ALGEBRAIC GEOMETRY

By

SOLOMON LEFSCHETZ

GEOFFREY CUMBERLEGE
OXFORD UNIVERSITY PRESS
LONDON
1953

Preface

The present volume grew out of a set of lithoprinted Lecture Notes issued in two parts in 1935–38 and long since out of print. The material of the Notes has been amplified considerably in places, and Chapters II and IV in parts, Chapters III and IX are new. In the main however the general program of the Notes has been preserved. In Chapters II, III, IV, on algebraic varieties the groundfield is generally merely taken infinite. In Chapters V to IX, which except for Chapter IX, are devoted to the classical study of algebraic curves, the groundfield is prudently taken to be algebraically closed and especially of characteristic zero.

It is no secret that the literature on algebraic geometry, now nearly a century old, is as indigestible as it is vast. This field is now undergoing an extensive process of recasting and reorganization in which the most advanced arsenal of modern algebra is playing a fundamental role. At all events one cannot write on algebraic geometry today outside of the general framework of algebra. On the other hand many have come to algebraic geometry and have been attracted to it through analysis, and it would seem most desirable to preserve this attraction and this contact. A common ground for algebra and analysis is found in the method of formal power series which was adopted in the earlier Lecture Notes and is utilized here again to the full. This method has made it possible for example to operate with a general groundfield of characteristic zero, and yet to provide for algebraic curves a treatment surprisingly close to the classical treatment of Émile Picard's *Traité d'Analyse*, vol. 2, or of Severi's *Vorlesungen über algebraische Geometrie.* It is not too much to say that the whole of the classical theory in which the periods play no role may be dealt with by means of formal power series.

By way of preparation it is assumed that the reader is in possession of the rudiments of modern algebra (rings, fields, ideals, polynomials and their factorization) such as are amply developed for our purpose in any recent text. On the geometric side he should also possess elementary information on affine and projective spaces. In point of fact, the topics required along these lines in the book have been summarized in the first chapter and the first few pages of the second.

We wish especially to give our thanks to Ernst Snapper, who read most carefully the whole manuscript and made many exceedingly valuable suggestions for improvement and corrections. We could scarcely exaggerate our debt to him.

S. LEFSCHETZ

Princeton, New Jersey

Published : 1953 *by Princeton University Press*
London : Geoffrey Cumberlege, Oxford University Press
L.C. CARD 52—13158

PRINTED BY THE PITMAN PRESS, BATH, ENGLAND

Contents

ALGEBRAIC GEOMETRY

I. *Algebraic Foundations*

§ 1. PRELIMINARIES

1. The reader is expected to be familiar with the elementary concepts of modern algebra: groups, rings, ideals, fields, and likewise with the customary notations of the subject. Multiplication is supposed to be commutative throughout. To avoid certain awkward points appeal is made to the well known device of an all embracing field Ω which includes all the elements of rings, $\cdots$, under consideration.

(1.1) *Notations.* Aggregates such as $x_0, \cdots, x_n$ or $\alpha_1, \cdots, \alpha_m$ will often be written x or α, the range being generally clear from the context. Accordingly the ring or field extensions $K[x_0, \cdots, x_n]$ or $K(\alpha_1, \cdots, \alpha_m)$ will be written $K[x]$ or $K(\alpha)$, with evident variants of these designations. Similarly for example for the functional notations: $f(x)$ or $\varphi(\alpha)$ for $f(x_0, \cdots, x_n)$, or $\varphi(\alpha_1, \cdots, \alpha_m)$. In this connection the "partial" extensions $K[x_0, \cdots, x_r]$, $K(\alpha_1, \cdots, \alpha_s)$, will also be written $K^r[x]$, $K^s(\alpha)$, with meaning generally clear from the context.

The following symbols of point-set theory will also be utilized throughout:

$\subset$: is contained in; $\supset$: contains; $\cap$: intersection, $\cup$ union; $\in$: is an element of.

(1.2) *The groundfield.* Very soon a certain fundamental field K, the *groundfield* will dominate the situation and all rings and fields will then be extensions of K. When K is of characteristic p the universal field Ω is also supposed to be of the same characteristic. The groundfield is always assumed to be *infinite* and *perfect* (irreducible polynomials have no multiple roots in an algebraic extension of K). Often also K is supposed to be *algebraically closed* (polynomials with coefficients in K have all their roots in K). The unique algebraic closure of a field Φ is denoted by $\overline{\Phi}$.

