



HAL
open science

KEY POLYNOMIALS, SEPARATE AND IMMEDIATE VALUATIONS, AND SIMPLE EXTENSIONS OF VALUED FIELDS

Gérard Leloup

► **To cite this version:**

Gérard Leloup. KEY POLYNOMIALS, SEPARATE AND IMMEDIATE VALUATIONS, AND SIMPLE EXTENSIONS OF VALUED FIELDS. 2022. hal-01876056v3

HAL Id: hal-01876056

<https://hal.science/hal-01876056v3>

Preprint submitted on 16 May 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

KEY POLYNOMIALS, SEPARATE AND IMMEDIATE VALUATIONS, AND SIMPLE EXTENSIONS OF VALUED FIELDS

GÉRARD LELOUP

ABSTRACT. We give a first-order definition of key polynomials, we show the links with previous definitions, that it is relevant to study key degrees, and to use a kind of valuations that we call partially multiplicative. We also prove or reprove several properties.

We have changed definitions from the first version of this paper, in order to make them consistent with those of other papers. Some computational and tedious proofs have been omitted in this new version. The reader can find them in versions 1 and 2 of this paper.

Valuations occur in different areas of mathematics, for example in algebraic geometry. In particular, some authors studied the extension of a valuation ν , defined on a field K , to $K[\chi]$. For this purpose, they construct K -module valuations which converges to ν . These K -module valuations are defined using polynomials which are called key polynomials. For his part, the author of the present article has studied the first order properties of extensions of valued fields. In this context, vs defectless extensions, immediate extensions and the initial segments $\nu(l - K)$ ($l \notin K$) play an important role. Now, there are similarities between these two types of studies. We found interesting to revisit the key polynomials and the associated valuations in the light of another background. The approach of the present paper relies on euclidean division of polynomials, bases of vector spaces or modules, and the notions of vs defectless and immediate extensions (Definitions 1.1 and 1.4). Indeed, vs defectless (or separate) and immediate extensions play a crucial role in the study of the first-order theory of extensions of valued fields ([2], [3], [6], [7], [11], [12]).

Let (K, ν) be a valued field and χ be algebraic or transcendental over K . Key polynomials were introduced to approximate an extension of ν to the field $K(\chi)$ by K -module valuations. In particular, this study uses K -module valuations such that there exists a monic polynomial Φ of degree d such that the family (Φ^n) ($n \geq 0$) is separated over the K -module $K_{d-1}[\chi]$ of polynomials of degree at most $d - 1$ (they are also called augmented valuations or truncated mappings). Here we denote them by ν_Φ . In the case where χ is algebraic over K , these K -module valuations cannot be valuations of fields since they do not satisfy the rule $\nu(fg) = \nu(f) + \nu(g)$. However, they can satisfy this rule if $\deg(f) + \deg(g) < [K(\chi) : K]$. If this holds, then we call them pm valuations. In fact, ν_Φ is a pm valuation if Φ is what we call here a weak key polynomial (in short w key polynomial). These w key polynomials are related to the key polynomials defined by MacLane (we show that Φ being a w key polynomial for ν is equivalent to being a MacLane key polynomial for ν_Φ), but we do not require to define families of w key polynomials by induction.

In order to construct families of pm valuations which approximate ν on $K(\chi)$, we can restrict to a subfamily of w key polynomials whose definition differs slightly. We call them key polynomials, because we prove that these polynomials are the key polynomials defined in [17], [5] and [16] (in [5] they are called abstract key polynomials). Here, we do not restrict to transcendental extensions and we give a characterization of key polynomials by means of first order formulas (in the language of valued fields together with a predicate interpreted by the generator of the simple extension).

We classify the key polynomials according to their degrees, that we call key degrees. On the one hand, key degrees d such that the set $\nu(\chi^d - K_{d-1}[\chi])$ has a greatest element, on the other hand key degrees d such that the set $\nu(\chi^d - K_{d-1}[\chi])$ has a no greatest element. This already appeared in the works of S. MacLane and of M. Vaquié. They construct the key polynomials by induction,

Date: May 16, 2022.

2010 Mathematics Subject Classification. 12J10, 12J20, 12F99.

Key words and phrases. simple extension, valuation, key polynomial.

starting from the degree 1 key polynomials, and two cases arise: the set $\nu(\chi^d - K_{d-1}[\chi])$ having or not a greatest element. We will show that in the first case we have a vs defectless subextension, which is generated by a valuation independent element, and in the last one this subextension is immediate. So in the first case we say that d is an independent key degree, and in the latter case we say that it is an immediate key degree. In the construction of key polynomials by induction on the degree, some authors introduced the definition of limit key polynomials. In fact, a key polynomial is a limit key polynomial if, and only if, the preceding key degree is an immediate one.

In the present paper we do not require the reader having any previous knowledge of key polynomials. As much as possible, we try to use only elementary properties of valuations. However, we use the graded algebra associated to a valuation in two proofs. Indeed, these graded algebras are a good tool for providing nice proofs of some properties of vs defectless extensions. With exception of Section 5, this paper is self-contained.

General properties.

A *valuation* on a field K is a morphism ν from the multiplicative group (K^*, \cdot) to an abelian linearly ordered group $(\nu K, +)$ called the *valuation group*, which enjoys an additional property. We add an element ∞ to νK ($\infty > \nu K$), we set $\nu(0) := \infty$, and we assume that $\nu(x + y) \geq \min(\nu(x), \nu(y))$, for every x, y in K . It follows that if $\nu(x) \neq \nu(y)$, then $\nu(x + y) = \min(\nu(x), \nu(y))$. If $\nu(x) = \nu(y)$, then $\nu(x + y)$ can be arbitrarily large. The set $\{x \in K \mid \nu(x) \geq 0\}$ is a local domain and $\{x \in K \mid \nu(x) > 0\}$ is its maximal ideal, they are called respectively the *valuation ring* and the *maximal ideal* of the valued field. The quotient of the valuation ring by the maximal ideal is a field which is denoted by K_ν , and is called the *residue field* of the valued field. The *residue characteristic* of (K, ν) is the characteristic of K_ν . We have $\text{char } K_\nu = 0 \Rightarrow \text{char } K = 0$. For x in the valuation ring of (K, ν) , its class modulo the maximal ideal will be denoted by x_ν . For every subset M of K we denote by $\nu(M)$, or νM , the set $\{\nu(x) \mid x \in M\} \setminus \{\infty\}$.

We assume that ν is a finite rank valuation (the *rank* of ν is the number of proper convex subgroups of νK), so that νK has countable cofinality. If the rank is 1, then νK embeds in the ordered group $(\mathbb{R}, +)$; we also say that ν is *archimedean*.

An extension $(L|K, \nu)$ of valued fields consists in an extension $L|K$ of fields, where L is equipped with a valuation ν . If $L|K$ is a field extension and ν is a valuation on K , then there is a least one extension of ν to L .

Assume that M is a K -module (where K is a field). A mapping ν from M to a linearly ordered group together with an element ∞ will be called a *K -module valuation*, if for every y_1, y_2 in M and $x \in K$: $\nu(y_1) = \infty \Leftrightarrow y_1 = 0$, $\nu(y_1 + y_2) \geq \min(\nu(y_1), \nu(y_2))$, $\nu(xy_1) = \nu(x) + \nu(y_1)$ (see. [10]). It follows that its restriction to K is a valuation of field.

Now, let $(K(\chi)|K, \nu)$ be a simple extension of valued fields. If there is no confusion, then for every polynomial $f(\chi)$ of $K[\chi]$ we write f instead of $f(\chi)$. Let ν_i be a K -module valuation on $K[\chi]$ such that $\forall f \in K[\chi] \nu_i(f) \leq \nu(f)$. Assume that χ is algebraic (so that $K(\chi) = K[\chi]$), and that there exists $f \in K[\chi]$ such that $\nu_i(f) < \nu(f)$. By hypothesis, we have $\nu_i(1/f) \leq \nu(1/f)$. Hence $\nu_i(f) < \nu(f) = -\nu(1/f) \leq -\nu_i(1/f)$. So $\nu_i(1/f) \neq -\nu_i(f)$. It follows that ν_i doesn't satisfy the rule $\nu_i(fg) = \nu_i(f) + \nu_i(g)$. Now, we will prove in Proposition 2.8 that, in some cases, if $\deg(f) + \deg(g) < [K[\chi]:K]$, then $\nu_i(fg) = \nu_i(f) + \nu_i(g)$. This motivates the following definitions.

Let ν be a K -module valuation. We say that ν is *partially multiplicative*, or a *pm valuation*, if for every f, g in $K[\chi]$ such that $\deg(f) + \deg(g) < [K[\chi]:K]$ we have $\nu(fg) = \nu(f) + \nu(g)$. In the case where $[K[\chi]:K] = \infty$ (i.e. χ is transcendental), we assume in addition that $g \neq 0$ implies $\nu(f/g) = \nu(f) - \nu(g)$, that is, ν is a field valuation in the usual sense. If ν is a field valuation (in the usual sense), then we will also say that it is *multiplicative*.

Summary of the paper.

In Section 1 we generalize the definitions of immediate and dense extensions to extensions of modules, equipped with K -module valuations. We also review definitions and properties of separated sequences and vs defectless extensions. Then we focus on the case of simple extensions. We characterize immediate simple extensions by the condition that the sets $\nu(\chi^n - K_{n-1}[\chi])$ have no greatest elements (Proposition 1.9), and we characterize vs defectless simple extensions by the

condition that the sets $\nu(\chi^n - K_{n-1}[\chi])$ have greatest element (Proposition 1.15). Then we recall definitions and properties of the graded algebras associated to valuations. In particular, we note that in the case of a generalized power series field, this graded algebra is isomorphic to the ring of generalized polynomials. Furthermore, we prove that a family is separated if, and only if, its image in the graded algebra is linearly independent (Proposition 1.16). In Section 2 we characterize w key polynomials, key polynomials and key degrees. In particular, we note that if Φ is an irreducible polynomial, then it is a w key polynomial if, and only if, the quotient field $K[\chi]/(\Phi)$ is a valued field. We define the vs defectless K -module valuations ν_ϕ . We deduce other characterizations of w key polynomials. These characterizations will be used in latter sections. In Section 3 we compare the definition of w key polynomials with the definition of S. MacLane and M. Vaquié (Proposition 2.12). We set properties of key degrees in Section 4. We show that in the case where $\nu(\chi^d - K_{d-1}[\chi])$ has a maximum, we only need to look at monic polynomials with maximal valuations. We characterize key degrees, that we call valational, by means of the value group (Proposition 4.3). We also focus on conditions for existing only a finite number of key degrees, since this makes simpler the constructions of families of pm valuations which approximate ν . We look at the case of a dense key degree, that is immediate key degrees d such that $\nu(\chi^d - K_{d-1}[\chi])$ is equal to $\nu(K[\chi]) \setminus \{\infty\}$ (Proposition 4.8). We also give characterizations of the successor of a given key degree (Theorems 4.9 and 4.10). These characterizations will be useful for proving the equivalence of our definition and the definition of abstract key polynomials. In Subsection 4.4 we give a construction of a family of pm valuations which approximate ν (defined by a family of key polynomials), without proceeding by induction on the degree (Theorem 4.12). In Section 5 we show that the key polynomials defined in [17], [5] and [16] are the same as the key polynomials defined here (Corollaries 5.3 and 5.5).

Before starting, let us set some notations. Let $l \in L$ and M be a K -submodule of L . We denote by $\nu(l - M)$ the subset $\{\nu(l - x) \mid x \in M\} \setminus \{\infty\}$ of νL . For any polynomial f , we denote by $\nu(f(M))$, or $\nu f(M)$, the subset $\{\nu(f(x)) \mid x \in M\} \setminus \{\infty\}$.

Note that $\nu(l - M) \cap \nu M$ is an initial segment of νM .

1. IMMEDIATE AND VS DEFECTLESS EXTENSIONS

In order to show the importance of vs defectless and immediate extensions of valued fields as well of the initial segments $\nu(l - K)$, we start by stating some results of model theory of extensions of valued fields. A valued field (K, ν) is said to be *algebraically maximal* if no extension of ν to an algebraic extension of K is immediate. If the residue characteristic is 0, then being algebraically maximal is equivalent to being *henselian*, i.e. ν having a unique extension to any algebraic extension of K . A famous theorem of J. Ax, S. Kochen and Y. Ershov ([1]) says that the elementary theory of a henselian valued field (K, ν) of residue characteristic 0 is determined by the elementary theory of its residue field and the elementary theory of its value group. Next, this result was extended to other families of algebraically maximal valued fields. The aim is to get similar results in the case of extensions of valued fields. Now, in [7] F. Delon proved that given a theory T_F of fields of characteristic 0 and a theory T_V of non trivial linearly ordered abelian groups, the theory of immediate henselian extensions $(L|K, \nu)$, where K_ν is a model of T_F and νK is a model of T_V , is undecidable and admits 2^{\aleph_0} completions. This theory also depends at least on the family of all initial segments $\nu(l - K)$, with $l \in L \setminus K$. Now, if K, L are henselian, $\text{char} K_\nu = 0$, and $(L|K, \nu)$ is vs defectless, then the first-order theory of the extension is determined by the theories of the residual extension and of the extension of valued groups. The same holds if $(L|K, \nu)$ is an extension of algebraically maximal Kaplansky fields or of real-closed fields (see [2], [3], [11], [12]). Furthermore, we have similar results with dense extensions. In the case where $(L|K, \nu)$ is an extension of valued fields of residue characteristic 0, there exists a henselian subfield H , $K \subseteq H \subseteq L$, such that $(H|K, \nu)$ is vs defectless and $(L|H, \nu)$ is immediate (see [6]). This shows that it can be interesting to focus on vs defectless and immediate extensions.

In this section, $L|K$ is an extension of fields and ν is a K -module valuation on L .

1.1. Immediate extensions. If M is a K -module, then we assume that νM has no greatest element. This holds if νK is not trivial. Indeed, for every $x \in K$ with $\nu(x) > 0$ and $y \in M$, we have $xy \in M$ and $\nu(xy) = \nu(x) + \nu(y) > \nu(y)$.

Definitions 1.1. Let $M \subseteq N$ be K -submodules of L , and $l \in L$.

We say that l is *pseudo-limit* over (M, ν) if $\nu(l - M) \subseteq \nu M$, and $\nu(l - M)$ has no maximal element.

We say that l is *limit* over (M, ν) if $\nu(l - M) = \nu M$.

The extension $(N|M, \nu)$ is said to be *immediate* if every element of N is pseudo-limit over (M, ν) .

The extension $(N|M, \nu)$ is said to be *dense* if every element of N is limit over M .

It follows that if $(N|M, \nu)$ is dense, then it is immediate.

The proof of the following is left to the reader (see for example [13]).

Let $l \in L$ and M be a K -submodule of L . The element l is pseudo-limit over (M, ν) if, and only if, for every $x \in M$ there exists $y \in M$ such that $\nu(l - y) > \nu(l - x)$.

Notations 1.2. For γ in νL and M a K -submodule of L , let $M_{\gamma, \nu}$ be the K_ν -module $\{x \in M \mid \nu(x) \geq \gamma\} / \{x \in M \mid \nu(x) > \gamma\}$. In the case where $\gamma = 0$, we often write M_ν instead of $M_{0, \nu}$. For $f \in M$ with $\nu(f) \geq \gamma$, we denote by $f_{\gamma, \nu}$ the class of f modulo $\{g \in M \mid \nu(g) > \gamma\}$.

Remark 1.3. .

1) $(N|M, \nu)$ is immediate if, and only if, $\nu N = \nu M$ and, for every $\gamma \in \nu M$, $N_{\gamma, \nu} = M_{\gamma, \nu}$.

2) $(N|K, \nu)$ is immediate if, and only if, $\nu N = \nu K$ and $N_\nu = K_\nu$.

Proof. Left to the reader (see for example [13]). □

1.2. Vs defectless extensions.

Definitions 1.4. ([2], [3], [4]). Let M be a K -submodule of L .

1) A sequence (l_1, \dots, l_n) of L is said to be *separated over M* (or ν -separated if necessary) if for every x_1, \dots, x_n in M , we have: $\nu(x_1 l_1 + \dots + x_n l_n) = \min_{1 \leq i \leq n} \nu(x_i l_i)$. If $M = K$, then we say separated instead of separated over K . An infinite sequence is called *separated* if every finite subsequence is separated.

2) The extension $(L|K, \nu)$ is said to be *vs defectless* if every finitely generated K -submodule of L admits a basis which is separated over K . If this holds, then we say that ν is *vs defectless* (or *vs defectless over K*).

Note that if (l_1, \dots, l_n) is separated, then l_1, \dots, l_n are linearly independent over K .

In [2] and [3] Baur introduces the terms separated families and separated extensions. The authors of [4] noted that the word separated can bring confusion in algebraic geometry (for example with separable extension). So they prefer use the terms valuation independent sets and vs defectless extensions. Following these authors we use the term vs defectless extension instead of separated extension. Concerning Baur's separated families, there is a slight difference with the definition of valuation independent families. A valuation independent set is separated, but if B is valuation independent, then $B \cup \{1\}$ remains separated.

