac{\lambda_s}{z^{r_s}} \) is contained in \( o' \) and thus is finite for \( z = \infty \), and from II. \( uz \) vanishes at each such point, thus it follows (§16, 5.) that \( \frac{y_s}{z^{r_s-1}} \) must vanish for \( z = \infty \), i.e. that the degree of the integral rational function \( y_s \) cannot exceed \( r_s - 2 \).

If \( r_s < 2 \) then \( y_s \) must vanish, so under all circumstances we have (§22, 2.)

\[
y_1 = 0; \quad S(u) = 0
\]

(Abel’s theorem for differentials of the first kind) and, if \( r_s \geq 2 \):

\[
(2.) \quad y_s = c_0 + c_1 z + c_2 z^2 + \ldots + c_{r_s-2} z^{r_s-2}.
\]

It has yet 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, equivalently, that if \( r_s \geq 2 \), then \( z^{r_s-1}\mu_s \) vanishes at all points where \( z \) is infinite. This is shown immediately by considering the integral functions of \( z' = z^2 \) from the system \( o' \), for which according to §22, 3. the functions

\[
\lambda'_1 = \frac{\lambda_1}{z'^1}, \quad \lambda'_2 = \frac{\lambda_2}{z'^2}, \ldots, \lambda'_n = \frac{\lambda_n}{z'^n}
\]

form a normal basis. The complementary basis for this is, according to §10, 5.,

\[
\mu'_1 = z'^1\mu_1, \quad \mu'_2 = z'^2\mu_2, \ldots, \mu'_n = z'^n\mu_n,
\]

and since (by applying the property I., to \( z' \) and \( \mu' \)) we have

\[
z'\mu'_1 = 0 \quad \text{for} \quad z' = 0,
\]

it follows that

\[
z^{r_s-1}\mu_s = 0 \quad \text{for} \quad z = \infty
\]

Q.E.D.
However, since the functions \( z^h \mu_s \), are linearly independent (because of the rational independence of the functions \( \mu_s \)), §24, (2.) gives us the following fundamental theorem:

*the dimension of the family of differentials of the first kind is*

\[
(r_2 - 1) + (r_3 - 1) + \ldots + (r_n - 1) = p,
\]

and therefore \( p \) is also the dimension of the class \( W \) of the complete polygons of the first kind.

As the basis for the family of the differential coefficients 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 \( \mathfrak{W}_1, \mathfrak{W}_2, \ldots \mathfrak{W}_p \) of the associated differentials \( d\tilde{\omega} \) form a basis of class \( W \).

3. For future application, the special case of a type of differential coefficient of the first kind \( u' \) shall be considered, that is when the condition II. is replaced by this more specific condition.

III. For each point \( \mathfrak{P} \) at which \( z \) is infinite, we require that

\[
(z^k u')_0 = 0,
\]

where \( k \) a given positive integer.

The functions \( u' \) can be represented by

\[
u' = \frac{u^{k+1} \mathfrak{W}'}{3}
\]

and likewise form a family; in the same way the polygons \( \mathfrak{W}' \) form a class \( W' \), whose order is

\[
w - n(k + 1) = 2p - 2 - n(k - 1).
\]

The polygons \( \mathfrak{W}' \) are not however independent of the choice of variable \( z \). The dimension of the class \( W' \) can be determined by the same method as that of the class \( W \). That is, since the condition I. is met, the functions \( u' \) are also included 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 rational function \( y_s \) cannot exceed the number \( r_s - k - 1 \). Thus \( y_s \) vanishes identically if \( r_s < k + 1 \); otherwise

\[
y_s = c_0 + c_1 z + \ldots + c_{r_s-k-1} z^{r_s-k-1}.
\]

Conversely, if \( y_s \) has this form, then the condition III. will be satisfied by the function

\[
u' = \sum y_s \mu_s,
\]
then, as demonstrated in 2.,
\[ z^k (z^{r_s - k - 1} \mu_s) = z^{r_s - 1} \mu_s \]
has the value 0 for \( z = \infty \).

It follows from this that the dimension of the family of functions \( u' \) and consequently the class \( W' \) is
\[ = \sum_i (r_i - k), \]
in which however only those terms in the sum that have a positive value are retained. If all the \( r_i - k \leq 0 \), then in general the required functions do not exist.

§27.
Polygon classes of the first and second kind.

If \( \mathfrak{A} \) is a polygon of the first kind then all polygons equivalent to \( \mathfrak{A} \) are also of the first kind. Because if \( \mathfrak{A} \) and \( \mathfrak{B} \) are complementary polygons and
\[ \mathfrak{A} \mathfrak{B} = \mathfrak{W}, \]
then if \( A \) and \( B \) are the classes of \( \mathfrak{A} \) and \( \mathfrak{B} \):
\[ A B = W, \]
and if \( \mathfrak{A}' \) is equivalent to \( \mathfrak{A} \) then \( \mathfrak{A}' \mathfrak{B} = \mathfrak{W}' \) is also equivalent to \( \mathfrak{W} \) (§18, 5.).

We therefore call such classes which contain polygons of the first kind polygon classes of the first kind, and the remainder polygon classes of the second kind. The class \( W \) of the complete polygons of the first kind is called the principal class and the two classes \( A \) and \( B \), satisfying the condition
\[ A B = W \]
complementary classes. If
\[ \eta = \frac{\mathfrak{A}'}{\mathfrak{A}} \]
is a function in \( \Omega \) and \( \mathfrak{A}' \) is relatively prime to \( \mathfrak{A} \), thus the class \( A \) of \( \mathfrak{A} \) is proper, then we call \( \eta \) a function of the first or second kind depending on whether the class \( A \) is of the first or second kind.