All rings will have a unit element and will always be *integral domains* (without zero divisors) and with unity element.

(1.3) *Noetherian rings.* This all important class of rings includes all those considered in the book. Consider the following two properties of a ring $\mathfrak{R}$:

(a) *Every sequence of distinct increasing ideals of* $\mathfrak{R}$: $\mathfrak{a}_1 \subset \mathfrak{a}_2 \cdots$, *is necessarily finite.*

(b) *Every ideal* $\mathfrak{a}$ *of* $\mathfrak{R}$ *has a finite base.*

That is to say there is a finite set $\{\alpha_1, \cdots, \alpha_n\}$ of elements of $\mathfrak{a}$, the *base* of the ideal, such that every $\alpha \in \mathfrak{a}$ satisfies a relation:

$$\alpha = \Sigma\lambda_i\alpha_i,\ \lambda_i \in \mathfrak{R}.$$

One refers to (a) as the *ascending chain* property, and to (b) as the *Hilbert base* property. And now:

(1.4) *The ascending chain property and the Hilbert base property are equivalent.*

A Noetherian ring is a ring which possesses one or the other of the two properties, and therefore both.

(1.5) *The polynomial ring $K[x]$ is Noetherian.*

(1.6) *Every ideal $\mathfrak{a}$ of a Noetherian ring and hence of $K[x]$ admits a canonical decomposition $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ where the $\mathfrak{q}_i$ are primary ideals. If $\mathfrak{p}_i$ is the prime ideal associated with $\mathfrak{q}_i$, then the $\mathfrak{p}_i$ are all distinct and unique.*

For a detailed treatment of the above properties see van der Waerden [1], II, Ch. XII.

(1.7) *Homogeneous rings, ideals, and fields.* By a *form* $f(x_0, x_1, \cdots, x_n)$ is meant a homogeneous polynomial. Let the quantities $x_0, \cdots, x_n$ be such that the only relations between them are of type $f_\alpha(x_0, \cdots, x_n) = 0$, where the f_α are forms with coefficients in K. Consider now a collection $\mathfrak{R}_H$ of forms $g \in K[x_0, \cdots, x_n]$ such that if $g, g' \in \mathfrak{R}_H$ then: (a) $gg' \in \mathfrak{R}_H$; (b) if moreover g and g' have the same degree then $g + g' \in \mathfrak{R}_H$ also. In other words $\mathfrak{R}_H$ behaves like a ring save that addition is restricted to forms of the same degree. We refer to $\mathfrak{R}_H$ as a *homogeneous ring* and denote it by $K_H[x_0, \cdots, x_n]$. *Homogeneous ideals* $\mathfrak{a}_H$ of $\mathfrak{R}_H$ are defined in the usual way save that addition is again restricted to forms of equal degree. Homogeneous integral domains, Noetherian rings, prime ideals, primary ideals, are also defined in the usual way and properties (1.4), (1.5), (1.6) hold with all ideals homogeneous. The quotients of forms of $\mathfrak{R}_H$ of the same degree make up a subfield of $K(x_0, \cdots, x_n)$, called a *homogeneous field* and written $K_H(x_0, \cdots, x_n)$.

The extension to *multiforms* $f(\cdots; x_i; \cdots)$ homogeneous separately in say n sets of variables $\cdots; x_i; \cdots$ is quite automatic. The rings and fields are written $K_H^n[\cdots; x_i; \cdots]$ and $K_H^n(\cdots; x_i; \cdots)$.

2. We shall now recall a certain number of properties of polynomials in indeterminates x_i, referring mainly to their factorization.

(2.1) *If $f(x) = f(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$ and $f \neq 0$, there exists an infinite number of sets $\alpha = (\alpha_1, \cdots, \alpha_n)$, $\alpha_i \in K$, such that $f(\alpha) \neq 0$.*

(2.2) *Factorization in the ring $K[x_1, \cdots, x_n]$ is unique to within a factor in K.*

(2.3) *Let $f, g \in K[x_1, \cdots, x_n, y] = K[x; y]$. If f is divisible by g in $K(x_1, \cdots, x_n)[y] = K(x)[y]$,* i.e., *when both are considered as polynomials*

in y with coefficients in $K(x)$, and if g has no factor free from y (i.e. in $K[x]$) then f is divisible by g in $K[x; y]$, or $f = gh$, $h \in K[x; y]$.

