JOURNAL OF NUMBER THEORY **28**, 17–61 (1988)

Local Differents of Algebraic and Finite Extensions of Valued Fields

MARC KRASNER

1, rue Ernest Gouin, 75017 Paris, France

Communicated by H. Zassenhaus

Received September 5, 1981

The properties of discriminants and differents were studied first by Dedekind and Hilbert in finite algebraic extensions of fields of algebraic numbers. From a local point of view, that is equivalent to a study of the p-adic case, where the results of Dedekind and Hilbert can be formulated as follows. Dedekind's theorem: The g.c.d. $\Delta(K/k)$ of differents of integral bases of a finite algebraic extension K/k (which I call an algebraic different if K/k) and the g.c.d $\delta(K/k)$ of differents of integral elements of K/k (which I call an arithmetic different of K/k) coincide; Hilbert's theorem (which is the basis of Herbrand's ramification theory of intermediate extensions): If $K \supset L \supset k$, $\delta(K/k) = \delta(K/L)\,\delta(L/k)$. These results are easily generalizable to the "classical case" of henselian valued basic fields, i.e., the case when the valuation is discrete and the residual extension $\bar{K}/\bar{k}$ of K/k is separable. But, in the general case of extensions K/k of valued fields (where k may be assumed to be henselian), Dedekind's and Hilbert's theorems are not always true: the algebraic different $\Delta(K/k)$ divides the arithmetic different $\delta(K/k)$, but generally $\delta(K/k) \neq \Delta(K/k)$, and Hilbert's theorem holds only for the algebraic different. When the valuation is discrete, I call an extension K/k *dedekindian* when $\delta(K/k) = \Delta(K/k)$ and *hilbertian* if, for every intermediate field L of K/k (i.e., $K \supseteq L \supseteq k$), Hilbert's theorem $\delta(K/k) = \delta(K/L)\,\delta(L/k)$ for arithmetic differents holds. When the valuation is dense, the situation is more complicated, because of the existence of two kinds of ideals (principal and other), and it is convenient to define dedekindian and hilbertian extensions in a slightly different manner and to introduce somewhat wider classes of extensions called *quasi-dedekindian* and *quasi-hilbertian.* I study the relations between $\Delta(K/k)$ and $\delta(K/k)$, and, in particular, I give a complete characterization of dedekindian extensions for both discrete and dense valuations; I also give examples of non-dedekindian and non-hilbertian extensions. In Section 4, some connections with the ramification theory (both for normal and non-normal extensions) are studied and a weak analog of Hilbert's theorem [$\delta(K/k)\,\delta(L/k)$ divides $\delta(K/k)$] is proved.

INTRODUCTION

Let k be a valued field[1] in the ordinary sense (i.e., its valuation takes real values; some of the definitions and results of this paper hold also when

[1] Which is supposed to be commutative.

0022-314X/88 $3.00

k is valued in the Krull sense [I say, is "hypervalued"], but I shall limit myself here to the case of ordinary valuations). In order to avoid minor complications, we shall suppose that k is henselian.[2] We shall denote $|\cdot\cdot|$ its valuation,[3] $v(\cdot\cdot) = -\ln|\cdot\cdot|$ its valuative order (or exponent), $i = \{x \in k;\ |x| \leqslant 1\}$ its valuation (or integrity) ring, $m = \{x \in k;\ |x| < 1\}$ the maximal ideal of i, $\bar{k} = i/m$ the residual field of k, p the characteristic of $\bar{k}$ (which is called the residual characteristic of k), $\bar{a} = a + m \in \bar{k}$ the rest of an $a \in i$, $\bar{f}(X) = \sum \bar{a}_i X^i$ the residual polynomial of a polynomial $f(X) = \sum a_i X^i \in i[X]$, $\Gamma(k) = \{|x|;\ x \in k, x \neq 0\}$ the valuation (multiplicative) group of k, $v(k) = \{v(x), x \in k, x \neq 0\}$ the "additive" valuation (or exponent) group of k (which is additive).

Let K/k be a separable extension of finite degree $n = [K : k]$.

The valuation of k can be prolonged, and only in one manner, to a valuation of K (even if K/k is only algebraic). By $|\cdot\cdot|$ and $v(\cdot\cdot)$ we shall denote this unique valuation of K prolonging that of k, and $v(\cdot\cdot)$ the corresponding exponent.

Sometimes we shall consider also a normal algebraic overextension K'/k of K/k, which may be its algebraic closure, and we shall still denote $|\cdot\cdot|$ and $v(\cdot\cdot)$ the unique prolongation of the valuation and of the exponent of k to K'.

We shall denote I, M, $\bar{K}$, $\Gamma(K)$, $v(K)$, respectively, the valuation ring, the maximal ideal of I, the residual field, the valuation, and the exponent groups of K, and by I', M', K', $\Gamma(K')$, $v(K')$ the corresponding objects for K'. Clearly $v(k)$ is a subgroup of $v(K)$, and the index $e = (v(K) : v(k))$ is called the *ramification order* of K/k.

The field $\bar{k}$ can be canonically identified (in identifying for every $a \in i$, $a + m \in \bar{k}$ with $a + M \in \bar{K}$) with a subfield of $\bar{K}$, and the degree $f = [\bar{K} : \bar{k}]$ of the "residual extension" $\bar{K}/\bar{k}$ of K/k is called the *residual degree* of K/k.

As it is well known, if the valuation of k is discrete, $n = fe$. If the valuation of k is dense, by the "defect theorem" of Ostrovski (see [16]), fe divides n, and $d = n/ef$, which is called the *defect* of K/k, is a power of p.

We shall denote $\tilde{S}$ the separable kernel (i.e., the maximal separable subextensions of an algebraic extension S/T, and, then, $[\tilde{S} : T]$ will be called the *separable degree* of K/k.

[2] As is well known, k is surely henselian when it is complete.

[3] I continue to call *valuation* what some people call now "absolute value." I do not see any valid reason for this change, and, besides, it can create some ambiguity, because, in some arguments, the ordinary absolute value of real numbers may coincide with this absolute value. So, the valuation of k is a mapping $|\cdot\cdot| : k \to R_+$ of k into the set R_+ of non-negative real numbers, such, that

$$1^\circ\ |x| = 0 \Leftrightarrow x = 0; \qquad 2^\circ\ |x + y| \leqslant \mathrm{Max}(|x|, |y|): \qquad 3^\circ\ |xy| = |x|\,|y|.$$

What some people call "valuation," will be called "valuative order" (or simply "order" if no ambiguity is possible) or "additive valuation" or, according to Shafarevitch and Borevitch, "exponent" [1]).

So the separable degree $\tilde{f}$ of $\bar{K}/\bar{k}$ will be called the *separable residual degree* of K/k.

If $e = \tilde{e}p^{\mu}$, where $\tilde{e}$ is prime to p, $\tilde{e}$ will be called the separable ramification order of K/k.[4] Let $G = G(K/k)$ be the set of all isomorphisms of K/k into some normal overextension K'/k of K/k. We denote 1_K the identical isomorphism of K, and by G^* the set $\{\sigma \in G; \sigma \neq 1_K\}$.

Generally, G will be written $\{\sigma_1, \sigma_2, ..., \sigma_n\}$, where the $\sigma \in G$ are numbered in some way. If $\sigma \in G$ and $a \in K$, $v(\sigma; a) = v(\sigma \cdot a - a)$ will be called the *characteristic number* (or *value*) of σ in a.[5] Clearly, $v(\sigma; a) = +\infty$ iff $\sigma \in G(K/k(a))$.

If not, it belongs to $v(K')$, but not always to $v(K)$ [that happens with certainty only when K/k is normal]. This notion belongs, in fact, to the ramification theory [in normal and in non-normal extensions] but we shall speak here not much about this theory, because, otherwise, we shall be led too far from our main purpose. If $a \in K$, let $f_a(X) = f_{a,K/k}(X)$ be the characteristic polynomial of a in K/k (which is the minimal polynomial of a over k if a is primitive in K/k).

Then, if $f'_a(X) = df(X)/dX$ is the derivative of $f_a(X)$, we have $f'_a(a) = \prod_{\sigma \in G^*} (a - \sigma \cdot a)$ so $v(f'_a(a)) = \sum_{\sigma \in G^*} v(\sigma; a)$ (for this addition, the sum is $+\infty$ if some of $v(\sigma; a)$, $\sigma \in G^*$, is $+\infty$).

The ideal $\delta_{K/k}(a)$ [which will be denoted by $\delta(a)$ if a is primitive in K/k; besides, if a is not primitive, $\delta_{K/k}(a) = (0)$] generated by $f'_a(a)$ is called the *arithmetic different* of a K/k, and the g.c.d. of $\delta_{K/k}(a)$, $a \in I$ which is equal to the g.c.d. of $\delta(a)$, where $a \in I$ and is primitive in K/k is called the *arithmetic different* of K/k and denoted $\delta(K/k)$.

Let $A = \{a_1, a_2, ..., a_n\}$ be a linear basis of K/k (which will be called *integral* if all a_i are $\in I$).

Then if $d(A)$ is the determinant $\det(\sigma_i \cdot a_j)$ of the matrix $(\sigma_i \cdot a_j)$ $(i = 1, 2, ..., n;\ j = 1, 2, ..., n)$ the ideal $D(A)$ generated by $d(A)^2$ (which, obviously, does not depend on the numbering of the elements of A and that of the elements of G) is called the *algebraic discriminant* of A, and the g.c.d. $D(K/k)$ of the algebraic discriminants $D(A)$ of all the integral bases A of K/k is called the *algebraic discriminant* of K/k.

The ideals $\Delta(A) = D(A)^{1/n}$ and $\Delta(K/k) = D(K/k)^{1/n} = \text{p.q.d. } \{\Delta(A);\ A \text{ integral}\}$ are called *algebraic differents* of, respectively, A and K/k. If $B_a = \{1, a, ..., a^{n-1}\}$ and a is primitive in K/k, we have $\delta(a) = \Delta(B_a)$, and, therefore, $\Delta(K/k)$ divides $\delta(K/k)$. When the valuation of k is discrete, the extension K/k is called *dedekindian* when $\delta(K/k) = \Delta(K/k)$ (because

[4] This terminology has some deep reasons, which cannot be given in this paper; see [13].

[5] When $f: A \to B$ is a mapping and $a \in A$, f, a will denote the image of a by f, and the point "$\cdot$" will have only this mathematical use. In particular, the product or multiplicatively written compositum of two objects ξ, η, will always be written $\xi\eta$ and never $\xi \cdot \eta$ even if ξ, η are mappings (but, in this last case, we may use the Bourbaki notation $\xi \circ \eta$).

Dedekind proved this equality in the case of finite degree, for fields of algebraic numbers, or what is practically the same, in the p-adic case). In case of dense valuations, more subtle distinctions must be introduced: Only some extensions (satisfying some additional conditions) such that $\delta(K/k) = \Delta(K/k)$ are considered as dedekindian; the other ones and as well as the extensions that satisfy conditions weaker than the one given in considered as quasi-dedekindian text.

Some even more subtle distinctions may be made among these extensions, but they will not even be defined in this paper.

It is easy to show (by slightly modifying Dedekind's and Hilbert's original proofs), that K/k is dedekindian if the valuation of k is discrete and the residual extension $\bar{K}/\bar{k}$ of K/k is separable (I call this situation the *classical case*). But even if the valuation is discrete, there exist non-dedekindian extensions.

I found the first example of such extensions (that of Example 1 of Sect. 3 of this paper) in June 1940, during the war, and I indicated it in a footnote of my note [2] of *Comptes Rendus* (1945). When E. Artin came to Paris in 1949, I learned from him that he also found (I do not know when) such examples independently.

So, the problem arises: When is a valued separable extension of finite degree dedekindian (or, in case of dense extensions only, quasi-dedekindian)? In this paper I give a complete answer to the first question ("dedekindian problem"). The study of the "quasi-dedekindian" problem, which is much more difficult and requires the introduction of some very new notions, will be reserved for another publication.

It is not difficult to show that the algebraic different satisfies Hilbert's Theorem 39: if L is an intermediate field of K/k (i.e., $K \supseteq L \supseteq k$), $\Delta_{K/k} = \Delta_{K/L}\, \Delta_{L/k}$. An extension K/k will be called *hilbertian* if, for every intermediate field L of K/k, $\delta_{K/k} = \delta_{K/L}\, \delta_{L/L}$ holds also. In the case of dense valuations, a wider class of extensions, satisfying a slightly weaker condition, can be defined, that of *quasi-hilbertian* extensions. It can be shown easily that dedekindian extensions and a certain subclass of quasi-dedekindians are hilbertian, and that all quasi-dedekindian extensions are quasi-hilbertian.

It is unknown if other hilbertian or quasi-hilbertian extensions exist. But the extension of the quoted Example 1 of Section 3 is not only non-dedekindian, but also non-hilbertian.

In another example (2) of the same section, I define some extensions, which are non-dedekindian, but, in case of dense valuations, are quasi-dedekindian (though that is not proved in this paper).

So, they are in this case, quasi-hilbertian, but it is shown that they are non-hilbertian. E. Artin, also knew that non-hilbertian extensions exist. For hilbertian extensions and, with only slight differences, for quasi-hilbertian,

Herbrand's theory of ramification properties of intermediate extensions holds (i.e., for a given K/k, the extensions L/M such that $K \supseteq L \supseteq M \supseteq k$), and it holds only for such extensions.

In order not to complicate too much formulations of notions, results and proofs a certain technical device seems absolutely necessary: semi-real numbers.

I hope that the reader will share the opinion that I introduced in [6] in 1944. This notion, which will be defined in Section 1 and used extensively throughout the paper is obtained by a certain completion of the ordered complete set $R^0 = R \cup \{-\infty, +\infty\}$ of real numbers (where R is the real field ordered in usual way); a particular case of a completion defined in 1935 by G. Kurepa in his Ph.D. thesis [15] for every totally ordered set. It is, besides, useful to define such completions for the set of values $\Gamma(k) \cup \{0\}$ of hypervaluations of the hypervalued field k. In that more general context, but in an implicit and artificial manner, the notion was, in fact, used already in the early 1930s by Krull and Deuring under the name of "symbolic function," though only from the point of view of order. But, in the theory of valuations also, some partial rational operation on semi-real numbers is needed (and also the prolongation of some real functions to semi-real domains). Some of them are defined and used in this paper. An $a \in I$ is called *discriminantial* if $\delta(a) = \delta(K/k)$.

Such elements exist certainly when the valuation of k is discrete. If, in that case, $v(\sigma) = \mathrm{Min}_{a \in I} v(\sigma; a)$ [such a minimum exists certainly when the valuation is discrete, but it is shown in Section 4 that it exists, in the case of dense valuations for every $\sigma \in G$, iff there exist discriminantial elements], it is shown that for a discriminantial $a \in I$, we have $v(\sigma; a) = v(\sigma)$. In the general case, with the help of the semi-real numbers, $v(\delta(K/k))$ and $v(\sigma)$ are also defined, and it is shown that for every $\varepsilon > 0$ an $a \in I$ exists such that, for every $\sigma \in G$, $v(\sigma; a) \leqslant v(\sigma) + \varepsilon$. This result is necessary for proving that, for any intermediate field L of K/k, $\delta(K/L)\,\delta(L/k)$ divides $\delta(K/k)$. The paper finishes with a certain study of $v(\sigma; a)$ and some related objects as functions not only of σ for fixed a, as is done in the "extrinsic" ramification theory (see Krull [14], Krasner [8, 10, 13]), but also as a function of a for a fixed σ, which permits few applications to the ramification theory, in particular for normal extensions. In Section 1, some preliminary (and mostly known) notions and results are expounded. In Section 2, the algebraic differents (and discriminants) of an extension and of its linear bases are defined and their properties are studied. In Section 3, the arithmetic differents are defined and their relation to algebraic differents are studied. In particular, the dedekindian, quasi-dedekindian, hilbertian, and quasi-hilbertian extensions are defined, the "dedekindian problem" is solved, and some examples of non-dedekindian and non-hilbertian extensions are given.

In Section 4, the characteristic numbers $v(\sigma)$ of $\sigma \in G$ are defined and the existence of $a \in I$, F is proved such that the $v(\sigma; a)$ approximate, as nearly as wanted, simultaneously all corresponding $v(\sigma)$ (and $v(\sigma; a) = v(\sigma)$ in the case of discrete valuations). That permits us to complete the study of properties of arithmetic differents and to give a few applications to the ramification theory.

1. Some Preliminary Notions

Let k be a henselian valued field. Let be $|\cdot\cdot|$ its valuation, $v(\cdot\cdot) = -\ln |\cdot\cdot|$ its valuative order, $d(x, y) = |x - y|$ its ultrametric distance,

$$C(a, r^-) = \{x \in k;\ d(a, x) < r\}$$

and

$$C(a, r) = \{x \in k;\ d(a, x) \leqslant r\}$$

non-circumferenced and circumferenced discs of k of center a and of radius r. The disc $i = C(0, 1) = \{x \in k;\ |x| < 1$ is a ring called a *valuation* (or *integrity*) ring of k, and discs $C(0, \rho)$, $\rho = r^-$, when $r > 0$, and $\rho = r$, when $r \geqslant 0$, are the only i-modules of k, and they are the ideals of i iff $\rho < 1$ (i.e., $\rho = r^-$ with $r \leqslant 1$ or r with $r < 1$); traditionally, these discs are called "fractional ideals of k" and we shall also adopt this terminology. We shall multiply these discs as subsets of k.

In order to understand the sense of the symbol ρ in $C(a, \rho)$, and also for other purposes, we shall introduce the notion of semi-real numbers. Let R^0 be the closed (i.e., comprising $-\infty$ and $+\infty$) ordered set of all real numbers, ordered by its natural order, and let be $\Xi = \{-, 0, +\}$, this set being ordered by the order $<$ such that $- < 0 < +$. Let us consider the set $R^0 \times \Xi$ ordered lexicographically (i.e., we have $(r, \xi) < (r', \xi')$ iff $r < r'$ or $r = r'$ and $\xi < \xi'$). We shall take out the extreme elements $(-\infty, -)$ and $(+\infty, +)$ of $R^0 \times \Xi$, and the remaining elements will be called semi-real numbers (and their ordered set will be denoted S and called the *semi-real straight line*). A real number r will be identified with the semi-real number $(r, 0)$, and we shall write r^- and r^+ instead of $(r, -)$ and $(r, +)$. If $\rho = (r, \xi)$, r will be called the *real value* and ξ the *species* of ρ.

Let $A \subseteq R^0$ be a set of real numbers (in the broad sense, i.e., the $-\infty$ and $+\infty$ may be $\in A$). This set always has an infimum and a supremum on R^0. If $a = \operatorname{Sup}_{R^0} A$, then the semi-real numbers permit us to distinguish explicitly the cases when this supremum is reached or not reached. Indeed, the supremum $\operatorname{Sup}_S A$ of A on the semi-real straight line S is a if it is reached and is a^- if it is not reached. In an analogous way, if $a = \inf_{R^0} A$, we have $\operatorname{Inf}_S A = a$ or a^+ if, respectively, the $\operatorname{Inf}_{R^0} A$ is reached or not.

If M is a metric space with the distance $d(x, y)$, and if $m \in M$ and $N \subseteq M$, we define the *semi-real radius* of N with respect to m the semi-real number $r_m(N) = \mathrm{Sup}_S\{d(m, x); x \in N\}$, and we define the *diameter* of N with the semi-real number

$$d(N) = \operatorname*{Sup}_S \{d(x, y); (x, y) \in N \times N\}.$$

Clearly, $d(N) = \mathrm{Sup}_S\{r_m(N); m \in N\}$. If M is an ultrametric space (i.e., $d(x, z)$ is always $\mathrm{Max}[d(x, y), d(y, z)]$), then there exists, for any $N \subseteq M$, the least disc (we consider also as disc $M = C(z, +\infty^-)$ for every $a \in M$) of M containing N (that is, the intersection of all discs of M containing N; in the ultrametric case, this intersection is, indeed, a disc which will be denoted by $C(N)$ and called the *circular envelope* of N), and if $m \in N$, it holds $r_m(N) = d(c(N))$, so $d(N)$ is also $= d(c(N))$ and $r_m(N) = d(N)$. So, if M is the field k with its distance $d(x, y) = |x - y|$, we have first that

$$C(a, \rho) = \{x \in k; d(a, x) \leqslant \rho\} \qquad \text{and} \qquad r_a(C(a, \rho)) = d(C(a, \rho))$$

is ρ. This $d(C(a, \rho))$ will be called the *proper* radius (or diameter of the disc $C = C(a, \rho)$. In particular, if $q = C(0, \rho)$ is a fractional ideal of k, $|q| = d(q)$ will be called the *valuation* of q. The function $-\ln X$ can be extended easily to semi-real positive values by putting $-\ln(r, \xi) = (-\ln r, -\xi)$, where (r, ξ) is supposed to be $\geqslant 0 = (0, 0)$ and $--=+$, $-0=0$ and $-+=-$. Then $v(q) = \ln|q| = \mathrm{Inf}_S\{v(x); x \in q\}$ is called the *valuative order* of q (in fact, this order was implicitly used already by Krull, who considered, for an ideal q, the real value $\mathrm{Inf}_{R^0}\{v(x); x \in q\}$ of $v(q)$, and also its species, which he called "symbolic function"; he did it also for the case of hypervaluations, where the semi-real numbers have to be replaced by a convenient completion of the valuation group, the so-called "Kurepa completion."

