MATHEMATICAL SURVEYS
NUMBER VI

INTRODUCTION TO THE THEORY OF ALGEBRAIC FUNCTIONS OF ONE VARIABLE

BY

CLAUDE CHEVALLEY

PUBLISHED BY THE
AMERICAN MATHEMATICAL SOCIETY
531 WEST 116TH STREET, NEW YORK
1951

To

SYLVIE CHEVALLEY

INTRODUCTION

An algebraic function y of a complex variable x is a function which satisfies an equation of the form $F(x, y) = 0$, where F is a polynomial with complex coefficients; i.e., y is a root of an algebraic equation whose coefficients are rational functions of x. This very definition exhibits a strong similarity between the notions of algebraic function and algebraic number, the rational functions of x playing a role similar to that played by the rational numbers. On the other hand, the equation $F(x, y) = 0$ may be construed to represent a curve in a plane in which x and y are the coordinates, and this establishes an intimate link between the theory of algebraic functions of one variable and algebraic geometry.

Whoever wants to give an exposition of the theory of algebraic functions of one variable is more or less bound to lay more emphasis either on the algebraico-arithmetic aspect of this branch of mathematics or on its geometric aspect. Both points of view are acceptable and have been in fact held by various mathematicians. The algebraic attitude was first distinctly asserted in the paper *Theorie der algebraischen Funktionen einer Veränderlichen*, by R. Dedekind and H. Weber (Journ. für Math., 92, 1882, pp. 181–290), and inspires the book *Theorie der algebraischen Funktionen einer Variabeln*, by Hensel and Landsberg (Leipzig, 1902). The geometric approach was followed by Max Noether, Clebsch, Gordan, and, after them, by the geometers of the Italian school (cf. in particular the book *Lezione di Geometria algebrica*, by F. Severi, Padova, 1908). Whichever method is adopted, the main results to be established are of course essentially the same; but this common material is made to reflect a different light when treated by differently minded mathematicians. Familiar as we are with the idea that the pair "observed fact—observer" is probably a more real being than the inert fact or theorem by itself, we shall not neglect the diversity of these various angles under which a theory may be photographed. Such a neglect should be particularly avoided in the case of the theory of algebraic functions, as either mode of approach seems liable to provoke strong emotional reactions in mathematical minds, ranging from devout enthusiasm to unconditional rejection. However, this does not mean that the ideal should consist in a mixture or synthesis of the two attitudes in the writing of any one book: the only result of trying to obtain two interesting photographs of the same object on the same plate is a blurred and dull image. Thus, without attacking in any way the validity *per se* of the geometric approach, we have not tried to hide our partiality to the algebraic attitude, which has been ours in writing this book.

The main difference between the present treatment of the theory and the one to be found in Dedekind-Weber or in Hensel-Landsberg lies in the fact that the constants of the fields of algebraic functions to be considered are not necessarily the complex numbers, but the elements of a completely arbitrary field. There are several reasons which make such a generalization necessary. First, the analogy between algebraic functions and algebraic numbers becomes even closer if one considers algebraic functions over finite fields of constants. In that case, on the one hand class field theory has been extended to the case of fields of functions, and, on the other hand, the transcendental theory (zeta function, L-series) may also be generalized (cf. the paper of F. K. Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p*, Math. Zeits., 33, 1931). Moreover, A. Weil has succeeded in proving the Riemann hypothesis for fields of algebraic functions over finite fields, thereby throwing an entirely new light on the classical, i.e., number theoretic, case (cf. the book of A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Paris, Hermann, 1948; this book contains an exposition of the theory from a geometric point of view, although this point of view is rather different from that of the Italian geometers). Secondly, if S is an algebraic surface, and R the field of rational functions on S, then R is a field of algebraic functions of one variable over $K\langle x\rangle$, where K is the basic field and x a non constant element of R. E. Picard, among others, has very successfully used the method of investigation of S which amounts to studying the relationship between R and various fields of the form $K\langle x\rangle$ (cf. E. Picard and G. Simart, *Théorie des fonctions algébriques de deux variables independantes*, Paris, Gauthier-Villars, 1897). Now, even when K is the field of complex numbers, $K\langle x\rangle$ is not algebraically closed, which makes it necessary to have a theory of fields of algebraic functions of one variable over fields which are not algebraically closed.

The theory of algebraic functions of one variable over non algebraically closed fields of arbitrary characteristic has been first developed by H. Hasse, who defined for these fields the notion of a differential (H. Hasse, *Theorie der Differentiale in algebraischen Funktionenkörpern mit volkommenen Konstantenkörper*, Journ. für Math., 172, 1934, pp. 55–64), and by F. K. Schmidt, who proved the Riemann-Roch theorem (F. K. Schmidt, *Zur arithmetischen Theorie der algebraischen Funktionen*, I, Math. Zeits., 41, 1936, p. 415). In this book, we have used the definition of differentials and the proof of the Riemann-Roch theorem which were given by A. Weil (A. Weil, *Zur algebraischen Theorie der algebraischen Funktionen*, Journ. für Math., 179, 1938, pp. 129–133).

As for contents, we have included only the elementary part of the theory, leaving out the more advanced parts such as class field theory or the theory of correspondences. However, we have been guided by the desire of furnishing a suitable base of knowledge for the study of these more advanced chapters. This is why we have placed much emphasis on the theory of extensions of fields of algebraic functions of one variable, and in particular of those extensions which are obtained by adjoining new constants, which may even be transcendental over the field of constants of the original field of functions. That the consideration of such extensions is desirable is evidenced by the paper of M. Deuring, *Arithmetische Theorie der Korrespondenzen algebraischen Funktionenkörper*, Journ. für Math., 177, 1937. The theory of differentials of the second kind has been given only in the case where the field under consideration is of characteristic 0. The reason for this restriction is that it is not yet clear what the "good" definition of the notion should be in the general case: should one demand only that the residues be all zero, or should one insist that the differential may be approximated as closely as one wants at any given place by exact differentials (or a suitable generalization of these)? Here is a net of problems which, it seems, would deserve some original research. The last chapter of the book is concerned with the theory of fields of algebraic functions of one variable over the field of complex numbers and their Riemann surfaces. The scissor and glue method of approach to the idea of a Riemann surface has been replaced by a more abstract definition, inspired by the one given by H. Weyl in his book on Riemann surfaces, which does not necessitate the artificial selecting of a particular generation of the field by means of an independant variable and a function of this variable. We have also avoided the cumbersome decomposition of the Riemann surface into triangles, this by making use of the singular homology theory, as developed by S. Eilenberg.