(2.4) *Forms.* The following properties may be stated: Let us describe the sets $(\alpha_0, \cdots, \alpha_n)$ and $(\beta_0, \cdots, \beta_n)$ of numbers of K as *essentially* distinct whenever not all the α_i, nor all the β_i are zero and there is no number $\rho \in K$ such that $\beta_i = \rho\alpha_i$, $i = 0, 1, \cdots, n$. Then:

(2.5) *Property* (2.1) *for $n > 1$ holds for forms when the infinite sets $(\alpha_0, \cdots, \alpha_n)$ under consideration are restricted to sets essentially distinct in pairs.*

(2.6) *The factorization properties* (2.2) *and* (2.3) *hold when all the polynomials are forms.*

A polynomial or form $f(x_1, \cdots, x_n)$ of degree s is said to be *regular* in x_i if it contains a term in x_i^s.

(2.7) *Given a polynomial or form $f(x_0, \cdots, x_n) \in K[x_0, \cdots, x_n]$ it is always possible to find a non-singular linear transformation*

$$x_i = \Sigma a_{ij} y_j, \quad a_{ij} \in K, \left| a_{ij} \right| \neq 0$$

which changes f into a new polynomial or form $g(y_0, \cdots, y_n)$ regular in some or all the variables y_j.

§ 2. Resultants and Elimination

3. We shall recall some elementary properties of resultants and elimination theory. For further elaboration and proofs the reader is referred to treatises on algebra, and notably to van der Waerden, [1], II, Chapter XI, and E. Netto, [1], II.

Consider first two polynomials in one variable x:

$$f = a_0 x^m + a_1 x^{m-1} + \cdots + a_m, \quad g = b_0 x^n + \cdots + b_n$$

where the a_i, b_j are indeterminates. The resultant $R(f, g)$ is a doubly homogeneous form in the a_i, b_j, whose coefficients are integers and whose explicit expression is well known but will not be required here. Let $\mathfrak{R}$ be the rational field, $\mathfrak{L}$ any finite algebraic extension of $\mathfrak{R}$ and let $\mathfrak{R}_H^2[a; b]$ and $\mathfrak{L}_H^2[a; b]$ be the associated doubly homogeneous rings of the a_i, b_i. Then the only pertinent facts as to the resultant are:

(3.1) *$R(f, g)$ is of degree n in the a_i and m in the b_j. One of its terms is $a_0^n b_n^m$.*

(3.2) *$R(f, g)$ is irreducible in every ring $\mathfrak{L}_H^2[a; b]$.* (This is so-called "absolute irreducibility.")

(3.3) *There exist unique polynomials A and B of degrees at most $n - 1$ and $m - 1$ in x, with coefficients in $\mathfrak{R}_H^2[a; b]$, such that*

(3.3a) $$Af + Bg = R.$$

(3.4) *Let the coefficients a_i, b_j and the roots ξ_i of f and η_j of g be elements of a field K. Then*

$$R(f, g) = a_0^n b_0^m \Pi(\xi_i - \eta_j) = a_0^n \Pi g(\xi_i) = (-1)^{mn} b_0^m \Pi f(\eta_j).$$

(3.5) *Let f and g have their coefficients in a field K. If they have a common factor $\in \bar{K}[x]$ then $R = 0$. Conversely if $R = 0$ and a_0 or $b_0 \neq 0$ then f and g have a common factor $\in \bar{K}[x]$.*

Let now f, g be forms of degrees m, n in $x_0, \cdots, x_r$. Let $R(f; g; x_i)$ denote the resultant as to x_i, i.e. as if f and g were polynomials in x_i. Then:

(3.6) *Let f or g have indeterminate coefficients. Then $R(f, g; x_r)$ is a form of degree mn in $x_0, \cdots, x_{r-1}$, and in* (3.3a) *A and B are forms in all the x_i and of degrees $\leq n - 1$ and $m - 1$ in x_r. Moreover a n.a.s.c. in order that f, $g \in K_H[x_0, \cdots, x_r]$ both containing x_r and one of them regular in x_r have a common factor containing x_r is that $R(f, g; x_r) = 0$. When it exists the common factor is in $K_H[x_0, \cdots, x_r]$.*