Example 1.5. Let (K, ν) be a valued field. Pick some x in K , some γ in an extension of νK , and, for every x_0, x_1, \dots, x_n in K , set $\nu'(x_n(\chi - x)^n + \dots + x_1(\chi - x) + x_0) := \min(\nu(x_n) + n\gamma, \dots, \nu(x_1) + \gamma, \nu(x_0))$. Then one can check that ν' defines a pm valuation on the ring $K[\chi]$. The pm valuation ν' is vs defectless and $1, (\chi - x), \dots, (\chi - x)^n, \dots$ is a separated basis of $(K[\chi], \nu')$.

Note that if ν'' is another K -module valuation on $K[\chi]$ which extends ν and such that $\nu(\chi - x) = \gamma$, then, for every f in $K[\chi]$, $\nu'(f) \leq \nu''(f)$.

The following properties provide other examples of vs defectless extensions.

- If (K, ν) is a maximal valued field, then every multiplicative extension of (K, ν) is vs defectless ([2, Lemma 3]).
- Assume that ν is multiplicative on L , that the residue characteristic of (K, ν) is 0 and that (K, ν) is *henselian* that is, ν admits a unique extension to every algebraic extension of K . Then any algebraic extension of (K, ν) is vs defectless ([6, Corollaire 7]).

• Assume that L is a finite algebraic extension of K . Then $(L|K, \nu)$ is vs defectless if, and only if, the K -module L admits a separated basis. This is an immediate consequence of the following lemma.

Lemma 1.6. ([6, Lemma 5]). *Let $M \subseteq N$ be two K -submodules of L such that M is finitely generated and N admits a separated basis. Then M admits a separated basis.*

The remainder of this subsection is dedicated to properties which make clear the difference between immediate and vs defectless extensions.

Assume that ν is multiplicative on L and that (K, ν) is henselian of residue characteristic 0. Then $(L|K, \nu)$ is vs defectless if, and only if, L is linearly disjoint over K from every immediate extension of (K, ν) ([6, p. 421]).

Theorem 1.7. ([6, p. 421], [4]) *Let N be a K -submodule of L . Then, $(N|K, \nu)$ is a vs defectless extension if, and only if, for every finitely generated K -submodule M of N and $l \in N \setminus M$, the set $\nu(l - M)$ has a maximal element.*

This theorem has been stated in [6, p. 421], assuming that (K, ν) is henselian and $\text{char}(K_\nu) = 0$. A general proof has been given independently in [4] and [13].

We know that if $L|K$ is finite and ν is multiplicative, then $1 \leq [L_\nu : K_\nu](\nu L : \nu K) \leq [L : K]$. Furthermore, by Remark 1.3, $(L|K, \nu)$ is immediate if, and only if, $1 = [L_\nu : K_\nu](\nu L : \nu K)$. The following theorem shows that $(L|K, \nu)$ being vs defectless can be seen as the opposite case. It has been proved independently in [4] and [13].

Theorem 1.8. *Assume that $L|K$ is a finite algebraic extension of fields and that ν is multiplicative on L . Then $(L|K, \nu)$ is vs defectless if, and only if, $[L : K] = [L_\nu : K_\nu](\nu L : \nu K)$.*

Let $(L|K, \nu)$ be a finite extension of valued fields (where ν is multiplicative). We say that $(L|K, \nu)$ is *defectless* if $\frac{[L : K]}{[L_\nu : K_\nu](\nu L : \nu K)}$ is equal to the number of extensions of $\nu|_K$ to L .

As a corollary of Theorem 1.8 we get that if (K, ν) is henselian, then every defectless finite algebraic extension of (K, ν) is vs defectless.

1.3. Extensions generated by one element. In this subsection χ is algebraic or transcendental over K . Recall that if d is a non-negative integer, then $K_d[\chi]$ denotes the K -module of polynomials of degree at most d . Note that $K_0[\chi] = K$ and in the transcendental case we let $K_\infty[\chi] = K[\chi]$.

Proposition 1.9. *Let $d < d'$ in $\mathbb{N} \cup \{\infty\}$ such that if χ is algebraic over K , then $d' < [K[\chi] : K]$.*

1) *$(K_{d'}[\chi]|K_d[\chi], \nu)$ is immediate if, and only if, for every integer $n \in \{d + 1, \dots, d'\}$, $\nu(\chi^n - K_{n-1}[\chi])$ has no maximal element.*

2) *Assume that ν is a pm valuation and that $\nu K_d[\chi]$ is a subgroup of $\nu(K[\chi])$. Then the extension $(K_{d'}[\chi]|K_d[\chi], \nu)$ is dense if, and only if, for every integer $n \in \{d + 1, \dots, d'\}$, $\nu(\chi^n - K_{n-1}[\chi]) = \nu K_d[\chi]$.*

Proof. 1) \Rightarrow . Assume that, for some integer $n \in \{d + 1, \dots, d'\}$, $\nu(\chi^n - K_{n-1}[\chi])$ has a greatest element $\nu(f)$. If $\nu(f)$ is not in $\nu K_d[\chi]$, then $\nu K_{d'}[\chi] \neq \nu K_d[\chi]$, and, by Remark 1.3 1), the extension is not immediate. Suppose that $\nu(f) \in \nu K_d[\chi]$, say $\nu(f) = \gamma$. For every $g \in K_d[\chi]$ we have $\nu(f - g) \leq \nu(f)$, hence $f_{\gamma, \nu} \neq g_{\gamma, \nu}$. It follows that $(K_{d'}[\chi])_{\gamma, \nu} \neq (K_d[\chi])_{\gamma, \nu}$, so the extension is not immediate.

\Leftarrow . Assume that $(K_{d'}[\chi]|K_d[\chi], \nu)$ is not immediate, and let n be the smallest integer such that, for some polynomial f of degree n , either $\nu(f) \notin \nu K_d[\chi]$ or, for every $g \in K_d[\chi]$, $f_{\gamma, \nu} \neq g_{\gamma, \nu}$, where $\gamma = \nu(f)$. Note that, by dividing f by an element of K , we can assume that f is a monic polynomial of degree n .

First assume that $\gamma \notin \nu K_d[\chi]$, and let g be a monic polynomial of degree n . Then $\deg(f - g) < n$, hence, by minimality of n , $\nu(f - g) \in \nu K_d[\chi]$. So $\nu(f - g) \neq \nu(f)$. It follows: $\nu(g) = \min(\nu(g - f), \nu(f)) \leq \nu(f)$, which proves that $\nu(f)$ is the greatest element of $\nu(\chi^n - K_{n-1}[\chi])$.

Assume that $\gamma = \nu(f) \in \nu K_d[\chi]$, and, for every $g \in K_d[\chi]$, $f_{\gamma, \nu} \neq g_{\gamma, \nu}$. Let g be a monic polynomial of degree n . If $\nu(g - f) \neq \gamma$, then $\nu(g) = \min(\nu(g - f), \nu(f)) \leq \nu(f)$. Now, assume that $\nu(g - f) = \gamma$. We have $\deg(f - g) < n$, hence, by minimality of n , $(g - f)_{\gamma, \nu} = h_{\gamma, \nu}$ for some

$h \in K_d[\chi]$. Therefore we have $f_{\gamma,\nu} \neq (g-f)_{\gamma,\nu}$. So $\nu(g) = \nu(g-f+f) = \min(\nu(g-f), \nu(f)) \leq \nu(f)$. Consequently, $\nu(f)$ is the greatest element of $\nu(\chi^n - K_{n-1}[\chi])$.

2) If $(K_d[\chi]|K_d[\chi], \nu)$ is dense, then it is immediate. Hence for every integer $n \in \{d+1, \dots, d'\}$ we have: $\nu(\chi^n - K_{n-1}[\chi]) \subseteq \nu K_d[\chi]$. Furthermore: $\nu(\chi^{d+1} - K_d[\chi]) = \nu K_d[\chi]$. Now, for every integer $n \in \{d+2, \dots, d'\}$ we have $\nu(\chi^n - K_{n-1}[\chi]) \supseteq \nu(\chi^n - \chi^{n-(d+1)} K_d[\chi]) = (n - (d+1))\nu(\chi) + \nu(\chi^{d+1} - K_d[\chi]) = \nu K_d[\chi]$ (since $\nu K_d[\chi]$ is a subgroup). It follows: $\nu(\chi^n - K_{n-1}[\chi]) = \nu K_d[\chi]$.

Conversely, assume that for every integer $n \in \{d+1, \dots, d'\}$ we have $\nu(\chi^n - K_{n-1}[\chi]) = \nu K_d[\chi]$. Then in particular it has no greatest element. So by a) $(K_d[\chi]|K_d[\chi], \nu)$ is immediate. Let $f \in K_d[\chi]$, n be its degree and x_n be the coefficient of χ^n in f . Without loss of generality we can assume that the integer n belongs to $\{d+1, \dots, d'\}$. We show that for every $\gamma \in \nu K_d[\chi]$ there is $g \in K_d[\chi]$ such that $\nu(f-g) > \gamma$. For every $g_{n-1} \in K_{n-1}[\chi]$ we have $f/x_n - g/x_n \in \chi^n - K_{n-1}[\chi]$. Hence since $\nu(\chi^n - K_{n-1}[\chi]) = \nu K_d[\chi]$ which is a subgroup, we can choose $g_{n-1} \in K_{n-1}[\chi]$ such that $\nu((f/x_n) - (g_{n-1}/x_n)) > \gamma - \nu(x_n)$. Hence $\nu(f - g_{n-1}) > \gamma$. In the same way, for $d \leq j \leq n-2$ we get $g_j \in K_j[\chi]$ such that $\nu(g_{j+1} - g_j) > \gamma$. Therefore $\nu(f - g_d) = \nu(f - g_{n-1} + \dots + g_{d+1} - g_d) \geq \min(\nu(f - g_{n-1}), \dots, \nu(g_{d+1} - g_d)) > \gamma$. So every element of $K_d[\chi]$ is limit over $K_d[\chi]$. This implies that $(K_d[\chi]|K_d[\chi], \nu)$ is dense. \square

We turn to vs defectless extensions, and we start with properties of separated sequences.

Lemma 1.10. ([3, p. 676]) *Let (l_1, \dots, l_n) be a separated sequence of elements of L , y in $L \setminus \{0\}$ and k_1, \dots, k_n in $K \setminus \{0\}$. The following holds.*

Every subsequence of (l_1, \dots, l_n) is separated.

The sequence $(k_1 l_1, \dots, k_n l_n)$ is separated.

If ν is multiplicative on L , then the sequence $(y l_1, \dots, y l_n)$ is separated.

Lemma 1.11. ([2], [3, (S4), p. 676]) *Let (l_1, \dots, l_n) be a sequence of elements of L such that: $\forall i, 1 \leq i \leq n, \nu(l_i) = 0$. Then (l_1, \dots, l_n) is separated if, and only if, $(l_1)_\nu, \dots, (l_n)_\nu$ are linearly independent over K_ν . This can be generalized in the following way. If $\nu(l_1) = \dots = \nu(l_n) = g$, then (l_1, \dots, l_n) is separated if, and only if, for every x_1, \dots, x_n in $\{x \in K \mid \nu(x) = 0\} \cup \{0\}$, either $\nu(x_1 l_1 + \dots + x_n l_n) = g$ or $x_1 = \dots = x_n = 0$.*

Proposition 1.12. *Let $l_{i1}, \dots, l_{in_i}, 1 \leq i \leq p$, be sequences which satisfy:*

$$\forall i, 1 \leq i \leq p, \forall j, 1 \leq j \leq n_i, \nu(l_{ij}) = \nu(l_{i1}) < \infty$$

and the $\nu(l_{i1})$ are pairwise non-congruent modulo νK . The following assertions are equivalent.

The sequence $l_{11}, \dots, l_{1n_1}, l_{21}, \dots, l_{2n_2}, \dots, l_{p1}, \dots, l_{pn_p}$ is separated.

For every i in $\{1, \dots, p\}$, $l_{i1}, l_{i2}, \dots, l_{in_i}$ is separated.

If ν is multiplicative on L then this condition is equivalent to:

for every i in $\{1, \dots, p\}$, $1, (l_{i2} l_{i1}^{-1})_\nu, \dots, (l_{in_i} l_{i1}^{-1})_\nu$ are linearly independent over K_ν .

Proof. Assume that the sequence is separated. Then by Lemma 1.10, for $1 \leq i \leq p$, the sequence $l_{i1}, l_{i2}, \dots, l_{in_i}$ is separated.

Conversely, let $x_{11}, \dots, x_{1n_1}, x_{21}, \dots, x_{2n_2}, \dots, x_{p1}, \dots, x_{pn_p}$ in K . For $1 \leq i \leq p$, set $y_i = x_{i1} l_{i1} + \dots + x_{in_i} l_{in_i}$. Since l_{i1}, \dots, l_{in_i} is separated, we have: $\nu(y_i) = \min\{\nu(x_{ij}) + \nu(l_{ij}) \mid 1 \leq j \leq n_i\}$. Therefore, the $\nu(y_i)$'s are pairwise non-congruent modulo νK . In particular, they are pairwise distinct, and $\nu(y_1 + \dots + y_p) = \min\{\nu(y_i) \mid 1 \leq i \leq p\}$. This proves that the sequence $l_{11}, \dots, l_{1n_1}, l_{21}, \dots, l_{2n_2}, \dots, l_{p1}, \dots, l_{pn_p}$ is separated.

If ν is multiplicative on L , then

$$l_{i1}, l_{i2}, \dots, l_{in_i} \text{ is separated if, and only if, } 1, (l_{i2} l_{i1}^{-1}), \dots, (l_{in_i} l_{i1}^{-1}) \text{ is separated.}$$

By Lemma 1.11, this in turn is equivalent to $1, (l_{i2} l_{i1}^{-1})_\nu, \dots, (l_{in_i} l_{i1}^{-1})_\nu$ are linearly independent over K_ν . \square

Lemma 1.13. *Assume that $(L|K, \nu)$ is vs defectless. Let M be a finite K -submodule of L and $l \in L \setminus M$. Then every separated basis of M extends to a separated basis of the K -submodule generated by M and l .*

Proof. The proof is left to the reader (see for example [13]). \square

Proposition 1.14. *Let $d \in \mathbb{N} \cup \{\infty\}$ such that $0 < d$ and if χ is algebraic over K , then $d < [K[\chi]:K]$. Then $(K_d[\chi]|K, \nu)$ is vs defectless if, and only if, the K -module $K_d[\chi]$ admits a separated basis. Furthermore, we can assume that every polynomial of this basis is monic and that the mapping $f \mapsto \deg(f)$, from this basis onto \mathbb{N} , is one-to-one.*

Assume that χ is transcendental over K , and that ν is multiplicative on $K(\chi)$. Then $(K(\chi)|K, \nu)$ is vs defectless if, and only if, the K -module $K[\chi]$ admits a separated basis. (\Rightarrow holds even if ν is not multiplicative).

Proof. Assume that $(K_d[\chi]|K, \nu)$ is vs defectless. By Lemma 1.13, the separated basis 1 of K extends to a separated basis of the module generated by 1 and χ . Necessarily, the second element of this basis has degree 1. Let $n \geq 1$ and assume that the K -module $K_n[\chi]$ of polynomials of degree at most n has a separated basis of $(n+1)$ elements of respective degrees $0, 1, \dots, n$. By Lemma 1.13, this separated basis can be completed in a separated basis of $K_{n+1}[\chi]$, and the degree of the new element is $n+1$. So we get the required separated basis by induction. By Lemma 1.10 we can assume that every polynomial of this basis is monic.

Conversely, assume that $K_d[\chi]$ contains a separated basis, and let M be a finitely generated K -submodule. By Lemma 1.6, M has a separated basis. Hence $(K(\chi)|K, \nu)$ is vs defectless.

We turn to the case where χ is transcendental over K . It follows from the definition (Definition 1.4 2)) that if $(K(\chi)|K, \nu)$ is vs defectless, then so is $(K[\chi]|K, \nu)$. Now we assume that $(K[\chi]|K, \nu)$ is vs defectless and that ν is multiplicative on $K(\chi)$. Let M be a finitely generated submodule of $K(\chi)$. Then there is a polynomial $f \neq 0$ such that $f \cdot M \subseteq K[\chi]$. We take a separated basis of $f \cdot M$, and we divide all its elements by f so that, since ν is multiplicative, by Lemma 1.10, we get a separated basis of M . \square

We state a refinement of Theorem 1.7, which characterizes vs defectless extensions by means of initial segments. This proposition completes Proposition 1.9.

Proposition 1.15. *Let $d \in \mathbb{N} \cup \{\infty\}$ such that $0 < d$ and if χ is algebraic over K , then $d < [K[\chi]:K]$. The extension $(K_d[\chi]|K, \nu)$ is vs defectless if, and only if, for every integer n , $1 \leq n \leq d$, $\nu(\chi^n - K_{n-1}[\chi])$ has a maximal element.*

Assume that χ is transcendental over K , and that ν is multiplicative on $K(\chi)$. Then $(K(\chi)|K, \nu)$ is vs defectless if, and only if, for every $n \in \mathbb{N} \setminus \{0\}$, $\nu(\chi^n - K_{n-1}[\chi])$ has a maximal element.