I have been greatly helped in the writing of this book by frequent conversations with E. Artin and O. Goldman; I wish to thank both of them sincerely for their valuable contribution in the form of advice and suggestions.

NOTATIONS FREQUENTLY USED

Con $_{R/S}$: conorm from R to S (IV, 7).

Cosp $_{R/S}$: cotrace from R to S (for repartitions, IV, 7; for differentials, VI, 2 and VI, 6).

$d(\mathfrak{a})$: degree of a divisor $\mathfrak{a}$ (I, 7).

$\mathfrak{d}(x)$: divisor of an element x (I, 8).

$\mathfrak{d}(\omega)$: divisor of a differential ω (II, 6).

$\delta(\mathfrak{a})$: dimension of the space of differentials which are multiple of a divisor $\mathfrak{a}$ (II, 5).

∂: boundary (VII, 3).

$H_n(X, Y)$: n-dimensional homology group of X modulo Y (VII, 3).

$i(\gamma, \gamma')$: intersection numbers of the 1-chains γ and γ' (VII, 6).

$j(\omega, \omega')$: (VII, 5).

$K\langle\cdots\rangle$: field obtained by adjunction to the field K of the element or elements or set of elements whose symbols are between the sign $\langle$ and the sign $\rangle$; special meaning for fields of algebraic functions of one variable defined in V, 4.

$l(\mathfrak{a})$: dimension of the space of elements which are multiples of a divisor $\mathfrak{a}$ (II, 1).

$\nu_{\mathfrak{p}}$: order function at a place $\mathfrak{p}$ (for elements, I, 5 and III, 1; for repartitions, II, 4; for differentials, II, 6).

$N_{S/R}$: Norm from S to R (IV, 7).

$N^{\mathfrak{P}}_{S/R}$: (IV, 5).

$\omega^{\mathfrak{p}}$: $\mathfrak{p}$-component of a differential ω (II, 7).

res $_{\mathfrak{p}}\omega$: residue of a differential ω at a place $\mathfrak{p}$ (III, 5).

Sp$_{S/R}$: Trace from S to R (for repartitions, IV, 7; for differentials, VI, 2).

Sp$^{\mathfrak{P}}_{S/R}$: (IV, 5).

$|\gamma|$: set of points of a chain γ (VII, 3).

COMPOSED AND PRINTED AT THE
WAVERLY PRESS, INC.
BALTIMORE, MD., U. S. A.

TABLE OF CONTENTS

CHAPTER I

PLACES AND DIVISORS

§1. Fields of algebraic functions of one variable

Let K be a field. By a *field of algebraic functions of one variable over* K we mean a field R containing K as a subfield and which satisfies the following condition: R contains an element x which is transcendental over K, and R is algebraic of finite degree over $K\langle x\rangle$.

The element x is of course not uniquely determined. If x' is any element of R which is transcendental over K, then R is algebraic of finite degree over $K\langle x'\rangle$. In fact, the degree of transcendency of R over K being one, R is algebraic over $K\langle x'\rangle$. In particular, x is algebraic over $K\langle x'\rangle$, and $K\langle x, x'\rangle$ is of finite degree over $K\langle x'\rangle$. Since R is of finite degree over $K\langle x\rangle$, it is *a fortiori* of finite degree over $K\langle x, x'\rangle$, which proves that it is of finite degree over $K\langle x'\rangle$.

Those elements of R which are algebraic over K are called *constants*. They form a certain subfield K' of R, the *field of constants*. The field R is also a field of algebraic functions of one variable over K'. In fact, any element x of R which is transcendental over K is also transcendental over K', and R, which is algebraic of finite degree over $K\langle x\rangle$, is also algebraic of finite degree over $K'\langle x\rangle$.

It is important to keep in mind that, when discussing properties of a field R of algebraic functions of one variable, we shall consider in fact not properties of the field R alone but properties of the pair formed by K and R. For instance, let Z be any field, and set $R = Z\langle x, y, z\rangle$, where x and y are algebraically independent over Z and z is algebraic over $Z\langle x, y\rangle$. Set $K_1 = Z\langle x\rangle$, $K_2 = Z\langle y\rangle$. Then R is a field of algebraic functions of one variable over either one of the fields K_1 or K_2; but its properties as a field of algebraic functions of one variable over K_1 may be quite different from its properties as a field of algebraic functions of one variable over K_2.

However, when considering a field R of algebraic functions of one variable over a field K, the field of constants of R will appear more and more to be the essential object instead of K itself, which will gradually fade into the background.

§2. Places

Let R be a field and K a subfield of R. By a *V-ring* in R (over K) is meant a subring $\mathfrak{o}$ of R which satisfies the following conditions:

1. $\mathfrak{o}$ contains K;
2. $\mathfrak{o}$ is not identical with R;
3. If x is an element of R not in $\mathfrak{o}$, then x^{-1} is in $\mathfrak{o}$.

Let $\mathfrak{o}$ be a V-ring. Those elements in $\mathfrak{o}$ which are not units in $\mathfrak{o}$ (we call them "non-units") form an ideal $\mathfrak{p}$ in $\mathfrak{o}$. In fact, if x is a non-unit and $z \in \mathfrak{o}$, then xz

is a non-unit, because, if xz had an inverse u in $\mathfrak{o}$, zu would be in $\mathfrak{o}$ and inverse of x. Now, let x and y be non-units in $\mathfrak{o}$. If either x or y is 0, $x - y$ is clearly a non-unit. If x and y are both $\neq 0$, one at least of the pair of inverse elements x/y and y/x is in $\mathfrak{o}$. If $x/y \in \mathfrak{o}$, then $x - y = y(x/y - 1)$ is a non-unit; if $y/x \in \mathfrak{o}$, then $x - y = x(1 - y/x)$ is a non-unit. Thus the non-units of $\mathfrak{o}$ form an ideal $\mathfrak{p}$. Any ideal in $\mathfrak{o}$ containing $\mathfrak{p}$ but $\neq \mathfrak{p}$ contains a unit and therefore coincides with $\mathfrak{o}$.