If \( A \) is any class of the first kind and \( q \) is the number of polygons \( \mathfrak{W} \) that are independent of each other and divisible by any polygon \( \mathfrak{A} \) from the class \( A \), then by §21, 2.
\[ q = (A, W) = (O, B) \]
i.e. equal to the dimension of the class \( B \) complementary to \( A \). Similarly \( (B, W) \) is equal to the dimension of 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. each class whose order is \( \leq p - 1 \) is of the first kind, and there are in the particular case of class \( A \) the sort of order \( p - k \) such that \( (A, W) = (O, B) = k \). It follows from a similar theorem that there are classes of order \( p \) which are of the second kind.
§28.  
The Riemann-Roch theorem for proper classes.

The Riemann-Roch theorem, which in its usual form gives the number of arbitrary constants included in a function that will be infinite at a certain number of given points, according to our account contains a relationship between the dimension and the order of a class and respectively a class and its complementary class. Whilst we restrict ourselves initially to a discussion of proper classes, we preface the derivation of this fundamental relation with the following remarks.

1. In a proper class \( A \), according to §19, one can always choose two polygons \( A \) and \( A' \) that are relatively prime to each other (one of them can be assumed to be in an arbitrary class). Then put

\[
z = \frac{A'}{A}
\]

and if \( A'' \) represents any third polygon of the class \( A \):

\[
\omega = \frac{A''}{A}, \quad \frac{\omega}{z} = \frac{A''}{A'}
\]

then according to §17 \( \omega \) is an integral function of \( z \) and \( \frac{\omega}{z} \) is an integral function of \( \frac{1}{z} \). Therefore (§22) the exponent of \( \omega \) is \( \leq 1 \).

Conversely, if \( \omega \) is an integral function of \( z \) whose exponent is \( \leq 1 \), then it has the form

\[
\omega = \frac{A''}{A}
\]

where \( A'' \) is a polygon of class \( A \). If say

\[
\omega = \frac{A''}{A_1}, \quad \frac{\omega}{z} = \frac{A''}{A_1} \frac{A}{A'}
\]

and \( A'' \) is assumed to be relatively prime to \( A_1 \), then at first, since \( \omega \) should be an integral function of \( z \), \( A_1 \) cannot contain a point that is not also contained in \( A \). In addition, \( A_1 \) cannot include a point more often than \( A \), because otherwise \( \frac{\omega}{z} \) may be infinite at such a point (which cannot be present in \( A_1 \)), so would not be an integral function of \( \frac{1}{z} \). Therefore, \( A \) is divisible by \( A_1 \) and \( \omega \) can be put in the form \( \frac{A''}{A} \).

2. So to get the totality of the polygons of class \( A \) we have to consider only those integral functions of \( z \) whose exponent is \( \leq 1 \).

If \( n \) is the order of the class \( A \), hence the order of the variable \( z \), and \( \lambda_1, \lambda_2, \ldots, \lambda_n \) form a normal basis of \( o \) with exponents \( r_1, r_2, \ldots, r_n \) including \( r_s \), the last for
which it is \( \leq 1 \), then, any function \( \omega \) with an exponent \( \leq 1 \) can by \( \S 22, 2. \) be expressed in the form

\[
\omega = c_1\lambda_1 + c_2\lambda_2 + \ldots + c_s\lambda_s + z\omega_1.
\]

Since the exponent of \( z\omega_1 \) cannot be greater than 1, \( \omega_1 \) must be a constant and therefore

\[
\omega = c_1\lambda_1 + c_2\lambda_2 + \ldots + c_s\lambda_s + c_{s+1}z.
\]

Conversely, every function of this form satisfies the stated requirement. Accordingly, the dimension of the class \( A \) is thus \( s + 1 \), which, in keeping with \( \S 21, 1. \), is always \( \leq n + 1 \). The upper limit \( n + 1 \) can actually be reached, but only in the case \( p = 0 \), because in this case \( r_2, r_3, \ldots r_n = 1 \). From this we have that \( p = 0 \) for a single point \( \mathfrak{P} \) only, when it belongs to a proper class.

3. If amongst the exponents \( r_{s+1}, r_{s+2}, \ldots r_n \), there is one that is greater than 2, then of course \( r_n > 2 \) also, and, in accordance with \( \S 26, 2. \), when \( \mathfrak{R} \) is the ramification polygon with respect to \( z \),

\[
\mu_n = \frac{\mathfrak{A}^2 \mathfrak{W}}{\mathfrak{R}}, \quad \mu_n z = \frac{\mathfrak{A}^2 \mathfrak{W}_1}{\mathfrak{R}} = \frac{\mathfrak{A} \mathfrak{A}' \mathfrak{W}}{\mathfrak{R}}
\]

are differential quotients of the first kind with respect to \( z \), thus

\[
\mathfrak{A}\mathfrak{W}_1 = \mathfrak{A}'\mathfrak{W}
\]

or, as \( \mathfrak{A} \) and \( \mathfrak{A}' \) 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 \( (z \) is a variable of the first kind). Therefore, if we initially make the assumption that \( A \) is a class of the second kind, then it follows that

\[
r_{s+1} = 2, \quad r_{s+2} = 2, \ldots r_n = 2
\]

and

\[
p = (r_2 - 1) + \ldots + (r_s - 1) + (r_{s+1} - 1) + \ldots + (r_n - 1) = n - s.
\]

The dimension \( s + 1 \) of the class \( A \) is therefore given by

\[
(O, A) = n - p + 1.
\]

4. Secondly, if we make the assumption that \( A \) is of the first kind and, as in \( \S 27 \)

\[
q = (A, W),
\]

then there exist \( q \) linearly independent complete polygons of the first kind that are divisible by \( \mathfrak{A} \) and the corresponding differential coefficients of the first kind with
respect to $z$, of which $q$ and no more are likewise linearly independent, have the form

$$v = \frac{\mathfrak{A}^2 \mathfrak{B}}{\mathfrak{B}},$$

where $\mathfrak{B}$ is a polygon with $2p - 2 - n$ points; the class $B$ of $\mathfrak{B}$ is the complementary class to $A$, and therefore its dimension is equal to $q$ ($\S 27$).