Proof. In both equivalences, \Rightarrow follows from Theorem 1.7. In order to prove the converse, we construct by induction a separated basis such that the mapping $f \mapsto \deg(f)$ is one-to-one. Then, by Proposition 1.14, $(K_d[\chi]|K, \nu)$ is vs defectless. The case where χ is transcendental also follows from Proposition 1.14. Trivially, 1 is a separated basis of $K_0[\chi] = K$. Assume that we have a separated basis (f_0, \dots, f_{n-1}) of $K_{n-1}[\chi]$. Let f_n be a monic polynomial such that $\nu(f_n) = \max(\nu(\chi^n - K_{n-1}[\chi]))$. Since the degree of f_n is n , $(f_0, \dots, f_{n-1}, f_n)$ is a basis of $K_n[\chi]$. Let $f := x_n f_n + \dots + x_0 f_0$ in $K_n[\chi]$. If $x_n = 0$, then by induction hypothesis $\nu(f) = \min_{0 \leq i \leq n-1} \nu(x_i f_i) = \min_{0 \leq i \leq n} \nu(x_i f_i)$.

Now we assume: $x_n \neq 0$. Since $\nu(f_n)$ is maximal, we have $\nu\left(\frac{f}{x_n}\right) \leq \nu(f_n)$. If $\nu\left(\frac{f}{x_n} - f_n\right) <$

$\nu(f_n)$, then $\nu\left(\frac{f}{x_n} - f_n\right) = \nu\left(\frac{f}{x_n}\right)$. So:

$$\begin{aligned} \nu(f) &= \nu(x_n) + \nu\left(\frac{f}{x_n}\right) = \nu(x_n) + \nu\left(\frac{f}{x_n} - f_n\right) = \nu(x_n) + \nu\left(\frac{x_{n-1}f_{n-1}}{x_n} + \dots + \frac{x_0 f_0}{x_n}\right) = \\ &= \nu(x_n) + \min_{0 \leq i \leq n-1} \nu\left(\frac{x_i f_i}{x_n}\right) = \min_{0 \leq i \leq n-1} \nu(x_i f_i) = \min_{0 \leq i \leq n} \nu(x_i f_i). \end{aligned}$$

If $\nu\left(\frac{f}{x_n} - f_n\right) \geq \nu(f_n)$, then $\min_{0 \leq i \leq n-1} \nu(x_i f_i) \geq \nu(x_n f_n) \geq \nu(f) \geq \min_{0 \leq i \leq n} \nu(x_i f_i)$.

Therefore: $\nu(f) = \min_{0 \leq i \leq n} \nu(x_i f_i)$. \square

1.4. Graded algebra associated to a valuation. In the proofs of Proposition 4.7 and Theorem 4.10 we will introduce the graded algebra associated to a valuation. Now, we review some observations.

Let (K, ν) be a valued field. Recall that, for every $\gamma \in \nu K$, $K_{\gamma, \nu}$ denotes the K_ν -module $\{x \in K \mid \nu(x) \geq \gamma\} / \{x \in K \mid \nu(x) > \gamma\}$. Now, let $G_\nu(K)$ be the graded algebra $G_\nu(K) = \bigoplus_{\gamma \in \nu K} K_{\gamma, \nu}$.

In the case where K is the valued field $k((\Gamma))$ of generalized formal power series with coefficients in a field k and exponents in a linearly ordered abelian group Γ :

$$k((\Gamma)) = \left\{ \sum_{\gamma \in \Lambda} x_\gamma X^\gamma \mid \Lambda \text{ is a well-ordered subset of } \Gamma, \text{ and } \forall \gamma \in \Lambda \ x_\gamma \in k \right\},$$

then $G_\nu(K)$ is isomorphic to the ring of generalized polynomials $k[\Gamma]$, the subring of all elements of $k((\Gamma))$ with finite support. Note that if $k_1|k_0$ is an extension of fields and $\Gamma_1|\Gamma_0$ is an extension of groups, then $k_1[\Gamma_1]$ is a $k_0[\Gamma_0]$ -module. Its dimension is finite if, and only if, both of $[k_1:k_0]$ and $(\Gamma_1:\Gamma_0)$ are finite. If this holds, then this dimension is $[k_1:k_0](\Gamma_1:\Gamma_0)$.

More generally, let $\gamma \in \nu K$ and pick an element x_0 of valuation γ . Then the mapping $x_{\nu(x), \nu} \mapsto (xx_0^{-1})_\nu$ induces a K_ν -module isomorphism between $\{x \in K \mid \nu(x) \geq \gamma\} / \{x \in K \mid \nu(x) > \gamma\}$ and K_ν . Hence, the K_ν -module $G_\nu(K)$ is isomorphic to the K_ν -module $K_\nu[\nu K]$ of polynomials with coefficients in K_ν and exponents in νK . If K contains a lifting of νK , then we can assume that these graded algebras are isomorphic. In particular, if $\nu K = \mathbb{Z}$, then they are isomorphic. If (K', ν') is an \aleph_1 -saturated elementary extension of (K, ν) , then it contains a lifting of its value group (see [9]). Hence $G_{\nu'}(K')$ is isomorphic to the ring of polynomials $K'_\nu[\nu'K']$. Therefore every graded algebra $G_\nu(K)$ embeds in a ring of polynomials. If (K, ν) contains a lifting K_0 of its residue field and a lifting Γ of νK , then it contains the algebra $K_0[\Gamma]$, which is isomorphic to $G_\nu(K)$. Now, if (K, ν) is henselian and $\text{char}(K_\nu) = 0$, then we know that it admits a lifting of K_ν . It follows that every valued field (K, ν) of residue characteristic 0 admits an extension (K', ν') which contains a subalgebra which is isomorphic to $G_\nu(K)$. Furthermore, (K', ν') embeds in the power series field $K'_0((\nu'K'))$ equipped with the canonical valuation.

For every $x \in K$, let $in_\nu(x) := x_{\nu(x), \nu}$ be the image of x in $K_{\nu(x), \nu}$, which is also its image

in $G_\nu(K)$. In the case of a subfield of a power series field, we have $in_\nu \left(\sum_{\gamma \in \Lambda} x_\gamma X^\gamma \right) = x_{\gamma_0} X^{\gamma_0}$,

where γ_0 is the smallest element of the *support* of the series (i.e. the well ordered subset Λ of νK such that $x_{\gamma_0} \neq 0$). In general, for every x, y in K , we have $in_\nu(x)in_\nu(y) = in_\nu(xy)$. Assume that $\nu(x) = \nu(y)$. If $in_\nu(x) = -in_\nu(y)$, then $\nu(x+y) > \nu(x)$ and $\nu(x+y)$ can be arbitrarily large, so we have $in_\nu(x+y) = 0$. Otherwise, $in_\nu(x+y) = in_\nu(x) + in_\nu(y)$.

An element of $G_\nu(K)$ is called *homogeneous* if it belongs to $\bigcup_{\gamma \in \nu K} K_{\gamma, \nu}$. In the case of a polynomial ring, this is equivalent to being a monomial. One can see that the invertible elements of $G_\nu(K)$ are the homogeneous ones.

For further purposes, if M is a K -submodule of L , we denote by $G_\nu(M)$ the additive group

$$\bigoplus_{\gamma \in \nu M} M_{\gamma, \nu}.$$

By Remark 1.3, an extension of valued fields $(L|K, \nu)$ is immediate if, and only if, $G_\nu(L) = G_\nu(K)$.

Now we turn to the vs defectless case.

Proposition 1.16. *Let $(L|K, \nu)$ be an extension of valued fields, and l_1, \dots, l_n in L . The family (l_1, \dots, l_n) is separated over (K, ν) if, and only if, $in_\nu(l_1), \dots, in_\nu(l_n)$ are linearly independent over $G_\nu(K)$.*

If (l_1, \dots, l_n) is a maximal separated family, then $(in_\nu(l_1), \dots, in_\nu(l_n))$ is a basis of $G_\nu(L)$.

Assume that $L|K$ is finite. Then $(L|K, \nu)$ is vs defectless if, and only if, $G_\nu(L)$ is a $G_\nu(K)$ -module of dimension $[L:K]$.

Proof. Recall that the family (l_1, \dots, l_n) is separated over (K, ν) if, and only if, for every x_1, \dots, x_n in K , $\nu(x_1 l_1 + \dots + x_n l_n) = \min(\nu(x_1 l_1), \dots, \nu(x_n l_n))$. Now, this equivalent to saying that for every x_1, \dots, x_n in K with $\nu(x_1 l_1) = \dots = \nu(x_n l_n)$, we have $\nu(x_1 l_1 + \dots + x_n l_n) = \nu(x_1 l_1)$. This last equality is equivalent to $in_\nu(x_1)in_\nu(l_1) + \dots + in_\nu(x_n)in_\nu(l_n) \neq 0$. So, if $in_\nu(l_1), \dots, in_\nu(l_n)$ are linearly independent in the $G_\nu(K)$ -module $G_\nu(L)$, then the family (l_1, \dots, l_n) is separated. Now, assume that for every x_1, \dots, x_n in K with $\nu(x_1 l_1) = \dots = \nu(x_n l_n)$, we have $\nu(x_1 l_1 + \dots + x_n l_n) = \nu(x_1 l_1)$. Let y_1, \dots, y_n in $G_\nu(K)$. Every y_j can be written as a finite sum of homogeneous elements: $y_j = in_\nu(x_{j,1}) + \dots + in_\nu(x_{j,i_j})$. It follows that $y_1 in_\nu(l_1) + \dots + y_n in_\nu(l_n)$ can be written as a sum of $in_\nu(x_{1,k_1})in_\nu(l_1) + \dots + in_\nu(x_{n,k_n})in_\nu(l_n)$'s, where the non-zero $in_\nu(x_{j,k_j})in_\nu(l_j)$ have the same valuation. Therefore, $y_1 in_\nu(l_1) + \dots + y_n in_\nu(l_n) \neq 0$. Consequently, the family (l_1, \dots, l_n) is separated over (K, ν) if, and only if, $in_\nu(l_1), \dots, in_\nu(l_n)$ are linearly independent over $G_\nu(K)$. Furthermore, if (l_1, \dots, l_n) is a maximal separated family, then $(in_\nu(l_1), \dots, in_\nu(l_n))$ is a basis of $G_\nu(L)$. Now, if $[L:K]$ is finite, then the dimension of the $G_\nu(K)$ -module $G_\nu(L)$ is $[L_\nu:K_\nu](\nu L:\nu K)$. Hence, by Theorem 1.8, $(L|K, \nu)$ is vs defectless if, and only if, $G_\nu(L)$ is a $G_\nu(K)$ -module of dimension $[L:K]$. \square

The following lemma shows that if, for $l \in L$, $in_\nu(l)$ satisfies a relation of algebraic dependence over $G_\nu(K)$, then we can define its irreducible polynomial.

Lemma 1.17. *Let $(L|K, \nu)$ be an extension of valued fields, and $l \in L$. Assume that $in_\nu(l)$ satisfies a relation of algebraic dependence over $G_\nu(K)$, and let n be the smallest degree such that $in_\nu(l)$ satisfies a relation of algebraic dependence of degree n . Then, $in_\nu(l)$ satisfies a relation of the form $in_\nu(l)^n + in_\nu(x_{n-1})in_\nu(l)^{n-1} + \dots + in_\nu(x_0) = 0$, where x_0, \dots, x_{n-1} belong to K and $\nu(x_0) = \dots = \nu(x_{n-1}l^{n-1}) = \nu(l^n)$.*

Proof. See for example [8]. \square

2. KEY POLYNOMIALS

In this section, χ is algebraic or transcendental over the field K and ν is a K -module valuation on $K(\chi)$.

2.1. Definitions.

Notation 2.1. Let Φ be a monic polynomial of degree $d \geq 1$. For f, g in $K_{d-1}[\chi]$, we will denote by $q_\Phi(f, g)$ and $r_\Phi(f, g)$ respectively (in short $q(f, g)$ and $r(f, g)$) the quotient and the remainder of the euclidean division of fg by Φ . In other words, $q(f, g)$ and $r(f, g)$ belong to $K_{d-1}[\chi]$ and $fg = \Phi \cdot q(f, g) + r(f, g)$.

Definitions 2.2. Let Φ be a monic polynomial of degree $d \geq 1$.

We say that Φ is a *weak key polynomial* for ν (or a *w key polynomial* for ν) if, for every f, g in $K_{d-1}[\chi]$ with $\deg(f) + \deg(g) < [K[\chi]:K]$, we have $\nu(fg) = \nu(r(f, g))$.

We say that Φ is a *key polynomial* for ν if, for every f, g in $K_{d-1}[\chi]$ with $\deg(f) + \deg(g) < [K[\chi]:K]$, we have $\nu(fg) = \nu(r(f, g)) < \nu(q(f, g) \cdot \Phi)$.

Let d be a positive integer.

We say that d is a *key degree* of $(K(\chi)|K, \nu)$ if there exists a key polynomial of degree d .

Assume that d is a key degree. If $\nu(\chi^d - K_{d-1}[\chi])$ has no maximal element, then we say that d is an *immediate* key degree. Otherwise, we say that d is an *independent* key degree. If this maximum does not belong to $\nu K_{d-1}[\chi]$, then we say that d is a *valuational* key degree. If this maximum belongs to $\nu K_{d-1}[\chi]$, then we say that d is a *residual* key degree.

Let d be a key degree. Then, by Proposition 1.9, d is an immediate key degree if, and only if, the extension $(K_d[\chi]|K_{d-1}[\chi], \nu)$ is immediate and by Proposition 1.15, d is a vs defectless key degree if, and only if, the extension $(K_d[\chi]|K_{d-1}[\chi], \nu)$ is vs defectless. However, we prefer to say that these degrees are independent because this word is easier to pronounce than vs defectless. We will see after Lemma 2.4 that this makes sense.

Proposition 2.3. *1) The integer 1 is a key degree. Furthermore, every monic polynomial of degree 1 is a key polynomial.*

- 2) Every w key polynomial is irreducible.
 3) If ν is partially multiplicative and Φ is a w key polynomial (resp. a key polynomial) for ν of degree d , then, for every pm valuation ν' such that the restriction of ν' to $K_{d-1}[\chi]$ is equal to the restriction of ν and $\nu'(\Phi) \geq \nu(\Phi)$, Φ is a w key polynomial (resp. a key polynomial) for ν' .
 4) Assume that ν is partially multiplicative. If Φ is a w key polynomial, then $\nu(\Phi) \geq \{\nu(r(f, g)) - \nu(q(f, g)) \mid f \in K_{d-1}[\chi], g \in K_{d-1}[\chi], \deg(f) + \deg(g) < [K[\chi]:K]\}$. If Φ is a monic polynomial, then Φ is a key polynomial if, and only if, $\nu(\Phi) > \{\nu(r(f, g)) - \nu(q(f, g)) \mid f \in K_{d-1}[\chi], g \in K_{d-1}[\chi], \deg(f) + \deg(g) < [K[\chi]:K]\}$.

Proof. 1) and 3) are trivial.

2) Assume that there exist two polynomials f, g in $K_{d-1}[\chi]$ such that $fg = \Phi$, then $r(f, g) = 0$, and $\nu(r(f, g)) = \infty > \nu(fg)$. Hence Φ is not a w key polynomial for ν .

4) Clearly, if Φ is a w key polynomial (resp. a key polynomial), then $\nu(\Phi) \geq \{\nu(r(f, g)) - \nu(q(f, g)) \mid f \in K_{d-1}[\chi], g \in K_{d-1}[\chi], \deg(f) + \deg(g) < [K[\chi]:K]\}$ (resp. $\nu(\Phi) > \{\nu(r(f, g)) - \nu(q(f, g)) \mid f \in K_{d-1}[\chi], g \in K_{d-1}[\chi], \deg(f) + \deg(g) < [K[\chi]:K]\}$). Now, if $\nu(\Phi) > \nu(r(f, g)) - \nu(q(f, g))$, then $\nu(q(f, g)\Phi) > \nu(r(f, g)) = \nu(fg - q(f, g)\Phi)$. Hence $\nu(r(f, g)) = \nu(fg)$. \square

The following lemma explains the distinction that we make between the valuational and the residual key degrees.