Some partial rational operations can (and must) be defined for semi-real numbers. That is done, in a general form, in accordance with some very natural reasons, having no connection with problems of valued fields. But the operations so-defined are such that for any two fractional ideals q_1, q_2, the sum $v(q_1) + v(q_2)$ (and, also, the product $|q_1|\,|q_2|$) exists and is equal to $v(q_1 q_2)$ (resp. $|q_1 q_2|$). Besides, when performable, these operations have the ordinary properties of commutative rings: addition and multiplication are commutative and associative, and the multiplication is distributive in respect to addition. We shall not proceed in this manner, but give the explicit definition of some operations in the cases where they are needed in this paper:

Two species $\xi_1, \xi_2 \in \Xi$ are called *opposite* if one of them is $+$ and the

other $-$. If ξ_1, ξ_2 are not opposed, their *dominant* $\mathrm{dom}(\xi_1, \xi_2)$ is defined by the rule

$$\mathrm{dom}(+,+)=\mathrm{dom}(+,0)=\mathrm{dom}(0,+)=+,$$

$$\mathrm{dom}(0,0)=0, \qquad \mathrm{dom}(-,-)=\mathrm{dom}(-,0)=\mathrm{dom}(0,-)=-.$$

(1) The sum $\rho_1+\rho_2$, where $\rho_1=(r_1,\xi_1)$ and $\rho_2=(r_2,\xi_2)$ is defined iff ξ_1 and ξ_2 are not opposite, and then it is

$$(r_1+r_2, \mathrm{dom}(\xi_1,\xi_2)).$$

(2) $-\rho$, where $\rho=(r,\xi)$ is always defined and is $(-r,-\xi)$. We write $\rho_1-\rho_2=\rho_1+(-\rho_2)$.

(3) If $\rho_1=(r_1,\xi_1)\geqslant 0$ and $\rho_2=(r_2,\xi_2)\geqslant 0$, $\rho_1\rho_2$ is defined in the following cases:

(a) ρ_1 or ρ_2 is 0; then $0\rho_2=\rho_1 0=00=0$,

(b) $\rho_1>0$ and $\rho_2>0$; then $\rho_1\rho_2$ is defined iff ξ_1, ξ_2 are not opposite, and $\rho_1\rho_2=(r_1r_2, \mathrm{dom}(\xi_1,\xi_2))$.

In particular, if s is a real number >0, $s\rho=s(r,\xi)$ is defined and (sr,ξ).

A fractional ideal of k is an ideal of i iff $|q|\leqslant 1$ (or $v(q)\geqslant 0$). The maximal ideal of i is $m=C(0,1^-)=\{x\in k;\ |x|<1\}$. The quotient ring $\bar{k}=i/m$ is a field called the *residual field* of k, and its characteristic p is called the *residual characteristic* of k. The characteristic of k will be denoted by p' (k is said to be *homotypic* if $p'=p$ and *heterotypic* if $p'\neq p$, which requires, as it is well known, $p'=0$). If k^* is the multiplicative group of k, $|k^*|=\{|a|;\ a\in k^*\}$ is a subgroup of the multiplicative group of R_+^* of positive real numbers (the set $R_+^*\cup\{0\}$ of non-negative real numbers will be denoted R_+). This group $\Gamma(k)$ will be called the *valuation group* of k. We exclude the case of trivial valuations, where $\Gamma(k)=\{1\}$. There remain two cases:

(1) *Discrete valuations.* When $\Gamma(k)$ has the greatest element $\gamma>1$, it is the infinite cyclic group (γ) generated by γ.

(2) *Dense valuations.* When such γ does not exist, then $\Gamma(k)$ is dense in R_+^*. The image $v(k)=-\ln\Gamma(k)=\{v(a);\ a\in k^*\}$ is a subgroup of the additive group of real numbers, having the least strictly positive element $\omega=-\ln\gamma$ in the case of discrete valuations (and this ω generates it) and dense over real straight line R in the case of dense valuations. It is clear that $|m|=1^-$ (and $v(m)=0^+$) when the valuation is dense, and $|m|=\gamma$ (and $v(m)=\omega$) when the valuation is discrete. So $m^2=m$ or $m^2\neq m$ when the valuation is dense (resp. discrete). The additive group $v(k)$ will be called the *order group* or additive *valuation group* of k.

Let K be an algebraic extension of k. As k is henselian, its valuation can be prolonged to K in one and only one manner, and this prolonged valuation (and corresponding order) will be denoted by the same symbols as that of k. Let I be the valuation ring of K, M the maximal ideal of I, $\bar{K}$ the residual field, and $\Gamma(k)$, $v(K)$ valuation and order groups of K with respect to the prolonged valuation. $\Gamma(k)$ is obviously a subgroup of $\Gamma(K)$, and $e = (\Gamma(K) : \Gamma(k))$ is called the *ramification order* of K/k. If C_k is a disc of k, there exists one and only one disc $C_k = C_k$ of K having the same diameter: $d(C_k) = d(C_k)$, and $C_k \to C_K$ is an injection of the set of all discs of k into that of K. We shall identify C_k with corresponding C_K. That identifies, in particular, every fractional ideal (i.e., i-module) of k with some such ideal (i.e., I-module) of K. So, if the valuation of k is dense, m is identified with M, and if the valuation of k and of K are both discrete, m is identified with M^e. Also the field $\bar{k} = i/m$ can be identified (by a slightly different identification) with a subfield of $\bar{K} = I/M$ and $f = [\bar{K} : \bar{k}]$ will be called the *residual degree* of K/k. If $n = [K : k]$ is finite, fe is a divisor of n, and is $= n$ if the valuation is discrete. If the valuation is dense $d = n$: fe is called the (ramificative) *defect* of K/k. According to the "defect theorem" of A. Ostrovski, this integer is a power of p. The extension K/k of finite degree will be called *non-defective* if $d = 1$ and completely defective if $d = n$. It will be called *not flat* if $f = 1$ and *completely flat* if $f = n$; and it will be called *not slim* if $e = 1$ and *completely slim* if $e = n$.

Let $\bar{k}_k^{(s)}$ be the separable Kernel of K/k, i.e., the greatest intermediate field of $\bar{K}/\bar{k}$ which is separable over $\bar{k}$. $\tilde{f} = [\bar{k}_k^{(s)} : \bar{k}]$ is called the *separable residual degree* of K/k. Supposing always $n = [K : k]$ finite, K/k is said to be *non-ramified* if $\tilde{f} = n$ and *completely ramified* if $\tilde{f} = 1$. If $e = \tilde{e}p^m$, where $e \not\equiv 0 \pmod{p}$, $\tilde{e}$ is called the *separable ramification order* of K/k, and K/k is said to be *separably ramified* or *non-overramified* if $\tilde{f}\tilde{e} = n$ (for deeper reasons of this terminology, see my preprint [13]; I prefer these terms to the zoomorphic term "tamely ramified") and it is said *overramified* if $\tilde{f}\tilde{e} = 1$. All these terms may be extended, besides, to algebraic extensions of infinite degree (see [13]).

Let K/k be an algebraic extension and K'/k its normal overextensions (e.g., we can take as K' the algebraic closure of K), valued by the valuation prolonging that of k. By what precedes, the fractional ideals of k and of K' are canonically identified with some fractional ideals of K', precisely with the I'-module, that they generate, where I' is the valuation ring of K'.

Let σ be an isomorphism of K/k into K' and let σ' be some automorphism of K'/k inducing it. If Q is a fractional ideal of K, consider its transform $\sigma \cdot Q$ by σ, which is a fractional ideal of the field $\sigma \cdot K \subseteq K'$. If $(\Omega)'$ and $(\sigma \cdot Q)'$ are the I'-modules generated by Q and $\sigma \cdot Q$, it is clear that $(\sigma \cdot Q)' = (\sigma' \cdot Q)' = \sigma'(Q)'$. But, as k is henselian, all automorphisms of K/k are, by the Ostrovski lemma, isometries. Therefore as $(Q)'$ is a disc of

K' of center 0, we have $\sigma' \cdot (Q) = (Q)'$. So Q and $\sigma \cdot Q$ are identified with the same fractional ideal of K', and, after this identification, we have $\sigma \cdot Q = Q$. But, then when $n = [K : k]$ is finite, we have, for any fractional ideal Q of K, $N_{K/k}(Q) = Q^n$.

Let $B = (b_1, b_2, ..., b_n)$ be a linear basis of a separable extension K/k of finite degree n, and let $G = (\sigma_1, \sigma_2, ..., \sigma_n)$ be the set of all isomorphisms of K/k into some normal overextension K'/k. For convenience sake we shall always suppose that σ_1 is the identical isomorphism 1_K of K. We call *discriminant* $D(B)$ of B the fractional ideal of K generated by the square $\det(\sigma_i \cdot b_j)^2$ of the determinant $\det(\sigma_i \cdot b_j)$ of the matrix $(\sigma_i \cdot b_j)$ $(i = 1, 2, ..., n, j = 1, 2, ..., n)$. We call the *different* (or sometimes, for certain reasons, *local different*) of B the ideal $\Delta(B) = D(B)^{1/n}$. If $B' = (b'_1, b'_2, ..., b'_n)$ is another linear basis of K/k and if $A(B', B)$ is the transition matrix from B to B', i.e., the square matrix of degree n over k such that $B' = A(B', B)B$ (where B and B' are considered as $n \times 1$ matrices), it is obvious that $\det(\sigma_i \cdot b'_j) = [\det A(B', B)][\det(\sigma_i \cdot b_j)]$, and, if $E_{B',B}$ is the fractional ideal generated by $\det A(B', B)$, we have $D(B') = E^2_{B',B} D(B)$ and $\Delta(B') = E^{2/n}_{B',B} \Delta(B)$.

Let $a \in K$ be a primitive element of K/k and $f_{a/k}(x)$ its minimal polynomial over k. We call the *different* of a the fractional ideal $\delta(a)$ generated by $f'_{a/k}(a) = \prod_{2 \leq i \leq n} (a - \sigma_i \cdot a)$ and we call the *discriminant* of a the fractional ideal $D(a) = N_{K/k}\, \delta(a) = \delta(a)^n$ of k. As a is primitive, $B_a = (1, a, ..., a^{n-1})$ is a linear basis of K/k, and the matrix $(\sigma_i \cdot a^{j-1})$ is a Vandermondian. So

$$\det(\sigma_i \cdot a^{j-1})^2 = \pm \prod_i \prod_{j,\, i \neq j} (\sigma_i \cdot a - \sigma_j \cdot a) = \pm N_{K/k} f'_{a/k}(a)$$

and

$$D(B(a)) = N_{K/k}\, \delta(a) = D(a),$$

so

$$\delta(a) = D(a)^{1/n} = D(B_a)^{1/n} = \Delta(B_a).$$

If $B = (b_1, b_2, ..., b_n)$ is a linear basis of K/k,

$$v(b_1 b_2 \cdots b_n) = v(b_1) + v(b_2) + \cdots + v(b_n)$$

will be called the *height* of B and will be denoted $h(B)$. The basis B is called integral if all b_i are $\in I$, i.e., $v(b_i) \geqslant 0$. Let $i(B) = ib_1 + ib_2 + \cdots + ib_n$ be the i-module generated by B. An integral basis B will be called an ε-basis (where $\varepsilon > 0$) if every a of K such that $v(a) \geqslant \varepsilon$, belongs to $i(B)$, i.e., $i(B)$

contains the disc $C(0, \exp(-\varepsilon))$ of K. In particular, B is a 0-basis iff $i(B) = I$. If B is an ε-basis and the valuation of k is dense, then for every $i = 1, 2, ..., n$, $0 < v(b) \leqslant \varepsilon$ hold. Indeed, if $v(b) > \varepsilon$ then there exists an $a \in k$ such that $\varepsilon - v(b_i) < v(a) < 0$, so that $a \notin i$ and $v(ab_i) > \varepsilon$, hence $ab_i \notin i(B)$ and B is not an ε-basis. So under these conditions, the height $h(B)$ of an ε-basis is $< n\varepsilon$ (and > 0), and, in particular, if B is a 0-basis, $h(B) = 0$. When the valuation is discrete, it is also easy to find an upper bound for the height of a 0-basis of K/k. Let Ω be the least positive element of $v(K)$ (so $\omega = e\Omega$), Π a generator of the maximal ideal M of I (so, $v(\Pi) = \Omega$), and $\bar{C} = (\bar{c}_1, \bar{c}_2, ..., \bar{c}_f)$ some linear basis of K/k. Then, if c_q is a representation of c_q in I (i.e., $\bar{c}_q = c_q + M$), it is well known that the elements $c_q \Pi^s$ $(q = 1, 1, ..., f; s = 0, 1, ..., e-1)$, form a 0-basis of[6] K/k and the height of this basis is

$$f(0 + \Omega + 2\Omega + \cdots + (e-1)\Omega) = fe(e-1)\Omega/2 = [f(e-1)/2]\omega.$$

It will be shown later that the height of a 0-basis cannot exceed this value.

If B and B' are two 0-bases of K/k, and $\Lambda(B', B)$ and $\Lambda(B, B')$ are both integral matrices in k (i.e., matrices in i) then

$$|\det \Lambda(B', B)| \leqslant 1 \qquad \text{and} \qquad |\det \Lambda(B, B')| \leqslant 1.$$

But, as $\Lambda(B, B') = \Lambda(B', B)^{-1}$, we must have

$$|\det \Lambda(B', B)| = |\det \Lambda(B, B')| = 1 \qquad \text{and} \qquad E_{B,B'} = (1).$$

If B is an ε-basis and the valuation of k is dense, consider an $a \in K$. It has the unique expression $a = \sum \lambda_i \cdot b_i$ as a linear combination of b_i, and we say that $v(\lambda_i) \geqslant v(a) - \varepsilon$. Indeed, if for some i, we have $v(\lambda_i) < v(a) - \varepsilon$, there exists a $\mu \in k$ such that $-v(a) + \varepsilon < v(\mu) < -v(\lambda_i)$. So, $\mu a = \sum (\mu\lambda_i) b_i$ and we have $v(\mu a) = v(\mu) + v(a) > \varepsilon$ and $v(\mu\lambda_i) = v(\mu) + v(\lambda_i) < 0$. It follows that $\mu\lambda_i \notin i$ and $\mu a \notin i(B)$, which contradicts that B is an ε-basis. But then, if $B' = (b'_1, b'_2, ..., b'_n)$ is another ε-basis all the elements of the matrix $\Lambda(B', B)$ must have their valuative order $\geqslant -\varepsilon + 0 = -\varepsilon$. So $v(E_{B',B}) = v(\det \Lambda(B', B) \geqslant -n\varepsilon$. As the same inequality holds for $E_{B,B'} = E_{B',B}^{-1}$ we have

$$-n\varepsilon \leqslant v(E_{B',B}) \leqslant n\varepsilon.$$

Let L be an intermediate field of K/k: $K \supset L \supset k$. Let $[K : L] = v$, $[L : k] = n^*$, $\beta = (\beta_1, \beta_2, ..., \beta_v)$ be a linear basis of K/L, $B^* =$

[6] *Proof.* Indeed, if $a \in K$ and $a = \sum \lambda_{q,s} c_q \Pi$, it is obvious that $|a| = \mathrm{Max}_{q,s} |\lambda_{q,s}| \gamma^s$, i.e., $v(a) = \mathrm{Min}_{q,s}[v(\lambda_{q,s}) + s\Omega]$. So, if $a \in I$, i.e., $v(a) \geqslant 0$, we must have $v(\lambda_{q,s}) \geqslant -s\Omega > -\omega$, which implies (as $v(\lambda_{q,s})$ is a multiple of ω), $v(\lambda_{q,s}) \geqslant 0$, and $\lambda_{q,s} \in i$.

$(b_1^*, b_2^*, ..., b_{n^*}^*)$, a linear basis of L/k. It is well known that all $b_i\beta_j$ are distinct and that their set

$$B^*\beta = \{b_i^*\beta_j; i = 1, 2, ..., n, j = 1, 2, ..., v\}$$

is a linear basis of K/k. A calculation, which can be found in Hilbert's "Zahlbericht" [3, Theorem 30] which applies without any change to the present situation (it is based only on formal calculations of determinants), shows that

$$D(B^*\beta) = N_{L/k} D(\beta) = D(B^*)^v.$$

As k is henselian, we have

$$N_{K/k} D(\beta) = D(\beta)^{n^*} \qquad \text{and so} \qquad D(B^*\beta) = D(\beta)^{n^*} = D(B^*)^v$$

and as $n = [K : k] = n^* v$, we have

$$\Delta(B^*\beta) = D(B^*\beta)^{1/n} = D(\beta)^{1/v} D(B^*)^{1/n^*} = \Delta(\beta)\,\Delta(B^*).$$

PROPOSITION 1. *If B^* is an ε-basis of L/k and β is an η-basis of K/L, $B^*\beta$ is an $(\varepsilon+\eta)$-basis of K/k.*

Proof. First, B^* and β being integral bases, $B^*\beta$ also is one. Let $a \in K$ be such that $v(a) \geqslant \varepsilon + \eta$. a is a linear combination $\sum a_j^*\beta_j$ of β over L, and, as β is an η-basis of K/L, we have for each $j = 1, 2, ..., v$, $v(a_j^*) \geqslant v(a) - \eta > \varepsilon$. For every j, $a_j^* \in L$ can be expressed as a linear combination $a_j^* = \sum \lambda_{ij} b_i^*$ of B^* over k, and as B^* is an ε-basis of L/k and $v(a_j^*) \geqslant \varepsilon$, we have $a_j^* \in i(B^*)$ and all λ_{ij} are $\in i$. So, $a = \sum\sum \lambda_{ij} b_i^*\beta_j$ is $\in i(B^*\beta)$ and $B^*\beta$ is an $(\varepsilon+\eta)$-basis of K/k.

2. ALGEBRAIC DIFFERENT, UNFOLDING AND DISCREPANCY OF BASES

Let K/k be an extension of finite degree $n = [K : k]$, and let J be the set of its integral bases. Then the g.c.d. $\Delta(K/k)$ of $\Delta(B)$, where B ranges over all integral bases of K/k is called the *algebraic different* of K/k. We also call, the g.c.d. $D_{\text{alg}}(K/k)$ of $D(B) = \Delta(B)^n$ for the same B the *algebraic discriminant*, and it is immediate that $D_{\text{alg}}(K/k) = \Delta(K/k)^n$. We call the *arithmetic different* of K/k the g.c.d. $\delta(K/k)$ of $\delta(a) = \Delta(B_a)$, where a ranges over I, and we call the *arithmetic discriminant* of K/k the g.c.d. $D_{\text{ar}}(K/k)$ of the same $D(a)$ (which is plainly also $= \delta(K/k)^n$).

We shall deal in this paragraph mainly with the algebraic different. We shall prove that, for any $\varepsilon > 0$, there exist ε-bases of K/k, and that, in the

case of discrete valuations, there exist 0-bases of K/k (in the case of dense valuation they exist iff K/k is a completely flat extension). And we shall show that, if B is a 0-basis, $\Delta(K/k) = \Delta(B)$ and, if such bases do not exist, $v(\Delta(K/k)) = \mathrm{Inf}_S\, v(\Delta(B))$, where B ranges over J, is a semi-real number of species $+$, and if B is an ε-basis

$$v(\Delta(B)) - v(\Delta(K/k)) \leqslant 2\varepsilon.$$

LEMMA 1. *If B is an ε-basis and B' is any integral basis, we have* $v(\Delta(B)) - v(\Delta(B')) \leqslant 2\varepsilon$.