These functions $v$ have the property that at the vertices of $\mathfrak{A}$, i.e. for $z = \infty$, not only $zv$ but also

$$z^2v = \frac{\mathfrak{A}^2 \mathfrak{B}^2}{\mathfrak{B}},$$

vanishes, and are completely determined by this and by the requirement to be a differential quotient of the first kind. For we have

$$v = \frac{\mathfrak{A}^2 \mathfrak{W}}{\mathfrak{B}}, \quad vz^2 = \frac{\mathfrak{A}^2 \mathfrak{W}}{\mathfrak{B}},$$

thus, as $z^2v$ vanishes at all points of $\mathfrak{A}$, $\mathfrak{W}$ must be divisible by $\mathfrak{A}$ since $\mathfrak{A}'$ is assumed to be relatively prime to $\mathfrak{A}$. Therefore, according to $\S 26$, 3. we have:

$$q = (r_{s+1} - 2) + (r_{s+2} - 2) + \ldots + (r_n - 2),$$

on the other hand

$$p = (r_{s+1} - 1) + (r_{s+2} - 1) + \ldots + (r_n - 1),$$

consequently

$$p - q = n - s, \quad s = n - p + q.$$  

The Riemann-Roch theorem is included in this, which for this case and taking $\S 27$ into account, we can express in the following way: If $A$ and $B$ are complementary classes of the first kind of which at least one is proper, and $a$ and $b$ are their orders, i.e.

$$a + b = 2p - 2,$$

then

$$(O, A) - \frac{1}{2}a = (O, B) - \frac{1}{2}b.$$  

5. If we include the case $(A, W) = 0$, we can combine the Riemann-Roch theorem for both cases as follows:

If $A$ is a proper class of order $n$, then its dimension is given by

$$(O, A) = n - p + 1 + (A, W).$$

Since the dimension of a proper class (provided only that it does not come from the null-gon) must be at least 2, then if $(A, W) = 0$, it follows that

$$n \geq p + 1$$
and from that, the theorem due to Riemann:

Any function whose order is \( \leq p \) is a function of the first kind.

6. With the help of this theorem it is easy to prove that the principal class \( W \) of a complete polygon of the first kind is always proper.

That is, if \( \mathfrak{M} \) divides \( W \), then in accordance with §19, 2, we can find in \( W \) a polygon of the form \( \mathfrak{A} \mathfrak{M} \) such that \( \mathfrak{A} \) is relatively prime to \( \mathfrak{M} \). The class \( \mathfrak{A} \) of \( \mathfrak{A} \) is a proper one (§21, 3.), and at the same time \( \mathfrak{A} \mathfrak{M} \) is the only polygon of class \( W \) divisible by \( \mathfrak{A} \) (because each polygon in \( W \) has the divisor \( \mathfrak{M} \)). So we have

\[
(A, W) = 1.
\]

Now if \( p \) is the dimension of \( W \) and also that of \( A \), then by the Riemann-Roch theorem the order of \( A \) is equal to \( 2p - 2 \), i.e. as large 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 divisor \( \mathfrak{M} \) and

\[
A = \mathfrak{M} A',
\]

then \( A' \) is a proper class of the first kind. Let \( B \) be the complementary class of \( A; \)
\( B' \) that of \( A' \); \( a \) and \( b \) the orders of the classes \( A \) and \( B; \) \( m \) the order of \( \mathfrak{M} \). The whole class \( B \) is obtained if for all of the polygons of class \( B' \) that are divisible by \( \mathfrak{M} \) the factor \( \mathfrak{M} \) is suppressed, then we have

\[
\mathfrak{A} \mathfrak{B} = \mathfrak{A'} \mathfrak{M} \mathfrak{B} = \mathfrak{W},
\]

thus \( \mathfrak{M} \mathfrak{B} \) belongs to the class \( B' \), and vice versa, when

\[
\mathfrak{A'} \mathfrak{B'} = \mathfrak{A} \mathfrak{M} \mathfrak{B} = \mathfrak{W}
\]

then \( \mathfrak{B} \) belongs to the class \( B \).

From this we have from §21, 2.

\[
(O, B) \geq (O, B') - m
\]

Now \( A' \) is a proper class of the same dimension as \( A \) and of the order \( a - m \), thus (§28, 5.)

\[
(O, A) = (O, A') = a - m - p + 1 + (A', W),
\]

or

\[
(O, A) = (O, B') - m + a - p + 1;
\]

therefore

\[
(O, A) \leq (O, B) + a - p + 1 = (O, B) + \frac{1}{2}(a - b)
\]
so
\[(O, A) - \frac{1}{2}a \leq (O, B) - \frac{1}{2}b.\]

But as the classes \(A\) and \(B\) can be swapped with each other, it follows in a similar fashion that
\[(O, B) - \frac{1}{2}b \leq (O, A) - \frac{1}{2}a,
\]
that is,
\[(O, A) - \frac{1}{2}a = (O, B) - \frac{1}{2}b,
\]
thus the Riemann-Roch theorem is generally established in the same form as in §28, 4 for Polygon classes of the first kind. ¹

§30.
Improper classes of the second kind.

Now the condition will be investigated under which a polygon class \(A\) of the second kind of order \(n\) can in any way be improper, from which the general validity of the Riemann-Roch theorem will result automatically.

1. Any class \(A\) can always be transformed into a proper class \(AN\) by multiplication by another class \(N\) of order \(v\). Because if \(\mathfrak{A}\) is an arbitrary polygon in \(A\), then choose a variable \(z\) which remains finite at all points of \(\mathfrak{A}\) (§15, 6.). Then if \(\eta\) is an arbitrary function in the ideal generated by \(\mathfrak{A}\) with respect to \(z\), the over-gon of \(\eta\) is divisible by \(\mathfrak{A}\) and hence is of the form \(\mathfrak{A}N\), and the class of \(\mathfrak{A}N\) is a proper one.