Lemma 2.4. *Let d be a positive integer and Φ be a monic polynomial of degree d . Then $\nu(\Phi)$ is the maximum of $\nu(\chi^d - K_{d-1}[\chi])$ if, and only if, either $\nu(\Phi) \notin \nu K_{d-1}[\chi]$, or $\Phi_{\nu(\Phi), \nu} \notin (K_{d-1}[\chi])_{\nu(\Phi), \nu}$.*

Proof. Assume that $\nu(\Phi)$ is the maximum of $\nu(\chi^d - K_{d-1}[\chi])$ and $\nu(\Phi) \in \nu K_{d-1}[\chi]$. Then, for every $f \in K_{d-1}[\chi]$ such that $\nu(f) = \nu(\Phi)$ we have $\nu(\Phi - f) = \nu(\Phi) = \nu(f)$. Hence $(\Phi)_{\nu(\Phi), \nu} \neq f_{\nu(\Phi), \nu}$. It follows that $\Phi_{\nu(\Phi), \nu} \notin (K_{d-1}[\chi])_{\nu(\Phi), \nu}$. Conversely, assume that $\nu(\Phi) \notin \nu K_{d-1}[\chi]$, or $\Phi_{\nu(\Phi), \nu} \notin (K_{d-1}[\chi])_{\nu(\Phi), \nu}$. Then for every $g \in K_{d-1}[\chi]$ we have $\nu(\Phi - g) = \min(\nu(\Phi), \nu(g)) \leq \nu(\Phi)$. Hence $\nu(\Phi)$ is the maximum of $\nu(\chi^d - K_{d-1}[\chi])$. \square

It follows that if $(K_d[\chi]|K_{d-1}[\chi], \nu)$ is vs defectless, then any monic polynomial Φ , such that $\nu(\Phi)$ is the maximum of $\nu(\chi^d - K_{d-1}[\chi])$, is valuation independent over $K_{d-1}[\chi]$ (i.e. for every $g \in K_{d-1}[\chi]$ we have $\nu(\Phi + g) = \min(\nu(\Phi), \nu(g))$). So the word independent key degree makes sense.

Let Φ be a monic irreducible polynomial of $K[X]$ of degree $d \geq 1$ ($K[X]$, the ring of formal polynomials with coefficients in K). Then $K[X]/(\Phi)$ is a field, such that the canonical epimorphism $\rho : K[X] \rightarrow K[X]/(\Phi)$ is an isomorphism from the K -module $K_{d-1}[X]$ onto the K -module $K[X]/(\Phi)$. Now, for f, g in $K_{d-1}[X]$, we set $f * g := r(f, g)$. Then $\rho(f * g) = \rho(r(f, g)) = \rho(fg)$. Hence $(K_{d-1}[X], +, *)$ is a field which is isomorphic to $K[X]/(\Phi)$. The same operation can be defined in $K[\chi]$ whenever $d \leq [K(\chi):K]/2$. The field $(K_{d-1}[\chi], +, *)$ will be denoted by K_Φ . Note that if ν is a pm valuation on the field $K(\chi)$, then its restriction to $K_{d-1}[\chi]$ induces a valuation of the K -modules K_Φ and $K[X]/(\Phi)$. If \mathcal{Y} is a root of $\Phi(X)$ in some algebraic extension, then the fields K_Φ and $K[\mathcal{Y}]$ are isomorphic.

Proposition 2.5. *Let Φ be an irreducible monic polynomial of degree d , $1 \leq d \leq [K(\chi):K]/2$, and assume that ν is a pm valuation on $K(\chi)$. Then Φ is a w key polynomial for ν if, and only if, the valued K -module (K_Φ, ν) is a valued field.*

Proof. Let f, g in $K_{d-1}[\chi]$. Then $\nu(f * g) = \nu(r(f, g))$ and $\nu(fg) = \nu(f) + \nu(g)$. Hence (K_Φ, ν) is a valued field if, and only if, for every f, g in $K_{d-1}[\chi]$ we have: $\nu(r(f, g)) = \nu(fg)$. This in turn is equivalent to saying that Φ is a w key polynomial. \square

Corollary 2.6. *Assume that ν is a pm valuation on $K(\chi)$ and let Φ be a w key polynomial of degree d , $1 \leq d \leq [K(\chi):K]/2$. Then $\nu K_{d-1}[\chi]$ is a subgroup of $\nu K(\chi)$.*

Proof. Indeed, if Φ is a w key polynomial, then by Proposition 2.5 $\nu K_{d-1}[\chi] = \nu K_\Phi$ is a subgroup of $\nu K(\chi)$. \square

Remark 2.7. Let Φ be a monic polynomial of degree d , $1 \leq d \leq [K(\chi):K]/2$, and assume that ν is a pm valuation on $K(\chi)$.

1) The polynomial Φ is a key polynomial if, and only if, for every f, g in $K_{d-1}[\chi]$, $\nu(fg) = \nu(r_\Phi(f, g))$ and $(fg)_{\nu(fg), \nu} = (r_\Phi(f, g))_{\nu(fg), \nu}$. Indeed, if $\nu(fg) = \nu(r_\Phi(f, g))$, then $\nu(fg - r_\Phi(f, g)) > \nu(fg)$ is equivalent to $(fg)_{\nu(fg), \nu} = (r_\Phi(f, g))_{\nu(fg), \nu}$.

2) If Φ is a key polynomial, then the group $G_\nu(K_{d-1}[\chi])$ is a subalgebra of $G_\nu(K(\chi))$. Indeed, if Φ is irreducible, then the group $G_\nu(K_{d-1}[\chi])$ is isomorphic to the group $G_\nu(K_\Phi)$. Since $(fg)_{\nu(fg), \nu} = f_{\nu(f), \nu} g_{\nu(g), \nu}$, Φ is a key polynomial if, and only if, for every f, g in $K_{d-1}[\chi]$, $(f * g)_{\nu(fg), \nu} = f_{\nu(f), \nu} g_{\nu(g), \nu}$. Therefore, the group $G_\nu(K_\Phi)$ is a subalgebra of $G_\nu(K(\chi))$.

3) It follows from 1) and Proposition 2.5 that if Φ is a key polynomial, then $K_{d-1}[\chi]_\nu$ is a subfield of $K(\chi)_\nu$.

2.2. Pseudo-valuations. In [19], χ is transcendental over K and ν is a valuation or a pseudo-valuation. A *pseudo-valuation* ν of $K[\chi]$ is a mapping from $K[\chi]$ onto a linearly ordered group $\nu(K[\chi])$ together with an element ∞ which shares the properties of multiplicative valuations except $\nu(f) = \infty \Rightarrow f = 0$. In this case the set $I := \{f \in K[\chi] \mid \nu(f) = \infty\}$ is a prime ideal of $K[\chi]$. Then ν induces a pm valuation on the integral domain $K[\chi]/I$. So, the case of algebraic extensions is obtained by means of a pseudo-valuation, by considering the quotient of $K[\chi]$ by the ideal $I := \{f \in K[\chi] : \nu(f) = \infty\}$.

Let Π be the monic polynomial which generates I . Since I is prime, Π is irreducible. If Φ is another irreducible polynomial, then Φ and Π are coprime. Hence there exist polynomials a and b in $K[\chi]$ such that $\deg(a) < \deg(\Phi)$, $\deg(b) < \deg(\Pi)$ and $a\Pi - b\Phi = 1$. Then $a\Pi = b\Phi + 1$, with $\nu(a\Pi) = \infty$, hence $\nu(b\Phi) = \nu(1) = 0 < \nu(a\Pi)$. It follows that if $\deg(\Pi) < \deg(\Phi)$, then Φ is not a w key polynomial. Now, Π satisfies the properties of Definitions 2.2, but since the aim is to study the quotient $K[\chi]/I$, we can restrict to polynomial of degrees less than $\deg(\Pi)$.

We generalize Definitions 2.2 to the case where ν is a pseudo-valuation by adding the hypothesis that $d = \deg(\Pi) < \deg(\Phi)$. In the case where ν is a pseudo-valuation, we also assume that χ is transcendental. The restriction of ν to $K_{d-1}[\chi]$ is a valuation, hence Proposition 2.3 remains true. In Lemma 2.4 we can also assume that ν is a pseudo-valuation by adding the condition $\nu(\Phi) < \infty$. The same holds for the other properties of Subsection 2.1, we only require that $d < \deg(\Pi)$.

More generally, all properties of Section 2 remain true with pseudo-valuations. Then we assume that the degrees are bounded by $\deg(\Pi) - 1$. In general, we replace $d < [K[\chi]:K]$ by $d < \deg(\Pi)$.

2.3. Vs defectless valuations defined by key polynomials. Assume that Φ is a monic irreducible polynomial of degree d , and let γ be an element of an extension of $\nu K(\chi)$.

For every $f := f_0 + f_1\Phi + \dots + f_m\Phi^m$ in $K[\chi]$ (with f_0, f_1, \dots, f_m in $K_{d-1}[\chi]$ and $\deg(f_m) + dm < [K[\chi]:K]$), set $\nu'(f) = \min_{0 \leq i \leq m} \nu(f_i) + i\gamma$.

Assume that ν is a pm valuation on $K(\chi)$ and that Φ is a w key polynomial for ν of degree d . We saw in Proposition 2.3 4) that the set $\{\nu(r(f, g)) - \nu(q(f, g)) \mid f \in K_{d-1}[\chi], g \in K_{d-1}[\chi], \deg(f) + \deg(g) < [K[\chi]:K]\}$ is bounded above by $\nu(\Phi)$. We extend the addition of elements of νK to the addition of Dedekind cuts in the usual way.

Proposition 2.8. *Let Φ be a monic irreducible polynomial of degree d , γ be an element of an extension of $\nu K(\chi)$, and ν' be defined as above.*

1) *The application ν' is a K -module valuation and the family (Φ^m) ($dm < [K[\chi]:K]$) is separated over $K_{d-1}[\chi]$.*

2) *Assume that ν is a pm valuation and that Φ is a w key polynomial for ν . Denote by β the upper-bound of the set $\{\nu(r(f, g)) - \nu(q(f, g)) \mid f \in K_{d-1}[\chi], g \in K_{d-1}[\chi], \deg(f) + \deg(g) < [K[\chi]:K]\}$ in a Dedekind completion of νK , and assume that $\gamma \geq \beta$.*

a) *For every $f = f_m\Phi^m + \dots + f_1\Phi + f_0$, $g = g_m\Phi^m + \dots + g_1\Phi + g_0$, with $f_0, \dots, f_m, g_0, \dots, g_m$ in $K_{d-1}[\chi]$ such that $\deg(f) + \deg(g) < [K[\chi]:K]$ we have:*

$$\nu'(fg) = \nu' \left(\sum_{j=0}^{2m} \left(\sum_{i=0}^j r(f_i, g_{j-i}) \right) \Phi^j \right) \leq \nu' \left(fg - \sum_{j=0}^{2m} \left(\sum_{i=0}^j r(f_i, g_{j-i}) \right) \Phi^j \right) - (\gamma - \beta).$$

(Here if $i > m$, then we let $f_i = g_i = 0$.) In particular, ν' is a pm valuation.

b) *The polynomial Φ is a w key polynomial such that the sequence (Φ^m) ($md < [K(\chi):K]$) is*

ν' -separated over $K_{d-1}[\chi]$. Furthermore it is a key polynomial if, and only if, $\gamma > \beta$ or β is not a maximum.

Proof. The proof is left to the reader (see for example [13]). \square

Notations 2.9. The K -module valuation ν' defined in Proposition 2.8 will be denoted by $\nu_{\Phi, \gamma}$. We set $\nu_{\Phi} = \nu_{\Phi, \nu(\Phi)}$. If Φ_1 and Φ_2 are irreducible polynomials such that $\deg(\Phi_1) < \deg(\Phi_2)$, then we denote by ν_{Φ_1, Φ_2} the K -module valuation $(\nu_{\Phi_1, \nu(\Phi_1)})_{\Phi_2, \nu(\Phi_2)}$. By induction, for every irreducible polynomials Φ_1, \dots, Φ_n , with $\deg(\Phi_1) < \dots < \deg(\Phi_n)$, we define the K -module valuation $\nu_{\Phi_1, \dots, \Phi_n}$.

These valuations ν_{Φ} generalize the augmented valuations of S. MacLane ([14] and [15]).

If the degree of Φ is 1, then for every f, g in $K_{d-1}[\chi] = K$, we have $q(f, g) = 0$. Hence the set $\{\nu(r(f, g)) - \nu(q(f, g)) \mid f \in K_{d-1}[\chi], g \in K_{d-1}[\chi], \deg(f) + \deg(g) < [K[\chi] : K]\}$ is equal to $\{-\infty\}$ and is bounded above by any element. Hence Proposition 2.8 proves the fact that the valuations defined in Example 1.5 are pm valuations.

Proposition 2.10. *Let Φ be a monic polynomial of degree $d < [K(\chi) : K]$ and assume that ν is a pm valuation on $K[\chi]$. Then Φ is a w key polynomial for ν if, and only if, there exists a pm valuation ν' of $K[\chi]$, such that its restriction to $K_{d-1}[\chi]$ is equal to the restriction of ν , and $\nu'(\Phi) > \nu(\Phi)$.*

If this holds, then for every $\gamma \geq \nu(\Phi)$ in an extension of $\nu K[\chi]$, $\nu_{\Phi, \gamma}$ is a pm valuation of $K[\chi]$ such that its restriction to $K_{d-1}[\chi]$ is equal to the restriction of ν , $\nu_{\Phi, \gamma}(\Phi) = \gamma$ and Φ is a w key polynomial for $\nu_{\Phi, \gamma}$ such that the sequence (Φ^m) ($md < [K(\chi) : K]$) is separated over $K_{d-1}[\chi]$.

Proof. Assume that ν' is a pm valuation of $K[\chi]$ such that its restriction to $K_{d-1}[\chi]$ is equal to the restriction of ν , and $\nu'(\Phi) > \nu(\Phi)$. Let f, g in $K_{d-1}[\chi]$ such that $\deg(f) + \deg(g) < [K[\chi] : K]$, $q = q(f, g)$ and $r = r(f, g)$. Without loss of generality we can assume that $q \neq 0$. We have $\nu(fg) = \nu(f) + \nu(g) = \nu'(f) + \nu'(g) = \nu'(fg)$. Therefore, $\nu(q\Phi + r) = \nu'(q\Phi + r)$ is greater or equal to both of $\min(\nu(q\Phi), \nu(r))$ and $\min(\nu'(q\Phi), \nu'(r))$, where $\nu(q\Phi) = \nu(q) + \nu(\Phi) < \nu'(q) + \nu'(\Phi) = \nu'(q\Phi)$. It follows that $\nu(fg) = \nu(r) = \nu(q\Phi) < \nu'(q\Phi)$. Now, if Φ is a w key polynomial for ν , then we can take ν' as in Proposition 2.8 2).

The last assertion also follows from Proposition 2.8. \square

If ν and ν' are K -module valuations on $K(\chi)$, then we set $\nu \leq \nu'$ if for every $f \in K[\chi]$ we have $\nu(f) \leq \nu'(f)$.

Remark 2.11. 1) By the definition of ν_{Φ} , for every K -module valuation ν' such that the restrictions of ν' and ν_{Φ} to $K_{d-1}[\chi]$ are equal and $\nu'(\Phi) = \nu_{\Phi}(\Phi)$, we have $\nu_{\Phi} \leq \nu'$.
2) Assume that χ is algebraic over K , that ν is multiplicative, and $\nu'(f) < \nu(f)$. If $\nu' \leq \nu$, then $\nu'(1/f) \leq \nu(1/f) = -\nu(f) < -\nu'(f)$. Hence $\nu'(1/f) \neq -\nu'(f)$. It follows that ν' is not multiplicative. Hence we cannot improve the conclusion that ν' is partially multiplicative in Proposition 2.8.

In valuation theory, we say that ν' is *finer* than ν if $\forall x \nu'(x) \geq 0 \Rightarrow \nu(x) \geq 0$ (see [18, p. 54]). Assume that χ is algebraic over K . Then $K(\chi) = K[\chi]$, so, if $\nu' \leq \nu$, then ν' is finer than ν . Now, any two distinct extensions of a valuation to an algebraic extension are incomparable (see [18, Corollaire 5, p. 158]). Therefore, this also proves that if $\nu' \neq \nu$, then ν or ν' is not multiplicative. In the case where χ is transcendental over K and ν, ν' are valuations such that $\nu' \leq \nu$, then we cannot deduce that ν and ν' are comparable in the sense of Ribenboim. Indeed, assume that $\nu(f) = \nu'(f) = \nu'(g) < \nu(g)$. Then, $\nu'(f/g) = 0 > \nu(f/g)$. Assume that $\nu'(f) < \nu(f) = \nu(g) = \nu'(g)$. Then $\nu'(f/g) < 0 = \nu(f/g)$.

Proposition 2.12. *Assume that ν is a pm valuation on $K[\chi]$, and let Φ be a non constant monic polynomial in $K[\chi]$ of degree $d < [K(\chi) : K]$. Then Φ is a w key polynomial for ν if, and only if, there exists a pm valuation $\nu' \leq \nu$ such that the restrictions of ν and ν' to $K_{d-1}[\chi]$ are equal, and Φ is a w key polynomial for ν' such that the sequence (Φ^m) ($md < [K(\chi) : K]$) is separated over $K_{d-1}[\chi]$. Furthermore, we can take $\nu' = \nu_{\Phi}$.*

Proof. \Leftarrow . If Φ is a w key polynomial for ν' , then, by 3) of Proposition 2.3, it is a w key polynomial for ν .

\Rightarrow . By Proposition 2.10, ν_Φ is a pm valuation such that Φ is a w key polynomial for ν_Φ such that the sequence (Φ^m) ($md < [K(\chi):K]$) is separated over $K_{d-1}[\chi]$. By construction, the restrictions of ν and ν_Φ to $K_{d-1}[\chi]$ are equal. By Remark 2.11 1) we have $\nu_\Phi \leq \nu$. \square

Thanks to the mappings ν_Φ we get useful criteria for being a w key polynomial or a key polynomial, as show the following propositions. We start with a lemma.