Proof. We have $B' = \Lambda(B', B)B$ and, if $E_{B',B}$ is the fractional ideal generated by $\det \Lambda(B', B)$, we have $\Delta(B') = E_{B',B}^{2/n}\, \Delta(B)$, i.e.,

$$v(\Delta(B')) = \frac{2}{n}\, v(\det \Lambda(B', B)) + v(\Delta(B)).$$

But, if $b_i' = \sum \lambda_{ij} b_j$, $v(b_i') \geqslant 0$ implies for any j, as B is an ε-basis, that $v(\lambda_{ij}) \geqslant -\varepsilon$. But then $v(\det \Lambda(B', B) \geqslant -n\varepsilon$ and

$$v(\Delta(B)) - v(\Delta(B')) = -\frac{2}{n}\, v(\det \Lambda(B', B)) \leqslant -\frac{2}{n}\,(-n\varepsilon) = 2\varepsilon.$$

In particular, if B is a 0-basis, we have, for every integral basis B', $v(\Delta(B)) = v(\Delta(B'))$. So if such basis B exists, we have $\Delta(K/k) = \Delta(B)$. And if an ε-basis B exists, we have

$$v(\Delta(B)) - 2\varepsilon < v(\Delta(K/k)) < v(\Delta(B)).$$

Let B a basis. We consider the transforms ΛB of B by the matrices Λ in k such that $|\det \Lambda| = 1$ (neither the basis B nor the matrix Λ are supposed to be integral; we shall call such matrices *univalued*). We call *discrepancy* of B the supremum

$$\Theta(B) = \operatorname*{Sup}_S\, [h(\Lambda B) - h(B)]$$

of the difference of heights $h(\Lambda B) - h(B)$ of ΛB and B when Λ ranges over all such matrices. We have

LEMMA 2. *The discrepancy of a basis B of K/k cannot be $+\infty^-$.*

Proof. Suppose, that $\Theta(B) = +\infty^-$. Then, for any real constant C, there exists a univalued matrix Λ such that $h(\Lambda B) > nC$. There exists a diagonal univalued matrix T over k such that for every element b_i of $B' = T(\Lambda B) = (T\Lambda)B = (b_1', b_2', \ldots, b_n')$, $v(b_i') > C$ holds and $\Lambda' = T\Lambda$ is also

univalued. Let be $A' = (\lambda'_{ij})$. Then, there exist some pair (i, j) such that $v(\lambda_{ij}) \leqslant 0$. Let $C_1, C_2, ..., C_q, ...$, be a sequence of real numbers converging to $+\infty^-$ on the semi-real axis S. Then, for each n, there exists a univalued matrix

$$A^{(q)} = (\lambda_{ij}^{(q)}) \qquad (i = 1, 2, ..., n; j = 1, 2, ..., n)$$

such that if

$$B^{(q)} = A^{(q)}B = (b_1^{(q)}, b_2^{(q)}, ..., b_n^{(q)})$$

for every $i = 1, 2, ..., n$, then $v(b_i^{(q)}) > C^{(q)}$ holds. As $A^{(q)}$ is univalued there exists some $\lambda_{ij}^{(q)}$ such that $v(\lambda_{ij}^{(q)}) \leqslant 0$. As the number of pairs (i, j) is finite, there is one of these pairs, such that $v(\lambda_{ij}^{(q)}) \leqslant 0$ for infinitely many q. If we replace the sequence $C_1, C_2, ..., C_q, ...$, by its partial sequence comprising only such C_q, that satisfy $v(\lambda_{ij}^{(q)}) \leqslant 0$ for the considered pair (i, j), the new sequence converges to $+\infty^-$ on S with $v(\lambda_{ij}^{(q)}) \leqslant 0$ for all its terms, and we can suppose that the initial sequence is the same way. Then let V be the k-vectorial space generated by the set $b_1, b_2, ..., b_{j-1}, b_{j+1}, b_{j+1}, ..., b_n$ of all elements of B except b_j. We have

$$b_i^{(q)} = \lambda_{ij}^{(q)} b_j - v^{(q)},$$

where v_q (and also $v_{ij}^{(q)-1} v_q$) is $\in V$. That implies

$$\begin{aligned} v(b_j - \lambda_{ij}^{(q)-1} v^{(q)}) &= v(\lambda_{ij}^{(q)-1} b_i^{(q)}) \\ &= v(b_i^{(q)}) - v(\lambda_{ij}^{(q)}) \geqslant C_q + 0 = C_q. \end{aligned}$$

So, there exists a sequence of elements

$$w^{(q)} = \lambda_{ij}^{(q)-1} v^{(q)} \qquad (q = 1, 2, ..., +\infty)$$

of V such, that $v(b_j - w^{(q)}) \to +\infty^-$, i.e., $|b_j - w^{(q)}| \to 0^+$. Let $\tilde{K}$ be the completion of the valued field K, and $\tilde{k}$, $\tilde{V}$ closures of k, V in $\tilde{K}$. We have $b_j \in \tilde{V}$. But $\tilde{k}$ is a completion of the valued field k and $\tilde{K} = \tilde{k}b_1 + \tilde{k}b_1 + \cdots + \tilde{k}b_n$. The $\tilde{k}$-vectorial space $\tilde{K}$ when we take as norm its valuation, is a normed vectorial space of finite dimension over the complete valued field $\tilde{k}$. So, its topology is equivalent to the product topology and $\tilde{V} = \tilde{k}b_1 + \cdots + \tilde{k}b_{j-1} + \tilde{k}b_{j+1} + \cdots + \tilde{k}b_n$ and we have $\tilde{K} = \tilde{V} + \tilde{k}b_j = \tilde{V}$.

So, $[\tilde{K} : \tilde{k}]$, which is equal to the dimension $(\tilde{K} : \tilde{k}) = (\tilde{V} : \tilde{k})$ of the $\tilde{k}$-vectorial space $\tilde{K}$, is $< n = [K : k]$. But that is impossible. Indeed, by Hasse's theory of prolongations of valuations, the number of primary components of the commutative algebra $L = L \otimes_k \tilde{k}$ is equal to the number of possible prolongations of the valuation $|\cdot\cdot|$ of k in its-extension K. As k is

supposed henselian, this number is 1, i.e., L is primary. If R is the radical of L, we have $K \simeq L/R$. But as K/k is separable, this radical must be $\{0\}$, so $\tilde{K} = L = K \otimes_k \tilde{k}$ and $[\tilde{K} : \tilde{k}]$ is the dimension $[L : \tilde{k}]$ of the $\tilde{k}$-vectorial space L, which is $[K : k] = n$.

PROPOSITION 2. *If an integral basis B is such that $\varepsilon \geqslant h(B) + \Theta(B)$, B is an ε-basis; if the valuation of k is discrete, $\Theta(B) = 0$ and, for any b_i, where $B = (b_1, b_2, ..., b_n)$, $v(b_i) < \omega$, B is a 0-basis.*

Proof. Let $a \in I$ be such that $v(a) \geqslant \varepsilon$, and let $a = \sum \lambda_i b_i$ be its expression as linear combination of B. Suppose $\lambda_i = 0$ and consider the basis

$$B' = (b_1, b_2, ..., b_{i-1}, \lambda_i^{-1} a, b_{i+1}, ..., b_n).$$

$\Lambda_{B',B}$ is a matrix which has non-diagonal elements only on the ith line, and all its diagonal elements are $= 1$. So,

$$\det \Lambda(B', B) = 1 \qquad \text{and} \qquad |\det \Lambda(B', B)| = 1.$$

The height $h(B')$ of B' is $h(B) - v(b_i) - v(\lambda_i) + v(a)$ and it must be $\leqslant h(B) + \Theta(B)$. So, as $v(a) \geqslant \varepsilon$, we have $\varepsilon - v(b_i) - v(\lambda_i) \leqslant \Theta(B)$. But $\varepsilon \geqslant h(B) + \Theta(B)$, $v(b_i) \leqslant h(B)$. So,

$$(h(B) + \Theta(B)) - h(B) - v(\lambda_i) = \Theta(B) - v(\lambda_i) \qquad \text{is} \quad \leqslant \Theta(B),$$

which implies $v(\lambda_i) \geqslant 0$ and $\lambda_i \in i$. So $a \in i(B)$ and B is an ε-basis. Suppose that the valuation of k is discrete and that B satisfies the above conditions. Let a be $\in I$, i.e., $v(a) \geqslant 0$. If $a = \sum \lambda_i a_i$ and if $\lambda_i \neq 0$, B' is the same basis as before, we have still $h(B) - v(b_i) - v(\lambda_i) + v(a) < h(B) + \Theta(B)$. But here $\Theta(B) = 0$ and $v(a) \geqslant 0$. So, we have $h(B) - v(b_i) - v(\lambda_i) \leqslant h(B_i)$, so $-v(b_i) < v(\lambda_i)$. But, by hypothesis, $v(b_i) < \omega$, so $v(\lambda_i) > -\omega$, and as there is no element of $v(k)$ between $-\omega$ and 0, we have $v(\lambda_i) \geqslant 0$. So, again, we have $a \in i(B)$.

On the other hand, it is almost obvious that in the case of dense valuations, if B is an ε-basis, $\Theta(B) \leqslant n\varepsilon$. Indeed, let be $B' = \Lambda B$ such that $|\det \Lambda| = 1$ and $h(B') \geqslant h(B) \geqslant 0$. Suppose the valuation is dense. Then, it is always possible to find a diagonal matrix T in k of determinant $\det T$ equal to 1, such that, if $\eta > 0$ is arbitrary, all elements of $B'' = TB' = T\Lambda B$ wouldbe $> (h(B') - \eta)/n$ and we have $|\det T\Lambda| = 1$. But, if $\Theta(B) > n\varepsilon$, we can find a B' such, that

$$h(B') > h(B) + n\varepsilon \geqslant n\varepsilon \qquad \text{and if} \qquad \eta < h(B') - n\varepsilon,$$

we have $(H(B') - \eta)/n > \varepsilon$. So, if $B'' = (b_1'', b_2'', ..., b_n'')$, we have $v(b_i') > \varepsilon$ for

every i. If $\lambda \in k$ is such, that $0 < v(\lambda) < \mathrm{Min}_i\, v(b_i'') - \varepsilon$ all $v(\lambda^{-1} b_i'')$ are $\geqslant \varepsilon$ and all $\lambda^{-1} b_i''$ are $\in i(B)$. So, if

$$\lambda^{-1} B'' = (\lambda^{-1} b_1'', \lambda^{-1} b_2'', \ldots, \lambda^{-1} b_n''),$$

the matrix $\Lambda(\lambda^{-1} B'', B)$ is integral, and $|\det \Lambda(\lambda^{-1} B'', B)| \leqslant 1$. But clearly $\Lambda(B'', B) = (\lambda 1_n)\, \Lambda(\lambda^{-1} B'' B)$ (where 1_n is the unity matrix of degree n). So

$$|\det \Lambda(B'', B)| = |\lambda|^n\, |\det \Lambda(\lambda^{-1} B'', B)| \leqslant |\lambda|^n < 1,$$

in contradiction to the hypothesis.

THEOREM 1. *For every $\Theta > 0$, there exist transforms ΛB of B by univalued matrices Λ such that $\Theta(\Lambda B) < \Theta$. If the valuation is discrete, then there exist such transforms without discrepancy, i.e., such that $\Theta(\Lambda B) = 0$.*

Proof. If Λ_0 and Λ are two univalued matrices in k, we have

$$\Lambda B = (\Lambda \Lambda_0^{-1})(\Lambda_0 B) \qquad \text{and} \qquad \Lambda \to \Lambda \Lambda_0^{-1}$$

is a permutation of the set of univalued matrices in k. So, $\mathrm{Sup}_S\, h(\Lambda B)$ and $\mathrm{Sup}_S\, h(\Lambda(\Lambda_0 B))$, when Λ ranges over all univalued matrices, are equal. So

$$\begin{aligned} \Theta(\Lambda_0 B) &= \operatorname*{Sup}_S h(\Lambda(\Lambda_0 B)) - h(\Lambda_0 B) \\ &= [\operatorname*{Sup}_S h(\Lambda B) - h(B)] - [h(\Lambda_0 B) - h(B)] \\ &= \Theta(B) - [h(\Lambda_0 B) - h(B)]. \end{aligned}$$

$\Theta(B)$ is a semi-real number of species 0 or $-$, and if the valuation is discrete, it is always of species 0 and is a multiple of $\Omega = \omega/e$. It is always $\geqslant 0$. In any case, if $\Theta > 0$, there exists a transform $\Lambda_0 B$ of B by a univalued matrix Λ_0 such that

$$h(\Lambda_0 B) > h(B) + \Theta(B) - \Theta,$$

so

$$\Theta(\Lambda_0 B) = \Theta(B) - [h(\Lambda_0 B) - h(B)] < \Theta.$$

If the valuation is discrete and $0 < \Theta < \Omega$, then we have $0 < \Theta(\Lambda_0 B) < \Theta < \Omega$, and as $\Theta(\Lambda_0 B)$ is a multiple of Ω, we have $\Theta(\Lambda_0 B) = 0$.

PROPOSITION 3. *When the valuation is discrete, a 0-basis B is without discrepancy iff $h(B) = [f(e-1)/2]\omega$.*

Proof. Let B be any 0-basis of K/k, and let $B' = AB$ be its transform by univalued matrix A such that $\Theta(B') = 0$. We can find a diagonal matrix T in k such that for all elements b_i'' of $B'' = TB' = (b_1'', b_2'', ..., b_n'')$, we have $0 \leqslant v(b_i) < \omega$. As obviously $\Theta(B'') = \Theta(B') = 0$, B'' is (by Proposition 2) a 0-basis of K/k. But then $A(B'', B) = TA(B', B) = TA$ is a integral univalued matrix of k, and so T is univalued. So, there exists a 0-basis of K/k without discrepancy.

Let $B = (b_1, b_2, ..., b_n)$ be such a basis. Let n_t be the number of b_i such that $v(b_i) \geqslant (e-t)\Omega$. We shall compare B with the particular 0-basis

$$B_0 = (c_q \Pi^s;\ q = 1, 2, ..., f;\ s = 0, 1, ..., e-1),$$

where the $\bar{c}_q = c_q + M$ form a basis of $\bar{K}/\bar{k}$, considered at the end of Section 1. Let be $b_i = \sum \lambda_{q,s}^{(i)} c_q \Pi^s$. Then, if $v(b_i) \geqslant (e-t)\Omega$, clearly $v(\lambda_{q,s}^{(i)})$ are > 0, so they are $\geqslant \omega$, if $s < e-t$, and for these q, s we have $v(\lambda_{q,s}^{(i)} c_s \Pi^s) \geqslant \omega$.

Let $\tilde{b}_i = \sum_{q,s \geqslant e-t} \lambda_{q,s}^{(i)} c_q \Pi^s$. If $n_t > ft$ and $U(t)$ is the set of all i such that $v(b_i) \geqslant (e-t)\Omega$, the $\tilde{b}_i$, $i \in U(t)$, are not linearly independent, and no one of them is zero. So there exists a non-trivial linear combination $\sum_{i \in U(t)} \mu_i \tilde{b}_i$ which is 0, and, by multiplying it by a convenient element of k, we may suppose that $\mathrm{Min}_{i \in U(t)} v(\mu_i) = 0$. But, then $v(\sum_{i \in U(t)} \mu_i b_i) \geqslant \omega$. So, if $\pi \in k$ is such that $v(\pi) = \omega$, we have for $a = \sum_{i \in U(t)} \pi^{-1} \mu_i b_i$, $v(a) > 0$, so $a \in I$ and $\mathrm{Min}_i v(\mu_i) = -\omega$, so some μ_i are $\notin i$. So B is not a 0-basis, and it is $n_t \leqslant ft$. It is easy to see that in this situation, it is possible to define a bijection $\varphi: B \to B_0$ such that $v(b_i) \leqslant v(\varphi \cdot b_i)$. Indeed, suppose that for U_t it is already defined as such an injection φ_t of $B_t = \{b_i;\ i \in U_t\}$ into

$$B_{0,t} = \{c_q \Pi^s;\ q = 1, 2, ..., f,\ s = e-t, e-t+1, ..., e-1\}.$$

Then $B_{0,t+1} \cdots (\varphi \cdot B_t)$ has $f(t+1) - n_t$ elements, and their orders are $> (e-t-1) \cdot \Omega$ and $B_{t+1} \cdots b_t$ has $n_{t+1} - n_t < f(t+1) - n_t$ elements, all of order $(e-t-1) \cdot \Omega$. If we prolong φ_t by injecting in any manner $B_{t+1} \cdots B_t$ into $B_{0,t+1} \cdots (\varphi_t \cdot B_t)$, we obtain an injection $\varphi_{t+1}: B \to_{t+1} B_{0,t+1}$ having the same property. And $\varphi = \varphi_e$ is such an injection of $B = B_e$ into $B_0 = B_{0,e}$. But both have the same number of elements $n = fe$. So φ is a bijection. But then we have

$$h(B) \leqslant h(B_0) = [f(e-1)/2]\omega.$$

As, B_0 is a transform of B by a univalued (and an even integral) matrix, we see that $\Theta(B_0) = 0$ and that $\Theta(B) = 0$ iff

$$h(B) = [f(e-1)/2]\omega.$$

PROPOSITION 4. *Let* $B=(b_1, b_2, ..., b_n)$ *be a linear basis of* K/k, $a\in K$ *and* $a=\sum \lambda_i(a)\, b_i$ *its representation as a linear combination of* B. *Then* $v(\lambda_i(a)\, b_i)\geqslant v(a)-\Theta(b)$.

Proof. Suppose that a K is such that for some $i=1, 2, ..., n$, we have $v(\lambda_i(a)\, b_i)<v(a)-\Theta(b)$. Let us consider the linear basis $B'=(b_1, b_2, ..., b_{i-1}, \lambda_i(a)^{-1}a, b_{i+1}, ..., b_n)$. Clearly, $\det \Lambda(B', B)=1$, so $\Lambda(B', B)$ is univalued. We have

$$\begin{aligned} h(B') &= h(B)-v(b_i)+v(a)-v(\lambda_i(a)\\ &= h(B)+v(a)-v(\lambda_i(a)\, b_i)>h(B)+\Theta(B), \end{aligned}$$

a contradiction.

COROLLARY. *If* $\Theta(B)=0$, *we have* $v(\lambda_i(a)\, b_i)\geqslant v(a)$, *i.e.*,

$$|\lambda_i(a)\, b_i|\leqslant |a| \qquad \textit{and} \qquad |a|=\operatorname*{Max}_i (|\lambda_i(a)\, b_i|).$$

Conversely, if this condition is satisfied for each $a\in K$, $\Theta(B)=0$. Indeed, if $B'=\Lambda B$, where $\Lambda=(\lambda_{ij})$ is univalued, then there must exist a permutation $i\to j(i)$ $(i=1, 2, ..., n)$ such that

$$v(\lambda_{1,j(1)}\lambda_{2,j(2)}\cdots\lambda_{n,j(n)})\leqslant 0.$$

But then

$$\begin{aligned} h(B') &= v(b'_1, b'_2, ..., b'_n)\\ &\leqslant v([\lambda_{1,j(1)}b_{j(1)}][\lambda_{2,j(2)}b_{j(2)}]\cdots[\lambda_{n,j(n)}b_n])\\ &= v(\lambda_{1,j(1)}\lambda_{2,j(2)}\cdots\lambda_{n,j(n)})+v(b_{j(1)}b_{j(2)}\cdots b_{j(n)})\\ &\leqslant 0+h(B)=h(B), \end{aligned}$$

because $b_{j(1)}b_{j(2)}\cdots b_{j(n)}=b_1 b_2\cdots b_n$. So $\Theta(B)=0$.

I introduced such bases in 1953 in [12] under the name of *skeletically free bases*. Later, J. P. Serre used them under the name of *orthonormal bases* (see [17]).

LEMMA 3. *If* B *is a basis and* T *is a diagonal matrix in* k *such that* $\det T\neq 0$, B *and* TB *have the same discrepancy.*

Proof. First, $h(TB)=v(\det T)+h(B)$. On the other hand, for any matrix Λ, as T commutes with every matrix, we have

$$\Lambda(TB)=T(\Lambda B) \qquad \text{and} \qquad h(\Lambda(TB))=v(\det T)+h(\Lambda B).$$

So

$$h(\Lambda(TB)) - h(TB) = h(\Lambda B) - h(B),$$

which proves the lemma.