2. The dimension of the proper class of the second kind \(AN\) is according to §28, 3.
\[(O, AN) = n + v - p + 1,\]
and it follows from this according to §21, 2. that
\[(O, A) \geq n - p + 1.
\]
Now if the divisor \(\mathfrak{M}\) of the class \(A\) is of order \(m\), and
\[A = \mathfrak{M}A',\]
then \(A'\) is a proper class of the same dimension as \(A\), and consequently (§28, 5.)
\[(O, A) = (O, A') = n - m - p + 1 + (A', W),\]

¹In the terminology of Christoffel (On the canonical form of Riemann integrals of the first kind, Annali di Matematica pura ed applicata, Series II, Tomo IX)
\[(A, W) + a - p = (O, B) + a - p = (O, A) - 1
\]
is the “excess”, and
\[(A, W) - 1 = (O, B) - 1
\]
is the “defect” of the system of points \(\mathfrak{A}\).
so
\[(A', W) \geq m,\]
that is \(A'\) must certainly be of the first class if \(A\) is an improper class. If \(B'\) is the
complementary class of \(A'\), then also
\[(O, B') \geq m.\]
But if \((O, B')\) were \(> m\), then by §20, 2. we would be able to find a polygon \(M \mathcal{B}\)
in \(B'\) that was divisible by \(M\) and we would have
\[\mathfrak{A} \mathcal{M} \mathcal{B} = \mathfrak{A} \mathcal{B} = \mathfrak{M},\]
so \(A\) would be of the first kind, contrary to the assumption. Therefore
\[(A', W) = m\]
and hence
\[(O, A) = n - p + 1,\]
where again in this case the Riemann-Roch theorem is given exactly in the form of
§28, 3.

3. If the class \(A\) contains only a single isolated polygon, then \((O, A) = n - p + 1 = 1\),
therefore \(n = p\), i.e. an isolated polygon of the second kind always
has order \(p\). Conversely, from 2., any polygon of the second kind of order \(p\) is an
isolated one.

4. Keeping to the definitions in 2., if \((O, B') = m\) and using the frequently
applied theorem (§20, 2.), a polygon can therefore be found in \(B'\) that is divisible
by an arbitrary \((m - 1)\)-gon. Picking an arbitrary point \(P\) of \(M\) we put
\[\mathfrak{M} = \mathfrak{P} \mathcal{M}',\]
then a polygon \(\mathfrak{M} \mathcal{B}'\) is contained in \(B'\) and thus
\[\mathfrak{A} \mathfrak{M} \mathcal{B} = \mathfrak{M}.\]
The polygon \(\mathfrak{A} \mathfrak{M}' = \mathfrak{A}'\) and its class \(A''\) are therefore of the first kind, and, if \(P\)
is the class of \(\mathfrak{P}\), \(A\) has the form
\[A = P A''.\]
At the same time we must have \((A'', W) = (O, B'') = 1\), i.e. the complementary
class \(B''\) of \(A''\) contains only a single isolated polygon \(\mathfrak{B}''\), otherwise there would
be a polygon in \(B''\) that was divisible by \(\mathfrak{P}\), and thus \(A\) would be of the first kind,
contrary to the assumption.

5. Conversely, if \(A''\) is a class of the first kind for which \((A'', W) = 1\), then
the complementary class \(B''\) of \(A''\) consists of an isolated polygon \(\mathfrak{B}''\); if also \(\mathfrak{P}\) is
a point not occurring in $\mathfrak{B}''$ and $P$ is its class, then $A = PA''$ is an improper class of the second kind of order $n$ in which the divisor $\mathfrak{P}$ occurs.

That $A$ is of the second kind is evident from the initial assumption that $\mathfrak{P}$ does not occur in $\mathfrak{B}''$. The dimension of $A$ is therefore from 2.,

$$(O, A) = n - p + 1,$$

where $n$ is the order of $A$; on the other hand, the dimension of the class $A''$ according to §§28 and 29, is:

$$(O, A'') = n - p + (A'', W) = n - p + 1;$$

thus $A$ and $A''$ are of the same dimension. All polygons in the class $A''$ are transformed by multiplication by $\mathfrak{P}$ into polygons in the class $A$, and because of the equality of dimensions, this also completely exhausts the latter class. Hence all polygons of the class $A$ have the factor $\mathfrak{P}$, it therefore also occurs in the divisor of $A$.

6. In the particular case where the genus $p$ of the field $\Omega$ has the value 0, polygons and classes of the first kind do not appear at all. Therefore in this case there are no improper classes. The dimension of each class is 1 greater than its order. In particular, every point $\mathfrak{P}$ thus belongs to a proper class of dimension 2 and therefore there exist in this case functions $z$ in $\Omega$ which are of the first order. Any other function in the field can be rationally expressed in terms of one such, because between $z$ and another variable in the field there exists an irreducible equation of the first degree with respect to the latter (§15, 7.).

§31.
Differentials of the second and third kind.

1. We now have from §25 the well-established relationship

$$d\omega = \frac{\mathfrak{A}}{\mathfrak{B}}$$

for any differential in $\Omega$, thus, when $a$ and $b$ are the orders of $\mathfrak{A}$ and $\mathfrak{B}$, we have

$$a = b + 2p - 2,$$

and if $\mathfrak{A}$ and $\mathfrak{B}$ are assumed to be relatively prime, then, if $\mathfrak{U}$ and $\mathfrak{Z}$ represent the under-gon and ramification polygon for any variable $z$, $\mathfrak{U^2A}$ must be equivalent to $\mathfrak{ZB}$ (§25). Denoting then by $U$, $Z$, $A$ and $B$ the classes of the polygons $\mathfrak{U}$, $\mathfrak{Z}$, $\mathfrak{A}$ and $\mathfrak{B}$, we must have

$$U^2A = ZB.$$

On the other hand however, when $W$ is the principal class of the first kind, we have

$$U^2W = Z.$$
resulting in the relation
\[ A = BW. \]
Conversely, if \( A \) is any polygon in the class \( BW \), then the equivalence of \( \frac{A}{B} \) in \( \mathcal{B} \) follows from this, hence the existence of a differential with the expression \( \frac{A}{B} \).