Lemma 2.13. *Assume that ν is a pm valuation. Let $d < [K[\chi]:K]$ in $\mathbb{N} \setminus \{0\}$, $d' := [K[\chi]:K] - d$, Φ be a non constant monic polynomial in $K[\chi]$ of degree d . We also assume that for every f, g in $K_{d-1}[\chi]$ with $\deg(f) + \deg(g) < [K[\chi]:K]$ and every h in $K_{d'-1}[\chi]$, we have $\nu(fg + h\Phi) = \min(\nu(fg), \nu(h\Phi))$. Then Φ is a w key polynomial such that the sequence (Φ^m) ($md < [K(\chi):K]$) is separated over $K_{d-1}[\chi]$. In particular, $\nu = \nu_\Phi$.*

Proof. By setting $h = -q_\Phi$, we have $\nu(r_\Phi) = \nu(fg - q_\Phi\Phi) = \min(\nu(fg), \nu(q_\Phi\Phi)) \leq \nu(fg)$. By setting $f' = r_\Phi$, $g' = 1$ and $h' = q_\Phi$, we get $\nu(fg) = \nu(r_\Phi + q_\Phi\Phi) = \min(\nu(r_\Phi), \nu(q_\Phi\Phi)) \leq \nu(r_\Phi)$. Therefore $\nu(fg) = \nu(r_\Phi)$. Hence Φ is a w key polynomial. Now, let $m \in \mathbb{N} \setminus \{0\}$ with $dm < [K[\chi]:K]$, f_0, \dots, f_m in $K_{d-1}[\chi]$. We have: $\nu(f_m\Phi^m + \dots + f_0) = \min(\nu((f_m\Phi^{m-1} + \dots + f_1)\Phi), \nu(f_0))$, $\nu(f_m\Phi^{m-1} + \dots + f_1) = \min(\nu((f_m\Phi^{m-2} + \dots + f_2)\Phi), \nu(f_1))$, and so on. So by induction we have $\nu(f_m\Phi^m + \dots + f_0) = \min(\nu(f_m\Phi^{m-1}), \dots, \nu(f_0))$. Hence the family (Φ^m) ($md < [K(\chi):K]$) is separated over $K_{d-1}[\chi]$. \square

Proposition 2.14. *Let ν, ν' be pm valuations on $K(\chi)$, and Φ be a monic polynomial of degree d , $1 \leq d < [K(\chi):K]$. Assume that their restrictions to $K_{d-1}[\chi]$ are equal, that $\nu' \leq \nu$ and $\nu'(\Phi) < \nu(\Phi)$.*

1) *Let $f \in K[\chi]$ and $f = q\Phi + r$ be the euclidean division of f by Φ . Then $\nu'(f) < \nu'(r) \Leftrightarrow \nu'(f) < \nu(f)$ and $\nu'(f) = \nu'(r) \Leftrightarrow \nu'(f) = \nu(f)$.*

2) *Φ is a w key polynomial for ν' and a key polynomial for ν .*

3) *$\nu' = \nu'_\Phi = \nu_{\Phi, \nu'(\Phi)}$.*

Proof. 1) We have $\nu'(r) = \nu(r)$ and $\nu'(q\Phi) < \nu(q\Phi)$. Assume that $\nu'(r) \leq \nu'(q\Phi)$. Then $\nu(f) = \min(\nu(q\Phi), \nu(r)) = \nu(r)$. Furthermore, $\nu(f) \geq \nu'(f) \geq \min(\nu'(q\Phi), \nu(r)) \geq \nu(r) = \nu(f)$. Hence $\nu'(f) = \nu(f) = \nu(r)$. Assume that $\nu'(q\Phi) < \nu(r) < \nu(q\Phi)$. Hence $\nu'(f) = \min(\nu'(q\Phi), \nu'(r)) = \nu'(q\Phi) < \nu'(r) = \min(\nu(q\Phi), \nu(r)) = \nu(f)$. Assume that $\nu(q\Phi) \leq \nu(r)$. Then $\nu'(f) = \min(\nu'(q\Phi), \nu'(r)) = \nu'(q\Phi) < \nu(q\Phi) = \min(\nu(q\Phi), \nu(r)) \leq \nu(f)$, and $\nu'(f) < \nu'(r)$.

2) Let f, g in $K_{d-1}[\chi]$ with $\deg(f) + \deg(g) < [K[\chi]:K]$. Since $\deg(f) < \deg(\Phi)$ and $\deg(g) < \deg(\Phi)$, we have: $\nu'(f) = \nu(f)$ and $\nu'(g) = \nu(g)$, therefore: $\nu'(fg) = \nu'(f) + \nu'(g) = \nu(f) + \nu(g) = \nu(fg)$. By 1) this implies $\nu'(fg) = \nu'(r(f, g))$ and Φ is a w key polynomial for ν' . Since the restrictions of ν and ν' to $K_{d-1}[\chi]$ are equal, it follows that Φ is also a w key polynomial for ν . Now, for f, g in $K_{d-1}[\chi]$ we have $\nu(r(f, g)) = \nu'(r(f, g)) \leq \nu'(q(f, g) \cdot \Phi) < \nu(q(f, g) \cdot \Phi)$. Hence Φ is a key polynomial for ν .

3) First we prove that for every f, g in $K_{d-1}[\chi]$ with $\deg(f) + \deg(g) < [K[\chi]:K]$ and $h \in K[\chi]$ such that $\deg(h) < [K[\chi]:K] - d$ we have: $\nu'(fg + h\Phi) = \min(\nu'(fg), \nu'(h\Phi))$. If $\nu'(fg) \neq \nu'(h\Phi)$, then the result is trivial. Assume that $\nu'(fg) = \nu'(h\Phi)$, and let $q = q(f, g)$, $r = r(f, g)$. Since Φ is a w key polynomial for ν' , we have $\nu'(fg) = \nu'(r)$. Hence $\nu'(fg + h\Phi) \geq \nu'(r)$. Since $\nu' \leq \nu$, we have $\nu'(fg + h\Phi) \leq \nu(fg + h\Phi)$. Note that $fg + h\Phi = (q + h)\Phi + r$. So by 1), $\nu'((q + h)\Phi + r) < \nu((q + h)\Phi + r) \Leftrightarrow \nu'((q + h)\Phi + r) < \nu'(r)$: a contradiction. Hence $\nu'(fg + h\Phi) = \nu(fg + h\Phi)$. We have also $\nu(fg) = \nu'(fg) = \nu'(h\Phi) < \nu(h\Phi)$, hence $\nu(fg + h\Phi) = \nu(fg) = \nu'(fg) = \min(\nu'(fg), \nu'(h\Phi))$. By Lemma 2.13 we have $\nu' = \nu'_\Phi$. Now, since ν' and ν coincide on $K_{d-1}[\chi]$ we have $\nu'_\Phi = \nu_{\Phi, \nu'(\Phi)}$. \square

Remark 2.15. We deduce from Proposition 2.14 that if ν is a valuation on $K(\chi)$, then every pm valuation $\nu' \leq \nu$, $\nu' \neq \nu$, which coincide on K with ν , can be written as $\nu' = \nu_{\Phi, \nu'(\Phi)}$ where Φ is a monic polynomial of minimal degree such that $\nu'(\Phi) < \nu(\Phi)$. This completes Proposition 2.10.

Proposition 2.16. *Let ν be a pm valuation on $K(\chi)$, Φ be a w key polynomial for ν and Φ' be a monic polynomial such that $d = \deg(\Phi) < \deg(\Phi') = d' < [K(\chi):K]$.*

- 1) If $\nu(\Phi') = \nu_{\Phi}(\Phi')$, then Φ' is not a key polynomial for ν .
 2) Assume that $\nu_{\Phi} = \nu$ on $K_{d-1}[\chi]$. Then, Φ' is a key polynomial for ν if, and only if, $\nu(\Phi') > \nu_{\Phi}(\Phi')$.

Proof. 1) Write Φ' as $\Phi' = f_m \Phi^m + \dots + f_1 \Phi + f_0$, with f_0, \dots, f_m in $K_{d-1}[\chi]$. By the definition of ν_{Φ} , we have $\nu(\Phi') = \nu_{\Phi}(\Phi') = \min(f_0, f_1 \Phi, \dots, f_m \Phi^m)$. Let $f = f_m \Phi^{m-1} + \dots + f_1$ and $g = \Phi$. Then $q_{\Phi'}(f, g) = 1$, $r_{\Phi'}(f, g) = -f_0$, and $\nu(q_{\Phi'}(f, g)\Phi') = \nu(\Phi') = \nu_{\Phi}(\Phi') \leq \min(\nu(f_1 \Phi), \dots, \nu(f_n \Phi^n)) \leq \nu(fg)$. This proves that Φ' is not a key polynomial.

- 2) \Leftarrow follows from Proposition 2.14, \Rightarrow follows from 1). \square

3. MACLANE'S KEY POLYNOMIALS

In [14] and [15] S. MacLane defined key polynomials in the case of discrete valuations. In these papers, the key polynomials are the ν -minimal and ν -irreducible polynomials (see definitions below). M. Vaquié ([19]) generalized this definition to arbitrary valuations. In [19] the key polynomials are defined on the ring of formal polynomials. Here we extend the definition of [19] to the case of an algebraic extension, and we do not require χ being transcendental.

In this section, ν is a K -module valuation on $K(\chi)$ or a pseudo-valuation. Recall that in the case where ν is a pseudo-valuation, we also assume that χ is transcendental

If ν is a pseudo-valuation, then the results below remain true, by assuming that d is lower than the degree of a generator of the ideal $\{f \in K[\chi] : \nu(f) = \infty\}$.

Let Φ be a monic polynomial of degree d and $d' := [K[\chi] : K] - d$ (if $[K(\chi) : K] = \infty$, then $d' = d' - 1 = \infty$). We say that Φ is ν -minimal if for every $f \in K_{d-1}[\chi]$ and every $h \in K_{d'-1}[\chi]$, $\nu(f - h\Phi) = \min(\nu(f), \nu(h\Phi))$. We say that Φ is ν -irreducible if for every f, g in $K[\chi]$ with $\deg(f) + \deg(g) < [K[\chi] : K]$ such that, for every $h \in K_{d'-1}[\chi]$, $\nu(f - h\Phi) = \min(\nu(f), \nu(h\Phi))$ and $\nu(g - h\Phi) = \min(\nu(g), \nu(h\Phi))$, we have: $\forall h \in K_{d'-1}[\chi] \nu(fg - h\Phi) = \min(\nu(fg), \nu(h\Phi))$.

By setting $h := 1$ in above definition, we see that every monic polynomial, which is ν -minimal and ν -irreducible, is irreducible.

Proposition 3.1. *Assume that ν is a pm valuation or a pseudo-valuation. Let $d < [K[\chi] : K]$ in $\mathbb{N} \setminus \{0\}$, $d' := [K[\chi] : K] - d$, Φ be a non constant monic polynomial in $K[\chi]$ of degree d . The following assertions are equivalent.*

- 1) Φ is ν -minimal and ν -irreducible.
- 2) For every f, g in $K_{d-1}[\chi]$ with $\deg(f) + \deg(g) < [K[\chi] : K]$ and every h in $K_{d'-1}[\chi]$, we have (*): $\nu(fg + h\Phi) = \min(\nu(fg), \nu(h\Phi))$.
- 3) Φ is a w key polynomial such that the sequence (Φ^m) ($md < [K(\chi) : K]$) is separated over $K_{d-1}[\chi]$.

Proof. 2) \Rightarrow 1). Assume that Φ satisfies the hypothesis of 2). By setting $g = 1$ in (*) it follows that Φ is a non constant monic polynomial in $K[\chi]$ of degree d such that for every f in $K_{d-1}[\chi]$ and every h in $K_{d'-1}[\chi]$ we have $\nu(f + h\Phi) = \min(\nu(f), \nu(h\Phi))$. Hence Φ is ν -minimal. In order to prove that Φ is ν irreducible, let f and g in $K[\chi]$ such that $\deg(f) + \deg(g) < [K[\chi] : K]$ and for every $h \in K_{d'-1}[\chi]$: (**): $\nu(f - h\Phi) = \min(\nu(f), \nu(h\Phi))$ and $\nu(g - h\Phi) = \min(\nu(g), \nu(h\Phi))$. By euclidean division, f and g can be written as $f = q\Phi + r$ and $g = q'\Phi + r'$. By setting $h = q$ in (**), we have $\nu(r) = \nu(f - q\Phi) = \min(\nu(f), \nu(q\Phi)) \leq \nu(f)$. By (*) we have $\nu(f) = \nu(r \cdot 1 + q\Phi) = \min(\nu(r \cdot 1), \nu(q\Phi)) \leq \nu(r)$. Therefore $\nu(f) = \nu(r)$. In the same way, $\nu(g) = \nu(r')$. Let $h \in K_{d'-1}[\chi]$. Then $\nu(fg - h\Phi) = \nu((qq'\Phi + qr' + q'r - h)\Phi + rr')$ = $\min(\nu((qq'\Phi + qr' + q'r - h)\Phi), \nu(rr'))$, by (*). Hence $\nu(fg - h\Phi) \leq \nu(rr') = \nu(fg)$ and $\min(\nu(fg), \nu(h\Phi)) \leq \nu(fg - h\Phi) \leq \nu(fg)$. So, $\nu(fg - h\Phi) = \min(\nu(fg), \nu(h\Phi))$. Hence Φ is ν -irreducible.

1) \Rightarrow 2). We assume that Φ is monic, ν -minimal and ν -irreducible. Let f, g in $K_{d-1}[\chi]$ with $\deg(f) + \deg(g) < [K[\chi] : K]$. Since Φ is ν -minimal, for every h in $K_{d'-1}[\chi]$ we have $\nu(f + h\Phi) = \min(\nu(f), \nu(h\Phi))$ and $\nu(g + h\Phi) = \min(\nu(g), \nu(h\Phi))$. Now, Φ is ν -irreducible, hence $\nu(fg + h\Phi) = \min(\nu(fg), \nu(h\Phi))$.

2) \Rightarrow 3) has been proved in Lemma 2.13.

3) \Rightarrow 2). We take f, g in $K_{d-1}[\chi]$ and h in $K_{d'-1}[\chi]$ with $\deg(f) + \deg(g) < [K[\chi] : K]$. The polynomial h can be written as $h = h_m \Phi^m + \dots + h_{\Phi} + h_0$, where h_m, \dots, h_1, h_0 belong to

$K_{d-1}[\chi]$. Let $q := q(f, g)$ and $r := r(f, g)$; since f and g belong to $K_{d-1}[\chi]$, we have $\deg(q) < d$, i.e. $q \in K_{d-1}[\chi]$. We have: $\nu(fg + h\Phi) = \nu(h_m\Phi^{m+1} + \dots + h_1\Phi^2 + (q + h_0)\Phi + r) = \min(\nu(h_m\Phi^{m+1}), \dots, \nu(h_1\Phi^2), \nu((q + h_0)\Phi), \nu(r))$. Since Φ is a w key polynomial, we have $\nu(fg) = \nu(r) \leq \nu(q\Phi)$. If $\nu(h_0\Phi) \geq \nu(r)$, then $\nu((q + h_0)\Phi) \geq \nu(r)$. Hence $\min(\nu((q + h_0)\Phi), \nu(r)) = \nu(r) = \min(\nu(h_0\Phi), \nu(r))$. If $\nu(h_0\Phi) < \nu(r)$, then $\min(\nu((q + h_0)\Phi), \nu(r)) = \nu(h_0\Phi) = \min(\nu(h_0\Phi), \nu(r))$. Therefore: $\nu(fg + h\Phi) = \min(\nu(h_m\Phi^{m+1}), \dots, \nu(h_1\Phi^2), \nu(h_0\Phi), \nu(fg)) = \min(\nu(h\Phi), \nu(fg))$. \square

We use the hypothesis “ ν is a pm valuation” for proving 2) \Rightarrow 1). For proving 2) \Rightarrow 3) the condition “for every $f \in K_{d-1}[\chi]$, $\nu(\Phi f) = \nu(\Phi) + \nu(f)$ ” is sufficient. The remainder of the proof remains true with a K -module valuation.

Proposition 3.1 shows that the definition of MacLane is stronger than the definition of w key polynomials. Now, we extend the definition of S. MacLane to K -module valuations.

Definition 3.2. Let Φ be a polynomial of degree d . We say that Φ is a *ML key polynomial* for ν if Φ is a w key polynomial such that the sequence (Φ^m) ($md < [K(\chi) : K]$) is separated over $K_{d-1}[\chi]$.

If ν is a pm valuation, then it follows from Proposition 2.8 that Φ is a ML key polynomial for ν if, and only if, Φ is a w key polynomial for ν and $\nu = \nu_\Phi$. This shows the difference between w key polynomials and MacLane key polynomials.

4. PROPERTIES OF KEY DEGREES

In this section, we list some properties of key degrees. In particular, we give sufficient conditions for existing a finite number of key degrees and a characterization of the successor of a key degree. This characterization takes place in the construction of complete families of key polynomials. In this construction, in the case of an independent key degree, we will choose monic polynomials with maximal valuation. However, the fact that the degree d of a key polynomial is independent does not imply that its valuation is maximal in $\nu(\chi^d - K_{d-1}[\chi])$. Indeed, we saw in Proposition 2.3 1) that every monic polynomial of degree 1 is a key polynomial. This holds whether 1 is an independent key degree or not.