Consider now $r + 1$ forms in $x_0, \cdots, x_r$ with indeterminate coefficients and let m_i be the degree of f_i and $m = \Pi m_i$. There exists a multiform $R_H(f_0, \cdots, f_r)$ in the sets of coefficients of the f_i, whose coefficients are integers, the *resultant* of the f_i, and with the following properties:

(3.7) *R_H is of degree m/m_i in the coefficients of f_i.*

(3.8) *R_H is absolutely irreducible in the ring of multiforms with integral coefficients.*

(3.9) *There take place identities*

$$\Sigma A_j^i f_j = x_i^{s_i} R_H, \quad i = 0, 1, \cdots, r$$

where the A_j^i are multiforms with integral coefficients in the coefficients of the f_j and in the x_i.

(3.10) *If one takes for the f_i forms of $K_H[x_0, \cdots, x_r]$ then $R_H = 0$ is a n.a.s.c. in order that the system*

$$f_0 = \cdots = f_r = 0$$

admit a solution with the x_i not all zero and in $\bar{K}$.

(3.11) *If $a_i x_i^{m_i}$ is the highest degree term in x_i of f_i then R_H contains a term $\Pi a_i^{m/m_i}$.*

More generally given any set of forms $f_0, \cdots, f_p$ with indeterminate coefficients there exists a resultant system $R_H^i(f_0, \cdots, f_p)$, $i = 1, 2, \cdots, q$ where each R_H^i is an irreducible multiform such as R_H above and now:

(3.12) *Same as* (3.10) *with $R_H^i = 0$, $i = 1, 2, \cdots, q$ as the n.a.s.c.*

§ 3. ALGEBRAIC DEPENDENCE. TRANSCENDENCY

4. Let Φ be a field over K. The elements $\alpha_1, \cdots, \alpha_p$ of Φ are said to be *algebraically dependent over K* whenever they satisfy a relation $P(\alpha_1, \cdots, \alpha_p) = 0$, $P(\alpha_1, \cdots, \alpha_p) \in K[\alpha_1, \cdots, \alpha_p]$. If the term α_1 is

actually present in P we say that α_1 is *algebraically dependent on* $\alpha_2, \cdots, \alpha_p$ *over* K. As the groundfield K is generally clear from the context the mention "over K" is usually omitted.

A *transcendence base* $\{\alpha_i\}$ *for* Φ *over* K is a set of elements of Φ such that: (a) no finite subset of the α_i is algebraically dependent; (b) every element $\alpha \in \Phi$ is algebraically dependent upon some finite subset of $\{\alpha_i\}$.

(4.1) *If the number p of elements in one transcendence base is finite (only such cases arise in the sequel) then it is the same for all other such bases.*

The number p of elements in a transcendence base is called the *transcendency* of Φ *over* K, written $\text{transc}_K \Phi$, or merely transc Φ when the particular K is clear from the context.

One may manifestly define the transcendency ρ over K of any set $\{\alpha_1, \cdots, \alpha_s\}$ of elements of Φ as the maximum number of elements which are algebraically independent over K. Let $\Psi = K(\alpha_1, \cdots, \alpha_s)$, so that Ψ is a field between K and Φ. It is readily shown that transc $\Psi = \rho$.

(4.2) *If $K \subset L \subset \Phi$, where all three are fields then* $\text{transc}_K \Phi = \text{transc}_L \Phi + \text{transc}_K L$.

(4.3) *Rational and homogeneous bases.* These two concepts will be found very convenient later. Given a field L over K we will say that a set $\{\alpha_1, \cdots, \alpha_n\}$ of elements of L is a *rational base* for L over K whenever $L = K(\alpha_1, \cdots, \alpha_n)$. A set of elements $\{\beta_0, \cdots, \beta_r\}$ of some field Ψ over L is known as a *homogeneous base* for L over K whenever

$$L = K(\{\beta_i/\beta_j\}), \ \beta_j \neq 0.$$

If $\beta_h \neq 0$ then this condition is equivalent to $L = K(\{\beta_i/\beta_h\})$ where β_h is now fixed.