From this we have that \( B \) can be the under-gon of a differential \( d\omega \) if and only if there exists in \( BW \) a polygon relatively prime to \( B \), i.e. if the divisor of the class \( BW \) is relatively prime to \( B \). Therefore the dimension of the class \( BW \) gives at the same time the dimension of the family of differentials \( d\omega \) associated with the under-gon \( B \) (§25). Since \( (W, W) = 1 \), the theorems §30, 4. and 5. provide the following result.

a) If \( B \) consists of a single point \((b = 1)\), then the class \( BW \) is improper with the divisor \( B \), thus the order \( b \) of the under-gon of a differential \( d\omega \) 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 arbitrary polygon with more than one point can be the under-gon of a differential, and there exist amongst them \( b + p - 1 \) linearly independent differentials associated with an under-gon of order \( b \).

2. With the assumption that \( b \geq 2 \), we now look for a basis for the class \( A \) of the kind that each element \( A_r \) of this basis is a differential \( d\omega_r \) of the simplest type, i.e. one whose under-gon is a power of a single point or product of only two different points.

Suppose that such a basis for the class \( BW \) has already been found
\[ (1.) \quad A_1, A_2, A_3, \ldots, A_{b+p-1}, \]
then, if \( P \) is the class of an arbitrary point \( \mathcal{P} \), we construct a similar basis from it for the class \( BPW \) of dimension \( b + p \), that is
\[ (2.) \quad PA_1, PA_2, \ldots, PA_{b+p-1}, A'. \]
The first \( b + p - 1 \) of these polygons really belong to the class \( BPW \) and are independent of each other since the polygons (1.) are, at the same time the differentials built from them
\[ d\omega_r = \frac{P}{P\mathcal{B}} \frac{A_r}{A_r} = \frac{A_r}{\mathcal{B}} \]
are identical to those formed from (1.). Thus it depends only on the form of \( \mathcal{A}' \) to distinguish between the two cases.

a) If \( \mathcal{P} \) divides \( \mathcal{B} \) and \( \mathcal{B} = M\mathcal{P}^m \) where \( M \) is not divisible by \( \mathcal{P} \), then \( P^{m+1}W \) is a proper class (while \( m + 1 \geq 2 \), §30, 4.) in which there is therefore a polygon \( \mathcal{A} \) that is not divisible by \( \mathcal{P} \); if we now put \( \mathcal{A}' = M\mathcal{A} \) so that \( \mathcal{A}' \)
belongs to the class $BPW$ and is not divisible by $\mathfrak{P}$ and thus not in the family $(\mathfrak{PA}_1, \mathfrak{PA}_2, \ldots \mathfrak{PA}_{b+p-1})$ of which $\mathfrak{P}$ is a divisor; consequently the polygons (2.) are independent of each other, and since they number $b + p$ they form a basis of the class $BPW$. The differential constructed from $\mathfrak{A}'$

$$d\tilde{\omega}' = \frac{\mathfrak{A}'}{\mathfrak{PB}} = \frac{\mathfrak{A}}{\mathfrak{PP}_1}$$

has the required form since its under-gon is a power of a single point.

b) If $\mathfrak{P}$ does not divide $\mathfrak{B}$, then choose once and for all a point $\mathfrak{P}_1$ from $\mathfrak{B}$ and set $\mathfrak{B} = \mathfrak{MP}_1$ (irrespective of whether the $\mathfrak{M}$ is divisible by $\mathfrak{P}_1$ or not). Then choose in the proper class $PP_1W$ a polygon $\mathfrak{A}$ that is not divisible by $\mathfrak{P}$ or $\mathfrak{P}_1$, so $\mathfrak{A'} = \mathfrak{MN}$ 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 for $BPW$. At the same time

$$d\tilde{\omega}' = \frac{\mathfrak{A}'}{\mathfrak{PB}} = \frac{\mathfrak{A}}{\mathfrak{MP}_1}$$

is thus of the required form.

It now remains to describe the beginning of this operation. If $b = 0$, that is $\mathfrak{B} = \mathfrak{O}$, then

$$BW = W = (\mathfrak{W}_1, \mathfrak{W}_2, \ldots \mathfrak{W}_p)$$

(the principal class of the first kind).

If $b = 2$, then choose from the proper class $BW$ a polygon $\mathfrak{A}$ which is relatively prime to $\mathfrak{B}$, so

$$BW = (\mathfrak{BW}_1, \mathfrak{BW}_2, \ldots \mathfrak{BW}_p, \mathfrak{A}).$$

If one starts from this basis to determine in the manner described above a basis (1.) corresponding to the arbitrarily given polygon

$$\mathfrak{B} = \mathfrak{P}_1^{m_1} \mathfrak{P}_2^{m_2} \mathfrak{P}_3^{m_3} \ldots ,$$

and determines the two polygons $\mathfrak{A}'$ and $\mathfrak{B}'$ from the condition

$$d\tilde{\omega}_r = \frac{\mathfrak{A}_r}{\mathfrak{B}} = \frac{\mathfrak{A}'_r}{\mathfrak{B}'_r},$$

so that they have no common divisor, then the polygons $\mathfrak{B}'_r$ that occur as under-gons of the differentials $d\tilde{\omega}_r$ are as follows:

a) the denominator $\mathfrak{O}$ occurs $p$-times and the accompanying differentials $d\tilde{\omega}_r$ are differentials of the first kind.

b) each under-gon $\mathfrak{P}_1^{m_1}, \mathfrak{P}_2^{m_2}, \ldots \mathfrak{P}_r^{m_r}$ (when $m_i \geq 2$), $\mathfrak{P}_2^2, \mathfrak{P}_3^2, \ldots \mathfrak{P}_r^2$; $\mathfrak{P}_2^3, \mathfrak{P}_3^3, \ldots \mathfrak{P}_r^3$, ... occurs once.