Now, let R be a field of algebraic functions of one variable over a field K. By a *place* in R we mean a subset $\mathfrak{p}$ of R which is the ideal of non-units of some V-ring $\mathfrak{o}$ of R (over K). This V-ring is uniquely determined when $\mathfrak{p}$ is given. In fact, it is the set of all $x \in R$ such that $x\mathfrak{p} \subset \mathfrak{p}$ (we mean by $x\mathfrak{p}$ the set of products of x by elements of $\mathfrak{p}$). To show this, we observe first that any $x \in \mathfrak{o}$ has the required property; on the other hand, if $x \notin \mathfrak{o}$, then x^{-1} is in $\mathfrak{o}$ and is not a unit, whence $x^{-1} \in \mathfrak{p}$ and $1 \in x\mathfrak{p}$, $x\mathfrak{p} \not\subset \mathfrak{p}$. The ring $\mathfrak{o}$ is called the *ring of the place* $\mathfrak{p}$. The elements of $\mathfrak{o}$ are said to be *integral* at the place $\mathfrak{p}$.

Since every element of $\mathfrak{o}$ not in $\mathfrak{p}$ is a unit in $\mathfrak{o}$, we see immediately that the residue ring $\mathfrak{o}/\mathfrak{p}$ is a field. This field is called the *residue field* of the place $\mathfrak{p}$.

The ring $\mathfrak{o}$ *is integrally closed in* R, i.e., every element x of R which satisfies an equation of the form $x^n + \sum_{i=1}^n a_i x^{n-i} = 0$, with $a_1, \cdots, a_n$ in $\mathfrak{o}$, itself belongs to $\mathfrak{o}$. For, were this not the case, then x^{-1} would belong to $\mathfrak{p}$, and we would have $1 = -\sum_{i=1}^n a_i(x^{-1})^i \in \mathfrak{p}$, which is impossible. It follows in particular that the ring of any place contains the field of constants K' of R. This shows that the notion of place in R is the same whether we consider R as a field of algebraic functions over K or over K'. On the other hand, we have $K' \cap \mathfrak{p} = \{0\}$, which proves that the natural homomorphism of $\mathfrak{o}$ onto the residue field $\Sigma = \mathfrak{o}/\mathfrak{p}$ of $\mathfrak{p}$ maps K' isomorphically upon a subfield of Σ. We shall allow ourselves, whenever convenient, to speak of Σ as of an overfield of K'; this amounts to not distinguishing between the elements of K' and their residue classes modulo $\mathfrak{p}$.

§3. Places of the field $K\langle x\rangle$

Let us consider the special case where $R = K\langle x\rangle$, with, of course, x transcendental over K. Let $f = f(x)$ be an irreducible polynomial in x with coefficients in K. Any element u of R may be written in the form $u = g/h$, with g and h in the ring $K[x]$. Let $\mathfrak{o}_f$ be the set of elements u of the form g/h, with h not divisible by f. Since f is irreducible, it cannot divide a product of polynomials without dividing one of them. Thus the formulas

$$\frac{g_1}{h_1} - \frac{g_2}{h_2} = \frac{g_1h_2 - g_2h_1}{h_1h_2}, \qquad \frac{g_1}{h_1}\frac{g_2}{h_2} = \frac{g_1g_2}{h_1h_2}$$

show that $\mathfrak{o}_f$ is a subring of R. It is clear that this subring contains K. Moreover, $1/f$ is not in $\mathfrak{o}_f$, because, if we write $1/f = g/h$, where g and h are polynomials in x, $h = gf$ is divisible by f; this shows that $\mathfrak{o}_f \neq R$. Now, let u be any element of R not in $\mathfrak{o}_f$. We may write u in the form g/h, where g and h are polynomials in x without common factor. Since $u \notin \mathfrak{o}_f$, f divides h, and therefore f does not divide g, whence $u^{-1} = h/g \in \mathfrak{o}_f$. Thus $\mathfrak{o}_f$ is a V-ring; we shall denote by $\mathfrak{p}_f$ the corresponding place. It is clear that $\mathfrak{p}_f$ consists of all elements of the form fg/h, where g and h are polynomials in x, and h is not divisible by f.

Thus, to every irreducible polynomial f in x with coefficients in K we have associated a place $\mathfrak{p}_f$ of $K\langle x\rangle$. If f and f' are essentially distinct irreducible polynomials (i.e., f'/f not in K), the places $\mathfrak{p}_f$ and $\mathfrak{p}_{f'}$ are distinct because f^{-1} belongs to $\mathfrak{o}_{f'}$ but not to $\mathfrak{o}_f$.

Now, observe that, if we set $x' = x^{-1}$, we have $K\langle x'\rangle = K\langle x\rangle$. It follows that to every irreducible polynomial in x' with coefficients in K, there is associated a place of $K\langle x\rangle$. This applies in particular to the irreducible polynomial x'; we shall denote by $\mathfrak{p}_{1/x}$ the place defined by x' and by $\mathfrak{o}_{1/x}$ the ring of this place. The place $\mathfrak{p}_{1/x}$ is distinct from all the places $\mathfrak{p}_f$ defined above, because, if f is any irreducible polynomial in x, we have $x \in \mathfrak{o}_f$, while x clearly does not belong to $\mathfrak{o}_{1/x}$.