(4.4) *If L has a finite rational base then $r = \text{transc}_K L$ is finite.*

Another noteworthy property is:

(4.5) *Let K have zero characteristic. Then if $\{\alpha_1, \cdots, \alpha_r\}$ is a transcendence base for L over K and L is a finite extension of $K(\alpha_1, \cdots, \alpha_r)$ there exists an element β of L such that $\{\alpha_1, \cdots, \alpha_r, \beta\}$ is a rational base for L. Hence if M is a field over L and $\alpha_0, \cdots, \alpha_r \in M$ are such that $\{\alpha_i/\alpha_0\}$ is a transcendence base for L and L is a finite extension of $K(\{\alpha_i/\alpha_0\})$, there exists an $\alpha_{r+1} \in M$ with $\alpha_{r+1}/\alpha_0 \in L$ such that $\{\alpha_0, \cdots, \alpha_{r+1}\}$ is a homogeneous base for L.*

§ 4. Extension of the Groundfield

5. In many questions arising naturally in the study of algebraic varieties it is necessary to replace the groundfield K by a finite *pure* transcendental extension, that is to say by an extension $K(u_1, \cdots, u_r)$ by a finite number of indeterminates.

We are particularly interested in what happens then to the polynomial ideals and their mutual relations. Since all questions are trivial for the ideal $\mathfrak{a} = 1$, consisting of all polynomials of the ring $K[x] = K[x_1, \cdots, x_n]$, we assume throughout $\mathfrak{a} \neq 1$.

Let us suppose that the ideal $\mathfrak{a}$ has the base $\{f_1(x), \cdots, f_r(x)\}$. Upon replacing K by any field $L \supset K$ the f_i will span in $L[x]$ a new ideal $\mathfrak{a}^*$ referred to as the *extension* of $\mathfrak{a}$. Let in particular $L = K(u_1, \cdots, u_s)$ be an extension by indeterminates u_j. If $f(x; u_1, \cdots, u_s) \in L[x]$ and disregarding a common denominator $\in L$, we may write

$$f(x; u_1, \cdots, u_s) = \Sigma f_{\alpha \cdots \beta}(x) u_1^{\alpha} \cdots u_s^{\beta}, f_{\alpha \cdots \beta} \in K[x].$$

Then $f \in \mathfrak{a}^*$ is equivalent to: every $f_{\alpha \cdots \beta} \in \mathfrak{a}$. If the extension is by a single variable u we will write

$$f(x; u) = f_0(x)u^n + f_1(x)u^{n-1} + \cdots, f_i \in K[x]. \tag{5.1}$$

The extension operation $\mathfrak{a} \to \mathfrak{a}^*$ has the following properties:

(5.2) *It preserves the relations of inclusion, sum, intersection and product.*

(5.3) *If* $\mathfrak{p}$, $\mathfrak{q}$ *are a prime and a primary ideal then so are* $\mathfrak{p}^*$, $\mathfrak{q}^*$.

(5.4) *If* $\mathfrak{p}$ *is the prime ideal of* $\mathfrak{q}$ *then* $\mathfrak{p}^*$ *is the prime ideal of* $\mathfrak{q}^*$ *and if* $\mathfrak{p}^v \subset \mathfrak{q}$ *then* $\mathfrak{p}^{*v} \subset \mathfrak{q}^*$.

(5.5) *The factorization into primary ideals is preserved.*

Observe at the outset that it is sufficient to consider a simple extension $K(u)$. Moreover since elements of the groundfield may be multiplied in without affecting our arguments we may always assume our polynomials to be polynomials in u also. Finally (5.2) and the derivation of (5.4), (5.5) from (5.2), (5.3) are elementary. Thus we only need to take up the proof of (5.3). The case of prime ideals is simple and indeed it reduces essentially to Eisenstein's classical lemma. We consider it first.