PROPOSITION 5. *The discrepancy of every linear basis B of K/k is of species* 0 *(zero) if K/k is not defective, and of species* $-$ *(minus) if K/k is defective.*

Proof. Suppose that K/k is not defective (i.e., $n = fe$). Let $(\bar{c}_1, \bar{c}_2, ..., \bar{c}_f)$ be a linear basis of $\bar{K}/\bar{k}$, and let c_q be some representative of $\bar{c}_q$ in I. Let $v(K)/v(k) = \{\bar{v}_1, \bar{v}_2, ..., \bar{v}_e\}$ and let v_s be some representative of $\bar{v}_s$ in $v(K)$ (i.e., $\bar{v}_s = v_s + v(k)$). Let Π_s be some representative of v_s in K, i.e., an element of K such that $v(\Pi_s) = v_s$. Consider the set

$$\{c_q \Pi_s;\ q = 1, 2, ..., f,\ s = 1, 2, ..., e\}.$$

If $a = \sum \lambda_{q,s} c_q \Pi_s$ is a linear combination (over k) of this set we have $v(a) = \mathrm{Min}_{q,s} v(\lambda_{q,s} c_q \Pi_s)$. Indeed, let μ be the set of all pairs (q, s) such that $\lambda_{q,s} c_q \Pi_s$ is a term of a of minimal order, i.e., of maximal value. Then, if $(q, s) \in \mu$ and $(q', s') \in \mu$, we have $v(\lambda_{q,s} c_q \Pi_s) = v(\lambda_{q',s'} c_{q'} \Pi_{s'})$. But as

$$v(c_s) = v(c_{s'}) = 0, \qquad v(\Pi_s) = v_{s'}, \qquad v(\Pi_{s'}) = v_{s'}, \qquad \text{and} \qquad v(\lambda_{q,s})$$

and $v(\lambda_{q',s'})$ are $\in v(k)$, that implies that $v_s \equiv v_{s'} \pmod{v(k)}$ and $s = s'$. But then this equality becomes $v(\lambda_{q,s}) = v(\lambda_{q',s'})$. So, for all $(q, s) \in \mu$, s has the same value and all $v(\lambda_{q,s})$ have the same value $w \in v(k)$. Let λ^* be an element of k such that $v(\lambda^*) = w$, and let $\lambda'_{q,s} = \lambda^{*-1} \lambda_{q,s}$. Then, if $\rho = \{q; (q, s) \in \mu\}$ the sum of maximal terms of a is $(\sum_{q \in \rho} \lambda'_{q,s} c_s)\, \lambda^* \Pi_s$. But $v(\lambda'_{q,s}) = v(\lambda_{q,s}) - v(\lambda^*) = w - w = 0$. So $\lambda'_{q,s} \in i$ and $v(\sum_{q \in \rho} \lambda'_{q,s} c_s) > 0$ iff the residue (mod M)

$$\overline{\sum_{q \in \rho} \lambda'_{q,s} c_s} \qquad \text{of} \quad \sum_{q \in \rho} \lambda'_{q,s} c_s \text{ is } \bar{0}.$$

But $a \to \bar{a} = a + M$ is a ring-homomorphism of I into K, so

$$\overline{\sum_{q \in \rho} \lambda'_{q,s} c_s} = \sum_{q \in \rho} \bar{\lambda}'_{q,s} \bar{c}_s.$$

But all $\bar{\lambda}'_{q,s}$ are $\in \bar{k}$, no one of them is $\bar{0}$ (because $v(\lambda'_{q,s}) = 0$) and the $\bar{c}_s$ are linearly independent over $\bar{k}$. So, this residue is $\neq \bar{0}$ and $v(\sum_{q \in \rho} \lambda'_{q,s} c_s) = 0$, *i*, i.e., $v(\sum_{q \in \rho} \lambda_{q,s} c_s \Pi_s) = w + v_s$. But then, by ultrametricity, $v(a) = w + v_s = \mathrm{Min}_{q,s} v(\lambda_{q,s} c_s \Pi_s)$. But that implies that $B_0 = (c_q \Pi_s;\ q = 1, 2, ..., f,\ s = 1, 2, ..., e)$ is a basis of K/k (because the dimension of the

vectorial k-space $k(B_0)$ is n) without discrepancy. Let B be an arbitrary basis of K/k, and let $\tilde{v} = v(\det \Lambda(B_0, B))$. Let T be a diagonal matrix of k such that $v(\det T) = -\tilde{v}$ (e.g., a diagonal matrix in k having all its diagonal elements but one equal to 1, and this last element of order $-\tilde{v}$). Then TB_0 is also a basis of K/k without discrepancy, and $\Lambda(TB_0, B) = T\Lambda(B_0, B)$, so

$$\begin{aligned} v(\det \Lambda(TB_0, B)) &= v(\det T\Lambda(B_0, B)) \\ &= v(\det T) + v(\det \Lambda(B_0, B) = -\tilde{v} + \tilde{v} = 0. \end{aligned}$$

So $\Lambda(TB_0, B)$ is a univalued matrix, and

$$\Theta(B) = \Theta(TB_0) + h(TB_0) - h(B) = h(TB_0) - h(B),$$

because $\Theta(TB_0) = 0$. So, $\Theta(B)$ is of species 0. Suppose now that K/k is defective, i.e., $fe < n$, and again let

$$v(K)/v(k) = \{\bar{v}_1, \bar{v}_2, ..., \bar{v}_e\} \qquad \text{and} \qquad B = (b_1, b_2, ..., b_n)$$

an arbitrary basis of K/k. Let $B_s = \{b_i; v(b_i) \in \bar{v}_s\}$. As the number of s is e and $n > ef$, there exists some s such that B_s contains more than f elements. Let

$$B_s = \{b_{i(1)}, b_{i(2)}, ..., b_{i(l)}\}, \qquad \text{where} \quad l > f.$$

All $v(b_{i(j)})$ are congruent (mod $v(k)$); so, there exist elements $w_1, w_2, ..., w_l$ of $v(k)$ such that all $w_j + v(b_{i(j)})$ have the same value u. Let $\xi_1, \xi_2, ..., \xi_l$ elements of k such that $v(\xi_j) = w_j$ and let b be an element of K such that $v(b) = u$. Then, for any j, we have $v(\xi_j b_{i(j)} b^{-1}) = w_j + v(b_{i(j)}) - u = 0$. So, $c_j = \xi_j b_{i,j} b^{-1}$ is $\in I$ and its residue $\bar{c}_j$ (mod M) is $\neq \bar{0}$; but, as the number of j is $> f$, the $\bar{c}_j$ are linearly dependent over $\bar{k}$. So, there exist $\bar{\mu}_1, \bar{\mu}_2, ..., \bar{\mu}_l \in \bar{k}$ such that not all are $\bar{0}$ and that $\sum_j \bar{\mu}_j \bar{c}_j = 0$. Let μ_j be some representative of $\bar{\mu}_j$ in i. Then,

$$\overline{\sum_j \mu_j c_j} = \sum_j \bar{\mu}_j \bar{c}_j = \bar{0} \qquad \text{and} \qquad v\left(\sum_j \mu_j c_j\right) > 0.$$

But then, if $\lambda_{i(j)} = \mu_j \xi_j$, we have

$$v\left(\sum_j \lambda_{i(j)} b_{i(j)}\right) = v\left(\sum_j \mu_j (\xi_j b_{i(j)})\right)$$

$$v\left(\sum_j \mu_j (c_j b)\right) = v\left(\left(\sum_j c_j \mu_j\right) b\right) = v\left(\sum_j c_j \mu_j\right) + v(b) > v(b)$$

$$= \operatorname{Min}_i v(\lambda_{i(j)} b_{i(j)}).$$

So the discrepancy of B is >0. Then the discrepancy of no basis B can be of species 0. Suppose, indeed, the $\Theta(B)$ is a real number. Then there exists a univalued matrix A in k such that $h(AB)-h(B)=\Theta(B)$. That implies $\Theta(AB)=0$, which is impossible.

PROPOSITION 6. *The species of $v(\Delta(K/k))$ is 0 if the valuation of k is discrete or K/k is completely flat, and + in all other cases.*

Proof. It is obvious that this species is 0 when the valuation of k is discrete. If K/k is completely flat, $C=(c_1, c_2, ..., c_f)$, where $c_1, c_2, ..., c_f$ are elements of I such that $(\bar{c}_1, \bar{c}_2, ..., \bar{c}_f)$ is a basis of $\bar{K}/\bar{k}$, is an integral basis of K/k such that $\Theta(C)=h(C)=0$. So, it is a 0-basis and $\Delta(K/k)=\Delta(C)$. If the valuation of k is dense and B is an integral basis of K/k, either $\Theta(B)>0$ or $\Theta(B)=0$ (which implies $d=1$), and we assume that K/k is not completely flat (i.e., $f<n$).

If $\Theta(B)>0$, then there exists a univalued matrix A such that $h(AB)>h(B)>0$. Then a diagonal matrix T in k can be found such that $-h(AB)<v(\det T)<0$ and TAB is an integral basis. And we have

$$v(\Delta(TAB))=\frac{2}{n}v(\det T)+v(\Delta(B))=\frac{2}{n}v(\det T)+v(\Delta(B))<v(\Delta(B)).$$

If $\Theta(B)=0$ (so $d=1$, $n=ef$), and if $e>1$, some of the elements b_i of B will be of order $v(b_i)>0$, so $h(B)>0$. But then there again exists a diagonal matrix T such, that $-h(B)<v(\det T)<0$ such that TB is integral, and

$$v(\Delta(TB))=\frac{2}{n}v(\det T)+v(\Delta(B))<v(\Delta(B)).$$

So, except when $f=n$, we always have $v(\Delta(B))>v(\Delta(K/k))$, and the species of $v(\Delta(K/k))$ is $+$.

Let L be an intermediate field of K/k: $K\supset L\supset k$. Then we shall prove

THEOREM 2 (Hilbert's Theorem 39). $\Delta(K/k)=\Delta(K/L)\,\Delta(L/k)$.

Proof. Let f, f^*, f' be the residual degrees, e, e^*, e' the ramification orders, and d, d^*, d' the defects of, respectively, K/k, L/k, K/L. Suppose that the valuation of K is dense and for some arbitrary $\varepsilon>0$, let B^* be an ε-basis of L/k and β an ε-basis of K/L. Then, by Proposition 1 of Section 1, $B=B^*\beta$ is a 2ε-basis of K/k. So, for any integral basis B' of K/k, we have $v(\Delta(B))-v(\Delta(B'))<2\varepsilon$ and $0\leqslant v(\Delta(B))-v(\Delta(K/k))<2\varepsilon$. In the same manner we have $0\leqslant v(\Delta(B^*))-v(\Delta(L/k))<\varepsilon$ and $0\leqslant v(\Delta(\beta))-v(\Delta(K/L))<\varepsilon$, so $0\leqslant v(\Delta(B^*)\,\Delta(\beta)-v(\Delta(L/k)\,\Delta(K/L))\leqslant 2\varepsilon$. But, as has been proved, we have $\Delta(B)=\Delta(B^*)\,\Delta(\beta)$. So

$|v(\Delta(K/k)) - v(\Delta(L/k)\,\Delta(K/L))|$ is $\leqslant 2\varepsilon$ for any $\varepsilon \geqslant 0$. But that signifies that the real values of $v(\Delta(K/k))$ and of $v(\Delta(L/k)\,\Delta(K/L))$ are the same.

Now the species of $v(\Delta(K/k))$, $v(\Delta(K/L))$, $v(\Delta(L/k))$ are 0 if the corresponding extension is completely flat, i.e., respectively, $f = n$, $f' = v$, $f^* = n^*$. But $f = n$ iff $f' = v$ and $f^* = n^*$. On the other hand, if ρ_1, ρ_2 are semi-real numbers of species 0 or $+$, then $\rho_1 + \rho_2$ is always defined and its species is 0 iff ρ_1, ρ_2 are both of species 0. So,

$$v(\Delta(K/k)) \qquad \text{and} \qquad v(\Delta(K/L)) + v(\Delta(L/k)) = v(\Delta(K/L)\,\Delta(L/k))$$

have also, the same species in case the valuation is dense.

Suppose now that the valuation of k is discrete. Let $\tilde{\omega} = e'\Omega = \omega/e^*$. Let B^* be a 0-basis of L/k such that

$$h(B^*) = [f^*(e^* - 1)/2]\omega,$$

and let β be a 0-basis of K/L such that

$$h(\beta) = [f'(e' - 1)/2]\tilde{\omega}.$$

Then, these bases are also without discrepancy and $\Delta(L/k) = \Delta(B^*)$, $\Delta(K/L) = \Delta(\beta)$. But $B = B^*\beta$ is a 0-basis of K/k. If $[L/k] = n^*$, $[K : L] = v$, $B^* = (b_1^*, b_2^*, ..., b_{n^*}^*)$, and $\beta = (\beta_1, \beta_2, ..., \beta_v)$, we have

$$\begin{aligned} h(B) &= \sum_{i,j} v(b_i^*\beta_j) < vh(B^*) + n^*h(\beta) \\ &= [vf^*(e^* - 1)/2]\omega + [n^*f'(e' - 1)/2](\omega/e^*) \\ &= [e'f'f^*(e^* - 1) + f^*f'(e' - 1)](\omega/2). \end{aligned}$$

But $f'f^* = f$, so $e'f'f^*(e^* - 1) + f^*f'(e' - 1) = e'f(e^* - 1) + f(e' - 1)f(e'e^* - e' + e' - 1) = f(e - 1)$, because $e = e'e^*$. So $h(B) = [f(e - 1)/2]\omega$ and $\Theta(B) = 0$. So, B is a 0-basis without discrepancy, and $\Delta(K/k) = \Delta(B) = \Delta(B^*\beta) = \Delta(K/k)\,\Delta(K/L)$.

I shall now expound a certain method of canonical determination of discrepancy of a given basis $B = (b_1, b_2, ..., b_n)$ of K/k, which will be useful, in particular, in the study of the arithmetic different, which I call "unfolding of bases." I have known this method since 1939 or 1940. L. Gruson found it independently and applied this method in 1969 in the more general frame of ultrametric Banach spaces. Let V be an (ultrametrically) normed vectorial space over an arbitrary valued field k, $\|\cdot\cdot\|$ the norm of V, $|\cdot\cdot|$ valuation of k. $w(\cdot\cdot) = -\ln \|\cdot\cdot\|$ will be called the *normative order* of V. Let $B = (b_1, b_2, ..., b_n)$ be a basis of the k-vectorial space V with fixed numbering of its elements (we shall speak about the *ordered* basis B) and $h(B) = \sum_i w(b_i)$. Let, for each $i = 1, 2, ..., n$, V_i be the subspace

$kb_i + kb_{i+1} + \cdots + kb_n$. Let $p_i(B) = \mathrm{Sup}_S\{w(a);\ a \in b_i + V_{i+1}\} - w(b_i)$. Clearly $p_n(B)$ is always 0. We call $p_i(B)$ the ith *fold* of B, and we call *folding* of B (so enumerated) the sum $p(B) = \sum_i p_i(B)$ of its folds. If $p(B)$ is real, and $a_i \in b_i + V_{i+1}$ is such that $v(a_i) - v(b_i) = p_i(B)$, the base $A = (a_1, a_2, ..., a_n)$, will be called an *unfolding* of B.

We return now to our extension K/k, considered as a k-vectorial normed space with the norm $\|\cdot\cdot\|$ coincident with the valuation $|\cdot\cdot|$ of K, and we prove the

THEOREM 3. *For a linear basis B of K/k, its folding $p(B)$ and its discrepancy $\Theta(B)$ are equal.*

Proof. First, if $a_i \in b_i + V_{i+1}$ and $A = (a_1, a_2, ..., a_n)$, $\Lambda(A, B)$ is a triangular matrix having all elements of its main diagonal $= 1$. So, $\Lambda(A, B)$ is univalued and

$$\sum_i [v(a_i) - v(b_i)] = h(A) - h(B) < \Theta(B).$$

But then $p(B) = \sum_i p_i(B) = \sum_i \mathrm{Sup}_s\{v(a_i) - v(b_i):\ a_i \in b_i + V_{i+1}\} = \mathrm{Sup}_S\{\sum_i [v(a_i) - v(b_i)];\ (a_1, a_2, ..., a_n) \in (b_1 + V_2) \times (b_2 + V_3) \times \cdots \times \{b_n\}\} \leqslant \Theta(B)$. For proving the inequality $\Theta(B) < p(B)$, suppose first that $\Theta(B)$ is real, i.e., K/k is non-defective. Let $B^* = (b_1^*, b_2^*, ..., b_n^*)$ be a basis of K/k without discrepancy and let be $B^* = \Lambda^* B$. We shall construct a basis B^{**} without discrepancy such that $\Lambda(B^{**}, B) = (\lambda_{ij}^{**})$ is a triangular matrix such that all its elements, which are below its main diagonal (i.e., such that $j < i$) are $= 0$. We shall do that by induction, constructing successively some bases $B_q^* = \Lambda_q^* B$, where $\Lambda_q^* = (\lambda_{q,i,j}^*)$ is a matrix such that $j < \mathrm{Min}[i, q+1]$ implies $\lambda_{q,i,j}^* = 0$. We can put $B^* = B_0^*$ and, if the construction is performed, $B^{**} = B_n^*$.

Suppose B_q^* is constructed. Then, if $i > q$, we have, if $B_q^* = (b_{q,1}^*, b_{q,2}^*, ..., b_{q,n}^*)$, that $b_{q,i}^* = \sum_{j \geqslant q+1} \lambda_{q,ij}^* b_j$ (because, for $j \leqslant q$, $\lambda_{q,i,j}^* = 0$). Let i^* be the index such that

$$v(b_{q,i^*}^*) - v(\lambda_{q,i,q+1}^*) = \mathrm{Max}_{i > q} [v(b_{q,i}^*) - v(\lambda_{q,i,q+1}^*)].$$

Perform first a permutation

$$\tau: \{q+1, ..., n\} \to \{q+1, ..., n\} \text{ of the set } \{q+1, ..., n\}$$

of indices such that $\tau \cdot i^* = q+1$, and let $b_{q,i}^{**} = b_{q,\tau \cdot i}^*$. It is clear that if

$$B_q^{**} = (b_{q,1}^*, b_{q,2}^*, ..., b_{q,q}^*, b_{q,q+1}^{**}, ..., b_{q,n}^{**}), \qquad \Theta(B_q^{**}) = \Theta(B_q^*) = 0.$$

We shall write $b_{q,i}^{**} = b_{q,i}^{*}$ when $i \leqslant q$. Suppose that $b_{q,i}^{**} = \sum_i \lambda_{q,i,j}^{**} b_j$ and let

$$b_{q+1,i}^{*} = b_{q,i}^{**} \qquad \text{if} \quad i \leqslant q+1$$

and

$$b_{q+1,i}^{*} = b_{q,i}^{*} - \lambda_{q,q+1,q+1}^{**} \lambda_{q,i,q+1}^{**} b_{q,q+1}^{**} \qquad \text{if} \quad i > q+1$$

Then first $b_{q+1,q+2}^{*}, \ldots, b_{q+1,n}^{*}$ generate the k-vectorial space V_{q+2} to which they all belong, and as for any $i > q+1$, $b_{q,i}^{**} = b_{q,\tau^{-1}i}^{*}$, where $i > q+1$ and $i \neq i^{*}$,

$$v(b_{q,q+1}^{**}) - v(\lambda_{q,q+1,q+1}^{**}) \geqslant v(b_{q,i}^{**}) - v(\lambda_{q,i,q+1}^{**}),$$

i.e.,

$$\begin{aligned} &v(\lambda_{q,q+1}^{**\,-1}{}_{1,q+1} \lambda_{q,i,q+1}^{**} b_{q,q+1}^{**}) \\ &\quad = v(\lambda_{qi,q+1}^{**}) - v(\lambda_{q,q+1,q+1}^{**}) + v(b_{q,q+1}^{**}) \geqslant v(b_{q,i}^{**}) \\ &\qquad - v(\lambda_{q,q+1}^{**\,-1} \lambda_{q,i}^{**} b_{q,q+1}^{**}) = v(\lambda_{q,i}^{**}) - v(\lambda_{q,q+1}^{**}) + v(b_{q,q+1}^{**}) \geqslant v(b_{q,i}^{**}). \end{aligned}$$

So $v(b_{q+1,i}^{*}) \geqslant \mathrm{Min}(v(b_{q,i}^{**}), v(\lambda_{q,q+1}^{**\,-1} \lambda_{q,i}^{**} b_{q,q+1}^{*})] \geqslant (b_{q,i}^{**})$. Then for any $i = 1, 2, \ldots, n$, we have $v(b_{q+1,i}^{*}) \geqslant v(b_{q,i}^{**})$ and

$$h(B_{q+1}^{*}) \geqslant h(B_{q}^{**}) \qquad \text{and} \qquad \Theta(B_{q+1}^{*}) \leqslant \Theta(B_{q}^{**}) = 0.$$

As $\Theta(B_{q+1}^{*}) \geqslant 0$, we have $\Theta(B_{q+1}^{*}) = 0$ and the matrix $\Lambda(B_{q+1}^{*}, B)$ satisfies the required condition. Then, if $B^{**} = B_{n}^{*}$, $\Lambda(B^{**}, B) = (\lambda_{ij}^{**})$ is a regular matrix such that $\lambda_{i,j}^{**} = 0$ if $j < i$. But if T is the diagonal matrix having the same diagonal elements as $\Lambda(B^{**}, B)$, the matrix $T^{-1}\Lambda(B^{**}, B) = \Lambda(T^{-1}B^{**}, B)$ has all its diagonal elements $= 1$ and is such, that all its elements, which are below the main diagonal, are 0. It is, in particular, univalued. So, on one hand, we have

$$\begin{aligned} \Theta(B) &= h(T^{-1}B^{**}) - h(B) + \Theta(T^{-1}B^{**}) = h(T^{-1}B^{**}) - h(B) + \Theta(B^{**}) \\ &= h(T^{-1}B^{**}) - h(B), \qquad \text{because } \Theta(B^{**}) = 0. \end{aligned}$$

And, on the other hand, we have

$$h(T^{-1}B^{**}) - h(B) = h(\Lambda(T^{-1}B^{**}, B)B) - h(B) \leqslant p(B).$$

So $\Theta(B) \leqslant p(B)$ and $p(b) = \Theta(B)$.