The differentials $d\tilde{\omega}_r$ associated with the under-gons $\mathfrak{P}_r^r$ will, if a precise distinction is required, be denoted by $dt_{(\mathfrak{P}_r^{r-1})}$ and called differentials of the second kind.
c) Finally, the products $P_1 P_2, P_1 P_3, \ldots$ (for fixed $P_1$) occur once each. The associated differentials $d\tilde{\omega}$, will be denoted by $d\pi_{(P_1, \mathcal{B})}$ and called differentials of the third kind.

Each differential $d\tilde{\omega}$ whose under-gon is $\mathcal{B}$ can be represented in the form

$$d\tilde{\omega} = \sum c_r d\tilde{\omega}_r$$

with constant coefficients $c_r$, which will be known as the normal form of the differential $d\tilde{\omega}$. If each of the individual differentials $d\tilde{\omega}_r$ have been chosen in a certain way, then the normal form can also be produced in only one way, which follows directly from the linear independence of the differentials $d\tilde{\omega}_r$.

§32. Residues.

1. If $d\tilde{\omega}_r$ is any differential in $\Omega$ and $P$ is a point that occurs $m$-times in the same under-gon $\mathcal{B}$ ($m \geq 0$), then choose a variable $z$ such that it will be $\infty$ at $P$. Then (according to §15, 4.), we can set in only one way

$$d\tilde{\omega} = a_{m-2}z^{m-2} + a_{m-3}z^{m-3} + \ldots + a_1 z + a_0 + a_{-1}z^{-1} + \eta z^{-2},$$

where the $a$ are constants and $\eta$ is a function in $\Omega$ which is finite at $P$. The coefficient $-a_{-1}$ of $-z^{-1}$ in this expression is called the residue of the differential $d\tilde{\omega}$ with respect to the point $P$. Arising from this definition we have the following theorem:

2. The residue with respect to a point $P$ can only be different from zero when $m > 0$, i.e. when the point $P$ actually occurs in the under-gon of $d\tilde{\omega}$, 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. That is if $\sigma$ is a function in $\Omega$, $b$ is a constant and $\sigma'$ is a function that is finite at $\mathcal{P}$, then

$$\sigma = b_m z^m + b_{m-1} z^{m-1} + \ldots + b_1 z + \sigma',$$

so it follows by differentiation of this expression with respect to $z$ that $\frac{d\sigma'}{dz}$ is infinitely small of at least the second order at $\mathcal{P}$ (§23, 10.), thus in the expression for $\frac{d\sigma}{dz}$ a term with $z^{-1}$ does not occur, which proves the claim.

5. The residue of a differential $d\tilde{\omega}$ is independent of the choice of the variable $z$. Specifically, if $z_1$, is a second variable of the same type as $z$, thus if $a$ is constant and $\zeta$ is finite at $\mathcal{P}$:

$$z = az_1 + \zeta,$$
then it follows that if as a shorthand we set
\[ \alpha = \frac{a_{m-2}z^{m-1}}{m-1} + \frac{a_{m-3}z^{m-2}}{m-2} + \ldots + a_0z \]
then:
\[ \frac{d\tilde{\omega}}{dz_1} = \frac{d\tilde{\omega}}{dz} \frac{dz}{dz_1} = \frac{d\alpha}{dz_1} + a_{-1} \frac{dz}{dz_1} - \eta \frac{dz^{-1}}{dz_1}. \]

Now if \( \zeta' \) and \( \zeta'' \) are functions that are finite at \( \mathcal{P} \), we have easily by §23 and §15,
4. that:
\[ z^{-1} \frac{dz}{dz_1} = z_1^{-1} + z_1^{-2} \zeta', \]
\[ dz^{-1} \frac{dz}{dz_1} = z_1^{-2} \zeta'', \]
and the correctness of the specified statement follows from 3. and 4.

6. The sum of the residues of each differential \( d\tilde{\omega} \) with respect to all points \( \mathcal{P} \) is always equal to zero.

In the proof of this important theorem we can restrict ourselves to the consideration of residues which belong to all of the distinct points occurring in the under-gon \( \mathcal{B} \) of \( d\tilde{\omega} \); however, we should add to these as many of the distinct arbitrary points that have vanishing residuals until we get from nothing but simple points to a polygon \( \mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_n \) belonging to a proper class. Then we choose a variable \( z \) of order \( n \) whose under-gon is precisely this polygon, so that it will be \( \infty \) at each of the points \( \mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_n \), and only at these. Then included in these are all the distinct points occurring in \( \mathcal{B} \). Under these conditions we have, for \( i = 1, 2, \ldots, n \),
\[ (3.) \quad \frac{d\tilde{\omega}}{dz} = a_{m-2}^{(i)}z^{m-2} + a_{m-3}^{(i)}z^{m-3} + \ldots + a_0^{(i)} + a_{-1}^{(i)}z^{-1} + \eta^{(i)}z^{-2}, \]
where \( \eta^{(i)} \) is a function that is finite at \( \mathcal{P}_i \). The constants \( a^{(i)} \) can also take the value 0, then the exponent \( m \) can be assumed to be independent of \( i \) (\( m \) is then, if not all the \( a_{m-2}^{(i)} \), vanish, the exponent of the highest power of a single point which occurs in \( \mathcal{B} \)). The theorem to be proved then is that \( \sum_i a_{-1}^{(i)} = 0 \). To prove it we construct the trace of the function \( \frac{d\tilde{\omega}}{dz} \) for the variable \( z \) (§2) and then make use of an extension of the procedure §16, 4. We choose a system of functions \( \rho_1, \rho_2, \ldots, \rho_n \) in \( \Omega \) as follows:
\[
\begin{array}{cccc}
\rho_1 & = & 0^m & \text{at} \ \mathcal{P}_2, \mathcal{P}_3, \ldots, \mathcal{P}_n, \ \text{finite and non-zero at} \ \mathcal{P}_1, \\
\rho_2 & = & 0^m & \text{at} \ \mathcal{P}_1, \mathcal{P}_3, \ldots, \mathcal{P}_n, \ " " " \mathcal{P}_2, \\
\vdots & \vdots & \vdots & \vdots \\
\rho_n & = & 0^m & \text{at} \ \mathcal{P}_1, \mathcal{P}_3, \ldots, \mathcal{P}_{n-1}, \ " " " \mathcal{P}_n.
\end{array}
\]