Suppose then $\mathfrak{p}$ prime and let

$$\begin{cases} a(x; u) = a_0(x)u^m + a_1(x)u^{m-1} + \cdots + a_m(x) \\ b(x; u) = b_0(x)u^n + \cdots + b_n(x), \end{cases} \tag{5.6}$$

where a_i, $b_j \in K[x]$. Suppose now that $ab \in \mathfrak{p}^*$. We may manifestly suppress in a and b the terms whose coefficients a_i, $b_j \in \mathfrak{p}$. If as a consequence say a reduces to zero then it was initially in $\mathfrak{p}^*$. Suppose that neither a nor b reduces to zero. Thus we will have (5.6) with a_0, b_0 not in $\mathfrak{p}$. Since $ab \in \mathfrak{p}^*$ all the coefficients of the powers of u in ab must be in $\mathfrak{p}$. Hence $a_0 b_0 \in \mathfrak{p}$ and since $\mathfrak{p}$ is prime one of the factors say $a_0 \in \mathfrak{p}$. This contradiction proves that, say in a, all the coefficients are in $\mathfrak{p}^*$. Hence $a \in \mathfrak{p}^*$ and $\mathfrak{p}^*$ is prime.

6. The case of the primary ideal $\mathfrak{q}$ is much more difficult. Following E. Snapper, its treatment will be made to rest upon a noteworthy lemma due to Dedekind.

(6.1) **Lemma.** *Let a, b be as in* (5.6) *and let*

$$ab = c(x; u) = c_0(x)u^{m+n} + \cdots + c_{m+n}(x).$$

If $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ are the ideals of $K[x]$ spanned respectively by the a_i, b_j, c_k then $\mathfrak{a}^{n+1}\mathfrak{b} = \mathfrak{c}\mathfrak{a}^n$.

We follow Dedekind's own proof as given in: Gesammelte Werke, pp. 36–38. It is clear that $\mathfrak{c} \subset \mathfrak{a}\mathfrak{b}$ hence $\mathfrak{c}\mathfrak{a}^n \subset \mathfrak{a}^{n+1}\mathfrak{b}$. All that is necessary then is to show that the inclusion may be reversed.

Consider first the ideal $\mathfrak{a}^{n+1}$. A finite base for $\mathfrak{a}^{n+1}$ consists of all the products α_j of any $n+1$ of the coefficients a_h. Now $\alpha_j = a_{r_0}a_{r_1-1}\cdots a_{r_n-n}$, $r_0 < r_1 < \cdots < r_n$. Let all the products α_j be ordered lexicographically, and let us agree to set $a_i = 0$ wherever $i > m$. Suppose also the elements of the base $\alpha_0, \alpha_1, \cdots, \alpha_s$ written in increasing order.

Now corresponding to α_j above we may introduce the determinant

$$\delta_j = \left| a_{r_i}, a_{r_i-1}, \cdots, a_{r_i-n} \right|, \quad i = 0, 1, \cdots, n.$$

In its expansion α_j, the diagonal term, is the term of highest order: $\delta_j = \alpha_j +$ terms α_h preceding α_j. Taking then successively $j = s$, $s-1, \cdots$, this relation will enable us to replace in succession, in the base $\{\alpha_j\}$, the elements $\alpha_s, \alpha_{s-1}, \cdots$ by $\delta_s, \delta_{s-1}, \cdots$. In other words $\Delta = \{\delta_j\}$ is a base for $\mathfrak{a}^{n+1}$.

Consider now the following system obtained by equating the powers of u in $ab = c$:

$$a_ib_0 + a_{i-1}b_1 + \cdots = c_i, \quad i = 0, 1, 2, \cdots m+n. \tag{6.2}$$

We may view (6.2) as a set of linear equations in the b_i. The equations beginning with $a_{r_0}, \cdots, a_{r_n}$ have δ_j for determinant of the b's. Hence if $\delta_j \neq 0$, i.e. if δ_j does figure in the base Δ, then the subsystem of the equations just mentioned yields relations

$$\delta_j b_h = \Sigma c_{r_i}\delta_{ji}, \quad h = 0, 1, \cdots, n$$

where the δ_{ji} are minors of order n of δ_j and thus elements of $\mathfrak{a}^n$. Since $\{\delta_j b_k\}$ is a base for $\mathfrak{a}^{n+1}\mathfrak{b}$, this relation implies $\mathfrak{a}^{n+1}\mathfrak{b} \subset \mathfrak{c}\mathfrak{a}^n$. This completes the proof of the lemma.