Suppose now that the species of $\Theta(B)$ is $-$, which implies that the valuation of k is dense. Let be $\varepsilon > 0$. For every $i = 1, 2, \ldots, n$, we can find an $a_i \in b_i + V_{i+1}$ such that $v(a_i) - v(b_i) > p_i(B) - \varepsilon$ and an $\lambda_i \in k$ such that $0 < v(\lambda_i a_i) < \varepsilon$. Let $b_i' = \lambda_i a_i$ and $B' = (b_1', b_2', \ldots, b_n')$. If $a = \sum \mu_i b_i'$ is a linear

combination of B', I say that $v(a) \leqslant \mathrm{Min}_i\, v(\mu_i) + n\varepsilon$. Indeed, if V_q is, as before, $kb_q + \cdots + kb_n = ka_q + \cdots + ka_n$, I shall show by induction that, if $a \in V_q$,

$$v(a) < \operatorname*{Min}_{i>q} v(\mu_i) + (n-q+1)\,\varepsilon.$$

That is true for $q = n$, because $v(\mu_n b'_n) = v(\mu_n) + v(b'_n) < v(\mu_n) + \varepsilon$. Suppose this inequality is proved for $q > 1$, and let

$$a = \sum \mu_i b'_i \in V_{q-1}.$$

Hence $a = \mu_{q-1} b'_{q-1} + a^*$, where $a^* \in V_q$, and thus

$$v(a^*) \leqslant \operatorname*{Min}_{i \geqslant q} v(\mu_i) + (n-q+1)\varepsilon.$$

Also $v(\mu_{q-1} b'_{q-1}) < v(\mu_{q-1}) + \varepsilon$. If $v(a^*) \neq v(\mu_{q-1} b'_{q-1})$, we have $v(a) = \mathrm{Min}[v(a^*), v(\mu_{q-1} b'_{q-1})]$, which is certainly

$$\leqslant \operatorname*{Min}_{i \geqslant q-1} v(\mu_i) + (n-q)\varepsilon.$$

If $v(a^*) = v(\mu_{q-1} b'_{q-1})$, we have

$$a = \mu_{q-1}\lambda_{q-1}(a_{q-1} + \mu_{q-1}^{-1}\lambda_{q-1}^{-1} a^*) = \mu_{q-1}\lambda_{q-1} b''$$

and

$$b'' = a_{q-1} + \mu_{q-1}^{-1}\lambda_{q-1}^{-1} a^* \in b_{q-1} + V_q.$$

So

$$v(b'') - v(b_{q-1}) < p_{q-1}(B) \qquad \text{and} \qquad v(b'_{q-1}) - v(b_{q-1}) > p_{q-1}(B) - \varepsilon,$$

so $v(b'') - v(b'_{q-1}) < \varepsilon$ and

$$v(a) - v(a^*) = v(\mu_{q-1}\lambda_{q-1} b'') - v(\mu_{q-1}\lambda_{q-1} b'_{q-1}) = v(b'') - v(b'_{q-1})$$

is $-\varepsilon$, so $v(a) < v(a^*) + \varepsilon = v(\mu_{q-1} b'_{q-1}) + \varepsilon$. But

$$v(a^*) + \varepsilon < \operatorname*{Min}_{i \geqslant q} v(\mu_i) + (n-q)\varepsilon$$

and

$$v(\mu_{q-1} b'_{q-1}) < v(\mu_{q-1}) + \varepsilon;$$

so,

$$v(a) < \underset{i \geqslant q-1}{\text{Min}}\, v(\mu_i) + (n-(q-1)+1)\varepsilon.$$

As $V_1 = K$, we have for any aK, $v(a) \leqslant \text{Min}_i\, v(\mu_i) + n\varepsilon$.

But, if $v(a) \geqslant n\varepsilon$, we must have, for any i, $v(\mu_i) > 0$. Hence B' is an $n\varepsilon$-basis, but then $\Theta(B') \leqslant n(n\varepsilon) = n^2\varepsilon$, and if $A = (a_1, a_2, ..., a_n)$, we have $\Theta(A) = \Theta(B')$. So $\Theta(B) < h(A) - h(B) + n^2\varepsilon$. But $h(A) - h(B) \leqslant p(B)$, so $\Theta(B) \leqslant p(B) + n^2\varepsilon$ for any $\varepsilon > 0$. So, the real values of $\Theta(B)$ and of $p(B)$ are the same. But as $p(B) \leqslant \Theta(B)$, and the species of $\Theta(B)$ are $-$, that of $p(B)$ cannot be 0, and we have $p(B) = \Theta(B)$.

Remark 1. Some of the folds $p_i(B)$ of a basis B are of species 0, and some of species $-$. They are called, respectively, *zero-folds* and *minus-folds*. It will be shown in another publication that the number of zero-folds of a basis B does not depend on its choice and is *fe*.

3. Arithmetic Different: Deviation, Dedekindian and Hilbertian Extensions; Examples of Non-Dedekindian and Non-Hilbertian Extensions

As we have already said, the arithmetic different $\delta(K/k)$ of K/k is the g.c.d. of $\delta(a) = (f'_{a/k}(a))$ when a ranges over I^*, i.e., the ideal of I generated by all $f'_{a/k}(a)$, $a \in I^*$. So

$$v(\delta(K/k)) = \underset{S}{\text{Inf}}\, \{v(\delta(a); a \in I^*\} = \underset{S}{\text{Inf}}\, \{v(\Delta(B_a)); a \in I^*\},$$

where I^* is the set of all primitive integral elements of K/k and, for such element a, B_a is the basis $(1, 1, ..., a^{n-1})$ of K/k.

If B is any integral basis of K/k, we have

$$v(\Delta(B_a)) - v(\Delta(B) = -\frac{2}{n} v(\det \Lambda(B, B_a)),$$

and so

$$v(\Delta(B_a)) - v(\Delta(K/k) = -\frac{2}{n} \underset{S}{\text{Sup}}\, v(\det \Lambda(B, B_a)),$$

where B ranges over the integral bases of K/k.

Let T be a diagonal matrix such that

$$-v(\det T) = v(\det \Lambda(B, B_a)).$$

Then, $T\Delta(B, B_a) = \Delta(TB, B_a)$ is univalued and $\Theta(TB) = \Theta(B)$. So,

$$\Theta(B_a) = h(TB) - h(B_a) + \Theta(B) = v(\det T) + h(B) - h(B_a) + \Theta(B)$$
$$= -v(\det \Delta(B, B_a)) + [h(B) - h(B_a)] + \Theta(B).$$

And we have $v(\Delta(B_a)) - v(\Delta(B)) = (2/n)\, v(\det \Delta(B, B_a))$. So

$$v(\Delta(B_a)) - v(\Delta(B)) + \frac{1}{n}\Theta(B) = -\frac{2}{n}\{[h(B) - h(B_a)] + \Theta(B_a)\}.$$

Suppose first that the valuation of k is discrete, and let B be a 0-basis of K/k without discrepancy, so $\Theta(B) = 0$ and $h(B) = [(e-1)f/2]\omega$. We have always

$$h(B_a) = v(1) + v(a) + v(a^2) + \cdots + v(a^{n-1}) = (1 + 2 + \cdots + n - 1)\, v(a)$$
$$= (n(n-1)/2)\, v(a).$$

So,

$$v(\Delta(B_a)) - v(\Delta(B)) = \frac{2}{n}\Theta(B_a) - \frac{1}{n}[(e-1)f\omega - n(n-1)\, v(a)]$$
$$= \frac{1}{n}[2\Theta(B_a) - (e-1)f\omega + n(n-1)\, v(a)].$$

Suppose now that the valuation of k is dense, and let B be an ε-basis of K/k $(\varepsilon > 0)$. Then, we have $h(B) \leqslant n\varepsilon$ and $\Theta(B) \leqslant n\varepsilon$, so $(2/n)(h(B) - \Theta(B)) < 2\varepsilon$ and

$$[v(\Delta(B_a)) - v(\Delta(B))] - \frac{2}{n}|\Theta(B_a) - n(n-1)/2\, v(a)| < 2\varepsilon.$$

If there is a 0-basis of K/k, i.e., K/k is completely flat, and if B is such a base, we have

$$v(\Delta(B_a)) - v(\Delta(B)) = \frac{2}{n}[\Theta(B_a) + (n(n-1)/2)\, v(a)].$$

We call $\Theta'(a) = \Theta(B_a) - \frac{1}{2}|(e-1)f\omega - n(n-1)\, v(a)|$, where we put $\omega = 0$ if the valuation of k is dense, the *reduced discrepancy* of a. Clearly, if $\lambda \in k$, we have $\Theta'(\lambda a) = \Theta'(a) + \frac{1}{2}n(n-1)\, v(\lambda)$.

The reduced discrepancy $\Theta'(a)$ is a semi-real number of the same species as $\Theta(B_a)$, i.e., of the species 0 when K/k is not defective (and, in particular, when the valuation of k is discrete), and of species $-$ when K/k is defective.

We define the *deviation* of K/k by $e(K/k) = \mathrm{Inf}_S\{\Theta'(a); a \in I\}$.

When this infimum is reached, $e(K/k)$ has the species 0 or $-$; when it is not reached, the species of $e(K/k)$ is $+$. So $e(K/k)$ may be a semi-real number of any species.

In the case of dense valuations, we have also

$$e(K/k) \geqslant \operatorname*{Inf}_S \{\Theta(B_a);\, a \in I^*\},$$

and these two semi-real numbers have the same real value and, if the species of $e(K/k)$ is not $+$, then they are equal.

Indeed, first, if $a \in I^*$, $\Theta(B_a) \leqslant \Theta'(a)$, so

$$\operatorname*{Inf}_S \{\Theta(B_a);\, a \in I^*\} \leqslant e(K/k).$$

If the species of $e(K/k)$ is 0 or $-$, the $\operatorname{Inf}_S\{\Theta'(a);\, a \in I^*\}$ is reached, so there exists an $a \in I^*$ such that $\Theta'(a) = e(K/k)$. But then $v(a) = 0$ and $\Theta'(a) = \Theta(B_a)$. Indeed, if $v(a) > 0$, then there exists $\lambda \in k$ such that $-v(a) < v(\lambda) < 0$ and so $\lambda a \in I$ and $\Theta'(\lambda a) = \Theta'(a) + \frac{1}{2}n(n-1)\, v(\lambda)$ is $< \Theta'(a)$, which is contradictory. So $\operatorname{Inf}_S\{\Theta(B_a);\, a \in I\} = e(K/k)$ in this case. If the species of $e(K/k)$ is $+$, we have also

$$e(K/k) = \operatorname*{Inf}_S{}_* \{\Theta'(a);\, 0 < v(a) < \varepsilon\}.$$

But, if $v(a) \leqslant \varepsilon$, we have $\Theta(B_a) > \Theta'(a) - \frac{1}{2}n(n-1)\varepsilon$, hence

$$\operatorname*{Inf}_S \{\Theta(B_a):\, a \in I^*\} \geqslant e(K/k) = \tfrac{1}{2}n(n-1)\varepsilon \qquad \text{for any } \varepsilon > 0.$$

Thus, it has the same real value as $e(K/k)$.

We have, if B is a 0-basis of K/k without discrepancy, the relation

$$\Delta(B) = \Delta(K/k)$$

and

$$\begin{aligned} v(\delta(K/k)) &= \operatorname*{Inf}_S \{v(\delta(a));\, a \in I^*\} \\ &= \operatorname*{Inf}_S \{v(\Delta(B_a));\, v(a) \geqslant 0\} \\ &= v(\Delta(K/k)) + \operatorname*{Inf}_S \left\{\frac{1}{2n}\Theta'(a);\, v(a) \geqslant 0\right\} \\ &= v(\Delta(K/k)) + \frac{1}{2n}e(K/k). \end{aligned}$$

So, if there exists such a basis B (i.e., iff the valuation is discrete or K/k is completely flat), the species of $v(\delta(K/k))$ is the same as that of $e(K/k)$.

Besides, as such extension K/k is non-defective, all $\Theta'(B_a)$ are of species 0, and $e(K/k)$ cannot be of species $-$.

Consider now the case, when the species of $v(\delta(K/k))$ is $+$, i.e., there exists no 0-basis. (So, in particular, the valuation of k is dense.) $\mathrm{Inf}_S\, \Theta'(a)$ is reached when a ranges over I^*. It must be reached, as we have seen, for some $a \in I^*$ such that $v(a) = 0$, and $\delta(K/k) = \delta(a) = \Delta(B_a)$. The real value of $v(\delta(K/k))$ (i.e., $v(\delta(K/k))$ itself) is the sum of that of $v(\Delta(K/k))$ and $(2/n)\, e(K/k)$, but we can write

$$v(\delta(K/k)) = v(\Delta(K/k)) + \frac{2}{n} e(K/k)$$

only if $v(\Delta(K/k))$ is of species 0, because if that is not the case, the species of $v(\Delta(K/k))$ and of $(2/n)\, e(K/k)$ are, respectively, $+$ and $-$ (i.e., opposite) and the addition cannot be performed; but in both cases, we can write

$$v(\Delta(K/k)) = v(\delta(K/k)) - \frac{2}{n} e(K/k)$$

and

$$e(K/k) = \frac{n}{2} [v(\delta(K/k)) - v(\Delta(K/k))].$$

Suppose now that the species of $v(\Delta(K/k))$ is $+$ and that $\mathrm{Inf}_S\, \Theta'(a)$ is not reached. Then, clearly $e(K/k)$ and $v(\delta(K/k))$ both have the species $+$. As $v(\Delta(K/k))$ has the species 0 or $+$, $v(\Delta(K/k))$ and $(2/n)\, e(K/k)$ can be always added, and $v(\delta(K/k)) = v(\Delta(K/k)) + (1/2n)\, e(K/k)$. But we cannot write

$$e(K/k) = \frac{n}{2} [v(\delta(K/k)) - v(\Delta(K/k))]$$

and

$$v(\Delta(K/k)) = v(\delta(K/k)) - \frac{2}{n} e(K/k).$$

But in all cases, the type of valuation of k with the residual degree of K/k and two of the expressions $v(\Delta(K/k))$, $v(\delta(K/k))$, $(e(K/k)$ determine the third. We have, indeed,

THEOREM 4. *The real value of* $v(\delta(K/k))$ *is the sum of that of*

$$v(\Delta(K/k) \qquad \text{and} \qquad \frac{2}{n} e(K/k).$$

Proof. Given already.

The species of $v(\Delta(K/k))$ is 0 if the valuation of k is discrete or K/k is completely flat and $+$ if the valuation of k is dense and $f < n$. The species of $v(\delta(K/k))$ cannot be $-$. If the valuation of k is discrete or $f = n$ the species of $e(K/k)$ and of $v(\delta(K/k))$ are the same. If the valuation of k is dense and $f < n$, then the species of $e(K/k)$ is $-$, if that of $v(\delta(K/k))$ is 0, but it is $+$ if that of $v(\delta(K/k))$ is $+$.

An element a of I primitive in K/k such that $\delta(a) = \delta(K/k)$ is said to be *discriminantial*, and we denote by I_d the set of all such elements.

Clearly, it is not empty iff $v(\delta(K/k))$ is real. In the general case, we define, for any $\varepsilon > 0$, *ε-elements* of K/k all $a \in I^*$ such that $v(\delta(a)) - v(\delta(K/k)) \leqslant \varepsilon$, and their set will be denoted $I_{d,\varepsilon}$. As $\delta(a)$ and $\delta(K/k)$ are both ideals of K, we have $I_{d,\varepsilon} = I_d$ if $\varepsilon < \omega$, when the valuation of k is discrete.

An extension K/k is called *quasi-dedekindian* if the real values of $v(\delta(K/k))$ and of $v(\Delta(K/k))$ are the same, i.e., the real value of $e(K/k)$ is 0. As $e(K/k) \geqslant 0$ its species can be, in this case, only 0 or $+$. If $e(K/k) = 0$ the extension K/k is called *dedekindian.*

We see from the preceding theorem that K/k cannot be dedekindian when the valuation of k is dense and K/k is not completely flat.

An extension K/k is called *hilbertian* if for every intermediate field L of K/k, we have

$$v(\delta(K/k)) = v(\delta(K/L)) + v(\delta(L/k))$$

[i.e., $\delta(K/k) = \delta(K/L)\,\delta(L/K)$].

If only the real value of $v(\delta(K/k))$ is the sum of that of $v(\delta(K/L))$ and $v(\delta(L/k))$, K/k is said *quasi-hilbertian.* Clearly, if the valuation of k is discrete, a quasi-dedekindian (resp. quasi-hilbertian) extension is dedekindian (resp. hilbertian).

We call *dedekindian problem* that of characterization of dedekindian and quasi-dedekindian extensions and *hilbertian problem* that of characterization of hilbertian and quasi-hilbertian extensions.

At the end of this section I shall give the characterization of dedekindian extensions, hence, in particular, the solution of the dedekindian problem in the case of discrete valuations, and the much more difficult solution of this problem for dense valuations (i.e., characterization of quasi-dedekindian extensions) will be given in some other publication.

An extension K/k will be called *classical* if $\bar{K}/\bar{k}$ is separable and the valuation of k is discrete. It will be called *quasi-classical* if K/k is separable, $v(K)/v(k)$ is cyclic, and K/k is not defective.

LEMMA 4. *An extension K/k is dedekindian iff there exists some $a \in I^*$ such, that some unfolding A of B_a would be a 0-basis of K/k without discrepancy. And K/k is quasi-dedekindian iff for any $\varepsilon > 0$ there exists an $a \in I^*$ such, that B_a is an ε-basis.*

Proof. If $b_i \in a^i + V_{i+1}$ and $B = (b_0, b_1, ..., b_{n-1})$, $\Delta(B, B_a)$ is certainly univalued and $\Delta(B) = \Delta(B_a)$. If B is a 0-basis of K/k we have $\Delta(B) = \Delta(K/k)$, and if B is an ε-basis of K/k we have $\Delta(B) - \Delta(K/k) \leqslant 2\varepsilon$.

We have in the first case,

$$v(\delta(K/k)) \leqslant v(\Delta(B_a)) = v(\Delta(B)) = v(\Delta(K/k))$$

and as $v(\delta(K/k)) \geqslant v(\Delta(K/k))$ we have $v(\delta(K/k)) = v(\Delta(K/k))$ and, as $v(\Delta(K/k)) = v(\Delta(B))$ is of species 0, we have $e(K/k) = 0$.

Besides, we must have $\Theta(B) = \Theta(B_a) - p(B_a) = 0$, so B is without discrepancy. If the valuation of k is dense and if B_a is an ε-basis, we have

$$v(\delta(a)) = v(\Delta(B_a)) \leqslant v(\Delta(K/k)) + 2\varepsilon$$

and

$$v(\delta(K/k)) \leqslant v(\Delta(K/k)) + 2\varepsilon.$$

So, if for every $e > 0$ there exists an $a \in I^+$ such, that B_a is an ε-basis, we have, for every ε, $v(\delta(K/k)) \leqslant v(\Delta(K/k)) + 2\varepsilon$ and $v(\delta(K/k))$ and $v(\Delta(K/k))$ have some real value, so $e(K/k) \leqslant 0^+$.

Suppose that K/k is dedekindian, i.e., $e(K/k) = 0$. That requires first that the species of $v(\delta(K/k))$ is 0, because otherwise that of $e(K/k)$ is $+$.

Let $a \in I^*$ be such that $\delta(K/k) = \delta(a) = \Delta(B_a)$. Then if K/k is dedekindian, we must have $\Delta(K/k) = \Delta(B_a)$. But that implies that $\Delta(K/k)$ is of species 0, i.e., that K/k has a 0-basis B, and that $\Delta(B_a) = \Delta(B)$ and $v(\det \Lambda(B_a, B)) = 0$. But as B is a 0-basis and B_a and integral one, $\Lambda(B_a, B)$ is integral, so B_a and B generate a same i-module, and B_a is a 0-basis of K/k.

In the case of discrete valuation, $\Theta(B_a) = p(B_a)$ is certainly real, so there exists an outfolding A of B_a, and A is also a 0-basis of K/k. Its discrepancy is $\Theta(B_a) - p(B_a) = 0$.