Except for Proposition 4.7, all properties of this section remain true if ν is a pseudo-valuation (and χ is transcendental). In this case we assume that the degrees are lower than the degree of a generator of the ideal $\{f \in K[\chi] : \nu(f) = \infty\}$ (in the settings, we can take $d < [K[\chi] : K]$ in place of $d < \deg(\Pi)$).

4.1. Independent key degrees. We start this subsection with some observations about monic polynomials with maximal valuations.

Proposition 4.1. *Let d be an integer and ν be a pm valuation on $K[\chi]$.*

1) *Let Φ be a w key polynomial of degree d . Then every monic polynomial Φ' of degree d , such that $\nu(\Phi') > \nu(\Phi)$, is a key polynomial. Therefore, if d is not a key degree, then $\nu(\Phi)$ is maximal in $\nu(\chi^d - K_{d-1}[\chi])$.*

2) *Assume that d is an independent key degree and let Φ be a key polynomial of degree d . Then every monic polynomial Φ' of degree d , such that $\nu(\Phi') \geq \nu(\Phi)$, is a key polynomial. In particular, any monic polynomial Φ' of degree d , such that $\nu(\Phi')$ is maximal in $\nu(\chi^d - K_{d-1}[\chi])$, is a key polynomial.*

This proposition is a consequence of the following lemma.

Lemma 4.2. *Let d be a positive integer, ν be a pm valuation on $K[\chi]$, Φ and Φ' be monic polynomials of degree d such that Φ is a w key polynomial for ν .*

- 1) *If $\nu(\Phi') > \nu(\Phi)$, then Φ' is a w key polynomial for ν_Φ , a key polynomial for ν , and $\nu_\Phi \leq \nu_{\Phi'}$.*
- 2) *If $\nu(\Phi') = \nu(\Phi)$ and Φ is a key polynomial for ν , then Φ' is a key polynomial for both of ν and ν_Φ . Furthermore, $\nu_\Phi = \nu_{\Phi'}$.*
- 3) *If $\nu(\Phi') = \nu(\Phi)$ and Φ, Φ' are w key polynomials for ν , then $\nu_\Phi = \nu_{\Phi'}$.*

Proof. Set $h = \Phi' - \Phi$. Assume that $\nu(\Phi') \geq \nu(\Phi)$. Then we have $\nu(h) \geq \nu(\Phi)$. Furthermore, Φ and Φ' are monic polynomials, so the degree of h is lower than d . Now, $\Phi' = \Phi + h$, hence $\nu_{\Phi}(\Phi') = \min(\nu(\Phi), \nu(h)) = \nu(\Phi)$. Let f, g in $K_{d-1}[\chi]$ with $\deg(f) + \deg(g) < [K[\chi] : K]$. We have: $\nu_{\Phi}(fg) = \nu_{\Phi}(f) + \nu_{\Phi}(g) = \nu(f) + \nu(g) = \nu(fg)$. Let $r' = r_{\Phi'}(f, g)$, $q' = q_{\Phi'}(f, g)$.

1) Since $\nu(\Phi') > \nu(\Phi)$, we have $\nu(h) = \nu(\Phi) (= \nu_{\Phi}(\Phi'))$. In order to get a contradiction, assume that $\nu_{\Phi}(q'\Phi') < \nu_{\Phi}(r')$ ($= \nu(r')$). Then $\nu_{\Phi}(fg) = \nu_{\Phi}(q'\Phi' + r') = \nu_{\Phi}(q'\Phi') = \nu(q'\Phi) = \nu_{\Phi}(q'\Phi)$. Now, $\nu(q'\Phi') > \nu(q'\Phi) = \nu(fg)$ and $\nu(r') > \nu_{\Phi}(q'\Phi') = \nu_{\Phi}(fg) = \nu(fg)$. Hence $\nu(fg) \geq \min(\nu(q'\Phi'), \nu(r')) > \nu(fg)$: a contradiction. Therefore, $\nu_{\Phi}(q'\Phi') \geq \nu_{\Phi}(r')$. Now, $\nu(r') = \nu_{\Phi}(r')$ and $\nu_{\Phi}(q'\Phi') = \nu(q'\Phi) < \nu(q'\Phi')$. Hence Φ' is a key polynomial for ν (so $\nu(fg) = \nu(r')$). Since $\nu_{\Phi}(fg) = \nu(fg) = \nu(r') = \nu_{\Phi}(r')$, Φ' is a w key polynomial for ν_{Φ} . Furthermore, ν_{Φ} and $\nu_{\Phi'}$ are equal on $K_{d-1}[\chi]$, and $\nu_{\Phi'}(\Phi) = \nu_{\Phi'}(\Phi' - h) = \min(\nu_{\Phi'}(\Phi'), \nu_{\Phi'}(h)) = \min(\nu(\Phi'), \nu(h)) = \nu(h) = \nu(\Phi) = \nu_{\Phi}(\Phi)$. By Remark 2.11, we have $\nu_{\Phi} \leq \nu_{\Phi'}$.

2) We assume that $\nu(\Phi') = \nu(\Phi)$ and Φ is a key polynomial for ν . Let $q_1 = q_{\Phi}(q', h)$ and $r_1 = r_{\Phi}(q', h)$. Since Φ is a key polynomial for ν , we have $\nu(q_1\Phi) > \nu(r_1) = \nu(q'h) \geq \nu(q'\Phi)$. Hence $\nu(q') < \nu(q_1)$ and $\nu(q' + q_1) = \nu(q')$. We have: $fg = q'\Phi' + r' = q'\Phi + q'h + r' = (q' + q_1)\Phi + r' + r_1$, hence $q' + q_1 = q_{\Phi}(f, g)$, $r' + r_1 = r_{\Phi}(f, g)$ and $\nu(fg) = \nu(r' + r_1) < \nu((q' + q_1)\Phi) = \nu(q'\Phi) \leq \nu(r_1)$. It follows: $\nu(r' + r_1) = \nu(r')$, so $\nu(fg) = \nu(r') < \nu(q'\Phi) = \nu(q'\Phi')$. This proves that Φ' is a key polynomial for ν . Now, $\nu_{\Phi}(fg) = \nu(fg) = \nu(r') = \nu_{\Phi}(r')$ and $\nu_{\Phi}(q'\Phi') = \nu_{\Phi}(q'\Phi) = \nu(q'\Phi) > \nu(r')$. Hence Φ' is a key polynomial for ν_{Φ} . In the same way as in 1), we have: $\nu_{\Phi} \leq \nu_{\Phi'}$. Now, since Φ' is a key polynomial, we have in a symmetric way: $\nu_{\Phi'} \leq \nu_{\Phi}$.

3) We assume that $\nu(\Phi') = \nu(\Phi)$ and Φ, Φ' are w key polynomials for ν . We have: $\Phi' = \Phi + h$, with $\nu(h) \geq \nu(\Phi)$ and $\deg(h) < d$. Hence $\nu_{\Phi}(\Phi') = \min(\nu(\Phi), \nu(h)) = \nu(\Phi) = \nu(\Phi') = \nu_{\Phi'}(\Phi')$. So by Remark 2.11 we have: $\nu_{\Phi'} \leq \nu_{\Phi}$. In the same way, $\nu_{\Phi} \leq \nu_{\Phi'}$, hence $\nu_{\Phi'} = \nu_{\Phi}$. \square

The following proposition gives a characterization of valuational key degrees by means of $\nu K_{d-1}[\chi]$.

Proposition 4.3. *Let ν be a pm valuation on $K[\chi]$ and d be a positive integer such that $1 \leq d \leq [K(\chi) : K]/2$. Then, d is a valuational key degree if, and only if, $\nu K_{d-1}[\chi]$ is a group and $\nu K_d[\chi] \neq \nu K_{d-1}[\chi]$. If this holds, then every monic polynomial Φ of degree d such that $\nu(\Phi)$ is the maximum of $\nu(\chi^d - K_{d-1}[\chi])$ (which is equivalent to saying that $\nu(\Phi) \notin \nu K_{d-1}[\chi]$) is a key polynomial.*

Proof. \Rightarrow follows from the definition and Corollary 2.6. Assume that $\nu K_{d-1}[\chi]$ is a group and $\nu K_d[\chi] \neq \nu K_{d-1}[\chi]$. By hypothesis, there is a polynomial Φ of degree d such that $\nu(\Phi) \notin \nu K_{d-1}[\chi]$. Since $\nu K_{d-1}[\chi]$ is a group, by dividing Φ by an element of K we can assume that Φ is a monic polynomial. Let $f \in K_{d-1}[\chi]$. Then $\nu(f) \neq \nu(\Phi)$. Hence $\nu(\Phi - f) = \min(\nu(\Phi), \nu(f)) \leq \nu(\Phi)$. Consequently, $\nu(\Phi)$ is the maximum of $\nu(\chi^d - K_{d-1}[\chi])$.

Let f, g in $K_{d-1}[\chi]$, $q = q_{\Phi}(f, g)$ and $r = r_{\Phi}(f, g)$. Since $\nu(q\Phi) \notin \nu K_{d-1}[\chi]$, we have that $\nu(q\Phi) \neq \nu(r)$. Hence $\nu(fg) = \min(\nu(q\Phi), \nu(r))$. Now, since $\nu K_{d-1}[\chi]$ is a group, $\nu(fg) = \nu(f) + \nu(g) \in \nu K_{d-1}[\chi]$. Hence $\nu(fg) \neq \nu(q\Phi)$. So, $\nu(q\Phi) > \nu(r)$. This proves that Φ is a key polynomial. Since $\nu(\phi)$ is the maximum of $\nu(\chi^d - K_{d-1}[\chi])$, d is an independent key degree. Therefore it is a valuational key degree. \square

Corollary 4.4. *Let ν be a pm valuation on $K[\chi]$ and d be a positive integer. Assume that $\nu K_{d-1}[\chi]$ is a group and let d' be the smallest integer such that $\nu K_{d'}[\chi] \neq \nu K_{d-1}[\chi]$ (if any). Then d' is a valuational key degree. In particular, the smallest degree d such that $\nu K_d[\chi] \neq \nu K$ (if any) is a valuational key degree.*

4.2. Maximal key degrees. If χ is algebraic over K , then there is a finite number of key degrees. We saw that if ν is a pseudo-valuation, then the degrees of the key polynomials are bounded by the degree of a generator of the ideal of elements with infinite valuation. We give sufficient conditions for a key degree being the maximal one. We start with a lemma.

Lemma 4.5. *Let ν be a pm valuation on $K[\chi]$ and Φ be a monic polynomial of degree d . Then, $\nu = \nu_{\Phi}$ on $K_d[\chi]$ if, and only if, $\nu(\Phi) = \max \nu(\chi^d - K_{d-1}[\chi])$.*

Proof. By the definition of ν_Φ , ν and ν_Φ are equal on $K_{d-1}[\chi]$. Hence, we can consider polynomials of degree d . So, we let f be a polynomial of degree d . Without loss of generality we can assume that f is a monic polynomial. Hence $f - \Phi$ has degree less than Φ . Assume that $\nu(f) = \nu_\Phi(f)$. Then $\nu(f) = \nu_\Phi(\Phi + f - \Phi) = \min(\nu(\Phi), \nu(f - \Phi)) \leq \nu(\Phi)$. This proves that $\nu(\Phi)$ is the maximum of $\nu(\chi^d - K_{d-1}[\chi])$. Conversely, assume that $\nu(\Phi) = \max \nu(\chi^d - K_{d-1}[\chi])$. We have $\nu(f - \Phi) \geq \min(\nu(f), \nu(\Phi)) = \nu(f)$. Therefore, $\nu(f) \geq \nu_\Phi(f) = \nu_\Phi(\Phi + f - \Phi) = \min(\nu(\Phi), \nu(f - \Phi)) \geq \nu(f)$. Hence $\nu_\Phi(f) = \nu(f)$. \square

Remark 4.6. Let d be a positive integer, ν be a pm valuation on $K[\chi]$.

- 1) It follows from Proposition 2.16 that if $\nu = \nu_\Phi$ for some w key polynomial Φ , then there is no key degree greater than d .
- 2) Assume that d is an independent key degree such that there is no key degree greater than d , and Φ is a key polynomial of degree d , with $\nu(\Phi) = \max(\nu(\chi^d - K_{d-1}[\chi]))$. By Lemma 4.5, ν and ν_Φ coincide on $K_d[\chi]$. Now, by Proposition 2.16, $\nu = \nu_\Phi$ on $K[\chi]$.

Proposition 4.7. *Let ν be a multiplicative valuation on $K(\chi)$. If the rational rank of $\nu K(\chi)$ over νK is 1, or the transcendence degree of $K(\chi)_\nu$ over K_ν is 1 (in other words, if χ is transcendental and Abhyankar's inequality is an equality), then there is a finite number of key degrees, and $\nu = \nu_\Phi$ for some w key polynomial Φ .*

Proof. Abhyankar's inequality states that the transcendence degree of $K(\chi)|K$ is at least equal to the sum of the transcendence degree of $(K(\chi))_\nu|K_\nu$ and the rational rank of $\nu(K[\chi])|\nu K$. Assume that the rational rank of $\nu K(\chi)$ over νK is 1. Let d be the smallest integer such that there exists a monic polynomial Φ of degree d such that $\nu(\Phi)$ is not rational over νK . If $d = 1$, then we know that Φ is a key polynomial. Otherwise, clearly, $\nu(\Phi) \neq \nu(\chi^d) = d\nu(\chi)$. If $\nu(\Phi) < \nu(\chi^d)$, then $\nu(\chi^d - \Phi) = \nu(\Phi)$, with $\deg(\chi^d - \Phi) < d$: a contradiction (since d is minimal). Hence $\nu(\Phi) > \nu(\chi^d)$. Then $\nu(\Phi) = \max \nu(\chi^d - K_{d-1}[\chi])$. Let f, g in $K_{d-1}[\chi]$ and $q = q(f, g)$, $r = r(f, g)$. Since d is minimal, we have: $\nu(r) \neq \nu(q\Phi)$ and $\nu(q\Phi) \neq \nu(f) + \nu(g) = \nu(fg)$. It follows that $\nu(fg) = \nu(r) < \nu(q\Phi)$ (the other cases lead to a contradiction). So Φ is a key polynomial for ν . Now, the elements $\nu(\Phi^k) = k\nu(\Phi)$ are pairwise non-congruent modulo $\nu K_{d-1}[\chi]$. In the same way as in Proposition 1.12, this implies that the family (Φ^k) is separated over $K_{d-1}[\chi]$. Therefore, $\nu = \nu_\Phi$. Now, by 1) of Remark 4.6, if $d' > d$, then d is not a key degree.

Now, assume that the transcendence degree of $K(\chi)_\nu$ over K_ν is 1. Let Φ be a polynomial such that $\nu(\Phi) = 0$. If $in_\nu(\Phi)$ is algebraic over $G_\nu(K)$, then by Lemma 1.17 $in_\nu(\Phi)$ is algebraic over K_ν (the converse is trivial). Consequently, $in_\nu(\Phi)$ is transcendental over K_ν if, and only if, it is transcendental over $G_\nu(K)$. In particular, there is Φ in $K[\chi]$ such that $in_\nu(\Phi)$ is transcendental over $G_\nu(K)$. Let d be the smallest integer such that there exists a polynomial Φ of degree d such that $in_\nu(\Phi)$ is transcendental over $G_\nu(K)$. Without loss of generality we can assume that Φ is a monic polynomial. Let f, g in $K_{d-1}[\chi]$, $q = q_\Phi(f, g)$, $r = r_\Phi(f, g)$. We have: $\nu(r) > \nu(fg) = \nu(q\Phi) \Leftrightarrow \nu(fg - q\Phi) > \nu(fg) = \nu(q\Phi) \Leftrightarrow 0 = in_\nu(fg) - in_\nu(q\Phi) \Leftrightarrow in_\nu(fg) = in_\nu(q\Phi)$. Now, $in_\nu(fg) = in_\nu(f)in_\nu(g)$ is algebraic over $G_\nu(K)$. Hence $in_\nu(fg) \neq in_\nu(q\Phi)$, which is transcendental over $G_\nu(K)$. It follows that $\nu(r) \leq \min(\nu(fg), \nu(q\Phi)) \leq \nu(fg)$. Now, $in_\nu(r) \neq in_\nu(q\Phi)$, hence in the same way we get $\nu(fg) \leq \min(\nu(q\Phi), \nu(r)) \leq \nu(r)$. Consequently, $\nu(fg) = \nu(r)$. This proves that Φ is a w key polynomial. Let f_0, \dots, f_n in $K_{d-1}[\chi] \setminus \{0\}$. By hypothesis, $in_\nu(f_0), \dots, in_\nu(f_n)$ are algebraic over $G_\nu(K)$. Hence $in_\nu(f_n)in_\nu(\Phi)^n + \dots + in_\nu(f_0) \neq 0$. Without loss of generality we can assume that $in_\nu(f_0) = \dots = in_\nu(f_n)$. It follows that $\nu(f_0 + \dots + f_n\Phi^n) = \min(\nu(f_0), \dots, \nu(f_n\Phi^n))$. This proves that the sequence (Φ^n) is separated over $K_{d-1}[\chi]$. Therefore, $\nu = \nu_\Phi$. By 1) of Remark 4.6, if $d' > d$, then d' is not a key degree. \square

Now we turn to a particular case of immediate key degrees that we can call *dense* key degrees. It follows that if a key degree is dense, then it is the greatest key degree.