\(^1\text{It is possible to base the definition of residuals on a variable } r \text{ which is in infinitely small of the first order at } \mathcal{P}. \text{ Then we have}
\[ \frac{d\tilde{\omega}}{dr} = a_m r^m + \ldots + a_1 r^{-1} + \eta \]
\text{where } \eta \text{ is finite at } \mathcal{P}, \text{ then } a_1, \text{ is the residue of } d\tilde{\omega} \text{ with respect to } \mathcal{P}.\]
Now, if \( x_1, x_2, \ldots x_n \) are rational functions of \( z \) and

\[
\eta = x_1 \rho_1 + x_2 \rho_2 + \ldots + x_n \rho_n
\]

is a function in \( \Omega \), which for \( z = \infty \), i.e. at \( \mathcal{P}_1, \mathcal{P}_2, \ldots \mathcal{P}_n \), is finite, then \( x_1, x_2, \ldots x_n \) must be finite for \( z = \infty \) as well. To be precise, if \( x_1, x_2, \ldots x_n \) are not all finite for \( z = \infty \) then there exists a positive exponent \( r \) such that the products \( x_1 z^{-r}, x_2 z^{-r}, \ldots x_n z^{-r} \) 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

\[
\eta z^{-r} = x_1 z^{-r} \rho_1 + x_2 z^{-r} \rho_2 + \ldots + x_n z^{-r} \rho_n
\]

contains the contradiction that at the point \( \mathcal{P}_1 \), the left-hand side and all the terms of the right-hand side except the first, vanish.

At the same time we have from this that when we put \( \eta = 0 \) the functions \( \rho_1, \rho_2, \ldots \rho_n \) form a basis of \( \Omega \). So, if we put

\[
(4.) \quad \frac{d\tilde{\omega}}{dz} \rho_i = x_{i,1} \rho_1 + x_{i,2} \rho_2 + \ldots + x_{i,n} \rho_n, \quad (i=1,2,\ldots n)
\]

where \( x_{i,i'} \) denote rational functions \( z \), then (§2)

\[
(5.) \quad S \left( \frac{d\tilde{\omega}}{dz} \right) = x_{1,1} + x_{2,2} + \ldots + x_{n,n}.
\]

Now, as shown in (3.), \( z^{-m+2} \frac{d\tilde{\omega}}{dz} \rho_i \) is finite for \( z = \infty \), from this and the property of the functions \( \rho \) just proved we have that

\[
z^{-m+2} x_{i,i'}
\]

are finite for \( z = \infty \). Now, for example, the functions \( \rho_1, \rho_3, \ldots \rho_n \) are infinitely small of the \( m^{th} \) order at the point \( \mathcal{P}_2 \), while \( \rho_2 \) is finite and non-zero there. Therefore at \( \mathcal{P}_2 \) the functions

\[
\frac{d\tilde{\omega}}{dz} \rho_1, \quad 2x_{1,1} \rho_1, \quad 2x_{1,3} \rho_3, \ldots \quad 2x_{1,n} \rho_n
\]

all vanish, and therefore \( z x_{1,2} \) must also vanish for \( z = \infty \). The same follows for \( z x_{1,3}, \ldots z x_{1,n} \) and generally for \( z x_{i,i'} \) whenever \( i \) and \( i' \) are different from each other. Therefore, \( z^2 x_{i,i'} \) will be finite for \( z = \infty \).

If now \( x_i \) represents a new rational function,

\[
(6.) \quad x_{i,i'} = a_{m-2}^{(i)} z^{-m-2} + a_{m-3}^{(i)} z^{-m-3} + \ldots + a_1^{(i)} z^{-1} + x_i z^{-2},
\]

then it follows from (3.) that

\[
x_{i,i'} - \frac{d\tilde{\omega}}{dz} = z^{-2}(x_i - \eta^{(i)}),
\]
and from (4.) that

\[(\eta^{(i)} - x_i)\rho_i = z^2 x_{i, i}\rho_1 + \ldots + z^2 x_{i, i-1}\rho_{i-1} + z^2 x_{i, i+1}\rho_{i+1} + \ldots + z^2 x_{i, n}\rho_n.\]

Now because \(\eta^{(i)}\) is finite and \(\rho_i\) is non-zero at \(P_i\), and further all the terms of the right-hand side are zero, it then follows that \(x_i\) is also finite at the point \(P_i\), and consequently is rational, and finite for \(z = \infty\). From (5.) and (6.) it follows then that

\[(7.) \quad S \left( \frac{d\tilde{\omega}}{dz} \right) = \sum_i a^{(i)}_{m-2}z^{m-2} + \sum_i a^{(i)}_{m-3}z^{m-3} + \ldots + \sum_i \rho^{-1}_i z^{-1} + \sum_i x_i z^{-2}.\]

Now we have on the other hand when again \(U\) is the under-gon and \(\mathfrak{B}\) is the ramification polygon of \(z\):

\[\frac{d\tilde{\omega}}{dz} = \frac{U^2 A}{\mathfrak{B} \mathfrak{B}},\]

and \(\mathfrak{B}\) does not contain any point that is not also contained in \(U\). From this as in §26 we get that \(\frac{d\tilde{\omega}}{dz}\), regarded as a function of \(z\), is a function in \(e\), the complementary module to \(\sigma\), and consequently

\[S \left( \frac{d\tilde{\omega}}{dz} \right)\]

is an integral rational function of \(z\) (§11, 4.). In view of this, it follows from (7.) that \(\sum_i x_i = 0\) and further the theorem that was to be proved

\[\sum_i a^{(i)}_{-1} = 0.\]

We can also state this theorem in the following way: The residue of a differential of the second kind \(dt_{(P')}\) with respect to the point \(P\) is zero.