In the case of dense valuations, K/k must be completely flat and $h(B_a)$ must be 0; i.e., $v(a) = 0$.

If $\Theta(B) = p(B) > 0$, there exists a univalued matrix Λ such that ΛB_a is integral and $h(\Lambda B_a) > 0$. But as B_a is a 0-basis, for every

$b = \sum_{1<i<n} \lambda_i a^{i-1} \in I$, all λ_i must be $\in i$. So, Λ is an integral matrix, and ΛB_a must also be a 0-basis which implies $h(\Lambda B_a) = 0$. This contradiction shows that $p(B_a) = \Theta(B_a) = 0$, so B_a is already unfolded.

If K/k is quasi-dedekindian, then there exists, for every $\varepsilon > 0$, an $a \in I^*$ such that $v(\Delta(B_a)) - v(\Delta(K/k)) < \varepsilon$, i.e., for any integral basis of K/k, $v(\Delta(B_a)) - v(\Delta(B)) < \varepsilon$. That implies $v(a) < \varepsilon$ and $\Theta(B_a) < n\varepsilon/2$. Indeed, if $v(a) \geqslant \varepsilon$, then there exists a $\lambda \in k$ such that

$$-v(a) \leqslant v(\lambda) \leqslant -\varepsilon, \quad \text{so} \quad v(\lambda a) \geqslant 0 \quad \text{and} \quad \det \Lambda(B_{\lambda a}, B_a) = \lambda^{n(n-1)/2},$$

so $v(\det \Lambda(B_{\lambda a}, B_a)) = [n(n-1)/2]\, v(\lambda) < [-n(n-1)/2]\varepsilon$, and

$$v(\Delta(B_a)) - v(\Delta(B_{\lambda a})) = -\frac{2}{n} v(\det \Lambda(B_{\lambda a}, B_a)) \geqslant (n-1)\varepsilon > \varepsilon.$$

And if $\Theta(B_a) \geqslant n\varepsilon/2$, then there exists a univalued matrix such, that $h(\Delta B_a) \geqslant h(B) + (n\varepsilon/2)$.

But then there exists a diagonal matrix T, such that $v(\det T) \leqslant -n\varepsilon/2$ and that $B = T\Lambda B_a$ is an integral basis. Thus

$$v(\Delta(B_a)) - v(\Delta(B)) = -\frac{2}{n} v(\det T\Lambda) = -\frac{2}{n} (\det T) \geqslant \frac{2}{n} (n\varepsilon/2) = \varepsilon,$$

which is impossible. But then B_a is $\varepsilon + (n\varepsilon/2) = (n+2)\varepsilon/2$-basis and the assertion is proved.

THEOREM 5. *If K/k is a classical extension, it is dedekindian. If it is quasi-classical, it is quasi-dedekindian.*

Proof. (The idea can already be found in the Zahlbericht [3], Theorem 29.) Let a' be an element of I such that its rest $\bar{a}' = a' + M$ (mod M) is a primitive element of $\bar{K}/\bar{k}$ (which exists because $\bar{K}/\bar{k}$ is separable).

Let be $f_{\bar{a}'/\bar{k}}(X)$ the minimal polynomial of $\bar{a}'$ over $\bar{k}$. Let $f(X) = c_0 + c_1 X + c_2 X^2 + \cdots + X^f$ be a unitary polynomial $i[X]$ of degree f such that its residual polynomial

$$\bar{c}_0 + \bar{c}_1 X + \cdots + X^f \qquad \text{is} \quad f_{\bar{a}'/\bar{k}}(X).$$

Then $f(a)$ becomes $f_{\bar{a}'/\bar{k}}(a') = \bar{0}$, so $v(f(a')) > 0$ and, if $f'(X)$, $f'_{\bar{a}'/\bar{k}}(X)$ are the derivations of $f(X)$, $f_{\bar{a}'\bar{k}}(X)$, $f'(a)$ has the residual polynomial $f'_{\bar{a}/\bar{k}}(a') \neq 0$, because a' is a simple root of $f_{\bar{a}'/\bar{k}}(X)$.

So, $v(f'(a')) = 0$. If K/k is completely flat, $(1, a', ..., a'^{f-1})$ is its 0-basis [and that does not require even the separability of K/k, but only the

existence of a primitive element a, i.e., its simplicity]. If $f < n$ and P is an element of K such that $V(P) > 0$, then we have

$$f(a' + P) = f(a') + f'(a')P + P^2 g(a, P), \qquad \text{where} \quad g(X, Y)$$

is some polynomial $\in i[X, Y]$, hence

$$v(f(a' + P) - f(a') - f'(a)P) \geqslant 2v(P).$$

Suppose first the valuation of k is discrete. If $v(f(a')) = \Omega$, we put $\Pi = f(a)$ and $a = a'$, and when $v(f(a'))$ is $> \Omega$ we choose some $P \in K$ such that $v(P) = \Omega$, and we put $a = a' + P$ and $\Pi = f(a + P)$.

In all cases, we have $\bar{a} = \bar{a}'$, and $v(\Pi) = \Omega$. So, if

$$b_{qf+s} = \Pi^{e-1-q} a^{f-s-1} (q = 0, 1, ..., e-1; s = 1, 2, ..., f),$$

$B = (b_1, b_2, ..., b_n)$ is a 0-basis of K/k without discrepancy, which is an outfolding of $(a^{n-1}, a^{n-2}, ..., 1)$, which is the permutation of B. So K/k is dedekindian. When the valuation of k is dense, then there exists for every $\varepsilon > 0$, a $P \in K$ such that $nv(P) < \varepsilon$ and $v(P)$ generates the cyclic group $v(K)/v(k)$. Then, if $\varepsilon < v(f(a'))$, we put $a = a' + P$ and $\Pi = f(a) = f(a' + P)$. We have $v(\Pi - f'(a')P) = v(P^2 g(a', P) + f(a')) > \text{Min}[\varepsilon, f(a')] > v(P)$ and as $v(f'(a')) = 0$, we have $v(\Pi) = v(P)$.

So, if B is again the same as before, we have, if $d = 1$, that B is a basis of K/k without discrepancy and

$$h(B) = [(e-1)f/2]\, v(P) < nv(P) < \varepsilon,$$

so, if B is an ε-basis of K/k and as $\Lambda(B, B_a)$ is univalent and integral, B_a is also. So K/k is quasi-dedekindian.

We have proved at the same time the following:

PROPOSITION 7. *If K/k is simple and K/k is completely flat, then it is dedekindian,*

and

PROPOSITION 8. *If the valuation of k is discrete, $\bar{K}/\bar{k}$ is simple, but not separable, K/k is not completely flat, and $v(f(a')) = \Omega$, then the extension is dedekindian.*

Also it is clear that for a fixed $\bar{a}'$, this property does not depend on the choice of f and of a', because first if $f_1(X)$ has also $f_{\bar{a}'/\bar{k}}(X)$ as residual polynomial, the order of all coefficients of $f_1(X) - f(X)$ is $> \omega = e\Omega > \Omega$

and $v(f(a')-f_1(a'))>\Omega$. Thus $v(f(a'))$ and $v(f_1(a'))$ are $=\Omega$ at the same time. On the other hand, if $\overline{a''}=\overline{a'}$, we have $a''=a'+P$ where $v(P)\geqslant\Omega$.

Then $f(a'')-f(a')=f'(a')P+P^2g(a', P)$.

But $\overline{f'(a)}=f'_{\bar{a}'/\bar{k}}(\overline{a'})$. As a is not separable over k, we have $f'_{\bar{a}'/\bar{k}}(\overline{a'})=\bar{0}$, so $v(f'(a'))>0$ and $(f(a'')-f(a'))>\Omega$. So $v(f(a''))$ and $v(f(a'))$ are $=\Omega$ at the same time. We shall see that this condition does not depend even on the choice of $\bar{a}'$. We shall put this condition in the following form.

PROPOSITION 9. *If the valuation of k is discrete and $\bar{K}/\bar{k}$ is simple, K/k is dedekindian then there exists an $a\in I$ such that $\bar{a}$ is a primitive element of $\bar{K}/\bar{k}$ and $f_{a/k}(X)$ has the form $f(X)^e+\sum_{i=0,1,\ldots,e-1,\,j=0,1,\ldots,f-1}\alpha_{i,j}f(X)^iX^j$ such that, for all i, j, $v(\alpha_{i,j})>0$ and $\mathrm{Min}_j v(\alpha_{0,j})=\omega$, and $f[X]\in i[X]$.*

Proof. First, as $n=ef$, $f(X)$ has the degree f, On the other hand, for every i, $0<i<e$, and for any $j=0, 1, \ldots, f-1$, we have $v(\alpha_{i,j})\geqslant\omega$, so $ev(f(a))=v(f(a)^e)\geqslant\omega$ and $v(f(a))\geqslant\Omega>0$. But then, if $0<i<n$, we have

$$v\left(\sum_{0\leqslant j\leqslant f}\alpha_{ij}f(a)^i a^j\right)>\omega.$$

Let π be an element of k such that $v(\pi)=\omega$. Then, for any j, $v(\pi^{-1}\alpha_{0,j})\geqslant 0$, i.e., $\pi^{-1}\alpha_{0,j}\in i$, and for *some* j we have $v(\pi^{-1}\alpha_{0,j})=0$, so the residue $\bar{\lambda}_j=\overline{\pi^{-1}\alpha_{0,j}}\in\bar{k}$ is $\neq\bar{0}$. So, the residue

$$\overline{\pi^{-1}\left(\sum_{0\leqslant j<f}\alpha_{0,j}a^j\right)} \quad \text{of} \quad \pi^{-1}\left(\sum_{0\leqslant j<f}\alpha_{0,j}a^j\right)$$

is $\sum_{0\leqslant j<f}\bar{\lambda}_j\bar{a}^j$ and not all $\bar{\lambda}_j\in\bar{k}$ are $\bar{0}$. But as $\bar{K}/\bar{k}$ is of degree f and $\bar{a}$ is its primitive element, $(1, \bar{a}, \ldots, \bar{a}^{f-1})$ is a linear basis of this extension, and the residue is $\neq 0$, so

$$v\left(\pi^{-1}\sum_{0<j<f}\alpha_{0,j}a^j\right)=0$$

and

$$v\left(\sum_{0<j<f}\alpha_{0,j}a^j\right)=v(\pi)=\omega=e\Omega.$$

But, as $v(\alpha_{i,j}a^jf(a)^i)>\omega$ for $i>0$ and any j, $f_{a/k}(a)=0$ implies $v(f(a))=\Omega$.

Let

$$f(X)=\sum_{0\leqslant j\geqslant f}\beta_jX^j.$$

Let $\mathrm{Min}_{0\leqslant j\leqslant f} v(\beta_j) > 0$, so $\geqslant \omega$. Then, $f(a) \geqslant \omega > \Omega$ and therefore, we must have $\mathrm{Min}_j\, v(\beta_j) = 0$. Let $\bar{\beta}_j$ be the residue of β_j. Then, not all $\bar{\beta}_j$ are $=\bar{0}$ and

$$\sum_{0\leqslant j\leqslant f} \bar{\beta}_j \bar{a}^j = \overline{f(a)} = \bar{0}.$$

But every combination over $\bar{k}$ of $1, \bar{a}, ..., \bar{a}^f$ which is $=\bar{0}$, is proportional to $f_{\bar{a}/\bar{k}}(a)$, so $\bar{\beta}_f \neq \bar{0}$ and

$$f_{\bar{a}/\bar{k}}(X) = \bar{\beta}_f^{-1} \bar{f}(X).$$

So, $\beta_f^{-1} f(X)$ is unitary, the residual polynomial of $\beta_f^{-1} f(X) \in i[X]$ is $f_{\bar{a}/\bar{k}}(X)$, and $v(\beta_f^{-1} f(a)) = \Omega$. So, the hypotheses of Proposition 8 are fulfilled, and K/k is dedekindian.

LEMMA 4. *If, with the notations of Proposition* 8, $v(f(a')) > \Omega$, $B_{a'}$ *is not a* 0*-basis of* K/k.

Proof. Let Π be an element of I such that $v(\Pi) = \Omega$. If $B_{a'}$ is a 0-basis, i.e., $I = i(B_{a'})$, then there exists a polynomial $g(X) \in i[X]$ such that $\Pi = g(a')$. If we divide $g(X)$ by $f(X)$, which is also $\in i[X]$ and is unitary, we have $g(X) = q(X) f(X) + r(X)$, where $q(X)$ and $r(X)$ are $\in i[X]$ and the degree of $r(X)$ is $< f$. Then, $v(q(a') f(a')) \geqslant v(f(a')) > \Omega$, and, as $v(g(a')) = v(\Pi) = \Omega$, we must have $v(r(a')) = \Omega$. But that is impossible. Indeed, $r(a') = \sum_{0\leqslant j<f} \lambda_j a'^j$, where all λ_j are $\in i$. If $\mathrm{Min}_j\, v(\lambda_j) > 0$, it is $\geqslant \omega > \Omega$, and $v(r(a')) > \Omega$. And if $\mathrm{Min}_j\, v(\lambda_j) = 0$, we have $\overline{r(a')} = \sum_j \bar{\lambda}_j \overline{a'}^j$, and not all $\bar{\lambda}_j \in \bar{k}$ are $\bar{0}$. But $\bar{1}, \overline{a'}, \overline{a'}^2, ..., \overline{a'}^{f-1}$ are linearly independent over $\bar{k}$. So, $\overline{r(a')} \neq \bar{0}$ and $v(r(a')) = 0 \neq \Omega$. So, $B_{a'}$ is not a 0-basis of K/k.

LEMMA 5. *If, for some primitive element* $\bar{a}$ *of* $\bar{K}/\bar{k}$, $v(f(a)) = \Omega$, *where* $a \in I$ *is such, that* $\bar{a}$ *is its residue, and where* $f(X) \in i[X]$ *is a unitary polynomial having* $f_{\bar{a}/\bar{k}}(X)$ *as its residual polynomial, the same condition holds for any other primitive element* $\bar{a}'$ *of* $\bar{K}/\bar{k}$.

Proof. As $\bar{a}'$ is primitive in $\bar{K}/\bar{k}$, $\bar{a}$ is a linear combination $\sum_{0\leqslant j<f} \bar{\lambda}_j \bar{a}'^j$ of $\bar{1}, \bar{a}', ..., \bar{a}'^{f-1}$. Let $a' \in I$ be such that its residue $\overline{a'}$ is $=\bar{a}'$, and let λ_j be an element of i such that its residue is $\bar{\lambda}_j$. Then $a^* = \sum_{0\leqslant j<f} \lambda_j \lambda_j a'^j$ is $\equiv 0 \pmod{M}$, so its residue is $\bar{a}$. Therefore, B_{a^*} is a 0-basis of K/k, so $i(B_{a^*}) = I$. We have $a^* \in i[a']$, so every a^{*j} is $\in i(a')$, and $B_{a^*} \subseteq i[a']$. So, $I \supseteq i[a'] \supseteq i(B_{a^*}) = I$, i.e., $i(a') = I$ and $B_{a'}$ is a 0-basis of K/k.

PROPOSITION 10. *Given a discrete valuation of* k, *let an element of* I *be such that its residue* $\bar{a}$ *is primitive in* $\bar{K}/\bar{k}$ *and* $f(X) \in i[X]$ *a unitary polynomial of degree* f *having* $f_{\bar{a}/\bar{k}}(X)$ *as residual polynomial. Then, if* $v(f(a)) > \Omega$, K/k *is not dedekindian.*

Proof. Suppose that K/k is dedekindian. Then, for some $\underline{a'} \in I$, $B_{a'}$ is a 0-basis of K/k. In particular, the ring $\bar{k}[\overline{a'}]$ must be $=\bar{K}$, so $\overline{a'}$ is primitive in $\bar{K}/\bar{k}$. But then, by Lemma 5, B_a is also a 0-basis of K/k, which contradicts Lemma 4.

EXAMPLE 1. Let $\bar{f}(X) \in \bar{k}[X]$ be an irreducible unitary non-separable polynomial, $f(X) \in i[X]$ a unitary polynomial having $\bar{f}(X)$ as residual polynomial, z a root of $f(X)$, $g(X) \in i[X]$ an Eisensteinian polynomial, Π a root of $g(X)$. Then, if $K = k(z, \Pi)$ and $\bar{z}$ is the rest of z, we have $\bar{K} = \bar{k}(\bar{z})$ and $\bar{f}(X) = f_{\bar{z}/\bar{k}}(X)$. But $f(z) = 0$, so $v(f(z)) = +\infty > \Omega$, and K/k is not dedekindian.

PROPOSITION 11. *If the residual extension $\bar{K}/\bar{k}$ of K/k is not simple, K/k is not dedekindian.*

Proof. Let be $a \leqslant I$. Suppose that B_a is a 0-basis of K/k. Then, for every $b \in I$, there is a polynomial $g(X) \in i[X]$ such, that $b = g(a)$. But then, if $\bar{g}(X)$ is the residual polynomial of $g(X)$, we have $\bar{b} = \overline{g(a)} = \bar{g}(\bar{a})\,\bar{k}(\bar{a})$. As $\bar{b}$ can be arbitrary elements of $\bar{K}$ for convenient $b \in I$, it follows that $\bar{K} = \bar{k}(\bar{a})$, i.e., $\bar{K}/\bar{k}$ is simple in contradiction with the hypothesis of the proposition. Thus, no B_a, $a \in I$, is a 0-basis, and K/k is not dedekindian.

EXAMPLE 2. Let $\bar{K}^* = \bar{k}(\bar{a}, \bar{b})$ be a non-separable extension of $\bar{k}$, which is not simple, $\bar{f}(X) = f_{\bar{a}/\bar{k}}(X)$ and $\bar{g}(X) = f_{\bar{b}/\bar{k}(\bar{a})}(X)$, and let d, d' be the degrees $[\bar{k}(\bar{a}) : \bar{k}]$ and $[\bar{K} : \bar{k}(\bar{a})]$ of $\bar{f}(X)$ and $\bar{g}(X)$. There exists a polynomial $\bar{h}(X, Y) \in \bar{k}[X, Y]$ of degree d' in X such, that $\bar{g}(X) = \bar{h}(X, \bar{a})$. Let $f(X) \in i[X]$ be a unitary polynomial of degree d having $\bar{f}(X)$ as its residual polynomial. Then, there exists a root a of $f[X]$ having $\bar{a}$ as its residue. Let $h(X, Y)$ be a polynomial $\in i[X, Y]$ of degree d' in X having $\bar{h}(X, Y)$ as its residual polynomial. Then $\bar{g}(X)$ is the residual polynomial of $g(X) = h(X, a)$, and there is a root b of $g(X)$ having $\bar{b}$ as residue. Let $K = k(a, b)$. We have $n = [K : k] = [k(a, b) : k(a)][k(a) : k] \leqslant dd'$ and $\bar{K} \supseteq \bar{k}(\bar{a}, \bar{b})$, so $f = [\bar{K} : \bar{k}] \geqslant [\bar{k}(\bar{a}, \bar{b}) : \bar{k}] = dd'$. Hence $f \geqslant n$, i.e., $f = n$, and $\bar{K} = \bar{K}^* = \bar{k}(\bar{a}, \bar{b})$. So, K/k is completely flat and $\bar{K}/\bar{k}$ is not simple. In particular, K/k is not dedekindian.

THEOREM 6. *A valued extension K/k is dedekindian only in the following three cases*:

(1) *the valuation of k is discrete and $\bar{K}/\bar{k}$ is separable* ("*classical case*");

(2) *K/k is completely flat and $\bar{K}/\bar{k}$ is simple*;

(3) *the valuation of k is discrete, $\bar{K}/\bar{k}$ is simple, and, for some $a \in I$*

such that its residue $\bar{a}$ is primitive in $\bar{K}/\bar{k}$, and for some unitary polynomial $f(X) \subset i[X]$ of degree $f = [\bar{K} : \bar{k}]$ having $f_{\bar{a}/k}(X)$ as its residual polynomial, $v(f(a))$ is $= \Omega$.

Remarks. (a) The case (3) can be restricted to not completely flat extensions K/k and to non-separable $\bar{K}/\bar{k}$, because the other cases enter in (1) and (2); (b) if the hypothesis of case (3) is fulfilled for some a and $f(X)$, it is fulfilled for every a and $f(X)$ satisfying the same conditions when $\bar{K}/\bar{k}$ is not separable.)

Proof. It is already proved that K/k is dedekindian in the cases (1), (2), and (3) (Theorem 5 and Propositions 7 and 8) and that K/k is not dedekindian in all other cases if the valuation of k is discrete (Proposition 10) or $\bar{K}/\bar{k}$ is not simple (Proposition 11) (Remark (b) is also proved by Lemma 5, and Remark (a) is obvious.) So, the only doubtful case is if the valuation of k is dense, K/k is not completely flat and $\bar{K}/\bar{k}$ is not simple. If so, $v(\Delta(K/k))$ is of species $+$. If $v(\delta(K/k))$ is of species 0, $e(K/k)$ is of species $-$, so is $>0^+$, and K/k is even not quasi-dedekindian. And if the species of $v(\delta(K/k))$ are $+$, those of $e(K/k)$ are the same, and K/k is or is not quasi-dedekindian, but never dedekindian.