Proposition 4.8. *Let $d \geq 2$, $\nu' \leq \nu$ be pm valuations on $K[\chi]$. Assume that χ^d is limit over $(K_{d-1}[\chi], \nu)$, that the restrictions of ν and ν' to $K_{d-1}[\chi]$ are equal, and that there exists a monic polynomial Φ of degree d such that $\nu'(\Phi) < \nu(\Phi)$. Let (Φ_i) be a sequence of monic polynomials of degree d such that the sequence $(\nu(\Phi_i))$ is increasing and cofinal in $\nu K[\chi]$, and $\nu(\Phi) < \nu(\Phi_i)$. Then.*

- 1) d is an immediate key degree for ν , Φ is a w key polynomial for ν and ν' , and $\nu' = \nu'_\Phi$.
- 2) The Φ_i 's are key polynomials for ν , and for every $f \in K[\chi]$ the sequence $(\nu_{\Phi_i}(f))$ is eventually equal to $\nu(f)$.
- 3) The extension $(K[\chi]|K_{d-1}[\chi], \nu)$ is dense.
- 4) There is no key degree greater than d .

Proof. 1) By Proposition 2.14, Φ is a w key polynomial for ν' , $\nu' = \nu'_\Phi$, and Φ is a key polynomial for ν . Hence d is a key degree for ν . Since $\nu(\chi^d - K_{d-1}[\chi]) = \nu K[\chi]$, d is an immediate key degree.

2) Since $\deg(\Phi_i - \Phi) < d$, we have $\nu(\Phi_i - \Phi) = \nu'(\Phi_i - \Phi)$, and $\nu'(\Phi_i) = \nu'_\Phi(\Phi_i) = \nu'_\Phi(\Phi + \Phi_i - \Phi) = \min(\nu'(\Phi), \nu'(\Phi_i - \Phi)) = \min(\nu'(\Phi), \nu(\Phi_i - \Phi)) = \min(\nu'(\Phi), \nu(\Phi)) = \nu'(\Phi) < \nu(\Phi) < \nu(\Phi_i)$. By Proposition 2.14, Φ_i is a key polynomial for ν . We have also: $\nu' = \nu'_{\Phi_i}$. Let $f \in K[\chi]$, k be the quotient of the euclidean division of $\deg(f)$ by d , $\lambda = \nu'(f) - k\nu'(\Phi)$, and i be such that $\nu(\Phi_i) > \max(\nu(f) - \lambda, \nu(f))$. Decompose f as $f = f_{i,k}\Phi_i^k + \dots + f_{i,1}\Phi_i + f_{i,0}$, where the $f_{i,j}$'s belong to $K_{d-1}[\chi]$. Then $\nu'(f) = \nu'_{\Phi_i}(f) = \min(\nu'(f_{i,j}\Phi_i^j))$. Therefore, for every j we have: $\nu(f_{i,j}) = \nu'(f_{i,j}) \geq \nu'(f) - j\nu'(\Phi_i) \geq \nu'(f) - k\nu'(\Phi_i) = \nu'(f) - k\nu'(\Phi) = \lambda$. Then for every j we have $\nu(f_{i,j}\Phi_i^j) = \nu(f_{i,j}) + j\nu(\Phi_i) > \lambda + j \max(\nu(f) - \lambda, \nu(f))$. If $j \geq 1$, then $\nu(f_{i,j}\Phi_i^j) > \nu(f)$. It follows that $\nu(f) = \nu(f_{i,0}) = \nu_{\Phi_i}(f)$. This proves that the sequence $(\nu_{\Phi_i}(f))$ is eventually equal to $\nu(f)$.

3) If $\nu(\Phi_i) > \max(\nu(f) - \lambda, \nu(f))$, then

$$\nu(f - f_{i,0}) = \nu\left(\sum_{j=1}^k f_{i,j}\Phi_i^j\right) \geq \min_{1 \leq j \leq k} (\nu(f_{i,j}) + j\nu(\Phi_i)) \geq \lambda + \nu(\Phi_i)$$

is cofinal in $\nu K[\chi]$, since the sequence $(\nu(\Phi_i))$ is. It follows that $(K[\chi]|K_{d-1}[\chi], \nu)$ is dense.

4) Let f be a monic polynomial of degree $d' > d$. Then, there exists i such that $\nu(f) = \nu_{\Phi_i}(f)$. By Proposition 2.16 1), f is not a key polynomial for ν . Hence d' is not a key degree. \square

4.3. Successors of key degrees. The following two theorems characterize the successor of a key degree. They will be useful for proving the equivalence of the definitions of key polynomials and abstract key polynomials. They are also involved in the construction of complete families of key polynomials.

Theorem 4.9. *Let ν be a pm valuation on $K(\chi)$, d be an immediate key degree, and let (Φ_i) be a sequence of key polynomials of degree d such that the sequence $(\nu(\Phi_i))$ is increasing and cofinal in $\nu(\chi^d - K_{d-1}[\chi])$. Then.*

- 1) The sequence (ν_{Φ_i}) converges to ν on $K_d[\chi]$ in the sense that for every $f \in K_d[\chi]$ the sequence $(\nu_{\Phi_i}(f))$ is eventually equal to $\nu(f)$.
- 2) Let d' be the smallest degree (if any) such that there exists a monic polynomial Φ' of degree d' satisfying $\nu_{\Phi_i}(\Phi') < \nu(\Phi')$ for every i . Then, Φ' is a key polynomial and d' is the next key degree.
- 3) The extension $(K_{d'-1}[\chi]|K_{d-1}[\chi], \nu)$ is immediate.

Proof. 1) The family (ν_{Φ_i}) is increasing, and for every $f \in K[\chi]$ we have $\nu_{\Phi_i}(f) \leq \nu(f)$. Assume that f is a polynomial of degree d . Without loss of generality we can assume that f is monic. Since the sequence $(\nu(\Phi_i))$ is cofinal in $\nu(\chi^d - K_{d-1}[\chi])$, there is an i such that $\nu(\Phi_i) > \nu(f)$. Now, for every i such that $\nu(\Phi_i) > \nu(f)$ we have $\nu(f - \Phi_i) = \nu(f)$, and $\nu_{\Phi_i}(f) = \min(\nu(\Phi_i), \nu(f - \Phi_i)) = \nu(f)$.

2) Let f, g in $K_{d'-1}[\chi]$ with $\deg(f) + \deg(g) < [K[\chi]:K]$ and $q = q_{\Phi'}(f, g)$, $r = r_{\Phi'}(f, g)$. By hypothesis there exists i such that $\nu_{\Phi_i}(f) = \nu(f)$, $\nu_{\Phi_i}(g) = \nu(g)$, $\nu_{\Phi_i}(q) = \nu(q)$ and $\nu_{\Phi_i}(r) = \nu(r)$. Then $\nu(q\Phi' + r) = \nu(fg) = \nu(f) + \nu(g) = \nu_{\Phi_i}(f) + \nu_{\Phi_i}(g) = \nu_{\Phi_i}(fg) = \nu_{\Phi_i}(q\Phi' + r)$, with $\nu(q\Phi') > \nu_{\Phi_i}(q\Phi')$. Assume that $\nu(q\Phi') \leq \nu(r)$. Hence $\nu_{\Phi_i}(q\Phi') < \nu(r) = \nu_{\Phi_i}(r)$, and $\nu(fg) = \nu_{\Phi_i}(fg) = \nu_{\Phi_i}(q\Phi') < \nu(q\Phi') = \min(\nu(q\Phi'), \nu(r)) \leq \nu(fg)$: a contradiction. Hence $\nu(q\Phi') > \nu(r)$, which proves that Φ' is a key polynomial for ν . Let f be a monic polynomial of degree $d'' < d'$. Then, there exists i such that $\nu(f) = \nu_{\Phi_i}(f)$. By Proposition 2.16 1), f is not a key polynomial.

3) Let f be a monic polynomial of degree n , $d < n \leq d' - 1$. We show that $\nu(f)$ is not the maximum of $\nu(\chi^n - K_{n-1}[\chi])$. It will follow by Proposition 1.9 1) that the extension $(K_{d'-1}[\chi]|K_{d-1}[\chi], \nu)$ is immediate. Let Φ_i be a w key polynomial of degree d such that $\nu(f) = \nu_{\Phi_i}(f)$, and let f be written as $f = f_k\Phi_i^k + \dots + f_1\Phi_i + f_0$, where f_0, f_1, \dots, f_k belong to $K_{d-1}[\chi]$, f_k is monic, and

$\deg(f_k) + kd = n$. Then $\nu(f) = \min(\nu(f_k\Phi_i^k), \dots, \nu(f_1\Phi_i), \nu(f_0))$. Assume that $\nu(f_0) > \nu(f)$. Then $\nu(f) = \min(\nu(f_k\Phi_i^k), \dots, \nu(f_1\Phi_i))$. Let Φ_j be a w key polynomial of degree d such that $\nu(\Phi_j) > \nu(\Phi_i)$, and set $g = f_k\Phi_j^k + \dots + f_1\Phi_j$. Then g is a monic polynomial of degree n , and $\nu(g) \geq \nu_{\Phi_j}(g) = \min(\nu(f_k\Phi_j^k), \dots, \nu(f_1\Phi_j)) > \nu(f)$. Now, assume that $\nu(f_0) = \nu(f)$. Then $\nu(f - f_0) \geq \nu(f_0)$. If $\nu(f - f_0) > \nu(f_0)$, then we can let $g = f - f_0$. If $\nu(f - f_0) = \nu(f_0) = \nu(f)$, then we let Φ_j be a w key polynomial of degree d such that $\nu(\Phi_j) > \nu(\Phi_i)$, and $g = f_k\Phi_j^k + \dots + f_1\Phi_j$. Then $\nu(g) \geq \nu_{\Phi_j}(g) = \min(\nu(f_k\Phi_j^k), \dots, \nu(f_1\Phi_j)) > \min(\nu(f_k\Phi_i^k), \dots, \nu(f_1\Phi_i)) \geq \nu(f)$. \square

Recall that if M is a K -submodule of $K(\chi)$, then we denote by $G_\nu(M)$ the additive group $\bigoplus_{\gamma \in \nu M} M_{\gamma, \nu}$.

Theorem 4.10. *Let ν be a pm valuation on $K(\chi)$, d be an independent key degree, Φ be a monic polynomial of degree d such that $\nu(\Phi)$ is the maximum of $\nu(\chi^d - K_{d-1}[\chi])$. Let d' be the next key degree if it exists or $d' = [K[\chi]:K]$ otherwise.*

- 1) Φ is a key polynomial, and d' is the smallest degree such that there exists a monic polynomial Φ' of degree d' with $\nu_\Phi(\Phi') < \nu(\Phi')$.
- 2) The restrictions of ν and ν_Φ to $K_{d'-1}[\chi]$ are equal.
- 3) If $d < [K[\chi]:K]/2$, then $G_\nu(K_{d'-1}[\chi])$ is a graded algebra and the fraction d'/d is equal to the dimension of the $G_\nu(K_{d-1}[\chi])$ -module $G_\nu(K_{d'-1}[\chi])$.
- 4) If $(K_{d-1}[\chi]|K, \nu)$ is vs defectless, then $(K_{d'-1}[\chi]|K, \nu)$ is vs defectless.

Proof. 1) Since $\nu(\Phi)$ is the maximum of $\nu(\chi^d - K_{d-1}[\chi])$, by 2) of Proposition 4.1, Φ is a key polynomial. By Proposition 2.16, if $d' < [K[\chi]:K]$, then d' is the smallest degree such that there exists a monic polynomial Φ' of degree d' with $\nu_\Phi(\Phi') < \nu(\Phi')$. If $d' = [K[\chi]:K]$, then $\nu = \nu_\Phi$, and by letting Φ' be the minimal polynomial of χ over K , we have $\nu(\Phi') = +\infty > \nu_\Phi(\Phi')$. Hence the assertion remains true. It also remains true in the case where $d' = +\infty$.

2) Since $\nu_\Phi \leq \nu$, by 1) the restrictions of ν and ν_Φ to $K_{d'-1}[\chi]$ are equal.

3) By Lemma 2.4 $in_\nu(\Phi) \notin G_\nu(K(\chi))$. Since $d \leq [K[\chi]:K]/2$, by Remark 2.7 $G_\nu(K_{d-1}[\chi])$ is a graded algebra. Assume that $in_\nu(\Phi)$ is transcendental over $G_\nu(K_{d-1}[\chi])$. Then χ is transcendental over K , so $[K(\chi):K]$ is infinite. In the same way as in the proof of Propositions 1.12 and 4.7 the family (Φ^n) is separated over $K_{d-1}[\chi]$ and $\nu = \nu_\Phi$. Furthermore, the dimension of the $G_\nu(K_{d-1}[\chi])$ -module $G_\nu(K(\chi))$ is also infinite. Assume that $d' = +\infty$. Then by 1) $\nu = \nu_\Phi$, the family (Φ^n) is separated over $K_{d-1}[\chi]$ and $\nu = \nu_\Phi$. So the dimension of the $G_\nu(K_{d-1}[\chi])$ -module $G_\nu(K(\chi))$ is also infinite. Now we assume that $d' < +\infty$. By 1) $\nu = \nu_\Phi$ on $K_{d'-1}[\chi]$ and there exists a monic polynomial Φ' of degree d' such that $\nu_\Phi(\Phi') < \nu(\Phi')$. Set $\Phi' = f_n\Phi^n + f_{n-1}\Phi^{n-1} + \dots + f_0$, with f_n, \dots, f_0 in $K_{d-1}[\chi]$ (and $f_n \neq 0$). We prove that $f_n = 1$. Since Φ is irreducible, there exists $g \in K_{d-1}[\chi]$ such that gf_n is congruent to 1 modulo Φ , i.e. $r_\Phi(gf_n) = 1$. For $0 \leq k \leq n$ set $r_k = r_\Phi(gf_k)$ ($r_n = 1$), $q_k = q_\Phi(gf_k)$ and $\Phi'' = \Phi^n + r_{n-1}\Phi^{n-1} + \dots + r_0$. We have

$$g(f_n\Phi^n + f_{n-1}\Phi^{n-1} + \dots + f_0) = q_n\Phi^{n+1} + q_{n-1}\Phi^n + \dots + q_0\Phi + \Phi^n + r_{n-1}\Phi^{n-1} + \dots + r_0.$$

Since Φ is a key polynomial, for every k we have $\nu(r_k\Phi^k) = \nu(gf_k\Phi^k) < \nu(q_k\Phi^{k+1})$. Hence

$$\nu(q_n\Phi^{n+1} + q_{n-1}\Phi^n + \dots + q_0\Phi) \geq \min(\nu(q_n\Phi^{n+1}), \nu(q_{n-1}\Phi^n), \dots, \nu(q_0\Phi)) >$$

$$\min(\nu(\Phi^n), \nu(r_{n-1}\Phi^{n-1}), \dots, \nu(r_0)) = \nu(g) + \min(\nu(f_n\Phi^n), \nu(f_{n-1}\Phi^{n-1}), \dots, \nu(f_0)) = \nu(g) + \nu_\Phi(\Phi').$$

Therefore

$$\begin{aligned} & \nu(\Phi^n + r_{n-1}\Phi^{n-1} + \dots + r_0) = \\ & \nu(g(f_n\Phi^n + f_{n-1}\Phi^{n-1} + \dots + f_0) - q_n\Phi^{n+1} + q_{n-1}\Phi^n + \dots + q_0\Phi) \geq \\ & \min(\nu(g(f_n\Phi^n + f_{n-1}\Phi^{n-1} + \dots + f_0)), \nu(q_n\Phi^{n+1} + q_{n-1}\Phi^n + \dots + q_0\Phi)) > \\ & \nu(g) + \min(\nu(f_n\Phi^n), \nu(f_{n-1}\Phi^{n-1}), \dots, \nu(f_0)) = \\ & \min(\nu(gf_n\Phi^n), \nu(gf_{n-1}\Phi^{n-1}), \dots, \nu(gf_0)) = \\ & \min(\nu(\Phi^n), \nu(r_{n-1}\Phi^{n-1}), \dots, \nu(r_0)) = \nu_\Phi(\Phi^n + r_{n-1}\Phi^{n-1} + \dots + r_0). \end{aligned}$$

So, $\nu(\Phi'') > \nu_\Phi(\Phi'')$, where $\deg(\Phi'') = d' - \deg(g)$. Since d' is minimal, we have $g = 1$, $f_k = 1$ and $d' = nd$.