Returning now to our main problem the proof of (5.3) for $\mathfrak{q}$ primary is immediate. Let $a, b \in K(u)[x]$ where b is not in $\mathfrak{q}^*$. If $c = ab$ then $c \in \mathfrak{q}^*$ implies $\mathfrak{c} \subset \mathfrak{q}$ and b not in $\mathfrak{q}^*$ implies that $\mathfrak{b}$ is not in $\mathfrak{q}$. By the lemma $\mathfrak{a}^{n+1}\mathfrak{b} = \mathfrak{c}\mathfrak{a}^n \subset \mathfrak{q}$. Since $\mathfrak{q}$ is primary and $\mathfrak{b}$ is not in $\mathfrak{q}$, $\mathfrak{a}^{n+1}$ is in $\mathfrak{p}$, hence $\mathfrak{a}$ is in $\mathfrak{p}$ since $\mathfrak{p}$ is prime. If $\mathfrak{p}^\sigma \subset \mathfrak{q}$, then in a^σ every coefficient of u is in $\mathfrak{p}^\sigma$ hence in $\mathfrak{q}$ and so $a^\sigma \in \mathfrak{q}^*$. Hence $\mathfrak{q}^*$ is a primary ideal and this completes the proof of (5.3).

§ 5. DIFFERENTIALS (CHARACTERISTIC ZERO)

7. We shall find it convenient to organise differentiation with differentials and not derivatives in the central position. The treatment, largely following Ernst Snapper, is confined to a field Φ of finite transcendency over a groundfield K.

Let Φ be of transcendency n over K. It is referred to as a *differential field* whenever there is: (a) an n dimensional vector space $\mathfrak{V}$ with Φ as its scalar domain; (b) an operation d: $\Phi \to \mathfrak{V}$ such that if $\alpha, \beta \in \Phi$ and $k \in K$ then:

I. $d(\alpha + \beta) = d\alpha + d\beta$; II. $d\alpha\beta = \alpha d\beta + \beta d\alpha$; III. $dk = 0$; IV. the $d\alpha, d\beta, \cdots$, are a set of generators for $\mathfrak{V}$.

The space $\mathfrak{V}$ is the *space of the differentials of* Φ *over* K, and $d\alpha$ is the *differential of* α *over* K.

Immediate consequences of I, II, III are

$$d(k\alpha) = kd\alpha; \qquad d\alpha^n = n\alpha^{n-1}d\alpha. \tag{7.1}$$

If $\gamma = \alpha/\beta$, then $\alpha = \beta\gamma$, hence quickly from II:

$$d\frac{\alpha}{\beta} = \frac{\beta d\alpha - \alpha d\beta}{\beta^2}. \tag{7.2}$$

If $R(\alpha_1, \cdots, \alpha_p) \in K(\alpha_1, \cdots, \alpha_p)$ denote by R_{α_i} the usual partial derivative (taken as if the α_i were indeterminates). Then:

(7.3) *If* $F(x_1, \cdots, x_p) \in K[x_1, \cdots, x_p]$ *where the* x_i *are indeterminates, then* $F_{x_i} = 0$ *is a n.a.s.c. for* F *not to contain* x_i.

(7.4) *If* $R(\alpha_1, \cdots, \alpha_p) \in K(\alpha_1, \cdots, \alpha_p)$, $\alpha_i \in \Phi$ *then* $dR = \Sigma R_{\alpha_i} d\alpha_i$.

It is first proved for a polynomial then by means of (7.2) for any R.

(7.5) *If* $\mathfrak{A} = \{\alpha_1, \cdots, \alpha_n\}$ *is a transcendence base for* Φ *then* $d\mathfrak{A} = \{d\alpha_i\}$ *is a linear base for* $\mathfrak{V}$.

If $\beta \in \Phi$ there is a relation

$$F(\alpha; \beta) = \beta^r + F_1\beta^{r-1} + \cdots + F_r = 0, \; F_i \in K(\alpha), \tag{7.6}$$

where $F(\alpha; x)$ is irreducible as an element of $K(\alpha)[x]$. Owing to this it has no common factor with

$$F_x = rx^{r-1} + (r-1)F_1x^{r-2} + \cdots$$

whose degree $< r$, and hence $F_\beta \neq 0$. Applying (7.4) we find

$$F_\beta d\beta + \Sigma F_{\alpha_i} d\alpha_i = 0$$

and hence

$$d\beta = -\sum \frac{F_{\alpha_i}}{F_\beta} d\alpha_i. \tag{7.7}$$

Therefore $d\mathfrak{A}$ spans $\mathfrak{V}$.