Now we assert that the places $\mathfrak{p}_f$ (for all irreducible polynomials f in x with coefficients in K) and $\mathfrak{p}_{1/x}$ exhaust all the places of R. Let $\mathfrak{p}$ be any place in R, and let $\mathfrak{o}$ be its ring. Assume first that $x \in \mathfrak{o}$. Since $\mathfrak{o}$ is a ring and contains K, it follows that $\mathfrak{o}$ contains the entire ring $K[x]$. Since $\mathfrak{p}$ is obviously a prime ideal in $\mathfrak{o}$, $\mathfrak{p} \cap K[x]$ is a prime ideal in $K[x]$. Thus $\mathfrak{p} \cap K[x]$ either is the zero ideal or is formed of all multiples of some irreducible polynomial f. The first case is impossible because every element $\neq 0$ of $K[x]$ would then be a unit in $\mathfrak{o}$, from which it follows immediately that every element of R would belong to $\mathfrak{o}$. Thus $\mathfrak{p} \cap K[x]$ consists of the multiples of some irreducible f. If g and h are in $K[x]$, and h is not divisible by f, then h is not in $\mathfrak{p}$ and is therefore a unit in $\mathfrak{o}$, whence $gh^{-1} \in \mathfrak{o}$, which proves that $\mathfrak{o}$ contains $\mathfrak{o}_f$. Let u be an element of R not in $\mathfrak{o}_f$; then we may write $u = g/h$, where g and h are in $K[x]$, have no common factor, and h is divisible by f. If u were in $\mathfrak{o}$, the same would be true of $h^{-1} = g^{-1}u$; but this is impossible because h, being in $\mathfrak{p}$, is not a unit in $\mathfrak{o}$. We have therefore proved that, if $x \in \mathfrak{o}$, then $\mathfrak{p}$ is one of the places $\mathfrak{p}_f$. If x is not in $\mathfrak{o}$, then $x' = x^{-1}$ is, and we see that $\mathfrak{p} \cap K[x']$ consists of all elements of $K[x']$ which are divisible (in $K[x']$) by some irreducible polynomial $f'(x')$ in x' with coefficients in K. Since x' is not a unit in $\mathfrak{o}$, it is in $\mathfrak{p} \cap K[x']$ and is therefore divisible by $f'(x')$ in $K[x']$. Thus we may assume that $f' = x'$; $\mathfrak{p}$ is then the place $\mathfrak{p}_{1/x}$.

It is clear that, if f is an irreducible polynomial in x with coefficients in K, then $\mathfrak{p}_f$ is the principal ideal generated in $\mathfrak{o}_f$ by f: $\mathfrak{p}_f = f\mathfrak{o}_f$. Similarly, $\mathfrak{p}_{1/x}$ is $(1/x)\mathfrak{o}_{1/x}$.

Let $\mathfrak{p}$ be any place of $R = K\langle x\rangle$. Denote by $\mathfrak{o}$ the ring of $\mathfrak{p}$ and by t a generator of $\mathfrak{p}$ (i.e., $\mathfrak{p} = t\mathfrak{o}$). Then no element $\neq 0$ of $\mathfrak{o}$ can belong to $t^n\mathfrak{o}$ for every $n > 0$. In fact, assume first that $\mathfrak{o} = \mathfrak{o}_f$ for some irreducible polynomial f in x. Let $u = g/h$ be an element of $\mathfrak{o}$ which belongs to $t^n\mathfrak{o}$ for every n (g and h are in $K[x]$, and h is not divisible by f). Since $\mathfrak{p} = t\mathfrak{o} = f\mathfrak{o}$, we see easily that $t^n\mathfrak{o} = f^n\mathfrak{o}$. We have by assumption, for each n, an equality of the form $g/h = f^n g_n/h_n$ with g_n and h_n in $K[x]$ and h_n not divisible by f. Thus $gh_n = f^n g_n h$; since f is irreducible and does not divide h_n, it follows easily that f^n divides g. This being true for every n, we have $g = 0$, whence $u = 0$. A similar argument applies if $\mathfrak{o} = \mathfrak{o}_{1/x}$.

Now, abandon for a moment the assumption that R is of the form $K\langle x\rangle$. Assuming only that R is a field of algebraic functions of one variable over K, let $\mathfrak{p}$ be a place of R which satisfies the following condition:

The ring $\mathfrak{o}$ *of* $\mathfrak{p}$ *contains an element t such that* $\mathfrak{p} = t\mathfrak{o}$ *and* $\bigcap_{n=1}^{\infty} t^n\mathfrak{o} = \{0\}$.
(We shall see later that every place of R satisfies this condition.) If $x \in R$, there exists at least one integer n (which may be negative) such that $x \in t^n\mathfrak{o}$. In fact, if $x \in \mathfrak{o}$, we may take $n = 0$. If not, then x^{-1} is in $\mathfrak{o}$ and is $\neq 0$; therefore there exists an $m > 0$ such that $x^{-1} \in t^m\mathfrak{o}$, $x^{-1} \notin t^{m+1}\mathfrak{o}$, which means that $t^{-m}x^{-1}$ is in $\mathfrak{o}$ but not in $t\mathfrak{o} = \mathfrak{p}$; i.e., $t^{-m}x^{-1}$ is a unit in $\mathfrak{o}$, and $x = t^{-m}(t^{-m}x^{-1})^{-1}$ is in $t^{-m}\mathfrak{o}$. If $x \neq 0$, there is by assumption a largest integer n such that $x \in t^n\mathfrak{o}$; denote by $\nu_\mathfrak{p}(x)$ this integer. If x and y are elements $\neq 0$ in $\mathfrak{o}$, then

$$\nu_\mathfrak{p}(x) + \nu_\mathfrak{p}(y) = \nu_\mathfrak{p}(xy) \tag{1}$$

and, if $x + y \neq 0$,

$$\nu_\mathfrak{p}(x + y) \geqq \min\{\nu_\mathfrak{p}(x), \nu_\mathfrak{p}(y)\}. \tag{2}$$