4. Connections with the Ramification Theory

Let be K/k a separable valued extension of finite degree of an henselian field k and G the set of all isomorphisms of K/k into some overfield K' of K normal and of finite degree over k with the valuation prolonging that of K/k and $G^* = \{\sigma \in G; \sigma \neq 1_K\}$. If $a \in K$ and $\sigma \in G$, we call $v(\sigma; a) = v(\sigma \cdot a - a) \in v(K') \cup \{+\infty\}$ the *characteristic number* (or *value*, which is the better term for Krull valuations, where the elements of $v(K')$ are generally not numbers; but here we consider only valuations with real values) of σ in a;

$$v(\sigma) = \operatorname*{Inf}_S \{v(\sigma; a); a \in I\}$$

is called the *characteristic number* (or *value*) of σ.

Theorem 7. *For every $\varepsilon > 0$, there exists an $a \in I$ such that $\sum_{\sigma \in G^*} [v(\sigma; a) - v(\sigma)] \leqslant \varepsilon$.*

Proof. Let us suppose first that the residual field $\bar{k}$ of k is infinite. For any $\sigma \in G^*$, we can find an $a_\sigma \in I$ such that $v(\sigma; a_\sigma) - v(\sigma) < \varepsilon/(n-1)$, where $n = [K : k]$. Consider $a = \sum_{\xi \in G^*} \lambda_\xi a_\xi$, where all λ_ξ are $\in i$ and $v(\lambda_\xi) = 0$. Then, if $\sigma \in G^*$, we have $\sigma \cdot a - a = \sum_{\xi \in G^*} \lambda\xi(\sigma \cdot a\xi - a\xi)$. Suppose that

$v_\sigma = \mathrm{Min}_{\xi \in G^*} v(\sigma \cdot a_\xi - a\xi) = \mathrm{Min}_{\xi \in G^*} v(\sigma; a_\xi)$, and let $\Pi_\sigma \in K'$ be an element such that $v(\Pi'_\sigma) = v_\sigma$. If $\bar{K}'$ is the residual field of K', and I' its valuation ring, we have $(\sigma \cdot a\xi - a\xi)/\Pi'_\sigma \in I'$ and the residue $\bar{\rho}_{\sigma,\xi}$ of this element of I' is $\in \bar{K}'$. So, if $\bar{\lambda}_\xi \in \bar{k}$ is the residue of λ_ξ, we have $\overline{\Pi'^{-1}_\sigma (\sigma \cdot a - a)} = \sum_{\xi \in G^*} \bar{\lambda}_\xi \bar{\rho}_{\sigma,\xi}$ and if $\sum_{\xi \in G^*} \bar{\lambda}\xi \bar{\rho}_{\sigma,\xi} \neq \bar{0}$, we have $v(\sigma \cdot a - a) = v(\Pi'_\sigma) = v_\sigma \leqslant v(\sigma \cdot a_\sigma - a_\sigma) \leqslant v(\sigma) + [\varepsilon/(n-1)]$. But as $\bar{k}$ is infinite, it is always possible to find elements $\bar{\lambda}_\xi$ of $\bar{k}$ such that $\sum_{\xi \in G^*} \bar{\lambda}_\xi \bar{\rho}_{\sigma,\xi}$, for all $\sigma \in G^*$, are $\neq \bar{0}$. So, if $a = \sum_{\xi \in G} \lambda_\xi a_\xi$ with λ_ξ having such residue $\bar{\lambda}_\xi (\xi \in G^*)$, we have $(\sigma \cdot a - a) \leqslant v(\sigma) + [\varepsilon/(n-1)]$. So $\sum_{\sigma \in G^*} [v(\sigma; a) - v(\sigma)] \leqslant (n-1)[\varepsilon/(n-1)] = \varepsilon$.

Suppose now that the valution is dense, and let $w_{\sigma,\xi} = v(\sigma; a_\xi) = v(\sigma \cdot a_\xi - a_\xi)$. Let $\eta > 0$ and $< [\varepsilon/(n-1)] - \mathrm{Max}_{\sigma \in G^*} [w_{\sigma,\sigma} - v(\sigma)] = [\varepsilon/(n-1)] - \mathrm{Max}_{\sigma \in G^*} [v(\sigma; a_\sigma) - v(\sigma)]$ (which is > 0).

Suppose that all $\lambda_\sigma \in i$ are such that $v(\lambda_\sigma) < \eta$. Then, if in addition, for $\sigma \in G^*$ all $v(\lambda_\xi [\sigma \cdot a_\xi - a_\xi]) = v(\lambda_\xi) + w_{\sigma,\xi}$ are distinct, we have $v(\sigma \cdot a) - a = v(\sum_{\xi \in G^*} \lambda_\xi [\sigma \cdot a_\xi - a_\xi]) = \mathrm{Min}_{\xi \in G^*} [v(\lambda_\xi) + w_{\sigma,\xi}] < \mathrm{Min}_{\xi \in G^*} w_{\sigma,\xi} + \eta \leqslant w_{\sigma,\sigma} + \eta$. So,

$$\begin{aligned}
\sum_{\sigma \in G^*} [v(\sigma \cdot a - a) - v(\sigma)] &\leqslant \sum_{\sigma \in G^*} [v(\lambda_\sigma(\sigma \cdot a_\sigma - a_\sigma)) - v(\sigma)] \\
&= \sum_{\sigma \in G^*} [v(\lambda_\sigma) + w_{\sigma,\sigma}] \leqslant \sum_{\sigma \in G^*} w_{\sigma,\sigma} + (n-1)\eta \\
&\leqslant \sum_{\sigma \in G^*} w_{\sigma,\sigma} + (n-1)[\varepsilon/(n-1) - \mathrm{Max}_{\sigma \in G^*} w_{\sigma,\sigma}] \\
&\leqslant \left[\sum_{\sigma \in G^*} w_{\sigma,\sigma}\right] + \varepsilon - (n-1) \mathrm{Max}_{\sigma \in G^*} w_{\sigma,\sigma} \\
&\leqslant \sum_{\sigma \in G^*} w_{\sigma,\sigma} + \varepsilon - \sum_{\sigma \in G^*} w_{\sigma,\sigma} = \varepsilon.
\end{aligned}$$

And, as the valuation is dense, such $\lambda_\sigma \in k$ can be found. So, the proposition is proved also in this case.

When the valuation is discrete and $\bar{k}$ is finite, k and K are locally compact, i.e., p-adic or fields of power series of one variable over a finite field. In this case, if $\Pi \in K$ is such that $v(\Pi) = \Omega$ and if $a \in I$ belongs to the maximal nonramified subextension of K_I/k of K/k (for their existence see, in the p-adic case, my paper [5] and in the general henselian case my preprint [13]. Also, see Ostrowski [16]) and $\bar{a}$ is primitive in $\bar{K}/\bar{k}$, we have, for every $\sigma \in G$, $v(\sigma) = v(\sigma; a + \Pi)$ (when K/k is completely slim, even $v(\sigma) = v(\sigma; \Pi)$; see the proof in the p-adic case in [5]; the proof in the other locally compact case is similar).

PROPOSITION 12. *The real values of* $v(\delta(K/k))$ *and of* $\sum_{\sigma \in G^*} v(\sigma)$ *are equal.*

Proof. We have first $v(\delta(a)) = v(\prod_{\sigma \in G^*} (a - \sigma \cdot a)) = \sum_{\sigma \in G^*} v(\sigma \cdot a - a) = \sum_{\sigma \in G^*} v(\sigma; a)$. There exists, for every $\varepsilon > 0$, an $a \in I$ such that $v(\delta(a)) - v(\delta(K/k)) < \varepsilon$, i.e., $v(\delta(K/k)) > v(\delta(a)) - \varepsilon = (\sum_{\sigma \in G^*} v(\sigma; a)) - \varepsilon \geqslant (\sum_{\sigma \in G^*} v(\sigma)) - \varepsilon$. But, by the preceding theorem, there exists an $a \in I$ such that $\sum_{\sigma \in G^*} [v(\sigma; a) - v(\sigma)] = v(\delta(a)) - \sum_{\sigma \in G^*} v(\sigma)$ is $< \varepsilon$, i.e., $v(\delta(a)) < (\sum_{\sigma \in G^*} v(\sigma)) + \varepsilon$ and, therefore, $|v(\delta(K/k)) - (\sum_{\sigma \in G^*} v(\sigma))| < \varepsilon$. The difference of the real values of $v(\delta(K/k))$ and of $\sum_{\sigma \in G^*} v(\sigma)$ is, for any $\varepsilon > 0$, less than ε in absolute value. So, these real values are equal.

THEOREM 8. *We have* $v(\delta(K/k)) = \sum_{\sigma \in G^*} v(\sigma)$.

Proof. Suppose first that $v(\delta(K/k))$ has the species 0 (that is always the case if the valuation of k is discrete). Then there exist discriminantial elements a, i.e., $a \in I$, such that $v(\delta(K/k)) = v(\delta(a)) = \sum_{\sigma \in G^*} v(\sigma; a)$. The value $v(\delta(a))$, which is real, is equal to the sum of real values of $v(\sigma)$, $\sigma \in G^*$. But, $v(\sigma; a) \geqslant v(\sigma)$, so is equal or greater than the real value of $v(\sigma)$. And the equality of sums of these real values and of (real) $v(\sigma; a)$ implies that $v(\sigma; a)$ is equal to the real value of $v(\sigma)$ and, as the species of $v(\sigma)$ is 0 or +, $v(\sigma; a)) \leqslant v(\sigma)$. But that implies $v(\sigma; a) = v(\sigma)$ and $v(\delta(K/k)) = \sum_{\sigma \in G^*} v(\sigma)$. Suppose now that the species of $v(\delta(K/k))$ is +, so the valuation is dense. The sum $\sum_{\sigma \in G^*} v(\sigma)$ has the same species iff some $v(\sigma)$ is of species +. Suppose that all $v(\sigma)$ are of species 0. Then, for every $\sigma \in G^*$ there exists an $a_\sigma \in I$ such that $v(\sigma; a_\sigma) = v(\sigma)$. We must have $v(a_\sigma) = 0$, because if $v(a_\sigma) > 0$, we can find a $\lambda \in k$ such that $-v(a_\sigma) < v(\lambda) < 0$, and, then λa_σ is $\in I$ and we have $v(\sigma, \lambda a_\sigma) = v(\lambda) + v(\sigma) < v(\sigma)$, which is absurd. If $\bar{k}$ is inifinite, we prove as previously the existence of an $a \in I$ such that for any $\sigma \in G^*$, $v(\sigma; a) = v(\sigma; a) = v(\sigma)$ and $v(\delta(K/k)) \leqslant v(\delta(a)) = \sum_{\sigma \in G^*} v(\sigma)$. But as $v(\delta(K/k))$ has the same real values as $\sum_{\sigma \in G^*} v(\sigma)$, which is real, and is of species +, we must have $v(\delta(K/k)) > \sum_{\sigma \in G^*} (v(\sigma))$, which is contradictory. If $\bar{k}$ is finite, $\bar{K}/\bar{k}$ is separable, and the greatest non-ramified extension K_T/k of K/k has $\bar{K}/\bar{k}$ as residual extension. Then, if $\sigma \in G^*_{K/K_T} = G_{K/K_T} \cap G^*$ and $a \in I$ is such that $v(a) = 0$, there exists an $\tilde{a} \in I_T$, where $I_T = I \cap K_T$, such that $v(a - \tilde{a}) > 0$ and $\sigma(a - \tilde{a}) - (a - \tilde{a}) = (\sigma \cdot a - a) - (\sigma \cdot \tilde{a} - \tilde{a}) = \sigma \cdot a - a$. So $v(\sigma; a) = v(\sigma; a - \tilde{a})$, and, as $v(a - \tilde{a}) > 0$ cannot be $= v(\sigma)$. So $G_{K/K_T} \cap G^*$ must be $\varnothing$, and $G_{K/K_T} = \{1_K\}$, $K = K_T$ and K/k is not ramified. But then (see [5]) if $a \in I$ is such that $\tilde{a}$ is primitive in K/k, we have, for every $\sigma \in G^*$, $0 = v(\sigma; a) \geqslant v(\sigma)$ and $v(\delta(a)) = 0 \geqslant v(\delta(K/k))$. As $v(\sigma)$ and $v(\delta(K/k))$ are $\geqslant 0$, we have for every $\sigma \in G^*$, $v(\sigma) = 0$ and $v(\delta(K/k)) = 0$, which proves the theorem.

COROLLARY 1. *If* $a \in I$ *is* ε*-discriminantial, we have* $\sum_{\sigma \in G^*} [v(\sigma; a) - v(\sigma)] \leqslant \varepsilon$(*obvious*).

THEOREM 9. *Always,* $v(\delta(K/k)) \geqslant v(\delta(K/L)\,\delta(L/k))$.

Proof. (Which, practically, is given already in the Zahlbericht [3] of Hilbert, Theorem 39.)

Let I^0 be the valuation ring of L, and K'/k being some normal overextension of K/k, let G, G^0, g be the sets of all isomorphisms of, respectively, K/k, K/L, L/k into K'. If $\bar{\sigma} \in g$, let $G(\bar{\sigma}) = \{\sigma \in G;\ (\sigma \mid L) = \bar{\sigma}\}$ [where $(\sigma \mid L)$ is the restriction of σ to L]. So, in particular, $G^0 = G(1_L)$. If an automorphism σ' of K'/k induces $\bar{\sigma}$ on L, we have obviously (in Bourbaki notation) $\sigma' \circ G^0 = \{\sigma' \circ \sigma;\ \sigma \in G^0\} = G(\bar{\sigma})$. Let $a \in I$ be a primitive element of K/k and let $f_{a/L}(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0 (c_0, c_1, \ldots, c_{n-1} \in L)$ be the minimal polynomial of a over L and $f_{a/k}(X)$ its minimal polynomial over k. We have $f_{a/k}(X) = \prod_{\sigma \in G}(X - \sigma \cdot a) = \prod_{\bar{\sigma} \in g}(\prod_{\sigma \in G(\bar{\sigma})}(X - \sigma \cdot a))$. But $\prod_{\sigma \in G(\bar{\sigma})}(X - \sigma \cdot a) = [\bar{\sigma}] f_{a/L}(X)$, where $[\bar{\sigma}] \cdot f_{a/L}(X) = X^n + (\bar{\sigma} \cdot c_{n-1})\ X^{n-1} + \cdots (\bar{\sigma} \cdot c_0)$. Indeed, let σ' be an automorphism of K'/k prolonging $\bar{\sigma}$. As $\sigma' \circ G^0 = G(\bar{\sigma})$, we have $\prod_{\sigma \in G(\bar{\sigma})}(X - \sigma \cdot a) = \prod_{\sigma \in G^0}(X - (\sigma' \circ \sigma) \cdot a) = \prod_{\sigma \in G^0}(X - \sigma'(\sigma \cdot a)) = X^n + (\sigma' \cdot c_{n-1})\ X^{n-1} + \cdots + (\sigma' \cdot c_0)$, and as $c_0, c_1, \ldots, c_{n-1}$ are $\in L$, we have $\sigma' \cdot c_i = \bar{\sigma} \cdot c_i$ and $\prod_{\sigma \in G(\bar{\sigma})}(X - \sigma \cdot a) = [\bar{\sigma}]\ f_{a/L}(X)$. But then $f'_{a/k}(a) = f'_{a/L}(a) \prod_{\bar{\sigma} \in g,\, \sigma \neq 1_L}([\bar{\sigma}] \cdot f_{a/L})(a)$, so $v(f'_{a/k}(a)) = v(f'_{a/L}(a)) + \sum_{\bar{\sigma} \in g, \bar{\sigma} \neq 1_L} v(([\bar{\sigma}] \cdot f_{a/L})(a))$. But as $f_{a/L}(a) = 0$, we have $[\bar{\sigma}] \cdot f_{a/L})(a) = [\bar{\sigma}] \cdot f_{a/L})(a) - f_{a/L}(a) = ([\bar{\sigma}] \cdot f_{a/L} - f_{a/L})(a)$. But $([\bar{\sigma}] f_{a/L} - f_{a/L})(X) = (X^n + (\bar{\sigma} \cdot c_{n-1})\ X^{n-1} + \cdots (\bar{\sigma} \cdot c_0)) - (X^n + c_{n-1}X^{n-1} + \cdots + c_0) = \sum_{0 \leqslant i \leqslant n-1}(\bar{\sigma} \cdot c_i - c_i)\ X^i$. So, $([\bar{\sigma}] \cdot f_{a/L})(a) = \sum_{0 \leqslant i \leqslant n-1}(\bar{\sigma} \cdot c_i - c_i) \cdot a^i$. As $v(a) \geqslant 0$, we have $v(([\bar{\sigma}] \cdot f_{a/L})(a)) \geqslant \mathrm{Min}_i\, v(\sigma \cdot c_i - c_i)$; so, as all c_i are $\in I^0$, it is $\geqslant v(\bar{\sigma})$ and $v(\prod_{\bar{\sigma} \in g, \bar{\sigma} \neq 1_L}([\bar{\sigma}] \cdot f_{a/L})(a))$ is $\geqslant \sum_{\sigma \in g, \bar{\sigma} \neq 1_L} v(\bar{\sigma}) = v(\delta(L/k))$. Now $v(f'_{a/L}(a))$ is the order of the different $\delta^0(a)$ of a in K/L, so it is $\geqslant v(\delta(L/L))$. So, $v((\delta(a)) \geqslant v(\delta(K/L)) + v(\delta(L/k)) = v(\delta(K/L)\,\delta(L/k))$. But $v(\delta(K/k)) = \mathrm{Inf}_S\{v(\delta(a));\ a \in I\}$. So $v(\delta(K/k))$ is also $\geqslant v(\delta(K/L)\,\delta(L/k))$.

PROPOSITION 13. *Every quasi-dedekindian extension is quasi-hilbertian. If K/k is dedekindian or quasi-dedekindian and not completely flat, it is hilbertian.*

Proof. For every intermediate field L of K/k,

$$v(\Delta(K/k)) = v(\Delta(K/L)) + v(\Delta(L/k))$$

and

$$v(\delta(K/k)) \geqslant v(\delta(K/k)) + v(\delta(L/k)),\ v(\delta(K/L)) \geqslant v(\Delta(K/L))$$

and

$$v(\delta(L/k)) \geqslant v(\Delta(L/k)).$$

We have the same equalities or inequalities for the real values of these semi-real numbers, and they imply that, if $v(\delta(K/k))$ and $v(\Delta(K/k))$ have a same real value, such is also the case for K/L and L/k. If K/k is dedekindian, K/k is non-defective and $v(\Delta(K/k))$, $v(\delta(K/k))$ are both real and equal. If $v(\delta(K/L))$ or $v(\delta(L/k))$ are not real, their real value is, respectively, $\Delta(K/L)$, $\Delta(L/k)$ and at least one has the species $+$. So $v(\delta(K/L)\ \delta(L/k))$ is $v(\Delta(K/L)\ \Delta(L/k))^+ = v(\Delta(K/k))^+ > v(\Delta(K/k)) = v(\delta(K/k))$ contrary to Theorem 9.

If K/k is not completely flat and non-dedekindian (so the valuation of k is dense), $v(\Delta(K/k))$, and one at least of $v(\Delta(K/L))$, $v(\Delta(L/k))$, have the species $+$, and if K/k is quasi-dedekindian, which implies that K/L and L/k are too , $v(\delta(K/k))$, $v(\delta(K/L))$, and $v(\delta(L/k))$ have the same property. So, $v(\delta(K/k)) = v(\Delta(K/k)) = v(\Delta(K/L)\ \Delta(L/k)) = v(\delta(K/L)\ \delta(L/k))$.

The extension $k(a, \Pi)/k$ of Example 1 is not only non-dedekindian but also non-hilbertian (and, even, non-quasi-hilbertian, because the valuation of k is discrete). Indeed, if $L = k(a)$, $L/k = k(a)/k$ is completely flat and has a simple residual extension $\bar{k}(\bar{a})/\bar{k}$ and $K/L = L(\Pi)/L$ is slim, so we have the classical case. So they are both dedekindian, and $\delta(K/k) \neq \Delta(K/k) = \Delta(K/L)\ \Delta(L/k) = \delta(K/L)\ \delta(L/k)$.

The extension $k(a, b)/k$ of Example 2 is non-hilbertian, because, if $L = k(a)$, $L/k = k(a)/k$, and $K/L = L(b)/L$ are both completely flat and have simple residual extensions, then they are dedekindian, but K/k is not.