We turn to $G_\nu(K_{d'-1}[\chi])$. Let $k_1 < \dots < k_j$ be the integers such that

$$\nu(f_{k_i}\Phi^{k_i}) = \min(\nu(f_n\Phi^n), \nu(f_{n-1}\Phi^{n-1}), \dots, \nu(f_0)), \text{ for } i \in \{1, \dots, j\}.$$

By properties of valuations we have

$$\nu(f_{k_1}\Phi^{k_1} + \dots + f_{k_j}\Phi^{k_j}) > \min(\nu(f_{k_1}\Phi^{k_1}), \dots, \nu(f_{k_j}\Phi^{k_j})).$$

In the same way as above, we can replace f_{k_j} by 1 in such an equality, and since d' is minimal we have $n = k_j$. Therefore, we can assume that for $k \in \{0, \dots, n\}$ we have either $\nu(f_k\Phi^k) = \nu_\Phi(\Phi^k)$ or $f_k = 0$. Consequently $in_\nu(\Phi)^n + in_\nu(f_{n-1})in_\nu(\Phi)^{n-1} + \dots + in_\nu(f_0) = 0$. Now, for every g_{n-1}, \dots, g_0 in $K_{d-1}[\chi]$ we have $\nu(g_{n-1}\Phi^{n-1} + \dots + g_0) = \min(\nu(g_{n-1}\Phi^{n-1}), \dots, \nu(g_0))$. Hence $in_\nu(g_{n-1})in_\nu(\Phi)^{n-1} + \dots + in_\nu(g_0) \neq 0$. It follows that $X^n + in_\nu(f_{n-1})X^{n-1} + \dots + in_\nu(f_0)$ is the minimal polynomial of $in_\nu(\Phi)$ over $G_\nu(K_{d-1}[\chi])$. This also shows that the group $G_\nu(K_{d-1}[\chi])$ is equal to $G_\nu(K_{d-1}[\chi])(in_\nu(\Phi))$, so it is a subalgebra of $G_\nu(K(\chi))$. Since for every g_{n-1}, \dots, g_0 in $K_{d-1}[\chi]$, $in_\nu(g_{n-1})in_\nu(\Phi)^{n-1} + \dots + in_\nu(g_0) \neq 0$, $in_\nu(1), in_\nu(\Phi), \dots, in_\nu(\Phi^{n-1})$ are linearly independent over $G_\nu(K_{d-1}[\chi])$. Therefore $(in_\nu(1), in_\nu(\Phi), \dots, in_\nu(\Phi)^{n-1})$ is a basis of the $G_\nu(K_{d-1}[\chi])$ -module $G_\nu(K_{d-1}[\chi])$. Hence its dimension is n .

4) By Proposition 1.15, it is sufficient to show that for every integer $n \leq d' - 1$, $\nu(\chi^n - K_{n-1}[\chi])$ has a maximum. Since $(K_{d-1}[\chi]|K, \nu)$ is vs defectless, we can assume that $n \geq d$ (Proposition 1.15). Let $f = f_k\Phi^k + \dots + f_1\Phi + f_0 \in \chi^n - K_{n-1}[\chi]$, where f_0, f_1, \dots, f_k belong to $K_{d-1}[\chi]$, f_k is monic, and $\deg(f_k) + kd = n$. Then $\nu(f) = \min(\nu(f_k\Phi^k), \dots, \nu(f_1\Phi), \nu(f_0)) \leq \nu(f_k\Phi^k)$. Let $j = n - dk$ be the degree of f_k . Since $j \leq d - 1$, there exists $g \in \chi^j - K_{j-1}[\chi]$ such that $\nu(g)$ is the maximum of $\nu(\chi^j - K_{j-1}[\chi])$. Then $\nu(f) \leq \nu(g\Phi^k)$, which proves that $\nu(g\Phi^k)$ is the maximum of $\nu(\chi^n - K_{n-1}[\chi])$. \square

4.4. Complete families of key polynomials. Let $\Phi_1, \dots, \Phi_n, \dots$ be monic irreducible polynomials of $K[\chi]$ of degrees $d_1 = 1, d_2, \dots, d_n$, respectively, where d_{n-1} divides d_n (if the family has a maximal element d_n , then we set $d_{n+1} = [K(\chi):K]$). We let \mathcal{B} be the family of the $\Phi_1^{e_1} \dots \Phi_n^{e_n}$, where for $0 \leq i \leq n - 1$ we have: $0 \leq e_i < \frac{d_{i+1}}{d_i}$. Since the mapping $\Phi_i^{e_i} \mapsto \deg(\Phi_i^{e_i})$ is one-to-one from \mathcal{B} onto $[0, [K(\chi):K]]$, \mathcal{B} is a basis of the K -module $K[\chi]$. Furthermore, for every m in \mathbb{N} , $\mathcal{B} \cap K_m[\chi]$ is a basis of the K -module $K_m[\chi]$. Now, we can define a basis even if some degree does not divide the following one. Indeed, in the case where we have only $d_1 = 1 < d_2 < \dots < d_n < \dots$, we require: for every n , $e_1 + e_2d_2 + \dots + e_nd_n < d_{n+1}$. We say that \mathcal{B} is *generated by polynomials* if it is constructed in the above way. If so, then $\Phi_1, \Phi_2, \dots, \Phi_n, \dots$, are called the *generating polynomials* for \mathcal{B} .

Remark 4.11. Let ν be a K -module valuation on $K(\chi)$, $\Phi_1, \dots, \Phi_k, \dots$ be generating polynomials for a basis \mathcal{B} . For $k \geq 1$, fix $\nu'(\Phi_k)$. For every e_1, \dots, e_k with $e_1 + e_2d_2 + \dots + e_kd_k < d_{k+1}$, let $\nu'(\Phi_1^{e_1} \dots \Phi_k^{e_k}) = e_1\nu'(\Phi_1) + e_2\nu'(\Phi_2) + \dots + e_k\nu'(\Phi_k)$ and for every pairwise distinct y_1, \dots, y_k in \mathcal{B} , x_1, \dots, x_k in K set $\nu'(x_1y_1 + \dots + x_ky_k) = \min_{1 \leq i \leq k} \nu(x_i)\nu'(y_i)$. Then ν' is a vs defectless K -module valuation. If for every $k \geq 1$ we have $\nu'(\Phi_k) = \nu(\Phi_k)$, then the K -module valuation ν' defined above is the K -module valuation $\nu_{\Phi_{d_1}, \dots, \Phi_{d_k}}$ defined in Notations 2.9.

Let ν be a pm valuation on $K(\chi)$, $1 = d_1 < d_2 < \dots < d_k < \dots$ be the sequence of key degrees of ν . Let \mathcal{F} be a family of key polynomials. We say that \mathcal{F} is a *complete family of key polynomials* for ν if ν is the supremum of the family of the pm valuations $\nu_{\Phi_{d_1}, \dots, \Phi_{d_k}}$, where $k \in \mathbb{N} \setminus \{0\}$, for $1 \leq i \leq k$ $\Phi_{d_i} \in \mathcal{F}$, $\deg(\Phi_{d_i}) = d_i$. This means that if f is a polynomial of degree d , then $\nu(f)$ is equal to the maximum of the family $\nu_{\Phi_{d_1}, \dots, \Phi_{d_k}}(f)$, where d_k is the greatest key degree at most equal to d .

For every pm valuation on $K[\chi]$ there exists a complete family of key polynomials (see for example [17], [5]). We complete this subsection by the construction of a complete family of key polynomials which does not require to be constructed by induction on the degree.

Theorem 4.12. *Let ν be a pm valuation on $K(\chi)$, $1 = d_1 < d_2 < \dots < d_k < \dots$ be the sequence of key degrees of ν and \mathcal{F} be a family of key polynomials for ν which satisfies the following properties for every $k \geq 1$.*

If d_k is an independent key degree, then \mathcal{F} contains exactly one key polynomial Φ_{d_k} of degree d_k , and $\nu(\Phi_{d_k}) = \max(\nu(\chi^{d_k} - K_{d_k-1}[\chi]))$. For notational convenience, for every integer m we set $\Phi_{d_k, m} = \Phi_{d_k}$.

If d_k is an immediate key degree, then the key polynomials of degree d_k of \mathcal{F} form a sequence $(\Phi_{d_k, m})$ such that the sequence $(\nu(\Phi_{d_k, m}))$ is increasing, cofinal in $\nu(\chi^{d_k} - K_{d_k-1}[\chi])$.

For every k , m_1, \dots, m_k , we let $\nu_{(m_1, \dots, m_k)} = \nu_{\Phi_{d_1, m_1}, \dots, \Phi_{d_k, m_k}}$ (see Notations 2.9 and Remark 4.11). Then \mathcal{F} is a complete family of key polynomials. Furthermore, for every f , there are infinitely many (m_1, \dots, m_k) 's such that $(\nu_{(m_1, \dots, m_k)}(f)) = \nu(f)$.

Proof. Note that, for every k , m_1, \dots, m_k , we have $\nu_{(m_1, \dots, m_k)} \leq \nu$. Let $f \in K[\chi]$ and d_k be the greatest key degree such that the degree of f is at least equal to d_k . By Theorems 4.10 and 4.9, there exists m_k such that $\nu(f) = \nu_{\Phi_{d_k, m_k}}(f)$. Furthermore, since the family $(\nu_{\Phi_{d_k, m_k}})$ is increasing, we have $m'_k \geq m_k \Rightarrow \nu_{\Phi_{d_k, m'_k}}(f) = \nu(f)$. Let $f = f_j \Phi_{d_k, m_k}^j + \dots + f_1 \Phi_{d_k, m_k} + f_0$, where f_0, f_1, \dots, f_j belong to $K_{d_k-1}[\chi]$. We know that there is some m_{k-1} such that $\nu(f_0) = \nu_{\Phi_{d_{k-1}, m_{k-1}}}(f_0), \dots, \nu(f_j) = \nu_{\Phi_{d_{k-1}, m_{k-1}}}(f_j)$. Then, $\nu(f) = \nu_{\Phi_{d_{k-1}, m_{k-1}}, \Phi_{d_k, m_k}}(f)$. So by induction we get a k -uple (m_1, \dots, m_k) such that $\nu(f) = \nu_{(m_1, \dots, m_k)}(f)$.

Now, we can do the same construction with any $m'_k \geq m_k$, which proves that there are infinitely many such k -uples. \square

5. ABSTRACT KEY POLYNOMIALS

In this section χ is assumed to be transcendental over K . The mapping ν is a valuation or a pseudo-valuation. If ν is a pseudo-valuation, then we assume that the degrees of Φ and Φ' are lower than the degree of a generator of the ideal $\{f \in K[\chi] : \nu(f) = \infty\}$. Our goal is to prove that our definition of key polynomials is equivalent to the definition of abstract key polynomials.

We start with some notations.

Let f be a polynomial degree of n . For $1 \leq i \leq n$, set $f_{(i)} = (1/i!) f^{(i)}$, where $f^{(i)}$ is the i -th formal derivative of f . If the characteristic of K is $p > 0$, then we do not replace $p \cdot x$ by 0; the simplification holds, if necessary, after the division by $i!$. For example, if $f(X) = X^p$, then we have $f_{(1)}(X) = pX^{p-1} = 0$, and $f_{(p)}(X) = (1/p!) \cdot p! = 1$.

For any polynomial f , let $\varepsilon_\mu(f)$ be the maximum of the set

$$\left\{ \frac{\nu(f) - \nu(f_{(i)})}{i} \mid i \in \mathbb{N} \setminus \{0\} \right\}.$$

We say that Φ is an *abstract key polynomial* (or a *key polynomial*) for ν if it is monic and for every $f \in K[\chi]$ such that $\varepsilon_\nu(f) \geq \varepsilon_\nu(\Phi)$ we have $\deg(f) \geq \deg(\Phi)$ ([5]).

Remark 5.1. ([17, Remark 2.1]) The monic polynomials of degree 1 are abstract key polynomials.

Proposition 5.2. ([17, Lemma 2.3 (iii)]) *Let Φ be an abstract key polynomial for ν , h_1, \dots, h_s be polynomials with degrees less than $\deg(\Phi)$ and q be the quotient of the euclidean division of $\prod_{i=1}^s h_i$*

by Φ . Then $\nu\left(\prod_{i=1}^s h_i - q\Phi\right) = \nu\left(\prod_{i=1}^s h_i\right) < \nu(q\Phi)$.

Corollary 5.3. *The abstract key polynomials are key polynomials as defined in Definitions 2.2.*

The converse is a consequence of the following theorem. In this theorem for a key polynomial Φ we let $\square(\Phi) := \{f \in K[\chi] \mid f \text{ is monic, } \nu_\Phi(f) < \nu(f)\}$, and $\boxminus(\Phi)$ be the subset of elements of $\square(\Phi)$ with minimum degree.

Theorem 5.4. ([17, Theorem 2.12]) *Let Φ be a monic polynomial. Then Φ is an abstract key polynomial if, and only if, there exists an abstract key polynomial Φ_- such that: either a) Φ belongs to $\boxminus(\Phi_-)$,*

or b)

- i) the elements in $\Xi(\Phi_-)$ have the same degree as Φ_- ,
- ii) the set of valuations of all elements in $\Xi(\Phi_-)$ has no maximum element,
- iii) for every Φ' in $\Xi(\Phi_-)$, $\nu_{\Phi'}(\Phi) < \nu(\Phi)$,
- iv) the degree of Φ is minimum among the degrees of polynomials satisfying iii).

Corollary 5.5. *The key polynomials as defined in Definitions 2.2 are abstract key polynomials.*

Proof. We prove this by induction on the degrees. By Proposition 2.3 1) and Remark 5.1 this is true for polynomials of degree 1. Let Φ be a key polynomial of degree $d > 1$, and assume that every key polynomial of degree less than d is an abstract key polynomial. We denote by d' the preceding key degree. If d' is an independent key degree, then by a) of Theorem 5.4 and Theorem 4.10, Φ is an abstract key polynomial. If d' is an immediate key degree, then by b) of Theorem 5.4 and Theorem 4.9, Φ is an abstract key polynomial. \square

REFERENCES

- [1] J. Ax, S. Kochen, Diophantine problems over local fields 1 & 2, Am. J. Math. 87 (1965) 605–630 & 631–648.
- [2] W. Baur, Die Theorie der Paare reell abgeschlossener Körper, Logic and Algorithmic (in honour of E. Specker), Monographies de l'Enseignement Mathématique, n° 30 (1982), Université de Genève, Geneva, 25–34.
- [3] W. Baur, On the theory of pairs of real closed fields, J. Symb. Logic 47 (1982) 669–679 (1982).
- [4] A. Blaszcok, P. Cubides Kovacsics, F.-V. Kuhlmann, On valuation independence and defectless extensions of valued fields, J. of Algebra, (2020) 555 69–95.
- [5] J. Decaup, W. Mahboub, M. Spivakovski, Abstract key polynomials and comparison theorems with the key polynomials of Mac Lane-Vaquié, Illinois J. Math. 62 (2018) 253–270.
- [6] F. Delon, Extensions séparées et immédiates de corps valués, J. Symb. Logic 53 (1988) 421–428.
- [7] F. Delon, Indécidabilité de la théorie des paires de corps valués henséliens, J. Symb. Logic 56 (1991) 1236–1242.
- [8] F.J. Herrera Govantes, M.A. Olalla Acosta, M. Spivakovsky, Valuations in algebraic field extensions, J. of Algebra 312 (2007) 1033–1074.
- [9] S. Kochen, The model theory of local fields, Logic Conference, Kiel 1974, Lecture Notes in Mathematics (499) (1975), Springer Verlag, Berlin.
- [10] F.-V. Kuhlmann, Book on valuation theory (in preparation) Chapter 3. Available at <https://math.usask.ca/fvk/Fvkbook.htm>.
- [11] G. Leloup, Théories complètes de paires de corps valués henséliens, J. Symb. Logic 55 (1990) 323–339.
- [12] G. Leloup, Properties of extensions of algebraically maximal fields, Coll. Math. 54 (2003) 53–72.
- [13] G. Leloup, Key polynomials, separate and immediate valuations, and simple extensions of valued fields. arxiv.org/abs/1809.07092, <https://hal.archives-ouvertes.fr/hal-01876056> (2018) (first and second versions).
- [14] S. MacLane, A construction for absolute values in polynomials rings, Trans. Amer. Math. Soc 40 (1936) 363–395.
- [15] S. MacLane, A construction for prime ideals as absolute values of an algebraic field, Duke Math. j. 2 (1936) 492–510.
- [16] J. Novakoski, Key polynomials and minimal pairs, J. Algebra 523 (2019) 1–14.
- [17] J. Novakoski, M. Spivakovski, Key polynomials and pseudo-convergent sequences, J. Algebra 495 (2018) 199–219.
- [18] P. Ribenboim, Théorie des valuations L,es Presses de l'université de Montréal, Montréal (1968).
- [19] M. Vaquié, Extension d'une valuation, Trans. Amer. Math. Soc. 359 7 (2007) 3439–3481.

GÉRARD LELOUP, LABORATOIRE MANCEAU DE MATHÉMATIQUES, LMM EA 3263, LE MANS UNIVERSITÉ, AVENUE OLIVIER MESSIAEN, 72085 LE MANS CEDEX, FRANCE.

Email address: gerard.leloup@univ-lemans.fr