In fact, xy clearly belongs to $t^{\nu_\mathfrak{p}(x)+\nu_\mathfrak{p}(y)}\mathfrak{o}$, whence $\nu_\mathfrak{p}(xy) \geqq \nu_\mathfrak{p}(x) + \nu_\mathfrak{p}(y)$. In particular, $0 = \nu_\mathfrak{p}(1) \geqq \nu_\mathfrak{p}(x) + \nu_\mathfrak{p}(x^{-1})$, i.e., $\nu_\mathfrak{p}(x^{-1}) \leqq -\nu_\mathfrak{p}(x)$. Now, if we write $x = t^{\nu_\mathfrak{p}(x)}u$, u belongs to $\mathfrak{o}$ but not to $t\mathfrak{o} = \mathfrak{p}$, i.e., u is a unit in $\mathfrak{o}$ and $x^{-1} = t^{-\nu_\mathfrak{p}(x)}u^{-1}$, whence $\nu_\mathfrak{p}(x^{-1}) \geqq -\nu_\mathfrak{p}(x)$, and therefore $\nu_\mathfrak{p}(x^{-1}) = -\nu_\mathfrak{p}(x)$. We conclude that $\nu_\mathfrak{p}(y) = \nu_\mathfrak{p}(xyx^{-1}) \geqq \nu_\mathfrak{p}(xy) - \nu_\mathfrak{p}(x)$, and, comparing with the inequality obtained above, $\nu_\mathfrak{p}(xy) = \nu_\mathfrak{p}(x) + \nu_\mathfrak{p}(y)$. On the other hand, if $\mu = \min\{\nu_\mathfrak{p}(x), \nu_\mathfrak{p}(y)\}$, we have $x \in t^\mu\mathfrak{o}$, $y \in t^\mu\mathfrak{o}$, whence $x + y \in t^\mu\mathfrak{o}$ and therefore $\nu_\mathfrak{p}(x + y) \geqq \mu$.

To complete the definition of the function $\nu_\mathfrak{p}$ (which has not been defined for 0), we make the convention to write $\nu_\mathfrak{p}(0) = \infty$, where ∞ is a symbol with which we compute according to the following rules: $\infty > n$ for every integer n; $\infty \geqq \infty$; $\infty + n = \infty$ for every integer n; $\infty + \infty = \infty$. Taking these conventions into account, the formulas (1) and (2) are valid in every case.

It should be observed that the equality $\nu_\mathfrak{p}(x + y) = \min\{\nu_\mathfrak{p}(x), \nu_\mathfrak{p}(y)\}$ holds whenever $\nu_\mathfrak{p}(x) \neq \nu_\mathfrak{p}(y)$. In fact, assume that $\nu_\mathfrak{p}(x) < \nu_\mathfrak{p}(y)$. We have $\nu_\mathfrak{p}(x) = \nu_\mathfrak{p}(x + y - y) \geqq \min\{\nu_\mathfrak{p}(x + y), \nu_\mathfrak{p}(-y)\}$; but it is easily seen that $\nu_\mathfrak{p}(-y) = \nu_\mathfrak{p}(-1) + \nu_\mathfrak{p}(y) = \nu_\mathfrak{p}(y)$; thus it is impossible that $\nu_\mathfrak{p}(x + y) > \nu_\mathfrak{p}(x)$.

More generally, we see easily by induction on m that, if $x_1, \cdots, x_m$ are any elements of R, then

$$\nu_\mathfrak{p}(x_1 + \cdots + x_m) \geqq \min\{\nu_\mathfrak{p}(x_1), \cdots, \nu_\mathfrak{p}(x_m)\}$$

and that the equality prevails if there is only one index i such that $\nu_\mathfrak{p}(x_i) = \min\{\nu_\mathfrak{p}(x_1), \cdots, \nu_\mathfrak{p}(x_m)\}$.

The definition of the function $\nu_\mathfrak{p}$ involves the choice of an element t such that $\mathfrak{p} = t\mathfrak{o}$; but actually the function $\nu_\mathfrak{p}$ depends only on the place $\mathfrak{p}$. In fact, assume that t' is any element of $\mathfrak{p}$ such that $\mathfrak{p} = t'\mathfrak{o}$. Then $t = t'u$ with $u \in \mathfrak{o}$, and, since $t' \in t\mathfrak{o}$, $u^{-1} \in \mathfrak{o}$. It follows immediately that $t^n\mathfrak{o} \subset t'^n\mathfrak{o}$ and $t'^n\mathfrak{o} \subset t^n\mathfrak{o}$ for every n, which proves our assertion. The function $\nu_\mathfrak{p}$ is called the *order function* at the place $\mathfrak{p}$; if $x \in R$, $\nu_\mathfrak{p}(x)$ is called the *order* of x at $\mathfrak{p}$. The knowledge of the order function at a place $\mathfrak{p}$ determines this place completely, because the ring $\mathfrak{o}$ of the place consists of all elements x for which $\nu_{\mathfrak{p}}(x) \geqq 0$. The elements of $\mathfrak{p}$ are the elements whose orders are >0, and the units of $\mathfrak{o}$ are the elements of order 0. The elements t for which $\mathfrak{p} = t\mathfrak{o}$ are the elements of order 1; they are also called *uniformizing variables* at $\mathfrak{p}$.

Now, let us return to the case where R is of the form $K\langle x\rangle$, with the supplementary assumption that K is the field of complex numbers. If $a \in K$, $x - a$ is an irreducible polynomial and every irreducible polynomial in x with coefficients in K is of the form $\lambda(x - a)$, $\lambda \in K$, $\lambda \neq 0$. Denote by $\mathfrak{p}_a$ the place which corresponds to the irreducible polynomial $x - a$. The polynomials h in x which are divisible by $x - a$ are those for which $h(a) = 0$. Thus the elements of the ring $\mathfrak{o}_a$ of $\mathfrak{p}_a$ are the rational fractions which do not admit a as a pole, while the elements of $\mathfrak{p}_a$ are the rational fractions which admit a as a zero. Furthermore, if ν_a is the order function at $\mathfrak{p}_a$, any rational fraction $u \neq 0$ may be written in the form $(x - a)^{\nu_a(u)}v$, where v admits a neither as a zero nor as a pole. It follows that, if $\nu_a(u) > 0$, then u admits a as a zero of order $\nu_a(u)$, while, if $\nu_a(u) < 0$, u admits a as a pole of order $-\nu_a(u)$.