The residues of a differential of the third kind \(d\pi_{(P_1, P_2)}\) with respect to \(P_1\) and \(P_2\) are equal and opposite, and certainly different from zero, otherwise \(d\pi\) would be a differential of the first kind.

These observations, still employing 4., mean that a proper differential \(d\sigma\) presented in normal form cannot contain a differential of the third kind. It also deserves to be mentioned that the residuals of logarithmic differentials \(\frac{d\sigma}{\sigma}\) are integers, namely the order numbers of the function \(\sigma\) (according to §23).
§33.
Relations between the differentials of first and second kinds.

1. Let $\sigma$ be a function in $\Omega$ with the under-gon
$$
\mathcal{B}' = \mathcal{P}_1^{m_1-1}\mathcal{P}_2^{m_2-1} \ldots \quad (m_1, m_2, \ldots \geq 2)
$$
and ramification polygon ($\S$16)
$$
\mathcal{S} = \mathcal{S}'\mathcal{P}_1^{m_1-2}\mathcal{P}_2^{m_2-2} \ldots ,
$$
where $\mathcal{S}'$ is not divisible by the points $\mathcal{P}_1, \mathcal{P}_2, \ldots$, all of which are assumed to be distinct. Accordingly, in the symbolic relationship from $\S$25 we have the proper differential
$$
\frac{d\sigma}{\mathcal{B}'^{\frac{1}{2}}} = \frac{\mathcal{S}'}{\mathcal{P}_1^{m_1}\mathcal{P}_2^{m_2} \ldots },
$$
from which it emerges at first that a proper differential can never be of the first kind.

2. The proper differential $d\sigma$, which in its representation in the normal form can only contain differentials of the first and second kind, belongs to the family of those differentials whose under-gon is
$$
\mathcal{B} = \mathcal{P}_1^{m_1}\mathcal{P}_2^{m_2} \ldots = \mathcal{B}'\mathcal{P}_1\mathcal{P}_2 \ldots .
$$
Conversely, assuming that in such a family $m_1, m_2, \ldots \geq 2$ and that $\mathcal{B}'$ belongs to a proper polygon class, one will always find at least one proper differential $d\sigma$. Because in addition from 1. it is only necessary that there is a function $\sigma$ in $\Omega$ with the under-gon $\mathcal{B}'$.

3. From this we now have the following important theorem. All differentials of the second kind can be represented as a linear combination with constant coefficients of $p$ suitably chosen special differentials of the second kind, by differentials of the first kind and by proper differentials.

To see this, choose an arbitrary polygon of the second kind $\mathcal{U}$ of order $p$. If now $\mathcal{P}$ is an arbitrary point and $r$ a positive exponent, then the polygon $\mathcal{P}\mathcal{P}'$ is also of the second kind and hence the divisor $\mathcal{M}$ of the associated class cannot be divided by $\mathcal{P}$, because otherwise $\mathcal{P}\mathcal{P}'^{-1}$ and thus also $\mathcal{P}$ would be a polygon of the first kind ($\S$30, 4.). So put
$$
\mathcal{P}\mathcal{P}' = \mathcal{M}\mathcal{B}',
$$
then $\mathcal{P}$ will not appear in $\mathcal{M}$ and hence $\mathcal{B}'$ contains the factor $\mathcal{P}$ exactly $r$-times more often than $\mathcal{U}$. At the same time $\mathcal{B}'$ belongs to a proper class. If now
$$
\mathcal{B}' = \mathcal{P}^{m+r}\mathcal{P}'^{\mathcal{m}'}\mathcal{P}^{\mathcal{m}''} \ldots ,
$$
then the point powers \( \mathcal{P}^m, \mathcal{P}^{m'}, \mathcal{P}^{m''} \ldots \) are all in \( \mathfrak{K} \). Thus if we put

\[
\mathfrak{B} = \mathcal{P}^{m+r+1} \mathcal{P}^{m' + 1} \mathcal{P}^{m'' + 1} \ldots = \mathcal{P} \mathcal{P} \mathcal{P} \mathcal{P} \mathcal{P} \ldots,
\]

then from 2., there is certainly a proper differential \( d\sigma \) in the family of differentials associated with the under-gon \( \mathfrak{B} \). The representation of the same in the normal form itself contains the differential

\[
(1.) \quad dt_{(\mathcal{P}^{m+r})}
\]

and also some or all of the differentials

\[
(2.) \quad \begin{cases}
   dt_{(\mathcal{P}^1)}, & dt_{(\mathcal{P}^2)}, & \ldots & dt_{(\mathcal{P}^m)}, & \ldots & dt_{(\mathcal{P}^{m+r-1})}, \\
   dt_{(\mathcal{P}^{m'})}, & dt_{(\mathcal{P}^{m'2})}, & \ldots & dt_{(\mathcal{P}^{m''})}, \\
   & \ldots & \ldots & \ldots & \ldots & \ldots
\end{cases}
\]

besides differentials of the first kind. The differential (1.) can thus be represented linearly with constant coefficients by (2.), by differentials of the first kind and by \( d\sigma \).

Therefore if

\[
\mathfrak{A} = \mathcal{P}_1^{m_1}, \mathcal{P}_2^{m_2} \ldots
\]

is a \( p \)-gon is the second kind, it will be seen by repeated application of the method described here, that all the differentials of the second kind may be represented in the way that our theorem is expressed by the \( p \) differentials

\[
(3.) \quad \begin{cases}
   dt_{(\mathcal{P}_1)}, & \ldots & dt_{(\mathcal{P}_1^{m_1})}, \\
   dt_{(\mathcal{P}_2)}, & \ldots & dt_{(\mathcal{P}_2^{m_2})}, \\
   & \ldots & \ldots
\end{cases}
\]

Brunswick and Königsberg in Prussia October 1880.