If K/k is hilbertian or quasi-hilbertian, the Herbrand theory of ramification properties of intermediate extensions holds completely in the case of discrete valuations and for the species of ramification numbers in the case of dense valuations. This theory and its deduction from the preceding theorem are too classical in the case of normal extensions for spending the time and space of this periodical in order to expound it. The results and the deduction in the ramification theory of non-normal extensions are quite similar (see my paper [4]).

LEMMA 6. *If $\sigma \in G^*$, $v(\sigma; a) = v(\sigma)$ implies $v(a) = 0$ if the valuation of k is dense and $v(a) \leqslant \Omega$ if the valuation of k is discrete.*

Proof. The assertion for dense valuations have been proved already. Suppose the valuation is discrete. Let $B = (\bar{b}_1, \bar{b}_2, ..., \bar{b}_f)$ be a basis of $\bar{K}/\bar{k}$ and Π an element of I such, that $v(\Pi) = \Omega$. Let $b_i \in I$ be some element having $\bar{b}_i$ as residue. Let a be an element of I with $v(a) > \Omega$, so $\geqslant 2\Omega$. Then if

$v(a) = i\Omega$, $a = a'\Pi^i$, where $i \geqslant 2$ and $\omega(a') = 0$, so $a' = (\sum \lambda_j b_j) + c$, where $\lambda_j \in i$ and $v(c) > 0$, so $a = (\sum \lambda_j b_j)\,\Pi^I + d$, where $v(d) \geqslant (i+1)\Omega$. If $i\Omega > v(\sigma)$, we have $v(\sigma; a) = v(\sigma \cdot a - a) \geqslant v(a) > v(\sigma)$. Suppose that $i \geqslant 2$ and that it is already proved that if $v(b) \geqslant (i+1)\Omega$, then $v(\sigma; b) > v(\sigma)$. Now $\sigma \cdot a - a = [\sigma \cdot (\sum \lambda_j b_j) - \sum \lambda_j b_j]\,\Pi^i + (\sum (\lambda_j b_j)[(\sigma \cdot \Pi)^i - \Pi^i] + (\sigma, d-d)$. We have $v(\sigma \cdot d - d) > v(\sigma)$, $v(\sigma \cdot (\sum \lambda_j b_j) - \sum \lambda_j b_j) = v(\sum \lambda_i(\sigma \cdot b_j - b_j)) \geqslant \mathrm{Min}_j[\mathrm{V}(\sigma \cdot b_j - b_j)] \geqslant v(\sigma)$, so $v([\sigma \cdot (\sum_j \lambda_j b_j) - \sum_j \lambda_j b_j]\,\Pi^i) > v(\sigma)$ (that holds even for $i = 1$). And $(\sigma \cdot \Pi)^i - \Pi^i = (\sigma \cdot \Pi - \Pi)[(\sigma \cdot \Pi)^{i-1} + (\sigma \cdot \Pi)^{i-2}\,\Pi + \cdots + \Pi^{-1}]$, so $v([\sum_j \lambda_j b_j][(\sigma \cdot \Pi)^i - \Pi^i]) \geqslant v((\sigma \cdot \Pi)^i - \Pi^i) \geqslant v(\sigma \cdot \Pi - \Pi) + (i-1)\Omega > v(\sigma)$. So $v(\sigma; a) > v(\sigma)$, and $v(\sigma; b) > v(\sigma)$ if $v(b) \geqslant i\Omega$. By induction, we prove that $v(\sigma; a) > v(\sigma)$ if $v(a) \geqslant 2\Omega$.

Let K be a valued field, and $r \in \Gamma(K)$. The discs $C(0, r)$ and $C(0, r^-)$ are additive groups and, so is $C_r = C(0, r)/C(0, r^-)$. For any $a \in C_r$, we shall denote by $\bar{\bar{a}}$ its class $a + C(0 \cdot r^-)$ modulo $C(0, r^-)$. We can define on C_r a canonical structure for the $\bar{K}$-module by defining, for every $a \in I$ and $x \in C_r$, $\bar{a}\bar{\bar{x}} = \overline{\overline{ax}}$. This definition is coherent, because $C(0, r)$ is an I-module, and if $\bar{a}' = \bar{a}$ and $\bar{\bar{x}}' = \bar{\bar{x}}$, we have $|a' - a| < 1$, $|x' - x| < r$, so $|a'x' - ax| = |(a' - a)\,x' + a(x' - x)| \leqslant \mathrm{Max}(|a' - a|\,|x'|, |a|\,|x' - x|) < \mathrm{Max}(r1, 1r) = r$, and $ax' - ax \in C(0, r^-)$.

A mapping $\beta: I \to C_r$ will be called a *bar-derivation* if $\beta \cdot (a+b) = \beta \cdot a + \beta \cdot b$ and $\beta \cdot ab = \bar{a}(\beta \cdot b) + \bar{b}(\beta \cdot a)$.

Let K/k again be the same valued extension as before (i.e., k is henselian, $n = [K : k]$ is finite), K'/k its normal algebraic over extension, $\sigma \in G^*$. We assume that $v = v(\sigma)$ is real. Let be $r = e^{-v}$ (so $r > 0$), and let $C'_r = C'(0, r)/C'(0, r^-)$, where $C'(0, \rho)$ is the disc of center 0 and radius ρ in K'. On C'_r we defined a canonical structure of the $\bar{K}'$-module, and also of the $\bar{K}$-module (that is, of vectorial $\bar{K}$-space). Then, if $a \in I$, $v(\sigma \cdot a - a) = v(\sigma; a) \geqslant v$ and $|\sigma \cdot a - a| \leqslant r$, so $\sigma \cdot a - a \in C'(0, r)$. Then, $\beta_v: a \to \beta_v(\sigma; a) = \overline{\overline{\sigma \cdot a - a}}$ is a mapping of I into C'_r. This mapping is, if $v > 0$, a bar-derivation. Indeed, we have $\sigma \cdot (a+b) - (a+b) = (\sigma \cdot a - a) + (\sigma \cdot b - b)$, so $\beta_v(\sigma; a+b) = \beta_v(\sigma; a) + \beta_v(\sigma; b)$. And $\sigma \cdot ab - ab = (\sigma \cdot a)(\sigma \cdot b) - ab = \underline{(\sigma \cdot a - a)(\sigma \cdot b)} + \underline{a(\sigma \cdot b - b)}$, so $\underline{\underline{\beta_v(\sigma; ab)}} = \underline{\underline{(\sigma \cdot a - a)(\sigma \cdot b)}} + \underline{\underline{(\sigma \cdot b - b)}} = \underline{\underline{(\sigma \cdot a - a)(\sigma \cdot b)}} + \underline{\underline{a(\sigma \cdot b - b)}} = \underline{\underline{(\sigma \cdot a - a)(\sigma \cdot b)}} + \bar{a}\underline{\underline{(\sigma \cdot b - b)}} = \overline{\overline{\sigma \cdot a - a}}\,\bar{b} + \bar{a}\underline{\underline{(\sigma \cdot b - b)}} = \bar{a}\beta_v(\sigma; b) + \bar{b}\beta_v(\sigma; a)$, because $v(\sigma \cdot b - b) \geqslant v > 0$ and $\overline{\sigma \cdot b} = \bar{b}$. The elements $a \in K$ such that $\beta_v(\sigma; a) = \bar{\bar{0}}$, i.e., $v(\sigma; a) > v$ will be called *σ-constants*, and their set will be denoted $\mathrm{Cons}(\sigma)$. Obviously, $\mathrm{Cons}(\sigma)$ is a subring of I, which contains its maximal ideal $M = C(0, 1^-)$ if the valuation of k is dense, and $M^2 = C(0, e^{-2\Omega})$ if the valuation of k is discrete. In this last case, there are two possibilities:

(1) $\mathrm{Cons}(\sigma) \supseteq M$, i.e., $v(\sigma \cdot \Pi) > v(\sigma)$. Then $\beta_v(\sigma; a)$ depends only on $\bar{a}$, and $\mathrm{Cons}(\sigma) = \{\bar{a};\, a \in \mathrm{Cons}(\sigma)\}$ is a subring of $\bar{K}$. In fact, it is a subfield of $\bar{K}$, because, if $v(a) = 0$ and $a \in \mathrm{Cons}(\sigma)$, then

$$\beta_v v(\sigma; a^{-1}) = \overline{\overline{(\sigma \cdot a^{-1} - a^{-1})}} = \overline{\overline{a^{-1}(\cdot a)^{-1}(\sigma \cdot a - a)}}$$
$$= \bar{a}^{-1}(\overline{\sigma \cdot a})^{-1}\beta_v(\sigma; a) = \bar{a}^{-1}(\overline{\sigma \cdot a})^{-1}\bar{0} = \bar{0},$$

and $a^{-1} \in \mathrm{Cons}(\sigma)$.

(2) $\mathrm{Cons}(\sigma) \not\supseteq M$. Then, there exists an $\Pi \in I$ such, that $v(\Pi) = \Omega$ and $\beta_v(\sigma; \Pi) \neq \bar{0}$, i.e., $v(\sigma; \Pi) = v(\sigma) = v$. If $a \in I$, we have

$$\beta_v(\sigma; a\Pi) = \bar{a}\beta_v(\sigma; \Pi) + \bar{\Pi}\beta_v(\sigma; a) = \bar{a}\beta_v(\sigma; \Pi).$$

So, if we consider M/M^2 as a $\bar{K}$-module, $\bar{a} \to \beta_v(\sigma; a\Pi)$ is a homomorphism of vectorial $\bar{K}$-spaces, and, in particular, for every Π such that $v(\Pi) = \Omega$, we have $v(\sigma; \Pi) = v(\sigma)$. So $\mathrm{Cons}(\sigma) \cap M = M^2$ and $\mathrm{Cons}(\sigma)/M^2$ is a subfield of I/M^2 isomorphic to $(\mathrm{Cons}(\sigma) + M)/M \subseteq \bar{K}$. When the valuation is dense, the situation is analogous to that of the case (1).

Suppose now, in addition, that K/k is normal. Then, we can take $K' = K$. If we are in the case (2), when a ranges over I, i.e., $\bar{a}$ ranges over $\bar{K}$, $\beta_v(\sigma; a\Pi) = \bar{a}\beta_v(\sigma; \Pi)$ ranges over $\bar{K}\beta_v(\sigma; \Pi) = C_r = C_r'$. So, if $a \in K$ and $v(a) = 0$, there exists some $b \in I$ such that $\beta_v(\sigma; a) = \beta_v(\sigma; b\Pi)$ and $\beta_v(\sigma; a - b\Pi) = \bar{0}$, i.e., $a - b\Pi \in \mathrm{Cons}(\sigma)$. So, $\mathrm{Cons}(\sigma) + M = I$ and I/M^2 is the direct sum $(\mathrm{Cons}(\sigma)/M^2) \oplus (M/M^2)$ of additive groups $\mathrm{Cons}(\sigma)/M^2$ and $M/M^2 = C_\Omega$, where $\mathrm{Cons}(\sigma)/M^2$ is a subfield of I/M^2 canonically (by $u \in \mathrm{Cons}(\sigma)/M^2 \to u + M$) isomorphic to $\bar{K}$.

K/k being any separable normal valued extension of finite degree, and $G = G(K/k)$ being its Galois group, I recall the definitions (due to Deuring [2] and Krull [19]; for analoguous theory for non-normal extensions, see my papers [8–10, 13]) of characteristic groups and ramification numbers of K/k (though I express them in the language of this paper) and some known results of their theory: the *decomposition* group $V_{-2}(K/k) = Z(K/k)$ is the set of all $\sigma \in G_{K/k}$ preserving the valuation $|\cdot\cdot|$, i.e., they are isometries; the *inertia group* is

$$V_{-1}(K/k) = T(K/k) = \{\sigma \in Z(K/k);\ |a| = 1 \Rightarrow |\sigma \cdot a - a| < 1\};$$

the *ramification group* is

$$V_0(K/k) = V(K/k) = \{\sigma \in Z(K/k);\ a \neq 0 \Rightarrow |\sigma \cdot a - a| < |a|\}.$$

As before the *characteristic number* $v(\sigma)$ of $\sigma \in V(K/k)$ is $\mathrm{Inf}_S\{v(\sigma \cdot a - a);\ a \in I\}$, and let $v_0 < v_1 < \cdots v_m < v_{m+1} = +\infty$ be all the values of $v(\sigma)$, $\sigma \in G$, written in increasing order. Then v_q is called the qth *ramification number* (or value) of K/k and $V_q(K/k) = \{\sigma \in V(K/k);\ v(\sigma) \geqslant v_q\}$ is called the qth *ramification* group of K/k. It is easily shown that all $V_q(K/k)$ are groups and V_{q+1} is invariant in V_q. $Z(K/k)/T_{K/k}$ is canonically isomorphic to the

Galois group $G_{\bar{K}/k}$ of $\bar{K}/\bar{k}$, $T_{K/k}/Z_{K/k}$ is isomorphic to the greatest subgroup of $v(K)/v(k)$ of order prime to the residual characteristic p of k, and the exponent of this group must divide that of the group $E(\bar{K})$ of the roots of unity $\in \bar{K}$ (in particular, if the valuation is discrete, $T(K/k)/V(K/k)$ is cyclic of order prime to p). If $v = v_q$ is real, and if there exists an $a \in I$ such that $v(\sigma; a) = v(\sigma)$ for all $\sigma \in V_q(K/k)$, which $\notin V_{q+1}(K/k)$ (if $\delta(K/k)$ is of species 0, i.e., there exist discriminantial elements; every such element a has this property for every q), $\sigma + V_{q+1}(K/k) \to \beta_v(\sigma; a)$, where $V = V_q$, is an isomorphism of $V_q(K/k)/V_{q+1}(K/k)$ onto the set $A_q(K/k; a) = \{\beta_v(\sigma; a); \sigma \in V_q(K/k)\}$ which is an additive subgroup of C_r, where $r = e^{-v}$. Indeed, if σ, σ' are $\in V_q(K/k)$ we have $\beta_v(\sigma\sigma'; a) = \overline{\overline{(\sigma\sigma' \cdot a - a)}} = \overline{\overline{\sigma \cdot (\sigma' \cdot a - a) + (\sigma \cdot a - a)}} = \overline{\overline{\sigma \cdot (\sigma' \cdot a - a)}} + \overline{\overline{(\sigma \cdot a - a)}}$. But, as $\alpha \in V_{K/k}$, we have, if $b = \sigma' \cdot a - a$, $|\sigma \cdot b - b| < |b|$ and $\overline{\overline{(\sigma \cdot b)}} = \bar{b}$. So $\beta_v(\sigma\sigma'; a) = \overline{\overline{(\sigma \cdot a - a)}} + \overline{\overline{(\sigma' \cdot a - a)}} = \beta_v(\sigma; a) + \beta_v(\sigma'; a)$. So $\sigma \to \beta_v(\sigma; a)$ is a homomorphism of $V_q(K/k)$ onto $A_q(K/k; a)$ with addition as composition. So $A_q(K/k; a)$ must be an additive group. Obviously, the kernel of this homomorphism is $V_{q+1}(K/k)$.

Suppose now, in addition, that k is henselian and its valuation is discrete. Clearly, $v(\delta(K/k))$ is real, and there exist such elements $a \in I$. But we can, in this case, if $q > 0$ (so $v_q > 0$), interpolate, in general, between V_q and V_{q+1} some other group $V'_q = V'_q(K/k)$. This group is $\{\sigma \in V_q(K/k); \mathrm{Cons}(\sigma) \supseteq M\}$. Indeed, V'_q is a group, because if $\mathrm{Cons}(\sigma) \supseteq M$, and $\mathrm{Cons}(\sigma') \supseteq M$, i.e., $\beta_v(\sigma; \Pi) = \beta_v(\sigma'; \Pi) = \bar{0}$ for some $\Pi \in I$ such, that $v(\Pi) = \Omega$, we have $\beta_v(\sigma\sigma'; \Pi) = \bar{0}$. Clearly $\beta_v : \sigma \to \beta_v(\sigma; \Pi)$ is an homomorphism of V_q onto $A_q(K/k; \Pi)$, but the kernel is now V'_q. So $V_q/V'_q \simeq (A_q(K/k); \Pi), +)$ and if $A'(K/k; a) = \{\beta_v(\sigma; a); \sigma \in V'_q/K/k)\}$ we have $V'_q/V_{q+1} \simeq (A'(K/k; a), +)$. Let us denote as n_q, n'_q the orders of $V_q(K/k)$, $V'_q(K/k)$, $t_q = n_q/n_q + 1$, $t'_q = n_q/n'_q$, $t''_q = n'_q/n_{q+1}$.

If, for $\sigma \in V_q$, d_σ is the bar-derivation $x \to \beta_v(\sigma; x)$ (where x ranges over I and $v = v_q$) we have clearly $d_{\sigma\sigma'} = d_\sigma + d_{\sigma'}$. So, $V_q V_{q+1}$ can be also represented as an additive group of bar-derivations (which can be also considered as derivations from I/M^2 to C_r, $r = e^{-v}$).

As, in Lemma 2, let $\tilde{K}$ be the completion of the valued field K, and $\tilde{k}$ the closure of k in $\tilde{K}$. When K/k is normal, $\tilde{K}/\tilde{k}$ is too. $A/\sigma \in G_{K/k}$ can be prolonged by continuity to $\tilde{K}$ iff it is an isometry, i.e., belongs to $Z(K/k)$, and this prolongation $\tilde{\sigma}$ is an automorphism of $\tilde{K}/\tilde{k}$. The mapping $\sigma \to \tilde{\sigma}$ is an isomorphy of $Z(K/k)$ onto $G(\tilde{K}/\tilde{k})$ and if we identify σ with $\tilde{\sigma}$, $Z(K/k)$ is identified with $G(\tilde{K}/\tilde{k})$, each $V_q(K/k)$ is identified with $V_q(\tilde{K}/\tilde{k})$, the $v_q(K/k)$ and $v_q(\tilde{K}/\tilde{k})$ are the same, etc.

As $\tilde{k}$ is henselian, all results that we considered hold for $\tilde{K}/\tilde{k}$, so also, if K/k is normal, for K/k. If K/k is not normal, the results for $\tilde{K}/\tilde{k}$ hold for K/k only partially (see my papers [4, 7]). If k is not henselian, $\Delta(\tilde{K}/\tilde{k})$ and

$\delta(\tilde{K}/\tilde{k})$ are called *local* algebraic and arithmetic differents of K/k, which explains the title of this paper.

References

1. Z. Borevitch and S. Shafarevitch, "Theory of Numbers," Edit. of phys. math. lith., Moscow, 1963. [Russian]; there are also french and english translations).
2. M. Deuring, Verzweigungstheorie bewerteter Körper, *Math. Ann.* **105** (1931), 277–305.
3. D. Hilbert, Bericht über die Theorie der algebraischen Zahlen ("Zahlbericht"), *Jahresber. Deutsch. Math-Verein.* **4** (1894–1895), 175–546.
4. M. Krasner, "Théorie de la ramification des idéaux des corps non-galoisiens de nombres algébriques," thèse de doctorat, *Acad. Roy. Belg. Cl. Sci.* **11**, No. 4 (1937), 1–110.
5. M. Krasner, Sur la primitivité des corps p-adiques, *Mathematica* (Cluj) **13** (1937), 72–191; reedited in "Eleftheria," Vol. 3, Athens, 1980.
6. M. Krasner, Espaces ultramétriques et nombres semi-réels, *Comptes Rendus* **219** (1944), 433–435.
7. M. Krasner, "Théorie de la ramification dans les extensions finies des corps valués: (I) hypergroupe de décomposition," Vol. 219, pp. 539–541, 1944.
8. M. Krasner, "(II) hypergroupes d'inertie et de ramification; théorie extrinsèque de la ramification," Vol. 220, pp. 28–30, 1945.
9. M. Krasner, "(III) différente et discriminant, théorie intrinsèque de la ramification," Vol. 220, pp. 761–763, 1945.
10. M. Krasner, Quelques méthodes nouvelles dans la théorie des corps valués complètes, Algèbre et théorie des nombres (Colloque Int. du CNRS n° 24, Paris 1949), Édit. du CNRS, Paris 1950.
11, 12. M. Krasner, Théorie de corps valués (Séminaire M. Krasner 1953–1954); Exposé n° 1, Espaces ultramétriques et hyperultrametriques; Exposé n° 4, Congruences multiplicatives. Corpoïdes et Squelettes, Vol. 1, Sécretariat Mathématiques de la Fac. des Sci. de Paris, 1954.
13. M. Krasner, Théorie de Galois des corpoïdes commutatifs sans torsion et ses applications à la théorie de la ramification des extensions algébriques des corps valués, preprint de l'Univ. de Paris VI, 1979.