Generalizing this terminology, we set up the following definitions (where R is a field of algebraic functions of one variable over a field K):

Let $\mathfrak{p}$ be a place of R. If an element $x \in R$ belongs to $\mathfrak{p}$, then we say that $\mathfrak{p}$ is a *zero of* x; if $x^{-1} \in \mathfrak{p}$, then we say that $\mathfrak{p}$ is a *pole of* x. Furthermore, if there exists an order function $\nu_{\mathfrak{p}}$ at $\mathfrak{p}$, and $\nu_{\mathfrak{p}}(x) > 0$, then we say that $\mathfrak{p}$ is a *zero of order* $\nu_{\mathfrak{p}}(x)$ *of* x, while, if $\nu_{\mathfrak{p}}(x) < 0$, we say that $\mathfrak{p}$ is a *pole of order* $-\nu_{\mathfrak{p}}(x)$ *of* x.

Consider in particular the case where $R = K\langle x\rangle$ and $\mathfrak{p} = \mathfrak{p}_{1/x}$. Let $g = a_0x^n + a_1x^{n-1} + \cdots + a_n$ be a polynomial of degree n in x with coefficients in K. If $x' = x^{-1}$, we can write

$$g = x'^{-n}(a_0 + a_1x' + \cdots + a_nx'^n).$$

Now, $a_0 + a_1x' + \cdots + a_nx'^n$ belongs to the ring $\mathfrak{o}$ of $\mathfrak{p}$ and is not in $\mathfrak{p}$ because $a_0 \neq 0$. It follows that a polynomial of degree n in x admits $\mathfrak{p}_{1/x}$ as a pole of order n. If $u = g/h \in R$ (where g and h are polynomials in x), the order of u at $\mathfrak{p}$ is clearly the difference between the degrees of h and g.

Still assuming that $R = K\langle x\rangle$, let f be any irreducible polynomial in x with coefficients in K; we propose to investigate the residue field Σ of the place $\mathfrak{p}_f$, i.e., the ring $\mathfrak{o}_f/\mathfrak{p}_f$. Set $\mathfrak{q} = \mathfrak{p}_f \cap K[x]$; then those residue classes modulo $\mathfrak{p}_f$ which are represented by elements of $K[x]$ form a subring Σ_1 of Σ which is clearly isomorphic with $K[x]/\mathfrak{q}$. But $\mathfrak{q}$ is the set of multiples of f in $K[x]$; it follows that $K[x]/\mathfrak{q}$ is a field which can be obtained from K by adjunction of an element ζ which satisfies the equation $f(\zeta) = 0$. Now, every element u of $\mathfrak{o}_f$ can be written in the form g/h, with g and h in $K[x]$ and h not in $\mathfrak{q}$. Let $\bar{g}$, $\bar{h}$, and $\bar{u}$ be the residue classes of g, h, and u respectively; then $\bar{g} = \bar{u}\bar{h}$, $\bar{h} \neq 0$, whence $\bar{u} = \bar{g}\bar{h}^{-1}$. But $\bar{g}$ and $\bar{h}$ are in Σ_1 which is a field; therefore $\bar{u} \in \Sigma_1$ and $\Sigma = \Sigma_1$. Thus, the residue field Σ of $\mathfrak{p}_f$ can be obtained from K by adjunction of an element ζ such that $f(\zeta) = 0$. In particular, we see that Σ *is algebraic over* K, *of finite degree equal* *to the degree of the polynomial f*. In the case where $f = x$, we have $\Sigma = K$; this shows that the field of constants of $K\langle x\rangle$, which contains K and is contained in Σ, must be K itself. Replacing the consideration of x by that of $1/x$, we see that the residue field of $\mathfrak{p}_{1/x}$ is K.

If K is algebraically closed, every irreducible polynomial in x with coefficients in K is of degree 1, and therefore the residue field of any place coincides with K. Let then $\mathfrak{p}_a$ be the place which corresponds to $x - a$, and let u be an element of $K\langle x\rangle$ which does not have a as a pole. Write $u = g/h$, with g and h in $K[x]$ and $h(a) \neq 0$. We have

$$u - u(a) = \frac{g(x)h(a) - h(x)g(a)}{h(a)h(x)}$$

and $g(x)h(a) - h(x)g(a)$ is divisible by $x - a$. Thus, the value $u(a)$ taken by u at a is also the residue class of u modulo $\mathfrak{p}_a$.

More generally, let R be a field of algebraic functions of one variable over an arbitrary field K, and let $\mathfrak{p}$ be a place of R. Let x be an element of R for which $\mathfrak{p}$ is not a pole. Then the residue class of x modulo $\mathfrak{p}$ (which is an element of the residue field of $\mathfrak{p}$) will be called the *value taken by x at* $\mathfrak{p}$. It should be observed that, if K is not algebraically closed, the value taken by x at $\mathfrak{p}$ is not in general an element of K. The value taken by x at $\mathfrak{p}$ is denoted by $x(\mathfrak{p})$; it is clear that, if neither x nor y has $\mathfrak{p}$ as a pole, then $(x + y)(\mathfrak{p}) = x(\mathfrak{p}) + y(\mathfrak{p})$, $(xy)(\mathfrak{p}) = x(\mathfrak{p})y(\mathfrak{p})$. The elements which admit $\mathfrak{p}$ as a zero are those which take the value 0 at $\mathfrak{p}$.

It is often convenient to say that an element of R which has $\mathfrak{p}$ as a pole takes the value ∞ at $\mathfrak{p}$; ∞ is here a symbol which has no intrinsic connection with the symbol ∞ which was used to complete the definition of the order function at a place.

§4. Existence of places

We shall prove in this section a theorem which implies that any field of algebraic functions of one variable admits infinitely many places.

Theorem 1. *Let R be a field of algebraic functions of one variable over a field K. Assume that we are given a subring $\mathfrak{o}$ of R containing K and an ideal $\mathfrak{p}$ in $\mathfrak{o}$ not containing* 1 *but* $\neq \{0\}$. *Then there exists a place $\mathfrak{P}$ of R whose ring $\mathfrak{O}$ contains $\mathfrak{o}$ and which is such that* $\mathfrak{p} \subset \mathfrak{P} \cap \mathfrak{o}$.