(7.8) The ordinary or partial successive derivatives of various orders are defined in the obvious way. We merely recall:

(7.9) *Let* $f(x) \in K[x]$, x *indeterminate. N.a.s.c. in order that* $c \in \bar{K}$ *be an* n*-tuple root of* $f(x)$ *are*:

$$f(c) = f'(c) = \cdots = f^{(n-1)}(c) = 0, \quad f^{(n)}(c) \neq 0.$$

(7.10) *Remark.* Ordinary or partial derivatives of any order may be defined for a groundfield of any characteristic and the formal properties (7.3) and (7.9) continue to hold.

8. Construction of a system of differentials. Take for the $d\alpha_i$ independent vectors and compute $d\beta$ for any $\beta \in \Phi$ by (7.7). This defines d obeying rules I, II, III over a simple extension $\Phi_\beta = K(\alpha; \beta)$. Let us show that it is unique over Φ_β. An element γ of Φ_β may have various representations

$$\gamma = R(\alpha; \beta) = R_1(\alpha; \beta) = \cdots,$$

and we must show that

$$dR(\alpha, \beta) = dR_1(\alpha, \beta) = \cdots.$$

In the last analysis we must prove that if $S(\alpha; \beta) \in K(\alpha; \beta)$ and $S(\alpha; \beta) = 0$ then $dS(\alpha; \beta) = 0$. This follows however by rule III.

Suppose now $\beta \in \Phi_\gamma$. Since d is uniquely defined throughout Φ_γ, $d\beta$ is the same whether obtained as element of Φ_β or of Φ_γ. Hence d is unique throughout Φ.

9. We shall now show that the system $(d, \mathfrak{V})$ is essentially unique.

Let Φ, Φ' be isomorphic fields over K under an isomorphism $\tau\colon \Phi \to \Phi'$ preserving K, and let d, $\mathfrak{V}$ and d', $\mathfrak{V}'$ have their natural meaning. A *differential isomorphism of* $\mathfrak{V}$ *onto* $\mathfrak{V}'$ is a mapping $\Delta\colon \mathfrak{V} \to \mathfrak{V}'$ such that if V, $V_1 \in \mathfrak{V}$ and $\alpha \in \Phi$ then

$$\Delta(V + V_1) = \Delta V + \Delta V_1; \quad \Delta(\alpha V) = \tau\alpha \Delta V; \quad \Delta d\alpha = d'(\tau\alpha).$$

(9.1) $\mathfrak{V}$ *and* $\mathfrak{V}'$ *are differentially isomorphic. Hence in a given field differentiation is unique to within a differential isomorphism.*

If we write α_i', β', R' for $\tau\alpha_i$, $\tau\beta$, τR then under our rules $d'\beta'$ is given by (7.7) with the appropriate changes. Define now $\Delta d\alpha_j = d'\alpha_j'$, $\Delta(\gamma d\alpha_j) = \gamma' d'\alpha_j'$, and extend Δ linearly to the whole of $\mathfrak{V}$ which can be done since $\{d\alpha_j\}$ is a base for $\mathfrak{V}$. As a consequence Δ is manifestly a differential isomorphism $\mathfrak{V} \to \mathfrak{V}'$.

10. (10.1) *If* $\alpha_1, \cdots, \alpha_k$ *are algebraically independent elements of* Φ *then* $d\alpha_1, \cdots, d\alpha_k$ *are linearly independent elements of* $\mathfrak{V}$ *and conversely.*

The algebraic independence of the α_i, $i \leq k$, implies $k \leq n =$ transc Φ. Hence one may then augment the set by elements $\alpha_{k+1}, \cdots, \alpha_n$, to form a transcendence base $\mathfrak{A} = \{\alpha_j\}$. Since the $d\alpha_j$, $j \leq n$, are linearly independent elements of $\mathfrak{V}$ (7.5) the same holds for those with $j \leq k$.