If $\mathfrak{o}'$ is any subring of R containing $\mathfrak{o}$, we shall denote by $\mathfrak{p}\mathfrak{o}'$ the ideal generated in $\mathfrak{o}'$ by the elements of $\mathfrak{p}$. We denote by $\mathcal{F}$ the family of all subrings $\mathfrak{o}'$ of R containing $\mathfrak{o}$ which are such that $\mathfrak{p}\mathfrak{o}' \neq \mathfrak{o}'$; in particular, $\mathfrak{o}$ itself belongs to $\mathcal{F}$. We shall prove that $\mathcal{F}$ contains at least one maximal element (i.e., there is a ring in $\mathcal{F}$ which is not properly contained in any other ring of the family $\mathcal{F}$), and that any such maximal element is a V-ring.

To prove the first assertion, it is sufficient, in virtue of Zorn's Lemma, to prove that the family $\mathcal{F}$ is inductive, i.e., that if $\mathcal{F}'$ is a non empty subfamily of $\mathcal{F}$ such that, of any two rings in $\mathcal{F}'$, one contains the other, then $\mathcal{F}$ contains a ring which contains all rings of the family $\mathcal{F}'$. To do this, denote by $\mathfrak{o}_1$ the set-theoretic union of all rings of $\mathcal{F}'$. If x and y are in $\mathfrak{o}_1$, then $x \in \mathfrak{o}'$, $y \in \mathfrak{o}''$, where $\mathfrak{o}'$ and $\mathfrak{o}''$ are in $\mathcal{F}'$; one of the rings $\mathfrak{o}'$, $\mathfrak{o}''$ contains the other. If for instance $\mathfrak{o}'$ contains $\mathfrak{o}''$, then x and y are both in $\mathfrak{o}'$, whence $x - y \in \mathfrak{o}'$, $xy \in \mathfrak{o}'$, which shows that $x - y$ and xy are in $\mathfrak{o}_1$. The same conclusion subsists if $\mathfrak{o}' \subset \mathfrak{o}''$; therefore, $\mathfrak{o}_1$ is a ring. Since every ring belonging to $\mathcal{F}$ contains $\mathfrak{o}$, $\mathfrak{o}_1$ contains $\mathfrak{o}$. We assert that $\mathfrak{p}\mathfrak{o}_1 \neq \mathfrak{o}_1$. In fact, were this not the case, then we could represent 1 in the form $1 = x_1y_1 + \cdots + x_hy_h$, with $x_i \in \mathfrak{p}$, $y_i \in \mathfrak{o}_1$ $(1 \leqq i \leqq h)$. Each y_i would belong to some ring $\mathfrak{o}^{(i)} \in \mathcal{F}'$. For each pair (i, j), one of the rings $\mathfrak{o}^{(i)}$, $\mathfrak{o}^{(j)}$ would contain the other; since there are only a finite number of rings $\mathfrak{o}^{(i)}$, it follows easily that they would all be contained in one of them, say in $\mathfrak{o}^{(k)}$. But then we would have $1 = \sum_{i=1}^{h} x_iy_i \in \mathfrak{p}\mathfrak{o}^{(k)}$, whence $\mathfrak{p}\mathfrak{o}^{(k)} = \mathfrak{o}^{(k)}$, which is impossible since $\mathfrak{o}^{(k)} \in \mathcal{F}'$. Thus we have $\mathfrak{p}\mathfrak{o}_1 \neq \mathfrak{o}_1$, whence $\mathfrak{o}_1 \in \mathcal{F}'$, which proves that $\mathcal{F}$ is inductive.

Let $\mathfrak{O}$ be a maximal ring in $\mathcal{F}$; we shall prove that $\mathfrak{O}$ is a V-ring. First we show that any element in $\mathfrak{O}$ which is $\equiv 1 \pmod{\mathfrak{p}\mathfrak{O}}$ has an inverse in $\mathfrak{O}$. Let Q be the set of these elements; it is clear that products of elements in Q are in Q. Let $\mathfrak{O}'$ be the set of elements of the form xq^{-1}, with $x \in \mathfrak{O}$, $q \in Q$; then the formulas

$$\frac{x'}{q'} - \frac{x}{q} = \frac{qx' - q'x}{qq'}, \qquad \frac{x}{q}\frac{x'}{q'} = \frac{xx'}{qq'}$$

show that $\mathfrak{O}'$ is a ring. Since $1 \in Q$, $\mathfrak{O}'$ contains $\mathfrak{O}$. We assert that $1 \notin \mathfrak{p}\mathfrak{O}'$. In fact, assume for a moment that

$$1 = \sum_{i=1}^{h} x_i \frac{y_i}{q_i} \qquad x_i \in \mathfrak{p}, \qquad y_i \in \mathfrak{O}, \qquad q_i \in Q \qquad (1 \leqq i \leqq h).$$

Set $q = q_1 \cdots q_h$; then $q \in Q$, whence $q = 1 + \sum_{i=1}^{h'} x_i'y_i'$, with $x_i' \in \mathfrak{p}$, $y_i' \in \mathfrak{O}$, and we have

$$1 = \sum_{i=1}^{h} x_i \,(\prod_{j \neq i} q_j) y_i - \sum_{i=1}^{h'} x_i' y_i' \in \mathfrak{p}\mathfrak{O},$$

which is impossible. Thus, $\mathfrak{O}'$ belongs to $\mathcal{F}$; since $\mathfrak{O}$ is maximal, we have $\mathfrak{O}' = \mathfrak{O}$, whence, if $q \in Q$, $q^{-1} \in \mathfrak{O}$. Now, let u be any element of R not in $\mathfrak{O}$; then $\mathfrak{O}[u] \neq \mathfrak{O}$, whence $\mathfrak{O}[u] \notin \mathcal{F}$ and $\mathfrak{p}\mathfrak{O}[u] = \mathfrak{O}[u]$. It follows that we may represent 1 in the form $1 = \sum_{i=0}^{n} x_iu^i$, with $x_i \in \mathfrak{p}\mathfrak{O}$ $(1 \leqq i \leqq n)$. Since $1 - x_0 \in Q$, we may also write $1 = \sum_{i=1}^{n} x_i'u^i$ with $x_i' = x_i(1 - x_0)^{-1} \in \mathfrak{p}\mathfrak{O}$. We may furthermore assume that, among all representations of 1 in this form, we have selected the one with the lowest n; i.e., it is impossible to represent 1 in the form $1 = \sum_{i=1}^{n'} x_i''u^i$ with $n' < n$, $x_i'' \in \mathfrak{p}\mathfrak{O}$ $(1 \leqq i \leqq n')$. Now, assume for a moment that $u^{-1} \notin \mathfrak{O}$. Then we see in the same way that we can represent 1 in the form $\sum_{i=1}^{m} y_i'u^{-i}$ with $y_i' \in \mathfrak{p}\mathfrak{O}$ $(1 \leqq i \leqq m)$; furthermore, we assume that, among all representations of 1 in this second form, we have selected the one with the smallest possible m. If $n \geqq m$, we may write $u^n = \sum_{i=1}^{m} y_i'u^{n-i}$, whence

$$1 = \sum_{i=1}^{n-1} x_i'u^i + x_n'\left(\sum_{i=1}^{m} y_i'u^{n-i}\right),$$

which is impossible in virtue of our choice of n. Exchanging the roles played by u and u^{-1}, we see in the same way that the assumption that $n \leqq m$ likewise leads to an impossibility. Thus the assumption that $u^{-1} \notin \mathfrak{O}$ leads to a contradiction, and we have $u^{-1} \in \mathfrak{O}$. Since $\mathfrak{p}\mathfrak{O} \neq \mathfrak{O}$, we have $\mathfrak{O} \neq R$; therefore $\mathfrak{O}$ is a V-ring.

Let $\mathfrak{P}$ be the ideal of non-units of $\mathfrak{O}$. Then $\mathfrak{P}$ is a place of R; since $\mathfrak{p}\mathfrak{O} \neq \mathfrak{O}$, an element of $\mathfrak{p}$ cannot be a unit in $\mathfrak{O}$, whence $\mathfrak{p} \subset \mathfrak{P} \cap \mathfrak{o}$. Theorem 1 is thereby proved.

Remark 1. Neither the definition of a V-ring in R nor the proof of Theorem 1 makes any use of the fact that R is a field of algebraic functions of one variable. It follows that our proof of Theorem 1 yields a result which is valid for any pair of fields (K, R) such that K is a subfield of R.

Remark 2. When R is a field of algebraic functions of one variable over K, and when $\mathfrak{p}$ is a prime ideal in $\mathfrak{o}$, it can be proved that the intersection $\mathfrak{P} \cap \mathfrak{o}$ is necessarily equal to $\mathfrak{p}$; however, we shall not have to make use of this more refined result.

Corollary 1. *Let R be a field of algebraic functions of one variable over a field K, and let $x_1, \cdots, x_r$ be elements of R which are not all in K. Let $\mathfrak{a}$ be the set of polynomials $F(X_1, \cdots, X_r)$ in r letters with coefficients in K such that $F(x_1, \cdots, x_r) = 0$. Let $\xi_1, \cdots, \xi_r$ be elements of K such that $F(\xi_1, \cdots, \xi_r) = 0$ for all $F \in \mathfrak{a}$. Then there exists a place of R which is a common zero of $x_1 - \xi_1, \cdots, x_r - \xi_r$.*

Set $\mathfrak{o} = K[x_1, \cdots, x_r]$; an element y of $\mathfrak{o}$ can be represented in the form $P(x_1, \cdots, x_r)$ where P is a polynomial in coefficients in K, and, if $P(x_1, \cdots, x_r) = P'(x_1, \cdots, x_r)$, then $P' - P$ is in $\mathfrak{a}$. It follows that $P(\xi_1, \cdots, \xi_r)$ has the same value for all polynomials P such that $y = P(x_1, \cdots, x_r)$. Let $\mathfrak{p}$ be the set of elements y in $\mathfrak{o}$ for which this value is 0. Then $\mathfrak{p}$ is clearly an ideal in $\mathfrak{o}$; it is $\neq \mathfrak{o}$ because it has only 0 in common with K. If $\mathfrak{P}$ is a place of R such that $\mathfrak{p} \subset \mathfrak{P}$, then $\mathfrak{P}$ is a common zero of $x_1 - \xi_1, \cdots, x_r - \xi_r$.

Corollary 2. *Let R be a field of algebraic functions of one variable over a field K, and let x, y be elements of R, not both constants. Let F be an irreducible polynomial with coefficients in K such that $F(x, y) = 0$. If ξ, η are elements of K such that $F(\xi, \eta) = 0$, then there exists a place of R which is a common zero of $x - \xi$ and $y - \eta$.*

Assume for instance that x is not constant; then y is algebraic over $K\langle x\rangle$. Let $Y^n + \rho_1(x)Y^{n-1} + \cdots + \rho_r(x)$ be a polynomial in Y with coefficients in $K\langle x\rangle$, irreducible in $K\langle x\rangle[Y]$, which admits y as a zero. We may write $\rho_i(x) = P_i(x)/Q_i(x)$, where P_i and Q_i are polynomials with coefficients in K, relatively prime to each other. Let Q be a least common multiple of $Q_1, \cdots, Q_n$; then it is well known that $F_1(X, Y) = Q(X)Y^n + \sum_{i=1}^{n} (Q(X)/Q_i(X))P_i(X)Y^{n-i}$ is irreducible in $K[X, Y]$. Let F' be any polynomial in $K[X, Y]$ such that $F'(x, y) = 0$; then $F'(x, Y)$ is divisible by $F_1(x, Y)$ in $K\langle x\rangle[Y]$; from this and from the irreducibility of F_1 it follows that F' is divisible by F_1. In particular, we have $F = \alpha F_1$, $\alpha \in K$, whence $F_1(\xi, \eta) = 0$ and $F'(\xi, \eta) = 0$. Corollary 2 therefore follows from Corollary 1.